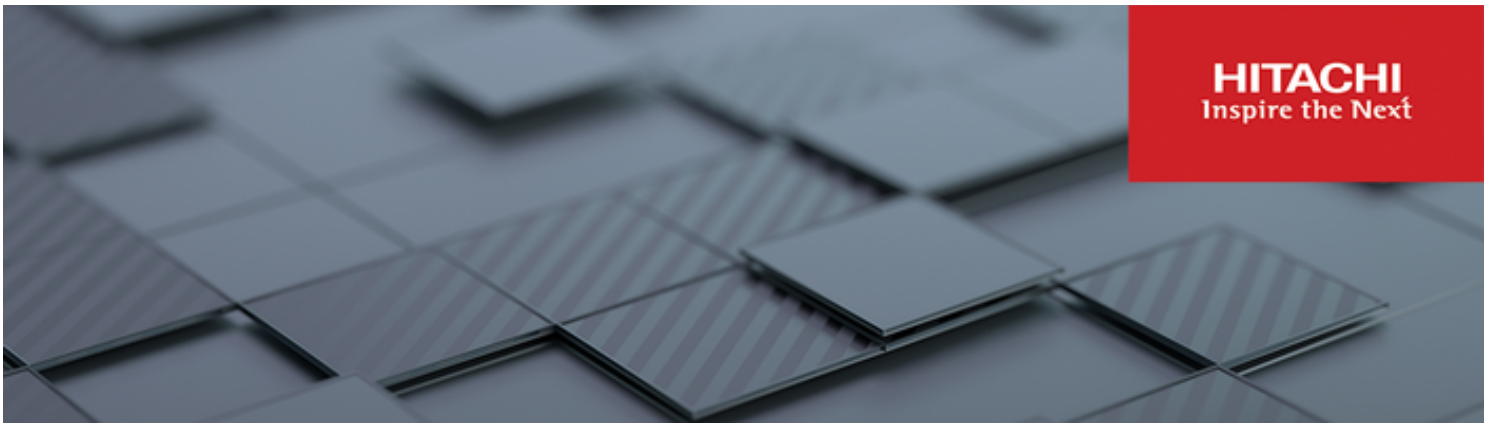


Content Platform System Management Help

9.7.x

Content Platform

MK-95HCPH001-20

Last updated: 2024-06-07

Generated from docs.hitachivantara.com

Hitachi Vantara

Administering HCP

Introduction to Hitachi Content Platform

Hitachi Content Platform (HCP) is a distributed data storage system designed to support large, growing repositories of fixed-content data. An HCP system comprises hardware (physical or virtual) and software.

Hitachi Content Platform stores objects that include data and the metadata that describes the data. HCP distributes these objects across the storage space. HCP represents objects either as URLs or as files in a standard file system.

An HCP repository is partitioned into *namespaces*. Each namespace consists of a distinct logical grouping of objects with its own directory structure. Namespaces are owned and managed by tenants.

HCP provides access to objects through a variety of industry-standard protocols as well as through HCP product-specific interfaces.

About the Hitachi Content Platform

Hitachi Content Platform is the distributed, fixed-content, data storage system from Hitachi Vantara. HCP provides a cost-effective, scalable, easy-to-use repository that can accommodate all types of data, from simple text files to medical images to multigigabyte database images.

A *fixed-content storage system* is one in which the data cannot be modified. HCP uses write-once, read-many (WORM) storage technology and a variety of policies and services to ensure the integrity of the stored data and the efficient use of storage capacity. HCP also provides easy access to the repository for adding, retrieving, and deleting or shredding data.

HCP has an open architecture that insulates stored data from technology changes, as well as from changes in HCP itself due to product enhancements. This open architecture ensures that users will have access to their data long after it's been added to the repository.

HCP runs on a networked HCP with internal storage or a HCP with SAN-attached storage.

HCP with internal storage systems use only the internal storage in each node. HCP with SAN-attached storage systems use both the internal storage in each node and the storage in Fibre Channel SAN arrays.

HCP VM systems run on virtual machines in a VMware® environment or in a KVM environment. HCP VM systems function mostly as a HCP with internal storage system, with the virtual storage emulating internal storage.

Object-based storage

HCP stores *objects* in a repository. Each object permanently associates data HCP receives (for example, a document, an image, or a movie) with information about that data, called *metadata*.

An object encapsulates:

Fixed-content data
: An exact digital reproduction of data as it existed before it was stored in HCP. After it's in the repository, this fixed-content data cannot be modified.

System metadata
: System-managed properties that describe the fixed-content data (for example, its size and creation date). System metadata includes policies, such as retention and data protection level, that influence how transactions and services affect the object.

Custom metadata
: Optional metadata that a user or application provides to further describe the object. Custom metadata is specified as one or more annotations, where each annotation is a discrete unit of information about the object. Annotations are typically specified in XML format.

  You can use custom metadata to create self-describing objects. Users and applications can use this metadata to understand and repurpose object content.

Access control list (ACL)
: Optional metadata consisting of a set of grants of permissions to perform various operations on the object. Permissions can be granted to individual users or to groups of users.

  ACLs are provided by users or applications and are specified in either XML or JSON format.

HCP also stores directories and symbolic links. These items have system metadata but no fixed-content data, custom metadata, or ACLs.

HCP can store multiple versions of an object, thus providing a history of how the data has changed over time. Each version is a separate object, with its own system metadata and, optionally, its custom metadata and ACL.

HCP supports *multipart uploads* with the Hitachi API for Amazon S3. *Multipart uploads* is the process of writing the data for an object to HCP in multiple parts. Multipart upload is supported only by the Hitachi API for Amazon S3. With a multipart upload, the data for an object is broken into multiple parts that are written to HCP independently of each other. Even though the data is written in multiple parts, the result of a multipart upload is a single object. An object for which the data is stored in multiple parts is called a *multipart object*.

Namespaces and tenants

An HCP repository is partitioned into namespaces. A *namespace* is a logical grouping of objects such that the objects in one namespace are not visible in any other namespace.

Namespaces provide a mechanism for separating the data stored for different applications, business units, or customers. For example, you could have one namespace for accounts receivable and another for accounts payable.

Namespaces also enable operations to work against selected subsets of objects. For example, you could perform a query that targets the accounts receivable and accounts payable namespaces but not the employees namespace.

Namespaces share the same underlying physical storage. This, together with the multitenancy feature described under "Tenants" below, enables HCP to provide support for cloud storage services.

HCP and default namespaces

An HCP system can have a maximum of 10,000 locally defined namespaces, including one special namespace called the *default namespace*. Applications are typically written against namespaces other than the default; these namespaces are called HCP namespaces. The default namespace is most often used with applications that existed before release 3.0 of HCP.

Note: Replication can cause an HCP system to have more than 10,000 namespaces.

The table below outlines the major differences between HCP namespaces and the default namespace.

Feature	HCP namespaces	Default namespaces
Storage usage quotas	✓	
Object ownership (not related to POSIX UID)	✓	
Access control lists (ACLs) for objects	✓	
Object versioning	✓	
Multiple custom metadata annotations	✓	
Namespace ownership by users	✓	
RESTful HTTP/HTTPS API for data access	✓	
Non-RESTful HTTP/HTTPS protocol for data access		✓
Data access authentication with HTTP/HTTPS	✓	
Hitachi API for Amazon S3, a RESTful, HTTP-based S3 compatible API for data access	✓	
NDMP for backup and restore		✓

Tenants

Namespaces are owned and managed by administrative entities called *tenants*. A tenant typically corresponds to an organization, such as a company or a division or department within a company.

HCP supports two types of tenants:

HCP tenants
: Own HCP namespaces. An HCP system can have multiple HCP tenants, each of which can own multiple namespaces. You can limit the number of namespaces each HCP tenant can own. In addition to being owned by a tenant, each HCP namespace can have an owner that corresponds to an individual HCP user. The owner of a namespace automatically has permission to perform certain operations on that namespace.

default tenant
: Owns the default namespace and only that namespace. An HCP system can have only one default tenant.

An HCP system can have a maximum of 1,000 locally defined tenants, including the default tenant.

Note: Replication can cause an HCP system to have more than 1,000 tenants.

An HCP system has both system-level and tenant-level administrators:

System-level administrators
: Concerned with monitoring the HCP system hardware and software, monitoring overall repository usage, configuring features that apply across the HCP system, and managing system-level users.

Tenant-level administrators
: Concerned with monitoring namespace usage at the tenant and namespace level, configuring individual tenants and namespaces, managing tenant-level users, and controlling access to namespaces.

System-level administrators create tenants. Tenant-level administrators create HCP namespaces. The default namespace is created automatically when the default tenant is created.

You can create the default tenant and namespace only if allowed to do so by the system configuration.

Data access methods

HCP supports access to namespace content through namespace access protocols, the HCP Namespace Browser, the HCP metadata query API, and the HCP Search Console.

Namespace access protocols

HCP supports access to namespace content through several industry-standard protocols:

- For HCP namespaces only:
  - REST API, which is a RESTful, HTTP-based API.
  - Hitachi API for Amazon S3, which is a RESTful, HTTP-based S3 compatible API. With the S3-compatible API, namespaces are called *buckets*.
- For the default namespace only, a non-RESTful implementation of HTTP.
- For all namespaces:
  - WebDAV
  - CIFS
  - NFS

These protocols support various operations: storing data, creating directories, viewing object data and metadata, viewing directories, modifying certain metadata, and deleting objects. You can use these protocols to access data with a web browser, third-party applications, Windows® Explorer, and other native Windows and Unix tools.

HCP allows special-purpose access to namespaces through SMTP. This protocol is used only for storing email.

For backup of the default namespace, HCP supports NDMP. Objects are backed up in OpenPGP format, which uses a tar file to package the files that represent an object. This standard format, which can be both signed and encrypted, allows backup objects to be restored to other storage systems.

HCP tenant administrators can create secure namespaces by enabling only REST and CIFS, configured to require authentication, and the S3-compatible which always require authentication.

HCP Namespace Browser

The HCP Namespace Browser lets you manage content in and view information about HCP namespaces. With the Namespace Browser, you can:

- List, view, and retrieve objects, including old versions of objects
- View custom metadata and ACLs for objects, including old versions of objects
- Store and delete objects
- Create empty directories
- Display namespace information, including:
  - The namespaces that you own or can access
  - Retention classes available for a given namespace
  - Permissions for namespace access
  - Namespace statistics such as the number of objects in a given namespace or the total capacity of the namespace

The Namespace Browser is not available for the default namespace. However, you can use a web browser to view the contents of that namespace.

HCP metadata query API

The HCP metadata query API lets you search HCP for objects that meet specified criteria. The API supports two types of queries:

- *Object-based* queries search for objects based on object metadata. This includes both system metadata and the content of custom metadata and ACLs. The query criteria can also include the object location (that is, the namespace and/or directory that contains the object). These queries use a robust query language that lets you combine search criteria in multiple ways.

  Object-based queries search only for objects that currently exist in the repository. For objects with multiple versions, object-based queries return only the current version.

- *Operation-based* queries search not only for objects currently in the repository but also for information about objects that have been deleted by a user or application, deleted through disposition, purged, or pruned. For namespaces that support versioning, operation-based queries can return both current and old version of objects.

  Criteria for operation-based queries can include object status (for example, created or deleted), change time, index setting, and location.

The metadata query API returns object metadata only, not object data. The metadata is returned either in XML format, with each object represented by a separate element, or in JSON format, with each object represented by a separate name/value pair. For queries that return large numbers of objects, you can use paged requests.

HCP Search Console

The HCP Search Console is an easy-to-use web application that lets you search for and manage objects based on specified criteria. For example, you can search for objects that were stored before a certain date or that are larger than a specified size. You can then delete the objects listed in the search results or prevent those objects from being deleted. Similar to the metadata query API, the Search Console returns only object metadata, not object data.

By offering a structured environment for performing searches, the Search Console facilitates e-discovery, namespace analysis, and other activities that require the user to examine the contents of namespaces. From the Search Console, you can:

- Open objects.
- Perform bulk operations on objects.
- Export search results in standard file formats for use as input to other applications.
- Publish feeds to make search results available to web users.

The Search Console works with either of these two search facilities:

HCP metadata query engine
: This facility is integrated with HCP and works internally to perform searches and return results to the Search Console. The metadata query engine is also used by the metadata query API. When working with the metadata query engine, the Search Console is called the Metadata Query Engine Console.

The Search Console can use only one search facility at any given time. The search facility is selected at the HCP system level. If no facility is selected, the HCP system does not support use of the Search Console to search namespaces.

Each search facility maintains its own index of objects in each search-enabled namespace and uses this index for fast retrieval of search results. The search facilities automatically update their indexes to account for new and deleted objects and changes to object metadata.

Not all namespaces support search. To find out whether a namespace is search-enabled, see your tenant administrator.

Object representation

HCP represents objects differently based on the namespace access protocol the client is using.

Object representation with HTTP

With HTTP, HCP represents each object as a URL. The root of the object path in the URL is always rest.

Here's an example of the URL for an object named wind.jpg in the images directory in a namespace named climate in a tenant named geo in an HCP system named hcp.example.com:

```
http://climate.geo.hcp.example.com/rest/images/wind.jpg
```

Users and applications represent system metadata and identify custom metadata by using query parameters appended to the URLs. HCP returns system metadata in HTTP response headers and returns custom metadata in the format in which it was originally specified.

Object representation with the S3 compatible API

With the S3 compatible API, HCP represents each object as a URL. The exact format of this URL depends on how the application used to access the object handles user authentication.

The S3 compatible API does not have the concept of directories. Slashes in object names are simply part of the name and are not directory separators. Thus, with the S3 compatible API, objects do not have paths.

Here's an example of one of the possible URLs for an object named images/wind.jpg in a namespace named climate in a tenant named geo in an HCP system named hcp.example.com:

```
http://climate.geo.hcp.example.com/hs3/images/wind.jpg
```

Users and applications represent system and custom metadata by using HTTP request headers. HCP returns system and custom metadata in HTTP response headers.

Object representation with other namespace access protocols

For namespace access protocols other than the HTTP and S3 compatible APIs, HCP includes a standard POSIX file system called HCP-FS that represents each object as a set of files. One of these files has the same name as the object. This file contains the fixed-content data. When downloaded or opened, this file has the same content as the originally stored item.

The other files that HCP-FS presents contain object metadata. These files, most of which are plain text, are called *metafiles*.

All files containing fixed-content data are in a directory hierarchy headed by data. All metafiles are in a directory hierarchy headed by metadata.

With this view of objects as conventional files and directories, HCP supports routine file-level calls and enables users and applications to find fixed-content data in familiar ways.

HCP nodes and storage

An HCP system includes multiple *nodes* that are networked together, where each node is either an individual server, a blade in a blade server, or a virtual machine. Each physical node can have multiple internal drives and/or can connect to SAN storage. Each virtual node emulates a server that has only internal drives.

The physical storage that's managed by the nodes in the HCP system is called *primary storage*. By default, primary storage consists entirely of *running storage*, which is storage on continuously spinning disks. However, an HCP with SAN-attached storage system can be configured to use SAN storage that includes both running storage and *spindown storage*, which is storage on disks that can be spun up or spun down as needed. HCP uses primary spindown storage for tiering purposes.

You can also add HCP S Series Nodes , known as *S Series storage*, to an HCP system. S Series Nodes are highly efficient, highly available, cost-effective storage devices that support very large amounts of data. An S Series Node uses commodity hardware which ensures that the costs of growth and repair remain low. To protect data, S Series Nodes use erasure coding. S Series Nodes also use several internal processes to continuously check the integrity of the stored data and the storage media.

You can use S Series Nodes as an alternative to primary running storage or as a tiering platform. This is configurable. HCP uses the S Series Node S3 compatible API to write, retrieve, and otherwise manage objects in an S Series Node. A single HCP system can seamlessly write data across multiple S Series Nodes, thereby enabling scalability in both capacity and performance.

Additionally, for tiering purposes, HCP can use *extended storage*. Extended storage is storage that's managed entirely outside of the HCP system.

Each node has its own set of *logical volumes*. Logical volumes on storage managed by HCP are *local storage volumes*. Logical volumes can also be *NFS volumes* (also called *external volumes*). These are volumes that are stored on extended storage and are accessed using NFS mount points.

General nodes

General nodes are the core components of an HCP system. These nodes manage the objects that reside in HCP system storage. To ensure data integrity and continuous availability in case of a hardware or software failure, HCP uses RAID technology for its primary storage and can also be configured to store the data and metadata for each object in multiple locations.

Each storage node runs all the HCP software. The nodes work together to serve both as a repository manager and as a gateway that enables access to the data in the repository.

All runtime operations are distributed among the storage nodes, thereby ensuring reliability and performance as capacity grows. If a node fails, the HCP system adapts by redirecting processing to other nodes, so the stored data remains available to users.

Linear scalability

A repository can accumulate a great deal of data over time. To accommodate more data, you can add nodes and storage to HCP. HCP capacity can grow smoothly from hundreds of gigabytes to terabytes to petabytes.

Because HCP uses a distributed processing scheme, primary storage in the HCP system can scale linearly as the repository grows in size and in the number of clients that have access to it. When you install HCP on new nodes, the system automatically integrates those nodes into the overall workflow, without manual intervention.

HCP architecture

HCP hardware consists of:

- Servers
- Internal and/or SAN storage
- Networking components such as cables and switches
- Additional infrastructure items such as racks and power distribution units

HCP uses back-end, front-end and optionally management networks, if the HCP hardware is configured to support it. The isolated back-end network connects the HCP nodes to each other through two redundant back-end Ethernet switches. Each node has a pair of bonded Ethernet ports that are used to connect the node to these switches.

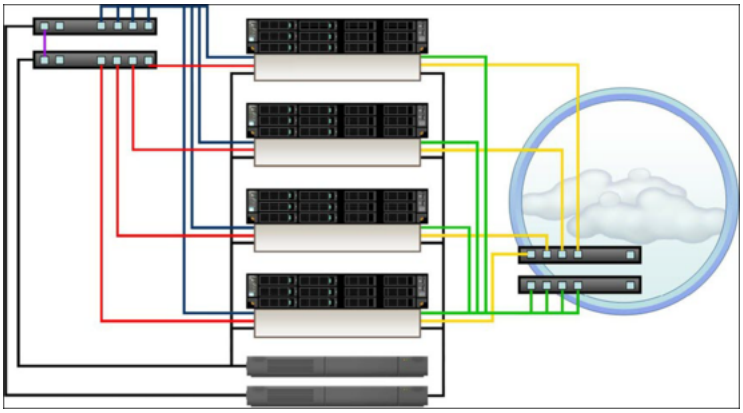
Each storage node is configured with an additional pair of bonded Ethernet ports that allows external applications to access the system. The recommended configuration options are:

- Two independent Ethernet switches that connect the ports to the front-end network
- One Ethernet switch, with both HCP and the switch configured for active-active bonding

For VM systems, this hardware configuration applies to the physical environment in which HCP VM runs.

HCP with internal storage system architecture

The following figure shows the architecture of an HCP system that uses internal storage. This system has four storage nodes, two back-end switches (on the left), and two front-end switches (on the right).

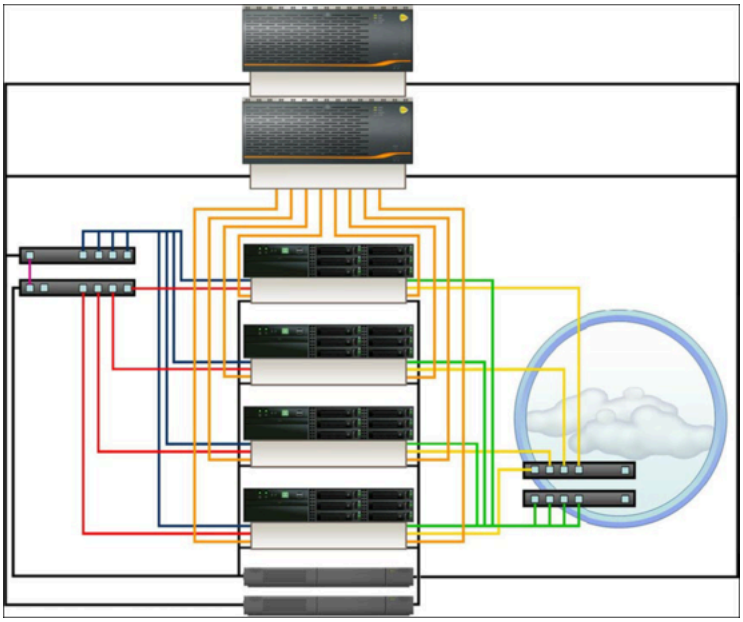


The table below describes the cables in this figure.

Cable	Connects from	Connects to
Red and blue Ethernet	Back-end NICs in each node	Back-end switches
Green and yellow Ethernet	Front-end NICs in each node	Front-end switches
Purple Ethernet	Back-end switches	Each other
Black power	Each node	Two PDUs
	Each back-end switch	One PDU

HCP with SAN-attached storage system architecture

The following figure shows the architecture of an HCP system that uses a Fibre Channel SAN storage system. This system has four storage nodes, two modular storage trays, two back-end switches (on the left), and two front-end switches (on the right). Each node has multipathed access to the shared SAN storage.



The table below describes the cables in this figure.

Cable	Connects from	Connects to
Red and blue Ethernet	Back-end NICs in each node	Back-end switches
Green and yellow Ethernet	Front-end NICs in each node	Front-end switches
Purple Ethernet	Back-end switches	Each other
Orange Fibre Channel	Each node	SAN array
Black power	Each node	Two PDUs
	Each back-end switch	One PDU
	Each storage tray	Two PDUs

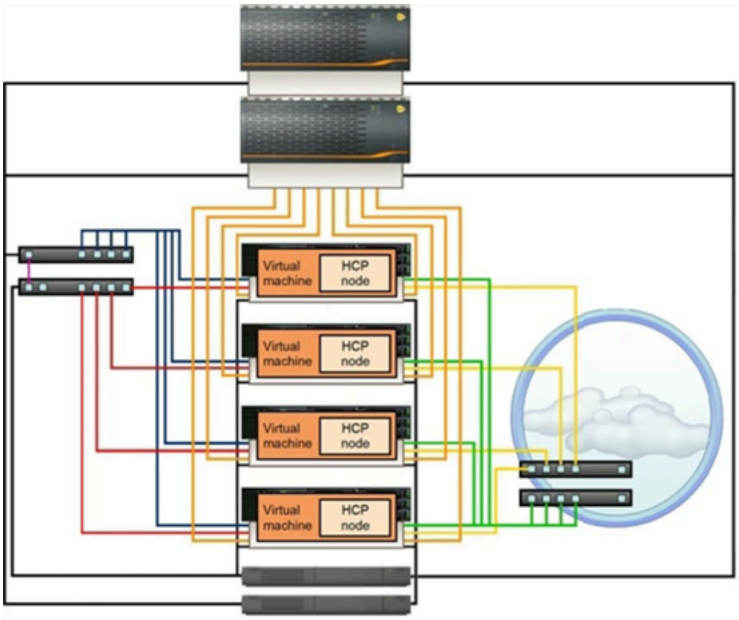
Note:

Nodes in HCP with SAN-attached storage systems are either individual servers or individual blades in blade servers. The figure above shows individual servers. Some HCP with SAN-attached storage systems include Fibre Channel switches between the nodes and the SAN arrays.

VM system architecture

The physical environment for an HCP VM system has the same architecture as an HCP with SAN-attached storage system. That is, the servers that host the virtual machines on which HCP runs have multipathed access to shared SAN storage. The physical switch and port configurations are the same as for HCP with SAN-attached storage systems.

Depending on the number of physical servers and the capabilities of those servers, a VM system can have one or more HCP nodes running on a host on each server. The following figure shows the physical environment for a VM system with four HCP nodes, each running in its own physical server. For information about the hardware configuration in this figure, see "HCP with SAN-attached storage system architecture" above.



Repository management

Repository management requires:

- Maintaining the integrity and security of stored data.
- Ensuring the continuous availability of that data.
- Keeping the data in compliance with local regulations.
- Optimizing the use of storage and network bandwidth.

HCP supports these requirements through:

- The hardware and network configuration of the system
- Software configuration options (both installation and runtime)
- Automated processes
- Individual namespace and object settings
- Object storage and retrieval options

Data integrity and security

HCP includes many features specifically designed to protect the integrity and ensure the security of stored data:

Write-once, read-many (WORM) storage
: After the data for an object is stored in the repository, HCP, by default, prevents that data from being modified or overwritten.

Node login prevention
: HCP does not allow system-console logins on its nodes. This provides a basic level of protection not only for the stored data but also for the system software.

Secure Sockets Layer (SSL)
: HCP can use SSL to ensure the privacy of HTTP and WebDAV access to namespaces. It always uses SSL to secure the Management and Search Consoles. Additionally, use of the HCP management API requires SSL.

Content Verification service
: Each object has a *cryptographic hash value* that's calculated from the object data. The Content Verification service ensures the integrity of each object by periodically checking that its data still matches its hash value.

Scavenging service
: The Scavenging service protects namespaces from the loss of system metadata. If the service encounters an object with invalid metadata, it restores the correct metadata by using a copy from another location.

Retention policy
: Each object has a *retention setting* that specifies how long the object must remain in the repository before it can be deleted; this duration is called the *retention period*. HCP ensures that objects are kept until their retention periods expire. The only exception to this behavior occurs in namespaces in enterprise mode. In these namespaces, users with explicit permission to do so can delete objects that are under retention. Such deletions are recorded in the tenant log.

Shredding policy

Objects can be marked for shredding. When such an object is deleted, HCP overwrites its storage location in such a way as to completely remove any trace that the object was there.

Data access authentication

The HTTP, S3 compatible, WebDAV, and CIFS protocols can be configured to require authentication for access to an HCP namespace. If these are the only protocols enabled for the namespace, users and applications must present valid credentials for access to the namespace content. HCP supports both local and remote authentication methods. For remote authentication, HCP supports Windows Active Directory® and RADIUS.

Data access permission masks

Data access permissions determine which operations a user or application can perform on the objects in an HCP namespace. These permissions can be:

- Associated with a tenant-level user or group account, in which case they apply to all objects in the namespace
- Specified in the namespace configuration as the minimum permissions for authenticated or unauthenticated users, in which case they apply to all objects in the namespace
- Specified in an ACL, in which case they apply to the individual object for which the ACL is defined

Virtual networking

Virtual networking is a technology that enables you to define multiple logical networks over which clients can communicate with HCP. You can assign different networks to different tenants, thereby segregating network traffic to and from the namespaces owned by one tenant from network traffic to and from the namespaces owned by other tenants. This segregation enhances the privacy and security of data transmitted between clients and the HCP system.

Data availability

HCP has these features that help ensure the continuous availability of stored data:

Multipathing

In an HCP with SAN-attached storage system, a single node can connect to more than one port on a storage system, either directly or through multiple Fibre Channel switches. This creates multiple physical paths between the node and any given logical volume that maps to it. With this setup, if one component of a physical path connecting such a node to the storage system fails, the node still has access to the logical volume through another physical path. Multiple means of access to a logical volume from a single node is called *multipathing*.

Zero-copy failover

In a HCP with SAN-attached storage system, one node can automatically take over management of storage previously managed by another node that has failed. This process is called *zero-copy failover*. To support zero-copy failover, each logical volume that stores objects or the metadata query engine index must map to two different storage nodes. The pair of nodes forms a set such that the volumes that map to one of the nodes also map to the other. This is called *cross-mapping*.

Service plans

Each namespace has a service plan that defines both a data protection strategy and a storage tiering strategy for the objects in that namespace. At any given point in the lifecycle of an object, its data protection strategy specifies the number of copies of the object that must exist in the HCP repository and the type of storage on which each copy must be stored. Because some types of storage are more highly available than others, you can use the service plan for a namespace to control both data redundancy and data availability for the objects in that namespace.

Protection service

HCP uses the Protection service to maintain the correct number of copies of each object in the HCP repository. When the number of existing copies of an object goes below the number of object copies specified in the applicable service plan (for example, because of a logical volume failure), the Protection service automatically creates a new copy of that object in another location. When the number of existing copies of an object goes above the number of object copies specified in the applicable service plan, the Protection service automatically deletes all unnecessary copies of that object.

Protection sets

To protect data availability against concurrent node failures, HCP stores multiple copies of each object on different nodes in an automatically predetermined set of nodes, called a protection set. If a node (or one of its logical volumes) fails, objects stored on its associated volumes (or on the failed volume) are still available through other nodes in the set.

Geo-protection

You can create a configuration in which selected tenants and namespaces are maintained on two or more HCP systems and the objects in those namespaces are managed across those systems. This cross-system management helps ensure that data is well-protected against the unavailability or catastrophic failure of a system.

Typically, the systems involved in cross-system data management are in separate geographic locations and are connected by a high-speed wide area network. This arrangement provides geographically distributed data protection (called *geo-protection*).

Geo-protection enables HCP to support a cloud storage model, where any type of client request can be serviced equally by any system in the topology. Additionally, each system may be able to provide faster data access for some applications than the other systems can, depending on where the applications are running.

HCP supports two methods of geo-protection: whole-object protection and erasure-coded protection. Both methods are implemented by the Replication service, which is responsible for the distribution of configuration information and either complete copies of object data or chunks for erasure-coded objects.

Read from remote

If an object in a replicated HCP namespace or default-namespace directory is unavailable on one system in a replication topology (for example, because a node is unavailable), HCP can try to read the object from another system in the topology. HCP tries this only if the namespace has the read-from-remote feature enabled and the object has already been replicated.

Note: The read-from-remote feature does not affect the ability of HCP to read the data for metadata-only objects from another system or to restore or reconstruct erasure-coded objects.

Automatic redirection to other systems in a replication topology

HTTP requests for access to an unavailable HCP system can be automatically redirected to any other system in a replication topology in which the unavailable system participates. This means that, to be satisfied, the request does not need to be reissued with a different URL.

For another system to satisfy the request, the target HCP namespace or default-namespace directory must be replicated to that system. Also, the namespace must be configured to accept requests directed to other HCP systems. Additionally, the DNS must be configured to support redirection between HCP systems in the replication topology, and the unavailable system must be configured to allow this redirection.

Regulatory compliance

HCP includes features that enable you to comply with local regulations regarding data storage and maintenance:

Data privacy

At HCP installation time, you can choose to encrypt all data and metadata stored in the repository, thereby ensuring data privacy in a compliance context. Encryption prevents unauthorized users and applications from directly viewing namespace content. Lost or stolen storage devices are useless to parties without the correct encryption key.

HCP handles data encryption and decryption automatically, so no access or process changes are required.

Retention classes

Some government regulations require that certain types of data be kept for a specific length of time. For example, local law may require that medical records be kept for a specific number of years.

A *retention class* is a named duration that can be used as the retention setting for an object. When an object is assigned to a retention class, the object cannot be deleted until the specified length of time past its creation date. For example, a retention class named HlthReg-107 could have a duration of 21 years. Objects assigned to that class then could not be deleted for 21 years after they were created.

Retention mode

A namespace can be created in either of two modes: enterprise or compliance. The retention mode determines which operations are allowed on objects that are under retention:

- In *enterprise mode*, users and applications can delete objects under retention if they have explicit permission to do so. This is called *privileged delete* (see below).

  Also, in enterprise mode, authorized administrative users can delete retention classes and shorten retention class durations.

- In *compliance mode*, objects that are under retention cannot be deleted through any mechanism. Additionally, retention classes (see above) cannot be deleted, and retention class durations cannot be shortened.

Privileged delete

Some localities require that certain data be destroyed in response to changing circumstances. For example, companies may be required to destroy particular information about employees who leave.

Privileged delete is an HCP feature that enables authorized users to delete objects even if they are under retention. This feature is available only in namespaces that are in enterprise mode. In compliance mode, objects can never be deleted while they are under retention.

When performing a privileged delete operation, the user is required to specify a reason for the deletion. HCP logs each privileged delete operation along with its specified reason, thereby creating an audit trail.

Retention hold

To support legal discovery, users and applications can place a hold on selected objects. While an object is on hold, it cannot be deleted through any mechanism, regardless of its retention setting.

Storage usage optimization

HCP uses a number of features to reclaim and balance storage capacity.

Compression/Encryption service

The Compression/Encryption service makes more efficient use of HCP storage by compressing object data, thereby freeing space for storing more objects.

Duplicate Elimination service

A repository can contain multiple objects that have identical data but different metadata. When the Duplicate Elimination service finds such objects, it merges their data to free storage space occupied by all but one of the objects.

Disposition service

The Disposition service automatically deletes objects with expired retention periods. To be eligible for disposition, an object must have a retention setting that is either a date in the past or a retention class with automatic deletion enabled and a calculated expiration date in the past.

Version pruning

An HCP namespace can be configured to allow storage of multiple versions of objects. Version pruning is the automatic deletion of previous versions of an object that are older than a specified amount of time.

Garbage Collection service

The Garbage Collection service reclaims storage space both by completing logical delete operations and by deleting objects left behind by incomplete transactions.

Capacity Balancing service

The Capacity Balancing service ensures that the percentage of space used is roughly equivalent across all the storage nodes in the system. Balancing storage usage across the nodes helps HCP balance the processing load.

Service plans

Specifies the types of storage on which copies of that object must be stored and specifies the number of object copies that must be stored on each type of storage.

By default, throughout the lifecycle of an object, HCP stores that object only on *primary running storage*, which is storage that is managed by the nodes in the HCP system and consists of continuously spinning disks. However, you can configure HCP to use other types of storage for tiering purposes.

Every service plan defines primary running storage as the initial storage tier, called the *ingest tier*. The default storage tiering strategy specifies only that tier.

Primary running storage is designed to provide both high data availability and high performance for object data storage and retrieval operations. To optimize data storage price/performance for the objects in a namespace, you can configure the service plan for that namespace to define a storage tiering strategy that specifies multiple storage tiers.

Storage Tiering service

HCP uses the Storage Tiering service to maintain the correct number of copies of each object in a namespace on the storage tiers that are defined by the storage tiering strategy for that namespace. When the number of object copies on a storage tier goes below the number of object copies specified for that tier in the applicable service plan, the Storage Tiering service automatically creates a new copy of that object on that tier. When the number of copies of an object on a storage tier goes above the number of object copies specified for that tier in the applicable service plan, the Storage Tiering service automatically deletes all unnecessary copies of that object from that tier.

Primary spindown storage

On a HCP with SAN-attached storage system, HCP can be configured to use primary spindown storage, which is primary storage that consists of disks that can be spun down when not being accessed, for tiering purposes. You can then configure the service plan for any given namespace to define primary spindown storage as a storage tier for the objects in that namespace. Using primary spindown storage to store object data that's accessed infrequently saves energy, thereby reducing the cost of storage.

HCP moves object data between primary running storage, primary spindown storage, and other types of storage that are used for tiering purposes according to rules that are specified in storage tiering strategies defined by service plans.

HCP S Series storage

HCP can be configured to use *S Series storage*, which is storage on external HCP S Series Nodes that are separate from the HCP system. S Series Nodes are used for tiering purposes, and the HCP system communicates with them through the S3 compatible API and management API.

Extended storage

HCP can be configured to use *extended storage*, which is storage that's managed by devices outside of the HCP system, for tiering purposes. HCP supports the following types of extended storage:

NFS

Volumes that are stored on extended storage devices and are accessed using NFS mount points

Amazon S3

Cloud storage that is accessed using an Amazon Web Services user account

Google Cloud

Cloud storage that is accessed using a Google Cloud Platform user account

Microsoft Azure

Cloud storage that is accessed using a Microsoft Azure user account

S3 compatible

Any physical storage device or cloud storage service accessed using a protocol that is compatible with the Amazon S3 API

ThinkOn cloud

S3 compatible cloud storage that is accessed using a ThinkOn cloud user account

Moving object data from primary storage to extended storage frees up HCP system storage space so that you can ingest additional objects.

Note: While all of the data for an object can be moved off primary running storage and stored only on extended storage, at least one copy of the system metadata, custom metadata, and ACL for that object must always remain on primary running storage.

In addition, you can optimize data storage price/performance for the objects in a namespace by configuring the service plan for that namespace to define a storage tiering strategy that defines storage tiers for multiple types of extended storage.

HCP moves object data between primary running storage, primary spindown storage (if it is used), and one or more types of extended storage according to rules specified in the storage tiering strategies defined by service plans.

Erasure-coded protection

Erasure-coded protection is a method of geo-protection where the data for each object in a replicated namespace is subject to erasure coding. With erasure coding, the data is encoded and broken into multiple chunks that are then stored across multiple HCP systems. All but one chunk contains object data. The other chunk contains parity for the object data.

With erasure-coded protection, each system stores one data or parity chunk for any given erasure-coded object. The size of each chunk for an object is the size of the object data divided by the number of data chunks for the object. This means that the total storage used for an object in a replicated namespace is at most the size of a chunk times the total number of data and parity chunks for the object. (Storage usage can be less due to compression and duplicate elimination.)

For whole-object protection (the other method of geo-protection) to provide the same level of data protection as erasure-coded protection provides, at least two systems must each store all the data for each object in a replicated namespace. With two systems, the total storage used for each object is at most two times the size of the object data, which is greater than the total storage used when the same object is erasure coded. This is true regardless of the number of systems across which the chunks for the erasure-coded object are distributed.

Additionally, with erasure-coded protection, the storage footprint on any individual system that stores chunks for objects is smaller than the storage footprint resulting from storing complete object data on that system.

Metadata-only objects

With multiple HCP systems participating in a replication topology, you may not need to store object data in every system. A metadata-only object is one from which HCP has removed the data, leaving the system metadata, custom metadata, and ACL for the object in place. HCP makes an object metadata-only only if at least one copy of the object data exists elsewhere in the topology.

Metadata-only objects enable some systems in a replication topology to have a smaller storage footprint than other systems, even when the same namespaces are replicated to all systems in the topology.

HCP makes objects metadata-only according to the rules specified in service plans. If the rules change, HCP can restore data to the objects to meet the new requirements.

Network bandwidth usage optimization

HCP offers these features to help maximize network throughput and reduce the use of network bandwidth by read and write operations:

Link aggregation

Each node in an HCP system has two bonded ports for connecting to the front-end network. When using a single front-end switch, you can take advantage of this setup by using two cables per node to connect to the switch and configuring both HCP and the applicable ports on the switch for active-active (802.3ad) bonding. The redundant ports and cables help ensure a high-availability connection to the front-end network and the active-active bonding allows for increased network throughput.

10Gb Ethernet connectivity

Optionally, for HCP with SAN-attached storage systems, HCP supports 10Gb Ethernet connectivity to the front-end network. The 10GbE network interface allows for greater network throughput than does the 1GbE interface option.

Systems with the 10GbE network interface on the front end also use 10GbE for the back-end network. This enables the HCP nodes to transmit data among themselves at a rate that supports the higher front-end throughput.

Compressed data transmission

Clients that use the HTTP protocol to communicate with HCP can reduce network bandwidth usage by sending and receiving data in a compressed format. Before sending data to HCP, the client uses the publicly available gzip utility to compress the data. Upon receiving the data, HCP uncompresses it automatically before storing it. When requested to do so, HCP uses gzip to compress data before sending it to the client. The client then uses gunzip to uncompress the data.

Combined data and custom metadata on reads and writes

Clients that use the HTTP protocol for namespace access can store or retrieve both the data and custom metadata for an object with a single request. Issuing a single request instead of separate requests for the data and custom metadata reduces the network load.

This feature can be used in conjunction with compressed data transmission to further reduce the network load.

HCP administration

As an HCP system-level administrator, you play a role in ensuring the continued viability and accessibility of the HCP system. The primary tool for these purposes is a web application called the System Management Console.

Note:

Tenant-level administrators use a separate web application called the Tenant Management Console to configure and manage tenants and namespaces.

Depending on the permissions you have, you can use the System Management Console to configure various aspects of the system and manage administrative user accounts, as well as monitor system activity. Additionally, the Console reports hardware problems as they occur, so you can initiate repairs in a timely manner.

System Management Console

The System Management Console is a system-specific web application that lets you monitor and manage HCP and its individual nodes. The Console shows you the status of the system in real time, so you can take action when necessary to ensure system health (for example, restarting a node that has failed). Through the Console, you can also modify various system settings, create tenants, and monitor repository usage across all namespaces. Changes you make through the Console take effect immediately.

Access to the System Management Console is available only through HTTP with SSL security (HTTPS).

To access the HCP System Management Console in Internet Explorer® on a Windows server, Internet Explorer Enhanced Security Configuration must be disabled for administrators on that server.

Console access

To use the System Management Console, you need either:

- A system-level user account defined in HCP.
- If the HCP system is configured to support Windows Active Directory (AD), an AD user account for a user that belongs to one or more AD groups for which corresponding system-level group accounts are defined in HCP. In the help, such an AD user account is referred to as a *recognized AD user account*.

Your HCP user account or group account configuration includes settings that specify what you have permission to do in the Console. The menu options, pages, and panels that you see in the Console depend on the permissions that have been configured for your user or group account.

If an AD user belongs to multiple AD groups for which HCP group accounts exist, that user has all the permissions associated with all those group accounts.

Console sessions

A System Management Console session begins when you take one of these actions:

- Log into the Console using an HCP user account or recognized AD user account.
- Access a Console page while logged in to Windows with a recognized AD user account. This is called *single sign-on*. With single sign-on, you don't need to explicitly log into the Console.

  Your web browser must be configured to support single sign-on.

A session ends when you log out. During a session, you can perform any actions for which you have permission.

During a session, if you don't take any action for a certain amount of time, the Console displays the *Idle Timeout* page. If you explicitly logged in to the session, the Console automatically logs you out and, when you click any tab on the *Idle Timeout* page, displays the login page. If you started the session by using single sign-on, when you click any tab, the Console displays the requested page. The amount of idle time allowed is configurable.

Note: Logging in to or out of the System Management Console has no effect on HCP operations.

HCP management API

HCP includes a RESTful HTTP interface to a subset of its administrative functions. Using this interface, called the *management API*, you can create, modify, and delete tenants and manage replication. If a tenant has been configured to allow system-level users to manage it and search its namespaces, you can also view available service plans that can be assigned to that tenant, and you can create, modify, and delete namespaces, user and group accounts, and content classes for that tenant. Additionally, you can create, modify, and delete retention classes for tenant namespaces.

You use the HCP System Management Console to enable the management API. To use the management API, you need a user account that includes the applicable permissions for the actions that you want to take.

If HCP is configured to support AD authentication, applications can also use recognized AD user accounts to access HCP through the management API. To do this, an application must use the SPNEGO protocol to negotiate the AD user authentication.

Hitachi Device Manager and Hitachi Tiered Storage Manager

As an alternative to the System Management Console, you can use Hitachi Device Manager (HDvM) to report on HCP storage usage. Additionally, when using USP or USP V storage, you can use Hitachi Tiered Storage Manager to migrate repository content to different storage tiers.

You cannot make changes to the HCP configuration through HDvM or Hitachi Tiered Storage Manager.

HCP supports IPv4 and IPv6 network connections to HDvM servers. However, HDvM support for IPv6 network connections varies based on the HDvM server operating system. For information about requirements for HDvM servers that support IPv6 networks, see the applicable Hitachi Command Suite documentation.

Hitachi Remote Ops

Hitachi Remote Ops is a Hitachi Vantara product that enables you and HCP support personnel to monitor your HCP system remotely. With Hitachi Remote Ops, you can monitor nodes, back-end switches, and front-end switches. For HCP with SAN-attached storage systems, you can also monitor SAN arrays and Fibre Channel switches.

Hitachi Remote Ops is used for monitoring and error notification purposes only. It does not allow any changes to the HCP system.

HCP supports IPv4 and IPv6 network connections to Hitachi Remote Ops servers. However, Hitachi Remote Ops support for IPv6 network connections varies based on the Hitachi Remote Ops server operating system. For information about requirements for Hitachi Remote Ops servers that support IPv6 networks, see the Hitachi Remote Ops documentation.

System Management Console URL

The URL for the System Management Console has this format:

```
https://admin.hcp-domain-name:8000
```

In this format, hcp-domain-name is the name of the domain associated with the [hcp_system] network.

For example, for access to the System Management Console for the HCP system with the domain name hcp-ma.example.com, you would use this URL:

```
https://admin.hcp-ma.example.com:8000
```

If the management network is enabled, you cannot access the System Management Console with the domain name associated with the [hcp_system] network. You need to use the domain name associated with the [hcp_management] network.

Normally, you specify the HCP system domain name in the System Management Console URL and let HCP choose the node on which the Console application runs. However, in certain situations, you may need to access the Console on a specific node. To do so, you specify a System Management Console URL that includes a valid [hcp_system] network IP

address for the node on which you want to access the Console.

For example, if a node has the IPv4 address 192.168.210.16 and the IPv6 address 2001:0db8::101 defined for the [hcp_system] network, you can access the System Management Console on that specific node by entering either of these URLs in your browser address field:

```
https://192.168.210.16:8000
```

```
https://[2001:0db8::101]:8000
```

Regardless of whether you access the System Management Console by specifying a domain name or a node IP address, the Console provides administrative capabilities for the entire system.

Using a hosts file

Typically, the HCP system is included as a subdomain in your DNS. If this is not the case, you can specify an IP address in the System Management Console URL, as described above. Alternatively, you can specify the HCP system domain name in the URL and use a hosts file to define mappings of one or more node IP addresses to the domain name.

The location of the hosts file depends on the client operating system:

- On Windows, by default: c:\windows\system32\drivers\etc\hosts
- On Unix: /etc/hosts
- On Mac OS® X: /private/etc/host

Note: Every HCP system has a domain that's associated with the [hcp_system] network. If HCP is not included in your DNS, this is a dummy domain with a name that follows the conventions for well-formed DNS names.

Hostname mappings

Each entry in a hosts file is a mapping of an IP address for a system to a fully qualified domain name (FQDN) for that system.

Each hosts file entry that you create for access to the HCP System Management Console must include:

- A valid [hcp_system] network IP address for an HCP node
- The FQDN used to access the HCP System Management Console, which consists of the prefix *admin.* followed by the HCP system domain name

For example, if the [hcp_system] network domain name is hcp-ma.example.com and one of the HCP nodes has the IPv4 address 192.168.210.16 and the IPv6 address 2001:0db8::101 defined for that network, you could add either or both of these lines to the hosts file on the client:

```
192.168.210.16 admin.hcp-ma.example.com
```

```
2001:0db8::101 admin.hcp-ma.example.com
```

You can include comments in a hosts file either on separate lines or following a mapping on the same line. Each comment must start with a number sign (#). Blank lines are ignored.

Hostname mapping considerations

In the hosts file, you can map IP addresses for any number of nodes to a single domain name. The way a client uses multiple IP address mappings for a single domain name depends on the client platform. For information about how your client handles hosts file entries that define multiple IP address mappings for a single domain name, see your client documentation.

If any of the HCP nodes listed in the hosts file are unavailable, timeouts may occur when you use a hosts file to access the System Management Console.

Sample hosts file

Here's a sample hosts file that contains mappings for both IPv4 and IPv6 addresses:

```
192.168.210.16    admin.hcp-ma.example.com
192.168.210.17    admin.hcp-ma.example.com
192.168.210.18    admin.hcp-ma.example.com
192.168.210.19    admin.hcp-ma.example.com
2001:0db8::101    admin.hcp-ma.example.com
2001:0db8::102    admin.hcp-ma.example.com
2001:0db8::103    admin.hcp-ma.example.com
2001:0db8::104    admin.hcp-ma.example.com
```

Logging in

Depending on the HCP system configuration, you can log in to the System Management Console with an HCP user account or a recognized AD user account.

To log into the System Management Console:

1. Open a web browser.
2. In the address field, enter the URL for the System Management Console for your HCP system.

   If you inadvertently use *http* instead of *https* in the URL, the browser returns an error. Enter the URL again, this time using *https*.

   One of these happens:

   - If all of these are true, you are automatically logged in to the System Management Console, and the Console Overview page appears:
     - You are currently logged in to Windows with a recognized AD user account.
     - HCP is configured to support AD.
     - Your web browser is configured to support single sign-on with AD.

     This is single sign-on. No further action is required.

   - If HCP is configured to support AD but any of the following apply, a message appears indicating that single sign-on was not possible:
     - You are not currently logged in to Windows with a recognized AD user account.
     - Your web browser is not configured to support single sign-on.
     - You are not on a Windows computer.

In these cases, you need to click Console login page in the message to display the System Management Console login page.
- If HCP is not configured to support AD, the System Management Console login page appears.

The System Management Console login page shows the specific version of the HCP release, the version numbers of any hotfixes that have been applied to the HCP system, and the serial number for the HCP system. After you enter the Console, this information appears at the bottom of each page.

3. In the Username field, type your username.
4. In the Password field, type your case-sensitive password.

   When using an HCP user account, if you try to log in with an invalid password multiple consecutive times, you are locked out of the Console. The exact number of times is configurable.

   AD can also be configured to disable user accounts after a given number of authentication attempts with an invalid password.

   Important: If you're using a locally authenticated HCP user account, you should change your password as soon as possible the first time you log into the System Management Console.
5. If HCP is configured to support AD, in the Domain field, select the applicable domain your user account:
   - If you're using an HCP user account, select the domain name of the HCP system.
   - If you're using a recognized AD user account, select the AD domain in which your user account is defined.

   If HCP is not configured to support AD, the login page does not display the Domain field.

6. Click Log In.
   The Console displays the Overview page or, if you're using an HCP user account and are required to change your password, the Change Password page.

   During system startup, you can log into the System Management Console before startup processing is complete. However, until more than half of the nodes have completed their startup processing, the Console displays only the Hardware page.

   The Console automatically switches to the Overview page or Change Password page, as applicable, when the required number of nodes is available.

Using the System Management Console

System Management Console pages display information about the HCP system. Some pages also let you configure various aspects of the system.

Console pages have menus and hyperlinks for navigation. Each page shows a horizontal menu at the top. Some of the menu options display a secondary menu when you hover your cursor over them. To navigate to a page, you click the corresponding menu option.

You can also use shortcut keys to navigate to pages in the System Management Console. Each link that has a shortcut key has the applicable letter underlined. To use the shortcut key, follow the convention for the browser you're using.

Each page of the System Management Console shows the username of the currently logged-in user in the upper right corner.

Note:

If you're an AD user and your username changes in AD while you're using the System Management Console, the Console may not reflect the new username until you log out and back in. If you're currently using any other HCP interfaces, you need to log out of those as well. Alternatively, you can force the Console to reflect the new username immediately by clearing the AD cache.

While the system is experiencing a heavy load, the System Management Console may be slower to present certain information.

If the HCP system restarts while you're using the System Management Console, clicking any menu option, hyperlink, or button causes the Console to display the Hardware page. The Console automatically switches to the Overview page when the system becomes available again.

Refreshing pages

System Management Console pages do not automatically refresh themselves while they remain open. To see the most recent values on a page, click again on the menu option that opens that page.

Note: Using the browser reload button to refresh a page that lets you create or modify an entity causes the Console to resubmit values you previously entered on the page.

Submitting changes

Most System Management Console pages and panels on which you can modify information have action buttons (such as Update Settings and Create Tenant) that submit your changes. Action buttons make the changes on a page permanent. These changes take effect immediately.

You need to submit the changes you make before switching to a different page or panel. If you switch without submitting your changes, the Console does not retain them.

For some checkbox options, selecting or deselecting the checkbox causes that change to take effect immediately.

After you submit changes, the Console displays a message indicating whether HCP successfully made the changes. To hide the message, click Dismiss in the message area.

Changing your password

Depending on how your HCP user account is set up, HCP might authenticate your username and password locally or remotely when you log in. If your account is set up for local authentication, you can change your password in the System Management Console. When you change your password in this Console, it also changes for any other HCP interfaces to which your user account gives you access.

If your account is set up for remote authentication or if you use an AD user account to access the Console, you use a method outside HCP to change your password.

The next procedure describes how to change your locally authenticated password using the System Management Console.

1. Log into the System Management Console using your existing password.
2. In the top right corner of the Console window, click Password.
3. On the Change Password page:
   a. In the Existing password field, type your current password.
   b. In the New password field, type your new password.
      Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters including white space. To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other. When changing your password, you cannot reuse your current password.
   c. In the Confirm New Password field, type your new password again.
4. Click Update Password.

Logging out

To log out of the System Management Console:

1. In the top right corner of the Console window, click Log Out.
2. If you explicitly logged in, close the browser window to ensure that other users cannot go back into the System Management Console using the credentials you used to log in.
   Tip: For extra security, clear the browser cache before closing the window.

HCP administrative responsibilities

HCP administrative responsibilities consist of:

- Managing HCP user and group accounts
- Monitoring the HCP system
- Configuring the system
- Managing the system hardware
- Managing tenants
- Managing repository access across all namespaces
- Ensuring HCP system recovery
- Helping with troubleshooting

Most system configuration activities are one-time operations that you perform when HCP is first installed. Most monitoring and management activities are ongoing.

You perform configuration, monitoring, and management activities in the HCP System Management Console.

Managing user and group accounts

HCP user and group accounts determine whether you can log into the HCP System Management Console, Tenant Management Console for the default tenant, or Search Console for access to the default namespace. For the System Management Console and Tenant Management Consoles, they also determine which actions you're allowed to perform after logging in.

You use the System Management Console to create, modify, and delete system-level user and group accounts. For each HCP user account, you specify whether it's authenticated locally or by RADIUS. To enable RADIUS authentication, you need to configure connections to one or more RADIUS servers.

You also use the System Management Console to configure login settings for the Console as a whole.

Additionally, you use the System Management Console to clear the AD cache. You may need to do this, for example, to immediately discontinue system access by a user whose AD user account is no longer valid.

Monitoring the system

HCP is a self-monitoring, self-healing system that automatically alerts you to problems it cannot resolve itself. It also provides the means for you to monitor it. This type of monitoring entails:

- Periodically checking the status of hardware, system resources, services, and available storage.
- Watching for alerts that may indicate conditions requiring human intervention.
- Periodically reviewing system resource usage and the system log to ensure that HCP is running smoothly and not exceeding its storage license.
- Reviewing and, if required, responding to system log messages received through syslog servers, SNMP managers, or email.
- If SNMP is enabled, evaluating and, if required, responding to trap-generated event notifications.

You can also generate chargeback reports. Typically, these reports are used as input to billing applications that need to determine charges for capacity and bandwidth usage at the tenant or namespace level. However, they are also a good source of information for system analysis, enabling you to adjust storage and bandwidth allocations based on usage patterns

Configuring the system

Configuring HCP entails:

- Optionally, making extended storage components such as NFS storage volumes and Amazon S3 compatible cloud storage known to HCP so that content can be offloaded from primary storage onto each type of extended storage
- Optionally, configuring user-defined networks so that you can segregate network traffic for different purposes.
- Enabling or disabling access to the HCP nodes.
- Managing domains and SSL server certificates.
- Controlling access to the System Management Console.
- Controlling access to the HCP management API.
- Configuring support for Windows AD or Windows workgroups.
- Enabling or disabling the use of SNMP for modifying system settings.
- Optionally, configuring HCP to send system log messages to syslog servers, SNMP managers, and/or specified email addresses.
- Scheduling and configuring HCP services to manage system load, ensure data and metadata integrity and availability, and optimize storage usage.

Managing the system hardware

An HCP system or any of its individual nodes may occasionally need to be shut down or restarted for a variety of reasons, including for hardware maintenance. When you want to retire a node or SAN array, you first need to migrate stored data off that device.

Managing tenants

HCP system-level administrators create all tenants. Once a tenant is created, you can change only some of its features. Tenant-level administrators are responsible for most tenant management.

In addition to creating and modifying tenants, you can delete tenants, but only if they don't own any namespaces.

Managing repository access

Managing repository access entails:

- Setting the systemwide permission mask, which provides the highest level of control over namespace access.
- Optionally, enabling and configuring the metadata query engine and API.
- Controlling access to the Search Console for the default tenant.

Ensuring HCP system recovery

Through its services, the HCP system is self-healing, so your intervention is not often required for recovery from unexpected events. Events that may require your intervention, however, include power outages and hardware failures.

To protect against a catastrophic failure of an HCP system, you can implement replication. When you do this, you are responsible not only for configuring the connections between the systems involved but also for managing failover and recovery should that become necessary.

Note: Default tenant administrators can use NDMP to back up and restore the default namespace.

Troubleshooting

From the system console for any HCP node, you can run selected diagnostics that can help you analyze and resolve issues with interactions between the node and other components in the HCP environment. Using these diagnostics, for example, you can troubleshoot problems with physical networks, virtual networking, external storage, and DNS.

Occasionally, you may need help resolving problems that occur with the HCP system. In such cases, your authorized service provider may ask you to download the logs HCP maintains internally and send them to the HCP support center.

You download the HCP internal logs from the System Management Console. You can also use the Console to insert comments into these logs to indicate when problems occur and describe their symptoms.

Account administration

As an HCP security administrator, you are responsible for creating and managing HCP system-level user and group accounts. These accounts give users permission to access the HCP System Management Console, the Tenant Management Console for the default tenant, the HCP management API, the HCP metadata query API, and/or the HCP Search Console for the default tenant. For the System Management Console and Tenant Management Consoles and the management API, these accounts also determine which actions the user is allowed to perform through the applicable interface.

When creating a user or group account, you associate roles with the account. For a user account, you also specify whether the account is authenticated locally or by RADIUS when used to access an HCP interface. To enable RADIUS authentication, you need to set up connections to one or more RADIUS servers.

You can create group accounts only if HCP is configured to support Active Directory (AD).

About user and group accounts

HCP uses system-level user and group accounts to control access to these interfaces:

- HCP System Management Console
- Tenant Management Console for managing the default tenant and namespace
- HCP management API for creating and managing tenants
- HCP metadata query API for querying the default namespace
- Search Console to search in the default namespace

Note: System-level user and group accounts do not control access to stored data and metadata other than through the metadata query API and Search Console.

User accounts

An HCP user account is a set of credentials that gives a user access to one or more of the interfaces listed above. You create and manage user accounts in the HCP System Management Console.

When you create a user account, you specify a username and password. You also associate roles with the account and specify whether the user credentials are authenticated locally or by RADIUS. Additionally, for locally authenticated users, you specify whether the account password must be changed the next time the account is used to access one of the Consoles.

You can enable and disable user accounts, as needed. While an account is disabled, it cannot be used to access any of the applicable interfaces. You might decide to disable an account, for example, while the user for whom you created it is on vacation.

Multiple people can use the same user account concurrently for the same or different interfaces. To prevent this from happening, you should create a separate account for each user, and users should keep their passwords confidential.

An HCP system can have at most 200 system-level user accounts.

Group accounts

An HCP group account is a representation of an Active Directory group. The group account enables AD users in the AD group to access one or more of the interfaces listed above. You create and manage group accounts in the HCP System Management Console.

When you create a group account, you associate roles with it. When an AD user accesses HCP, that user has all the roles associated with all the group accounts that correspond to AD groups to which the user belongs.

An HCP system can have at most 100 system-level group accounts.

Roles and permissions

A *role* is a named collection of permissions that are granted to a user either through an HCP user account or through one or more HCP group accounts. Each permission in a role lets the user perform some specific interaction or set of interactions with the HCP system. Roles generally correspond to job functions.

You can associate any number of roles with a user or group account. The account user then has all the permissions granted by each of those roles.

Before associating roles with a user or group account, make sure the permissions granted by those roles are consistent with the job functions of the user or group of users for whom you're creating the account.

Note:

An AD user can be added to an AD group while that user is using the System Management Console. If the AD group corresponds to an existing HCP group account, the user may not automatically get the roles associated with that group account for up to eight hours. To get the roles immediately, the user needs to log out of the System Management Console and then log back in. If the user is also currently using the Tenant Management Console or Namespace Browser, logging out of either of those interfaces has the same effect.

Alternatively, you can force the roles to be recognized immediately by clearing the AD cache.

Available roles

The roles that you can associate with a user or group account are:

Monitor
: Grants permission to use the System Management Console to view the HCP system status and most aspects of the system configuration, including tenant configurations. The monitor role also grants read-only permission to view user and group accounts.

Administrator
: Grants permission to use the System Management Console to view the HCP system status, perform most system configuration activities, create and manage tenants, and download the HCP internal logs. The administrator role also grants read-only permission to view user and group accounts. The administrator role does not grant permission to configure user or group accounts.

Security
: Grants permission to use the System Management Console to view the HCP system status, create and manage user accounts, configure remote authentication, modify system security settings, configure syslog and SNMP logging and email notification, and view security events in the system log.

Compliance
: Grants permission to use the Tenant Management Console to work with retention classes and retention-related settings and perform privileged deletes, as well as to use the System Management Console to view the HCP system status. Using the Tenant Management Console is possible only for the default tenant and for HCP tenants that are configured to allow system-level users to manage them and search their namespaces

Service
: Grants permission to use the System Management Console to view the HCP system status and perform advanced system reconfiguration and management activities. The service role does not grant permission to view or configure user or group accounts.
Important: You should perform activities restricted to the service role only after consulting your authorized HCP service provider.

Search
: Grants permission to use the metadata query API and Search Console to query or search the default namespace and any namespaces owned by HCP tenants that are configured to allow system-level users to manage them and search their namespaces. To use the metadata query API or Search Console for access only to the HCP namespaces owned by a specific tenant, a user must have a tenant-level user account or an AD user account that's recognized at the tenant level.

The monitor, administrator, security, and compliance roles also grant access to use the HCP management API for specific activities.

Tenant-level administration

Tenants, except the default tenant, have their own user and group accounts that can enable access to the Tenant Management Console and HCP management API. The roles available for these accounts are monitor, system, security, and compliance. Tenant security administrators define tenant-level user and group accounts in the Tenant Management Console.

HCP system-level users with the monitor, administrator, security, or compliance role automatically have access to the Tenant Management Console and HCP management API functions for the default tenant. The default tenant does not have user or group accounts of its own.

A tenant-level user with the administrator role can configure an HCP tenant to allow system-level users to manage it and search its namespaces. This enables system-level users with the monitor, administrator, security, or compliance role to log into the Tenant Management Console or use the HCP management API for the tenant. System-level users with the monitor or administrator role can also access the Tenant Management Console directly from the System Management Console. For the default tenant, access by system-level users is enabled automatically and cannot be disabled.

Note:

If a tenant-level user account has the same username and password as your system-level user account, you cannot use your system-level account to log into the Tenant Management Console for that tenant. You can, however, access that Console directly from the System Management Console, in which case, you are still using your system-level user account.

After accessing the Tenant Management Console or HCP management API for a tenant that is configured to allow system-level users to manage it and search its namespaces, system-level users can perform the activities allowed by the tenant-level roles that correspond to their system-level roles.

An AD user can belong to AD groups for which corresponding HCP group accounts exist at both the system and tenant levels. When such a user accesses the Tenant Management Console, that user has the roles associated with both the applicable system-level group accounts and the applicable tenant-level group accounts.

When logged in to the Search Console for the default tenant, system-level users with the search role can search the namespaces owned by HCP tenants that are configured to allow system-level users to search their namespaces. These system users can also use the metadata query API to query those namespaces.

Permissions granted by role

The following tables show the user permissions that each role grants for the System Management Console, Search Console, and Tenant Management Console.

System Management and Search Console permissions

The following table lists the permissions that apply to the System Management Console and Search Console. Checkmarks indicate the permissions granted by each role.

	Role					
Permission	Monitor	Administrator	Security	Service	Compliance	Search
View user accounts	✓	✓	✓			
View group accounts	✓	✓	✓			
Create, modify, delete, and manage user accounts			✓			
Create, modify, and delete group accounts			✓			
Specify message text for the System Management Console and Search Console login pages			✓			
Configure support for Active Directory			✓			

	Role					
Permission	Monitor	Administrator	Security	Service	Compliance	Search
Clear the Active Directory cache			✓			
View and modify the RADIUS server configuration			✓			
View the system overview	✓	✓	✓	✓		
Stop and restart the system		✓		✓		
View the system hardware status	✓	✓	✓	✓		
View individual nodes	✓	✓	✓	✓	✓	
Stop and restart individual nodes		✓		✓		
Eject the CD tray from a node				✓		
Remove a node from the HCP system				✓		
View storage pools, components, and volumes	✓	✓				
Create, modify, retire, and delete storage pools, components, and volumes		✓				
View networks	✓	✓		✓		
Set global IP mode support for front-end networks				✓		
Modify the [hcp_system] and [hcp_backend] networks				✓		
Enable creation of user-defined networks				✓		
Create, modify, and delete user-defined networks		✓				
Enable the [hcp_management] network		✓				
Create, modify, and delete tenants		✓				
View the tenant list	✓	✓				
View individual tenants, including tenant settings	✓	✓				
Reset tenant security		✓				
Select a search facility for the Search Console		✓				
View service statuses and configurations	✓	✓				
Modify service configurations and manage service activity, including configuring and managing data migrations, replication links, and erasure coding topologies		✓				
Start, stop, enable, and disable services				✓		
View the current service schedule	✓	✓				
Create, modify, activate, and delete service schedules		✓				
View service plans	✓	✓				
Create, modify, retire, and delete service plans		✓				
Assign service plans to tenants		✓				
Start, stop, enable, and disable services				✓		
View network security settings	✓	✓				
Modify network security settings		✓				
View the current SSL server certificate	✓	✓				
Manage SSL server certificates		✓				
View and modify System Management Console security settings			✓			
View and modify HCP management API security settings			✓			
View and modify Search Console security settings			✓			
View the systemwide permission mask	✓	✓				
Modify the systemwide permission mask		✓				
View HCP system log messages about all events except security events	✓	✓	✓			
View HCP system log messages about security events			✓			
View the syslog configuration	✓	✓	✓		✓	
Modify the syslog configuration and test syslog connections		✓	✓			
View SNMP settings	✓	✓	✓		✓	
Modify SNMP settings and test SNMP connections		✓	✓			
View email notification settings	✓	✓	✓		✓	
Modify email notification settings and test email server connections		✓	✓			
View the Hitachi Device Manager connection configuration	✓	✓				
Configure the Hitachi Device Manager connection		✓				
Monitor system resource usage	✓	✓				

	Role					
Permission	Monitor	Administrator	Security	Service	Compliance	Search
Generate chargeback reports	✓	✓				
Add comments to the HCP internal logs		✓	✓			
Download the HCP internal logs		✓				
Modify the system DNS settings, time settings, serial number, HTTP persistent connection timeout interval, custom thread count for replication, and SNMP broken-link reporting interval				✓		
Enable creation of the default tenant and namespace				✓		
Make back-end switches known to HCP				✓		
Commit an HCP system upgrade				✓		
Use the Search Console for the default tenant						✓
Change your own locally authenticated password in the System Management Console	✓	✓	✓	✓	✓	
Change your own locally authenticated password in the Search Console						✓
View HCP documentation from the System Management Console	✓	✓	✓	✓	✓	
View HCP documentation from the Search Console						✓
Renewing the storage license		✓				
Optimize for cloud		✓				
Update and create networks				✓		
Download the HCP system logs for diagnostics				✓		
Add comments to HCP system logs				✓		
Configure AD authenticated CIFS support.			✓			
View and modify AD domain controller filter			✓			
Setting the tenant management and data networks		✓				
Upload and download encryption keys		✓				
Apply exclusive Hitachi Vantara Support access credentials		✓		✓		
View Hitachi Vantara Support access credentials	✓	✓	✓	✓		

Tenant Management Console permissions

The following table lists the permissions that apply to the Tenant Management Console. Checkmarks indicate the permissions granted by each role.

	Role			
Permission	Monitor	Administrator	Security	Compliance
View the user account list (HCP tenants only)	✓	✓	✓	
View the full definition of individual user accounts (HCP tenants only)			✓	
View the description, allow namespace management property, and data access permissions for individual user accounts (HCP tenants only)	✓	✓		
Create, associate roles with, delete, and otherwise manage user accounts, except modifying the allow namespace management property and data access permissions (HCP tenants only)			✓	
Modify the allow namespace management property and manage data access permissions for user accounts (HCP tenants only)		✓		
View the group account list (HCP tenants only)	✓	✓	✓	
View the full definition of individual group accounts (HCP tenants only)			✓	
View the description, allow namespace management setting, and data access permissions for individual group accounts (HCP tenants only)	✓	✓		
Create, associate roles with, and delete group accounts, (HCP tenants only)			✓	
Modify the allow namespace management setting and manage data access permissions for group accounts (HCP tenants only)		✓		
Specify message text for the Tenant Management and Search Console login pages (HCP tenants only)			✓	
View the tenant overview	✓	✓	✓	✓
Modify the tenant contact information, permission mask, and description		✓		
Allow or disallow access to the Tenant Management Console by HCP system-level users (HCP tenants only)		✓		
View and modify Tenant Management Console security settings (HCP tenants only)			✓	
View and modify HCP management API security settings (HCP tenants only)			✓	
View and modify Search Console security settings (HCP tenants only)			✓	
View content classes and content properties	✓	✓		
Create, modify, and delete content classes and content properties		✓		
View namespace associations with content classes	✓	✓		
Modify namespace associations with content classes		✓		

	Role			
Permission	Monitor	Administrator	Security	Compliance
View tenant log messages about all events except compliance and security events	✓	✓	✓	✓
View tenant log messages about compliance events				✓
View tenant log messages about security events			✓	
View syslog and SNMP logging options	✓	✓		
Enable or disable syslog and SNMP logging		✓		
View email notification settings	✓	✓		
Modify email notification settings		✓		
Generate chargeback reports (HCP tenants only)	✓	✓		
Create and delete namespaces (HCP tenants only)		✓		
View the namespace list (HCP tenants only)	✓	✓		✓
View namespace overviews	✓	✓		✓
Modify namespace names and quotas (HCP tenants only)		✓		
View namespace permission masks and descriptions	✓	✓		✓
Modify namespace permission masks and descriptions		✓		
View namespace owners (HCP namespaces only)	✓	✓		✓
Change namespace owners (HCP namespaces only)		✓		
View the tags associated with namespaces (HCP namespaces only)	✓	✓		
Modify the tags associated with namespaces (HCP namespaces only)		✓		
View namespace default retention settings (HCP namespaces only)	✓	✓		✓
Modify namespace default retention settings (HCP namespaces only)				✓
View namespace default shred settings (HCP namespaces only)	✓	✓		✓
Modify namespace default shred settings (HCP namespaces only)				✓
View namespace default index settings (HCP namespaces only)	✓	✓		
Modify namespace default index settings (HCP namespaces only)		✓		
View minimum data access permissions (HCP namespaces only)	✓	✓		
Modify minimum data access permissions (HCP namespaces only)		✓		
View namespace ACL settings (HCP namespaces only)	✓	✓		
Manage the use of ACLs in namespaces (HCP namespaces only)		✓		
View namespace retention-related settings	✓	✓		✓
Modify namespace retention-related settings				✓
View the custom metadata XML checking setting for namespaces	✓	✓		
Modify the custom metadata XML checking setting for namespaces		✓		
View namespace object versioning configurations (HCP namespaces only)	✓	✓		
Configure object versioning in namespaces (HCP namespaces only)		✓		
View namespace compatibility settings	✓	✓		
Modify namespace compatibility settings		✓		
View namespace disposition settings	✓	✓		✓
Modify namespace disposition settings				✓
View namespace replication-related settings	✓	✓		
Modify namespace replication-related settings		✓		
View the service plans associated with namespaces	✓	✓		
Associate service plans with namespaces		✓		
View namespace retention modes	✓	✓		
Modify namespace retention modes		✓		
View default settings for namespace creation (HCP namespaces only)	✓	✓		
Modify default settings for namespace creation (HCP namespaces only)		✓		
View the maximum number of namespaces per user (HCP namespaces only)	✓	✓		
Modify the maximum number of namespaces per user (HCP namespaces only)		✓		
View namespace access protocol configurations	✓	✓		
Configure namespace access protocols for namespaces		✓		
View search and indexing options for namespaces	✓	✓		
Modify search and indexing options for namespaces		✓		

	Role			
Permission	Monitor	Administrator	Security	Compliance
Reindex namespaces		✓		
Monitor replication	✓	✓		
Select namespaces for replication (HCP namespaces only)		✓		
View all namespace log messages except messages about compliance events	✓	✓	✓	✓
View namespace log messages about compliance events				✓
View the list of irreparable objects	✓	✓		
Acknowledge irreparable objects		✓		
Create, modify, and delete retention classes				✓
View the list of retention classes	✓	✓		✓
View individual retention classes	✓	✓		✓
Perform privileged delete operations				✓
Change your own locally authenticated password in the Tenant Management Console	✓	✓	✓	✓
View HCP documentation from the Tenant Management Console	✓	✓	✓	✓
Optimize namespaces for cloud		✓		
View, add, modify, and delete KM servers.			✓	
View certificates and generate CSR			✓	
Download domain certificates.		✓	✓	
Enforce global encryption of data on HCP S series nodes or public cloud.			✓	
View all security events and alerts.		✓	✓	
View system level encryption related metrics.		✓	✓	

User authentication

To use the System Management Console or the Search Console for the default tenant, a user needs to supply a username and password for authentication. *User authentication* is the process of checking whether the combination of the specified username and password is valid.

For user accounts defined in HCP, the system supports local and RADIUS authentication. User accounts defined in AD must be authenticated by AD. RADIUS and AD authentication are types of remote authentication.

To use the HCP management API with an HCP user account, the user specifies the account credentials in each request. To use the API with a recognized AD user account, applications must use the SPNEGO protocol to negotiate the AD user authentication themselves.

Local authentication

For locally authenticated users, the user account password is stored in the HCP system. At user login, HCP checks the submitted username and password internally.

HCP lets the user into the target Console if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- The user account is associated with a role that grants permission to access the target Console.

If any of these conditions is not true, HCP doesn't let the user in.

You can change the passwords of locally authenticated users in the System Management Console. These users can also change their own passwords in the System Management Console, if they have access to it, or in the Search Console, if they have access to that.

RADIUS authentication

For RADIUS-authenticated users, the user account password is stored outside the HCP system. At user login, HCP securely sends the submitted username and password to a RADIUS server. That server checks whether the username and password are valid and sends the result to HCP.

HCP lets the user into the target Console if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- The user account is associated with a role that grants permission to access the target Console.

If any of these conditions is not true, HCP doesn't let the user in.

All password management for RADIUS-authenticated users is handled by the RADIUS server. You cannot use the System Management Console to set or change the passwords of RADIUS-authenticated users.

Active Directory authentication

For AD-authenticated users, the username and password for the user account are stored in AD. If the user is signed into a Windows client, HCP relies on Windows to have already validated the username and password with AD (this is single sign-on). However, if the user provides an AD username and password on the System Management Console or Search Console login page, HCP securely sends the specified username and password to AD for authentication.

HCP lets an authenticated user into the target Console only if these conditions are true:

- The user belongs to at least one AD group for which a corresponding group account exists in HCP.

Note: Alternatively, the user can belong to an AD group that's nested at any level under another group for which a corresponding HCP group account exists. In this case, however, any parent groups that are defined in a domain other than the user's domain must be universal.
- At least one such group account is associated with a role that grants permission to access the target Console.

If either of these conditions is not true, HCP doesn't let the user in.

All password management for AD-authenticated users is handled by the AD. You cannot use the System Management Console to set or change the passwords of AD-authenticated users.

Starter account

When HCP is first installed, one user account is already defined.

The username and password for the predefined user account are:

```
Username: security
```

```
Password: Chang3Me!
```

This account has only the security role and is authenticated locally.

You need to use the security account the first time you log into the System Management Console after HCP is installed. When you log in, you are immediately required to change the password for this account. Then you can create new accounts as needed, including new accounts with the security role.

You can delete the `security` account as long as at least one other locally authenticated HCP user account has the security role and is enabled.

Note: Your authorized HCP service provider may have changed the password and roles for the security account while verifying and completing the installation of the HCP system. If this is the case, you need to get the new password for the security account from the service provider.

Working with user accounts

To view, create, and manage user accounts, you use the Users page in the HCP System Management Console.

Note:

To view user accounts, you need the monitor, administrator, or security role. To create and manage user accounts, you need the security role.

To display the Users page, in the top-level menu, select Security ► Users.

About the Users page

The Users page lets you create, modify, and delete user accounts. It also lists the existing user accounts.

Understanding the user account list

The Users page lists existing user accounts. For each account, the list shows:

- The user name
- Whether the account is enabled or disabled
- The full name of the account user
- Whether the user login is authenticated locally or by RADIUS

To view additional information about an individual user account, click the account user name.

Managing the user account list

By default, the user account list on the Users page includes all existing user accounts. The accounts are listed 20 at a time in ascending order by username.

You can page through, sort, and filter the list of user accounts. The Users page indicates which accounts are shown out of the total number of accounts in the current list.

Paging

You can change the number of user accounts shown at a time on the Users page. To do this, in the Items per page field, select the number of tenants you want. The options are 10, 20, and 50.

To page forward or backward through the user account list, click the next ( ) or back ( ) control, respectively.

1. In the Page field, type the page number you want.
2. Press Enter.

Sorting

You can sort the user account list in ascending or descending order by username. To change the sort order, click the Username column heading. Each time you click the column heading, the sort order switches between ascending and descending.

Filtering

You can filter the user account list by username. The filtered list includes only those user accounts with a username that begins with or is the same as a specified text string.

1. In the entry field above the list, type the text string you want to use as a filter.
   This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
2. Click the find control ( ).

To redisplay the entire list of user accounts after filtering it, click the clear filter control ( ).

Creating a user account

To view user accounts, you need the monitor, administrator, or security role. To create and manage user accounts, you need the security role.

1. On the Users page in the System Management Console, click Create User Account.
2. In the Create User Account pane:
   a. (Optional) To initially disable the user account, clear Enable account.
   b. In the Username field, type a unique login name.
      User names:
      - Can be from one through 64 characters long and can contain any valid UTF-8 characters but cannot start with an opening square bracket ([). White space is allowed.
      - Are not case sensitive.
      - Cannot be names that are currently in use.

      Tip: Consider using email addresses as user names. This gives you easy access to email addresses should you need to contact users.
   c. In the Full Name field, type the name of the person for whom you are creating the account.
      This name can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
   d. For Authentication, select either Local for local authentication or RADIUS for remote authentication.
      - If you select Local, the pane displays the Password and Confirm Password fields and the Force change on next login option.
      - If you select RADIUS, these fields are hidden.
   e. If you select local authentication:
      i. Fill in the Password and Confirm password fields.

         Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters including white space. To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

      ii. (Optional) Select Force change on next login.

         When this option is selected, the next time a user logs into the System Management Console or Search Console, the Console automatically displays the Change Password page. The user cannot perform any other Console functions until you change the password. After the you change the password, this option gets cleared.

   f. In the Roles section, select any roles for the user account.
   g. (Optional) Specify a description for the user account.
      i. Click Description.
      ii. In the Description field, describe the user account.

         This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
3. Click Create User Account.

Modifying a user account

You can change this information about a user account:

- The user name
- The full name
- The password
- The roles associated with the account
- Whether the account is enabled. If you disable an account while the user is currently logged in, the user is immediately prevented from taking any further actions. You can disable your own account. After you disable it, however, you cannot reenable it yourself.
- Whether to force a password change at the next login

You cannot change the user ID or type of authentication. (The user ID is displayed with other account details when you view an individual account as a user with the security role.)

To view user accounts, you need the monitor, administrator, or security role. To create and manage user accounts, you need the security role.

1. In the list of user accounts on the Users page, click the user name for the account you want to modify.
2. In the panel that opens, make the changes you want.
   Note:

   When changing the password for a user account, you can reuse the current password. You cannot do this when changing your own password on the Change Password page.

   If you leave the Password field empty, the previously set password remains in effect.
3. Click Update Settings.

   If you are modifying the user account you used to log into the Console and:

   - You changed the roles associated with the user account, a message appears indicating that the page will be reloaded. Click Close in the message window to reload the page.
   - You selected Force change on next login, the Console displays the Change Password page. You need to change your password on this page in order to continue working in the Console.

Deleting a user account

You can delete a user account at any time. If you delete an account while the user is currently logged in, the user is immediately prevented from taking any further action. After you delete the account, the user can no longer log in.

Tip: For a RADIUS-authenticated user, if the user account becomes invalid on the RADIUS server while the user is logged in, the user may still be able to take action in the current Console session for as long as ten minutes. To ensure that the user is immediately prevented from taking further action, delete the user in HCP before deleting the remote account.

You cannot recreate a deleted account. However, you can reuse the user name from the deleted account to create a new account. The new account will have different user ID from the deleted account.

You cannot delete the account you used to log into the current System Management Console session. Additionally, if no existing AD group has the security role, you cannot delete the last locally authenticated user account with the security role.

To view user accounts, you need the monitor, administrator, or security role. To create and manage user accounts, you need the security role.

1. In the list of user accounts on the Users page, click the delete control ( ) for the account you want to delete.
2. In response to the confirming message, click Delete.

Generating a user authorization token

User authorization tokens convert the HCP user account user name and password into a token that can be used by RESTful APIs to authenticate with HCP. A user authorization token is the HCP user account user name encoded in base64 and HCP user account password encoded in an md5 hash. The token does not expire unless the HCP user account user name or password changes.

To view user accounts, you need the monitor, administrator, or security role. To create and manage user accounts, you need the security role.

1. Click Generate Authorization Token.
2. In the Generate Authorization Token window that opens, type the user name in the Username field.
3. In the Generate Authorization Token window that opens, type the password in the Password field.
4. Click Generate Authorization Token.

Working with group accounts

To view, create, and manage HCP group accounts, you use the Groups page in the HCP System Management Console. This page is available only while support for AD is enabled.

If you disable HCP support for AD, HCP does not delete existing group accounts. If you subsequently reenable AD support, the group accounts become accessible again.

To display the Groups page, in the top-level menu, select Security > Groups.

Note:

To view group accounts, you need the monitor, administrator, or security role. To create and manage group accounts, you need the security role.

Groups page

The Groups page lets you create, modify, and delete HCP group accounts. It also lists the existing group accounts.

By default, the group account list includes all existing group accounts. The accounts are listed 20 at a time in ascending order by group name.

You can page through, sort, and filter the list of group accounts. The Groups page indicates which accounts are shown out of the total number of accounts in the current list.

To view additional information about an individual group account, click the group name.

Paging

You can change the number of group accounts shown at a time on the Groups page. To do this, in the Items per page field, select the number of group accounts you want. The options are 10, 20, and 50.

To page forward or backward through the group account list, click the next ( ) or back ( ) control, respectively.

1. In the Page field, type the page number you want.
2. Press Enter.

Sorting

You can sort the group account list in ascending or descending order by group name. To change the sort order, click the Name column heading. Each time you click the column heading, the sort order switches between ascending and descending.

Filtering

You can filter the group account list by group name. The filtered list includes only those group accounts with a name that begins with or is the same as a specified text string.

1. In the entry field above the list, type the text string you want to use as a filter.
   This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
2. Click the find control ( ).

To redisplay the entire list of group accounts after filtering it, click the clear filter control ( ).

Creating group accounts

You create group accounts by first displaying a list of AD groups and then selecting the ones from which you want to create HCP group accounts. After selecting the groups you want, you select the roles you want to associate with those group accounts.

You can create up to the maximum supported number of group accounts in a single operation (that is, 100).

In HCP, each AD group is identified by both the group name and the name of the AD domain in which the group is defined (for example, hcp-admin@ad.example.com). The HCP group account created from an AD group has the same name as the AD group, including the domain name. Internally, however, the HCP group account is associated with the security ID (SID) of the AD group.

You can create an HCP group account from any group defined in the AD forest that HCP uses for user authentication. The only exceptions are predefined groups such as Administrators that have the same SID in all domains.

You can use a single operation to both create new group accounts and change the roles associated with existing group accounts. In this case, all the accounts involved end up with the same roles.

To view group accounts, you need the monitor, administrator, or security role. To create and manage group accounts, you need the security role.

1. On the Groups page in the System Management Console, click Add Active Directory Groups.

   The Find and Select Groups section lists all the AD groups HCP knows about. Groups for which system-level HCP group accounts already exist are marked with a checkmark ( ).

2. Optionally, filter the list of AD groups:
   a. In the Find and Select Groups field, type a text string to use as a filter for the list of AD groups. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case-sensitive.

b. If Trusted Forests is enabled, in the From drop down menu, select the forest in which the group exists. This filters the groups down to only the groups that exist in the selected forest.

c. Click the find control ( ).

To redisplay the entire list of AD groups after filtering it, click the clear filter control ( ).

3. For each AD group from which you want to create an HCP group account, click the add control ( ) to select the group. The group row turns green.

   Also, for each AD group with an existing HCP group account for which you want to change the associated roles, click the add control ( ) to select the group. The group row turns green.

   To select all the groups in the list, click Select All.

   To deselect a selected group, click the remove control ( ) for the group.

   To deselect all the selected groups, click Clear.

4. In the Assign Roles to Selected Groups section, select the roles you want to associate with all the new group accounts you're creating and all the existing group accounts for which you're changing the associated roles. You can select any number of roles, including none.
5. Click Add Groups.

Modifying a group account

You can change the roles associated with HCP group accounts at any time. You can do this for an individual group account, as described below, or for multiple group accounts in a single operation.

To view group accounts, you need the monitor, administrator, or security role. To create and manage group accounts, you need the security role.

1. In the list of HCP group accounts on the Groups page in the System Management Console, click the name of the group account you want to modify.
2. In the Roles section, select or deselect roles as applicable.
3. Click Update Group.

Deleting a group account

You can delete a group account at any time. Deleting a group account has no effect on the corresponding group in AD.

When you delete a group account, AD users in the corresponding AD group immediately lose the roles granted by that group account.

When a group is deleted in AD, the corresponding HCP group account is not automatically deleted. However, the name of the group account changes to the SID of the deleted AD group. HCP group accounts that correspond to deleted AD groups serve no purpose and should be deleted.

Note:

The System Management Console may not immediately reflect the change to the HCP group account name. To force the displayed name to change, you can clear the AD cache. However, this also affects any AD users currently using HCP interfaces.

To view group accounts, you need the monitor, administrator, or security role. To create and manage group accounts, you need the security role.

1. In the list of group accounts on the Groups page in the System Management Console, click the delete control ( ) for the group account you want to delete.
2. In response to the confirming message, click Delete.

Changing user account and login settings

Several system settings affect user accounts and logins to the HCP System Management Console and Search Console (for the default namespace only). To view and change these settings, you use the Console Security page in the System Management Console.

To display the Console Security page, in the top-level menu of the System Management Console, select Security > Console Security.

Note: To view and change user account and login settings, you need the security role.

User account and login settings control:

- The minimum password length for locally authenticated HCP user accounts is six. The password should not contain commonly used phrases (for example, letmegetin). As a best practice, we recommend that you use a mix of uppercase and lowercase letters, numbers, and special characters. The password must contain at least one character from the following four requirements:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (~!@#$%^&*()-_+={}[]|\:;"'<>,.?/)
- The password should not contain usernames or a part of a username.
- If an HCP user account is locked out due to failed login attempts, it is unlocked automatically after five minutes.
- The HCP keeps a history of your passwords and does not allow you to reuse last five passwords.
- The number of days after which locally authenticated users are automatically forced to change their passwords. Valid values are integers in the range one through 999,999. The default is 180 days. Password expiration affects the use of only the System Management Console, Tenant Management Console, Search Console, and HCP management API. Users with expired passwords can continue to use those passwords with the HCP metadata query API. Password changes affect all HCP interfaces.
- For security, the HCP automatically disables user accounts that have been inactive for 180 days and that users are logged out after 10 minutes of inactivity.
- The consecutive number of times a locally authenticated or RADIUS-authenticated user can enter an incorrect password before the user account is automatically disabled. Valid values are integers in the range zero through 999. The default is five. A value of zero means accounts are never disabled due to failed login attempts.

  After a user account is automatically disabled, you need to reenable it manually to allow the user to log in again.

  If the last locally authenticated user account with the security role is disabled due to failed login attempts, it is reenabled automatically after one hour.

- The number of days an HCP user account can remain inactive before it's automatically disabled. Valid values are integers in the range zero through 999. The default is 180 days. A value of zero means accounts are never automatically disabled due to inactivity.

The last locally authenticated user account with the security role is never automatically disabled due to inactivity.

- The number of minutes a System Management Console or Search Console session can be inactive before it times out. Valid values are integers in the range zero through 999. The default is ten minutes. A value of zero means Console sessions never time out due to inactivity.

  If HCP is configured to use Active Directory, domain user sessions always time out after fifteen minutes while using the System Management Console or Search Console. The Active Directory inactivity timer does not reset when you use HCP.

  When a session times out, the Console displays the Idle Timeout page. If you then select a page to display:

  - If the user explicitly logged in, the Console login page appears.
  - In the case of single sign-on, the Console displays the selected page in the System Management Console or the Simple Search page in the Search Console, as applicable. If the HCP system supports AD and has no HCP user accounts, the recommended session timeout interval is eight hours. In this case, AD users should ensure that their screens are set to lock automatically after a short amount of idle time.
- Message text to appear on the login pages of the System Management Console and the Search Console for the default tenant. This text is optional. If specified, it can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

  The text you specify appears at the bottom of the login pages. You can use this text, for example, for messages such as "Authorized Users Only" or “Welcome to the Example Corporation HCP System".

Login settings

You can change one or more login settings on the Console Security page.

To view and change user account and login settings, you need the security role.

1. In the Login Settings section, make the changes you want.
2. Click Update Settings.

Login message

You can change one or more login settings on the Console Security page.

To view and change user account and login settings, you need the security role.

1. In the Login Message section, type the message you want.
2. Click Update Login Message.

System-level administration

To monitor the HCP system as a whole, you use the Overview page in the System Management Console. You use this page to view system activity, including service runs, repository usage, and search facility indexing progress. Additionally, this page notifies you of conditions that may require intervention, such as physical drive failures and low storage capacity.

About the Overview page

When you log into the System Management Console, the first page you see is the Overview page. This page lets you monitor the health of the HCP system as a whole.

The System Management Console Overview page performs these functions:

- Provides notification of problems with hardware, capacity, object integrity, and various aspects of the system configuration
- Displays current service status
- Displays a capsule view of the system log
- Contains graphs that show:
  - The ingested object count, the indexed object count, and the ingested volume.
  - The total storage capacity of all primary storage volumes and the used storage capacity.
  - The total storage capacity of all HCP S Series storage volumes and the used storage capacity. If your system does not have an HCP S Series storage component, this graph does not appear.
  - External SAN, internal storage, or a VM system (displayed as an internal storage). This is an indication where the storage volumes are located.

The Overview page also shows the HCP system time (see Configuring the system time).

To return to the Overview page from other Console pages, click Overview in the top-level menu.

To view the Overview page, you need the monitor, administrator, security, service, or compliance role.

Alerts

To ensure the continuous availability of the HCP repository, a strict majority of the HCP storage nodes must be running and healthy. For example, a six-node system requires at least four running nodes. If this condition is not true, namespaces cannot accept write requests, including requests to store new data or change object metadata.

At any given time, the unused HCP storage space must be sufficient to allow the creation of new objects and to ensure proper behavior in the event that a node fails.

The top section of the Overview page serves as an early warning system for violations of these requirements. It also reports system configuration issues and provides other system status information, such as notification that the system is rebalancing metadata. When the system is functioning normally, this section indicates that no problems exist.

The information in this section is represented by three categories of alert icons:

Hardware Status
: Alerts in this category identify nodes that are reporting problems relating to drives, network interface cards (NICs), HCP S Series Node tiering, and other internal components.

System Status
: Alerts in this category report on storage usage and indicate systemwide conditions such as a high rate of page swapping.

Object Integrity
: Alerts in this category report on the state of object data and metadata. They also identify situations in which the protection or Content Verification service is fixing errors or has found errors it cannot fix.

The background color in an alert icon indicates the status of the relevant component:

- A green background indicates that the component is within normal operating parameters.

- An orange background indicates that the component is disabled or needs attention in some way. The text that accompanies icons with an orange background appears automatically below the icon area. This text may contain links to Console pages that you can use to view more information about the problem and, in some cases, change one or more specific configuration settings in order to resolve the problem. For example, the text may contain a network name that's a link to the page on which you can view and change the IP configuration settings for that network.
- A red background indicates that the component is malfunctioning. The text that accompanies icons with a red background appears automatically below the icon area. This text may contain links to more information about the problem and, in some cases, change one or more specific configuration settings in order to resolve the problem. For example, the text may contain a node number that's a link to more detailed information about a problem with the hardware on that node.

Note:

If the entire HCP system is read-only because of metadata unavailability, a message about the situation appears at the top of every System Management Console page. While the system is read-only, configuration changes and changes to namespace content are not allowed. Additionally, statistics that describe repository content might be inaccurate.

If the message says that the system has limited functionality and the situation persists, contact your HCP support center for help.

Current service status

The Services section on the Overview page displays the status of each HCP service except Fast Object Recovery, Migration, Replication, Replication Verification, and Shredding. The information in this section is rolled up from all the HCP storage nodes. For example, if the Content Verification service is running on at least one storage node, the status of the service is running, regardless of whether it is running on any other nodes.

For each service, the Services section shows:

Service
: The name of the service.

Status
: The current status of the service. Possible values are:

  Running
  : The service is currently running.

  Completed
  : The service stopped running because it completed all of its work before the end of its scheduled run time period.

  Stopped
  : The service stopped running at the end of its scheduled run time period.

  Stopping
  : The service is in the process of transitioning from Running to Completed or Stopped.

  Waiting
  : The service has never run.

  Fixing
  : The service is fixing violations that it has detected.

  Irreparable
  : The service failed to fix violations. This is a severe condition and should be evaluated immediately.

  Disabled
  : The service cannot run because it has been manually disabled (for example, during problem resolution) or because another service that has precedence is currently running.

  If unforeseen or user-initiated events violate a service setting at the object, node, or system level, the status of the service changes as HCP detects the violation and attempts to correct it.

Time
: The time of the most recent change to the service status, shown for the time zone that's used for the HCP system time. The service was enforced until the specified time. For example, if the Protection service finishes at 10:00 PM on March 9, 2011 and the status of the service is Completed, the Time column displays:

  10:00 PM 03/09/2011

  The only exception to this is while a service is waiting for its first run. During this time, the Time column shows the current time.

Major events

The Major Events section on the Overview page lists log messages, reasons for the message, and suggested actions about major events that have occurred since the HCP system was installed (for example, the addition or failure of a node). The list of messages in this section is a subset of the messages in the HCP system log. You can view all the messages in the system log in the All Events panel on the System Events page.

By default, the messages in the Major Events section are listed ten at a time in reverse chronological order.

System graphs

The System section on the Overview page contains two graphs: *Objects* and *Ingested Volume*. It also indicates the system type and the location of the storage volumes.

In an External SAN HCP system, the data volumes reside on the SAN storage attached to the HCP system. The system metadata in this type of system is located on internal drives. However, the storage information in the graph includes only the storage on the external SAN. If there are any HCP S Series Nodes attached to this system, storage graphs display them as HCP S Series Nodes.

In an Internal HCP system, the data and metadata reside on internal drives, without an external SAN storage. It can also be an HCP S Series Node attached to this system indicated by HCP S Series Node storage graphs in the display.

A VM appear as an Internal HCP system on this page. The storage is virtualized through ESXi or KVM. To identify where each logical volume of the HCP system resides and for more information, see the documentation of the respective virtualization solution provider.

Objects graph

The Objects graph shows the total number of objects that were stored in the repository during the past 30 days (or since HCP was installed if that was less than 30 days ago). The number shown reflects the number of objects stored in all namespaces.

Each version of an object counts as a separate object. However, the object count does not include object versions that are *delete markers* or *delete records*. When you delete an object from a versioning-enabled namespace, a delete marker is created to indicate that the object has been deleted. A delete marker has a version ID but does not have any data or metadata. For more information on delete markers and delete records please see the *Enabling delete markers* section in Versioning.

Each multipart object counts as a single object. Objects that are in the process of being created by multipart uploads are not included in the object count.

While either of the two search facilities is selected for use with the Search Console, the Objects graph also shows the total number of indexed objects in the repository during the past 30 days. For any point in time for which the indexed object count is shown, the count reflects the index maintained by the search facility that was selected for the Search Console at that time.

The x-axis in the Objects graph marks the passage of time. The y-axis measures the number of objects. As the number of objects increases, the intervals on the y-axis get larger. The graph heading indicates the current measurement unit (for example, thousands or millions).

To see the number of objects in the repository at a given point in time, hover over the top edge of the colored portion of the graph at the time you want.

Ingested Volume graph

The Ingested Volume graph shows the total size of the ingested data and custom metadata during the past 30 days (or since HCP was installed if that was less than 30 days ago). This value is the total size of the data and custom metadata before they were added to the repository. The value tells you how much data and custom metadata has been stored, not the amount of storage used.

Ingested volume includes the parts of in-progress multipart uploads that have already been written to the repository. Ingested volume does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

The x-axis in the Ingested Volume graph marks the passage of time. The y-axis measures the ingested volume in gigabytes, terabytes, or petabytes, depending on the system capacity. As the ingested volume increases, the intervals on the y-axis get larger. The graph heading indicates the current measurement unit (gigabytes (GB), terabytes (TB), or petabytes (PB)).

To see the ingested volume in the repository at a given point in time, hover over the top edge of the colored portion of the graph at the time you want.

Because of compression and duplicate elimination, the ingested volume can be greater than the used storage capacity.

Updating the information

Below the System section option, the Overview page shows the most recent values for the number of objects stored (*Ingested objects*), the number of indexed objects, if applicable (*Indexed objects*), and the ingested volume (*Ingested volume*). The bottom left corner of the Overview page shows the date and time these values and the Objects and Ingested Volume graphs were last updated. To update these values and the graphs to show the most current information, click Refresh Now in the bottom right corner of the Overview page.

Storage graphs

The Primary Storage section on the Overview page contains a graph showing the amount of used primary storage (both running and spindown) during the past 30 days (or since HCP was installed if that was less than 30 days ago). The used storage value is the total amount of storage occupied by object data, system and custom metadata, the metadata query engine index, and any redundant data required to satisfy data protection level and metadata protection level settings in service plans.

If the HCP system has HCP S Series storage available to it, the Overview page also has an S Series Storage section that contains a graph showing the amount of used HCP S Series storage during the past 30 days (or since HCP was installed if that was less than 30 days ago). The used storage value is the total amount of storage occupied by object data, system metadata, and any redundant data required to satisfy data protection level settings in service plans.

Used storage includes storage occupied by the parts of in-progress multipart uploads that have already been written to the repository. Used storage does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

The x-axes in the Primary Storage and S Series Storage graphs mark the passage of time. The y-axes measure the used storage in megabytes, gigabytes, terabytes, or petabytes, depending on the amount of used storage. As the amount of used storage increases, the intervals on the y-axis get larger. The graph heading indicates the current measurement unit (megabytes (MB), gigabytes (GB), terabytes (TB), or petabytes (PB)).

To see the amount of used storage at a given point in time, hover over the top edge of the colored portion of the graph at the time you want.

Above the Primary Storage graph heading, the Overview page shows the total amount of primary storage in the HCP system, excluding the space required for system overhead and the operating system. Above the S Series Storage graph heading, the Overview page shows the total amount of HCP S Series storage available to the HCP system.

Below the Primary Storage section option, the Overview page shows the most recent value for the amount of used primary storage. Below the S Series Storage section option, the Overview page shows the most recent value for the amount of used HCP S Series storage. The bottom left corner of the Overview page shows the date and time these values and the Primary Storage and S Series Storage graphs were last updated. To update these values and the graphs to show the most current information, click Refresh Now in the bottom right corner of the Overview page.

Note:

When merging data from identical objects, the Duplicate Elimination service flags the redundant data for deletion. Similarly, when compressing an object, the Compression/Encryption service flags the uncompressed version for deletion. The Primary Storage and S Series Storage graphs do not reflect space reclaimed by either service until the flagged data is actually deleted.

Considerations for monitoring your HCP system

You need to keep these considerations in mind when monitoring your HCP system Overview page:

- When an HCP system begins to approach its total storage capacity, you need to add nodes, hard drives, or arrays depending on the type of system you have. For more information about the different types of available storage upgrades, contact your HCP sales representative. There are two ways to determine when it is time to add storage:
  - A `Storage usage` *`percent-used`* warning appears on the Overview page when the system has used 75 to 90 percent of its primary storage capacity. The warning becomes an alert when the system is over 90 percent of its total storage capacity.
  - You can also monitor your HCP system by checking the object count on the Overview page. The page contains a graph that shows the total number of objects that were stored in the repository during the past 30 days out of a maximum storage capacity.

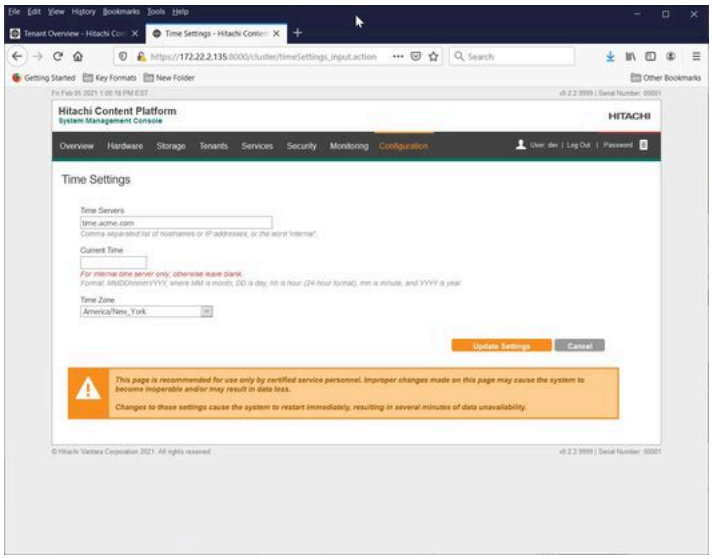
Configuring the system time

HCP can be configured to maintain the system time internally or to synchronize the system time to one or more external time servers. In the latter case, if either of the following events occurs, the HCP system restarts automatically:

- The time on the time server is changed by more than 1,000 seconds.
- The HCP system starts using a new time server whose time differs from the original time server by more than 1,000 seconds.

Note: Changing the system time restarts the HCP system automatically, which makes system data unavailable for several minutes.

1. On the Configuration menu, click Time.
   The Time Settings dialog box appears.



2. Perform one of the following steps:
   - To configure the HCP system to use an external time server, enter the server's hostname or IP address in the Time Servers field. If specifying more than one time server, separate each one with a comma.
   - To configure the HCP system to use an internal time server, enter the current time in the Current Time field, and then use the Time Zone drop-down list to select the time zone with which the current time will be associated.
3. Click Update Settings.

Shutting down or restarting HCP

Shutting down HCP means shutting down the system and powering off the nodes. After shutting down HCP, you need to manually power the nodes back on to start it again.

Restarting HCP means shutting down and restarting the system without powering off the nodes.

While HCP is shut down or in the process of restarting, clients have no access to the data in it, and the System Management Console is unavailable.

Under normal operating conditions, you don't need to shut down or restart HCP. However, situations where shutting down the system may be appropriate include:

- You are physically moving the HCP system to another location and need to shut it down first.
- You need to perform maintenance on the HCP power sources.

When you shut down or restart the HCP system, you are required to specify a reason for the action.

Important: Restarting HCP without shutting it down is very rarely necessary. If you believe you need to take this action, contact your authorized HCP service provider before you do so.

To shut down or restart the HCP system, you need the administrator or service role.

Shutting down HCP

When you shut down HCP, the hardware configuration determines whether the nodes power off automatically. To complete the action, you may need to power off each node manually after shutting down the system.

To ensure that HCP has enough time to shut down cleanly, wait a few minutes before powering nodes off manually. If a node is connected to a console, the console displays `System halted` when you can safely power off the node.

Important:

If you shut down HCP while objects are being stored, the repository may then contain incomplete objects. Therefore, if possible, before shutting down HCP, you should notify all tenant administrators about the upcoming shutdown. The tenant administrators can then notify namespace users to suspend all client activity before the shutdown occurs.

If you take an entire HCP with SAN-attached storage system offline, including the storage system, you need to power the storage system and, if applicable, the Fibre Channel switches back on before powering on the nodes.

To shut down or restart the HCP system, you need the administrator or service role.

1. In the top-level menu of the System Management Console, click Hardware.
2. At the top of the Hardware page, click Shut Down.

   The Shut Down System window appears.

3. In the Reason field, type the reason why you're shutting down the system. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
4. Click Shut Down System.

   The nodes shut down HCP and, if possible, power off.

   If HCP doesn't shut down, contact your authorized HCP service provider.

Restarting HCP

Restarting an HCP system causes all the nodes in it to reboot.

To shut down or restart the HCP system, you need the administrator or service role.

1. In the top-level menu of the System Management Console, click Hardware.
2. At the top of the Hardware page, click Restart.

   The Restart System window appears.

3. In the Reason field, type the reason why you're restarting the system. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
4. Click Restart System.

Hardware administration

The System Management Console offers both a summary view of all the nodes in the HCP system and a detailed view of each node on the Hardware and Storage Node pages, respectively. The Hardware page also provides a view of other hardware components used in the system. Using these pages, you can monitor both system hardware and system storage.

This section of the help:

- Describes the information available on the Hardware and Storage Node pages
- Explains how to interpret this information to make informed decisions about hardware management
- Contains instructions for shutting down and restarting individual nodes

About the Hardware page

The Hardware page of the HCP System Management Console lists all the nodes in the HCP system, including HCP S Series Nodes, and provides general information about each one.

The Hardware page also shows the status of all other hardware components of the HCP system that can be monitored in the System Management Console.

To display the Hardware page, click Hardware in the top-level menu.

Note:

To view the Hardware page, you need the monitor, administrator, security, service, or compliance role.

About the Nodes page

The Hardware > Nodes page lists all the HCP General Nodes and HCP S Series Nodes in the HCP system. General Nodes remain listed on this page regardless of whether they are running, starting up, stopping, or not running. Nodes that have been permanently removed from the system are not displayed in the list.

For each node in the HCP system, the General Node list on the Hardware > Nodes page shows:

Node ID
: The unique number assigned to the node.

Model
: The type of node. Possible models are:

  G11
  : A Hitachi Advanced Server DS220 that can exist in a HCP with internal storage or HCP with SAN-attached storage system

  G10
  : A Hitachi Advanced Server that is the predecessor to the HCP G11. A HCP G10 can exist in a HCP with internal storage or HCP with SAN-attached storage system.

  VM
  : A server running a HCP VM system

Status
: The node status. Possible values are:

  Available
  : The node is running.

  Unavailable
  : The node is either not running, starting up but not yet able to perform HCP functions, or shutting down and no longer able to perform HCP functions. If a node is unavailable because of a hardware problem, you might be able to determine the cause by reviewing the Hardware Status section on the individual Storage Node page.

  Migrating
  : The node is available, and the Migration service is currently migrating data off the storage managed by the node.

  Alert
  : The node is unavailable, and HCP can detect which components are experiencing problems. One or more alerts identifying the problems are displayed in the Alerts column.

  Note: If the status of a node changes from available to unavailable and the node does not restart automatically, contact your authorized HCP service provider. Do not try to restart the node manually; this action might cause the loss of information that is required to diagnose the problem.

Alerts
: None, one, or more icons representing components are experiencing problems.

  For more information about any problem, click the node number.

Logical Volumes
: The status of the logical volumes managed by the node. Each logical volume can be one of these types:

  Data volume
  : Primary running storage that stores object data, but does not store the metadata query engine index. *Primary running storage* is storage that is managed by the nodes in the HCP system and consists of continuously spinning disks.

    Data volumes have numeric IDs in the range 1 (one) through 63 and 92 through 95.

  Index volume

(HCP with SAN-attached storage systems only) Primary running storage that stores only the metadata query engine index. All storage nodes should have the same number of index volumes.

Index volumes have numeric IDs in the range 64 through 91.

Shared volume

Primary running storage that stores both object data and the metadata query engine index. All storage nodes have one shared volume.

The shared volume for each node has a numeric ID in the same range as data volumes.

Spindown volume

(HCP with SAN-attached storage systems only) Primary spindown storage that is used for tiering purposes. *Primary spindown storage* is storage that is managed by the nodes in the HCP system and consists of disks that can be spun down and spun up as needed. Primary spindown storage stores object data, but it does not store the metadata query engine index. All storage nodes should have the same number of spindown volumes.

Spindown volumes have numeric IDs in the range 96 through 127. The volume numbering starts at 96.

A HCP with SAN-attached storage system can have spindown volumes only if both of these conditions are true:

- One or more logical volumes used by the system are capable of being spun down. This means that they are on storage systems that support spindown.
- The system is configured to use one or more spindown-capable logical volumes as primary spindown storage.

NFS volume

(also called an *external volume*) Extended storage that is accessed using an NFS mount point. *Extended storage* is storage that is managed by devices outside of the HCP system and is used for storage tiering. NFS storage is one of six types of extended storage that you can configure HCP to use. NFS storage can be used to store object data only.

NFS volumes have numeric IDs in the range 96 through 127. The volume numbering starts from 127 and goes down.

Database volume

A volume that holds database transaction logs and indexes. Optional rear mounted SSD volumes are also available for G10 and G11 nodes. SSD volumes store only indexes.

The Logical Volumes column displays a status icon for each logical volume managed by the node. The hover text for each icon shows the volume type, volume ID, and, for NFS volumes, the share path and the name of the extended storage pool that contains the NFS volume.

The next table describes the logical volume status icons.

Icon	Volume type	Volume status
	Data	Available — The volume is available and functioning properly.
	Data	Unavailable — The volume is unavailable, likely because the node is not running. If the volume does not become available soon, contact your authorized HCP service provider.
	Data	Shutting down — The volume is shutting down and is no longer accessible.
	Data	Broken — The volume is experiencing errors or has failed and requires replacement. Contact your authorized HCP service provider.
	Data	Migrating — The Migration service is migrating data off the volume.
	Database	Available — The volume is available and functioning properly.
	Database	Degraded — The volume is experiencing errors or has failed. Contact your authorized HCP service provider.
	Database	Initialized — The volume is started up and accessible.
	Database	Initializing — The volume is starting up but is not yet accessible.
	Database	Migrating — The Migration service is migrating data off the volume.
	Database	Rebuilding — The volume is rebuilding and is therefore inaccessible.
	Database	Unavailable — The volume is unavailable, likely because the node is not running. If the volume does not become available soon, contact your authorized HCP service provider.
	Index	Available — The volume is available and functioning properly.
	Index	Unavailable — The volume is unavailable, likely because the node is not running. If the volume does not become available soon, contact your authorized HCP service provider.
	Index	Initializing — The volume is starting up but is not yet accessible.
	Index	Shutting down — The volume is shutting down and is no longer accessible.
	Index	Broken — The volume is experiencing errors or has failed and requires replacement. Contact your authorized HCP service provider.
	Index	Migrating — The Migration service is migrating data off the volume.
	Shared	Available — The volume is available and functioning properly.
	Shared	Unavailable — The volume is unavailable, likely because the node is not running. If the volume does not become available soon, contact your authorized HCP service provider.
	Shared	Initializing — The volume is starting up but is not yet accessible.

Icon	Volume type	Volume status
	Shared	Shutting down — The volume is shutting down and is no longer accessible.
	Shared	Broken — The volume is experiencing errors or has failed and requires replacement. Contact your authorized HCP service provider.
	Shared	Migrating — The Migration service is migrating data off the volume.
	Spindown	Available — The volume is spun up, available, and functioning properly.
	Spindown	Spun down — The volume is spun down.
	Spindown	Unavailable — The volume is unavailable, likely because the node is not running. If the volume does not become available soon, contact your authorized HCP service provider.
	Spindown	Initializing — The volume is starting up but is not yet accessible.
	Spindown	Shutting down — The volume is shutting down and is no longer accessible.
	Spindown	Spinning up — The volume is spinning up but is not yet accessible.
	Spindown	Spinning down — The volume is spinning down and is no longer accessible.
	Spindown	Error spinning up — The volume is experiencing errors while in the process of spinning up. Contact your authorized HCP service provider.
	Spindown	Error spinning down — The volume is experiencing errors while in the process of spinning down. Contact your authorized HCP service provider.
	Spindown	Broken — The volume is experiencing errors or has failed and requires replacement. Contact your authorized HCP service provider.
	Spindown	Migrating — The Migration service is migrating data off the volume.
	NFS (External)	Available — The volume is mounted, available, and functioning properly.
	NFS (External)	Initializing — The volume is starting up but is not yet accessible.
	NFS (External)	Broken — HCP cannot mount the volume. Possible reasons include the exported share is not configured correctly, or the NFS server is not running on the device. Check the export configuration and verify that the NFS server is running. If the configuration is correct and the NFS server is running, ensure that the device is functioning properly and that the network connecting HCP to the device is healthy. If this status persists, contact your authorized HCP service provider.
	NFS (External)	Unavailable — HCP is in the process of mounting, updating, or deleting the volume. If you just created or updated the volume and the volume status does not quickly change to available or broken, try remounting the volume. If this status persists, contact your authorized HCP service provider for help.

The following information applies to the logical volume display:

- Each node also has a logical volume for the operating system; however, that logical volume is not included in this display.
- For HCP with SAN-attached storage systems that also have internal storage, this display does not include the logical volumes on the internal drives.
- When a logical volume is removed from a node, the System Management Console might not show the change immediately. Heavy read or write activity causes more access to HCP storage and results in faster detection of the volume removal.

Volume Usage
: A graphical representation of the amount of primary storage currently in use compared to the total amount of primary storage that is managed by the node. The Volume Usage column also displays text indicating the total number of bytes of primary storage and the percent of primary storage space that is currently in use.

For each node that was permanently removed from the system, the first column in the display shows Removed.

For each HCP S Series Node associated with the HCP system, the S Series Nodes list on the Hardware > Nodes page shows:

Name
: The name of the S Series Node.

Serial Number
: The serial number of the HCP S Series Node.

Model
: The type of S Series Node. Possible models are:

- S11
- S10
- S30
- S31

Status
: The node status. Possible values are:

Normal
: The S Series Node is running and has no problems that require attention.

Degraded
: The S Series Node has one or more noncritical problems that may require attention.

Critical

The S Series Node has one or more critical problems that require attention.

Unavailable

The S Series Node is either not running, starting up but not yet able to perform functions, or shutting down and no longer able to perform functions. If an S Series Node is unavailable because of a hardware problem, you might be able to determine the cause by reviewing the Hardware Status section on the individual Overview page.

Alerts

None, one, or more icons representing components that are experiencing problems.

Capacity

A graphical representation of the amount of storage that is currently in use compared to the total amount of storage that is on the node. The Capacity column also displays text indicating the total number of bytes of storage and the percent of storage space that is currently in use.

Monitoring individual HCP general nodes

Each HCP general node has its own page on the HCP System Management Console that shows detailed information about the node. The page title indicates the node number and the node status.

To view an individual HCP general node page, you need the monitor, administrator, security, service, or compliance role.

1. Go to the Hardware > Nodes page.
2. Click the node that you want to examine.

Monitoring individual HCP S Series Nodes

The Overview panel on the page for an individual HCP S Series Node provides information about various components of the node. The pie chart at the top right of the page shows the total storage capacity of the S Series Node (dark blue) and the total storage capacity used (light blue).

The Server Modules section lists the names and statuses of HCP S Series Node server modules. Server modules run the software that manages the HCP S Series Node, provide data access, and ensure data protection.

The Enclosure section lists names and statuses of S Series Node enclosures. The enclosure is a container for the power, cooling, and server modules, along with the hard disk drives inside the node. S11 nodes have only one enclosure. S30 nodes support up to 16 enclosures.

The Events section shows the messages about warning-level and error-level alerts that occur on the HCP S Series Nodes. The messages in this panel are a subset of all the messages on the HCP system log.

To see more detailed information about the HCP S Series Node, click the HCP S Series Node URL located above the pie chart. This opens the HCP S Series Management Console.

Modifying HCP S Series Nodes

To view an individual HCP general node page, you need the monitor, administrator, security, service, or compliance role.

1. On the Hardware > Nodes page, click the Settings tab.
2. In the Name field, type the new name you want to give the S Series Node.
3. In the Description field, type the new description you want to give the S Series Node.
4. Optionally, if the Storage Network field is visible, select a network for tiering.
5. In the Domain Name or Virtual IP field, type the new domain or virtual IP address of the S Series Node.
6. Select Compliant if the S Series Node meets the compliancy expectations of your service plan.
7. Select Use HTTPS for management to use HTTP with SSL security for S Series Node management requests.
8. Click Update Settings.

Clicking Advanced Settings redirects you to the Advanced tab on the S Series Node Storage > Components page.

About the Switches page

On the Hardware > Switches page you can add, delete, and monitor your HCP system switches. With the Service role enabled you can add and delete switches. With the Administrator role you can monitor the status of existing switches, but you cannot add or delete them.

For each switch, the page displays the following information:

Type

The type of component.

Model

The make and model of the component (for example, Dell® PowerConnect™ 2824).

IP address

The IP address of the switch.

Status

The status of the component. Possible values are:

Normal

The component is available and functioning properly.

Warning

The component has detected an error. For switches, possible causes include:

- A fan in the switch is not operating normally.
- A sensor in the switch is detecting an abnormal temperature.
- One of two power supplies in the switch is not connected.
- One or more ports in the switch are malfunctioning.

Unavailable

HCP does not have connectivity to the component.

HCP also reports a component as unavailable if it has not yet contacted the component for status information. To determine whether this is the reason for the unavailable status, refresh the Hardware > Switches page in five minutes.

If the status of a component is unhealthy or if a component remains unavailable for more than five minutes, contact your authorized HCP service provider for help.

Adding a switch

1. Click the drop down menu located in the top right of the Switches tab and select the switch type you want to add.
2. Click Add.

   A new switch, highlighted in green, appears in the window.

3. Click the Model drop down menu in the new switch, and select the applicable model.
4. Type the IP address.
5. Click Update Settings.

Switches can be deleted by clicking the garbage can icon on the left side of the switch and confirming that you want the switch removed.

About the Chassis tab

For HCP with SAN-attached storage systems that use CB 320 servers, the Hardware > Chassis page shows the IPMI sensor information for the fans and power supplies on the server chassis.

Note:

HCP uses SNMP to retrieve the IPMI sensor information from the CB 320 servers. To enable this, for each server, you need to add the lowest-numbered storage node in the HCP system to the list of SNMP managers in the server configuration. To identify the node, use a valid [[hcp_system]] network IP address for the node. For the community name, use *public*.

If the lowest-numbered node changes at any time (for example, because of prolonged node unavailability or the addition of a node with a lower number), you need to update the each CB 320 server configuration accordingly.

For information about configuring CB 320 servers, see the applicable Hitachi documentation.

About the individual HCP G Series Node pages

On the Hardware > Nodes page you can click any of the general nodes to go to their individual page. The General Node page contains information about the node's hardware status and events.

Hardware status

The Hardware Status section of an individual General Node page summarizes the current operating conditions of various components of the node you're examining, and provides links to more detailed information about each component.

To display more detailed information about a given component, click the table row containing the component summary. To hide the details, click on the row again.

If any component is malfunctioning, the Hardware Status section automatically displays detailed information about that component.

Logical volume usage details

When you click Logical volume usage, the Console displays the following information for each logical volume that's managed by the node you're currently viewing:

Volume ID
: The logical volume type and ID and, for NFS volumes, the share path and the name of the extended storage pool that contains the NFS volume. The volumes are not necessarily listed in numeric order.

Status
: The logical volume status.

Capacity
: The total number of bytes of storage on the logical volume.

Used
: The number of bytes of storage that are currently in use on the volume. This number includes bytes occupied by parts of in-progress multipart uploads, including replaced parts, parts uploaded for aborted multipart uploads, and unused parts of completed multipart uploads until these parts are automatically deleted by the Garbage Collection service.

Percent Used
: The percentage of storage space that's currently in use on the volume.

Note: Each node also has a logical volume for the operating system, but that logical volume is not included in this display.

For HCP with SAN-attached storage systems that also have internal storage, this display does not include the logical volumes on the internal drives.

Core hardware details

When you click Core hardware, the Console displays the following information about the core hardware for the node you're currently examining:

Platform Hardware
: The type of hardware used for the node:

  - For a standalone server, this is the type of server, as reported by the server.
  - For a blade in a CB 320 server, this is Hitachi Compute Blade 320.
  - For a node in an HCP VM system, this is VMware Virtual Platform.

  When connecting the switch to the HCP system, use the following figures to identify the ports in these figures:

  - Blue denotes the back-end network.
  - Red denotes the front-end network.
  - Orange denotes the Fiber HBA and is present in SAN configurations only.

  Note: The BMC connector on the server is designated by a wrench icon.

Figure. G11-BaseT FE and BE Interfaces

Figure. G11-BaseT-FE SFP+BE Interfaces

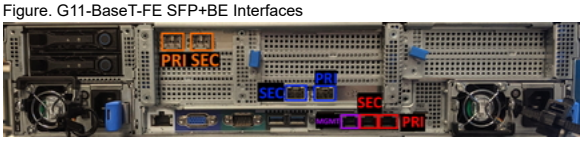


Figure. G11-SFP+ FE and SFP+ BE Interfaces

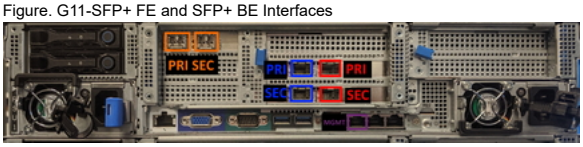
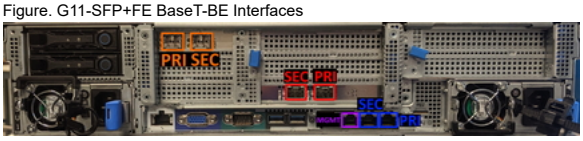


Figure. G11-SFP+FE BaseT-BE Interfaces



Status
: The status of the node. Possible values are:

  Available
  : The node is running.

  Unavailable
  : The node is either not running, starting up but not yet able to perform HCP functions, or shutting down and no longer able to perform HCP functions.

  Migrating
  : The Migration service is currently migrating data out of the storage managed by the node.

  If the status of a node changes spontaneously from available to unavailable and the node does not restart automatically, contact your authorized HCP service provider. Do not attempt to restart the node manually; doing so could cause the loss of information needed to diagnose the problem.

Last Status Update Time
: The time of the last update to the node status.

Node ID
: The number assigned to the node.

[hcp_system]
: All IPv4 and IPv6 addresses assigned to the node for the [hcp_system] network.

[hcp_management]
: All IPv4 and IPv6 addresses assigned to the node for the [hcp_management] network.

[hcp_backend]
: The IP address assigned to the node for the [hcp_backend] network.

Boot Time
: The date and time the node last started.

Usage/Capacity
: The total amount of storage space on all of the primary storage volumes managed by the node and the amount of that primary storage space that's currently in use.

Memory
: The amount of RAM in the node.

Swap
: The status of the swappable memory in the node:

  Using
  : The amount of storage set aside for swappable memory, in GB, and the percentage of that amount that's currently in use

  Pages In
  : The number of pages currently swapped in

  Pages Out
  : The number of pages currently swapped out

Load Average
: The average process workload on the node over the past minute, five minutes, and 15 minutes. The load average is based on all processes, regardless of their current state (for example, running, waiting for CPU time, or sleeping).

CPU
: Make and model of the CPUs in the node, listed one per line. The CPUs are numbered and are listed in numeric order starting with CPU 0.

File systems on storage devices managed by a node

The Hardware Status section on the Storage Node page for any given node shows the number of file systems the node supports on primary storage and the number of physical storage devices to which those file systems are mapped. When you click x file systems on y storage devices, the Console displays the following information for each file system on the physical storage that's managed by the node you're currently examining:

- The directory path that identifies the file system
- Whether or not the file system is currently mounted
- Each level of mapping that ultimately associates the file system with one or more low-level block devices
- Some device diagnostic information, if available. For example, for configurations that include SSDs, the SSD expected write life remaining.

- Additional RAID-specific information, if available

Additionally, for HCP with SAN-attached storage systems, the details include this information for each low-level block device: vendor, array type, serial number, device number, and worldwide port number.

Note: For HCP with SAN-attached storage systems that also have internal storage, the number of file systems includes those located on the internal drives.

For HCP with SAN-attached storage systems, if multipathing is degraded, one or more of the low-level block devices will be missing from the display details.

IPMI information

Intelligent Platform Management Interface (IPMI) is a specification that defines a method of monitoring the internal hardware components of a server. If IPMI is implemented on a node, sensors in that node can detect abnormal conditions such as a high fan speed or a failed power supply.

The IPMI data that's displayed on the Storage Node page for a given node is organized by sensor type. The list of sensors that you see for each sensor type depends on the specific IPMI implementation.

The details displayed, by sensor type, are:

Temperatures
: For each temperature sensor, the current temperature reading, and for some sensors, the normal range for the temperature.

Power Supplies
: For each power supply sensor, a text string read from the applicable power supply. If only one power supply is working, this section displays the message, `No redundancy`.

Fans
: For each fan sensor, the current fan speed.

Processors
: For each processor sensor, a text string giving the status of the applicable processor.

Voltages
: For each voltage sensor, the current voltage reading.

Note: For fans and power supplies in CB 320 server chassis, IPMI information appears on the Hardware page. Nodes that are individual blades do not have their own fans and power supplies.

HCP does not report IPMI information for nodes in HCP VM systems.

Network interface cards (NICs)

Each HCP node has two pairs of bonded ports:

- One pair of ports is used for connecting to the front-end networks, including the [hcp_system] network and all user-defined networks. These ports share all front-end network IPv4 and IPv6 addresses assigned to the node.
- One pair of ports is used for connecting to the back-end network. These ports share the back-end IP address assigned to the node.

The name assigned to each front-end and back-end port includes the NIC port number (for example, eth0 and eth1). By default, HCP uses the lower-numbered port in each bonded pair. If the lower-numbered port for a network fails, HCP automatically switches to the other port in the pair.

Optionally, depending on your HCP system hardware configuration, an HCP node may have an extra port connected to the management network. The name assigned to the management port is eth4.

On the Storage Node page for a given node, the Console displays information about each of the NICs in the node. The NIC information is organized by network. For each port assigned to a network, the Console displays these details:

Interface
: The name assigned to the port.

Active
: An indication of whether the port is available for use. Possible values are `true` and `false`.

Duplex
: An indication of whether the port is full-duplex (`full`) or half-duplex (`half`).

Active in Bond
: An indication of whether the port is currently the one being used. Possible values are `true`, `false`, and `N/A`.

Speed
: The current rate of data transmission through the port.

Maximum Supported Speed
: The maximum supported rate of data transmission for the port.

File system status

Each node in an HCP system has multiple file systems on its primary storage. At installation time, a fixed amount of space and a fixed number of inodes are allocated to each of those file systems. Each NFS volume associated with a node has a single file system with a fixed amount of space and a fixed number of inodes.

Inodes determine the total number of files and directories a file system can have. (These files and directories do not have a direct correspondence to the objects and directories that users create.)

On the Storage Node page for a given node, when you click the row that shows the file system status summary, the Console displays the following information about each file system on each primary storage volume and NFS volume that's managed by the node:

Path
: The directory path

Free 1K Blocks
: The amount of available storage associated with the file system, in one-KB blocks

Total 1K Blocks
: The total amount of storage associated with the file system, in one-KB blocks

Block Usage
: The percent of the storage blocks currently in use

Inode Usage
: The percent of the allocated inodes currently in use

Note: The file systems listed include those used for the operating system. Therefore, the total amount of storage associated with all the file systems for a node is greater than the total amount of storage associated with the logical volumes displayed for that node.

Node events

The Node Events section on the Storage Node page for a given General Node lists all event messages logged for that node since the HCP system was installed. The list of messages in this section is a subset of the messages in the HCP system log. You can view all the messages in the system log in the All Events panel on the System Events page.

By default, the messages are listed ten at a time in reverse chronological order.

Shutting down or restarting individual nodes

Under normal operating conditions, the HCP nodes manage themselves. However, because hardware failures are possible, the System Management Console provides controls for shutting down and restarting individual nodes.

- *Shutting down a node* means shutting down the HCP software on it and powering it off. After shutting down a node, you need to manually power it back on to start HCP on it again.
- *Restarting a node* means shutting down and restarting the HCP software on it without powering it off.

Shutting down or restarting a node has no effect on the data in the primary storage volumes and the NFS volumes that are associated with the node. However, while a node is shut down or in the process of restarting, clients have no access to that node.

Shutting down or restarting a node is rarely necessary and can cause extra service activity, which increases the load on the system. However, situations in which shutting down a node may be appropriate include:

- A hardware failure has occurred.
- The node requires maintenance.
- You plan to remove the node from the system.

The most frequent reason for restarting a node is that your authorized HCP service provider has requested it during the assessment or resolution of a problem.

When you shut down or restart a node, you are required to specify a reason for the action.

Note: After a node shuts down, HCP may perform a file-system check when the node reboots. This can take several hours to complete.

To shut down or restart a node, you need the administrator or service role.

Shutting down an individual node

When you shut down a node, the hardware configuration determines whether it powers off automatically. To complete the action, you may need to power off the node manually after stopping it.

To ensure that HCP has enough time to shut down cleanly, wait a few minutes before powering the nodes off manually. If the node is connected to a console, the console displays `System halted` when you can safely power off the node.

To shut down or restart a node, you need the administrator or service role.

1. Take one of these actions:
   - On the Hardware > Nodes page, click the shutdown icon for the node.
   - On the Storage Node page for the node, click Shut Down Node.

   The Shut Down Node window appears.

2. In the Reason field, type the reason why you're shutting down the node. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
3. Click Shut Down Node.

   The nodes shut down and, if possible, power off.

Restarting an individual node

Restarting an HCP node causes it to reboot. While the node is in the process of restarting, clients have no access to it.

Note:

When you restart a node in a system with zero-copy failover enabled, the storage managed by the node fails over to the paired node during the shutdown part of the restart. The failover process always finishes before the restarted node completes its shutdown process. Therefore, the data outage caused by the failover lasts less than three minutes.

When the node comes back up, the failback process extends the reboot by 15 to 30 seconds. The data outage caused by the failback lasts less than five minutes.

To shut down or restart a node, you need the administrator or service role.

1. Take one of these actions:
   - On the Hardware > Nodes page, click the restart icon for the node.
   - On the Storage Node page for the node, click Restart Node.

   The Restart Node window appears.

2. In the Reason field, type the reason why you're restarting the node. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
3. Click Restart Node.

   The node reboots. When the node has finished rebooting, it is again available for client access.

Storage administration

By default, HCP stores all objects in a repository on primary running storage. However, you can use HCP S Series Nodes as an alternative to primary running storage. HCP also supports the use of primary spindown storage (HCP with SAN-attached storage systems only), HCP S Series storage (storage provided by S Series Nodes), and extended storage for tiering purposes.

HCP is automatically configured to access and use primary running storage and primary spindown storage. HCP can also be configured to write directly to S Series Nodes. To configure HCP to store objects on S Series Nodes, you need to set up a service plan that targets S Series Node storage as the ingest tier.

HCP S Series storage and extended storage can be used for tiering object data. To enable tiering, you need to manually configure HCP to access each physical storage device and cloud storage service endpoint. Regardless of the tier on which the data is stored, a copy of the object metadata must always remain on primary running storage.

A service plan defines the ingest tier and one or more storage tiers that can be used to store objects in a namespace. For each object, at any point in the object lifecycle, the service plan specifies the criteria that determines where the objects are initially ingested, which storage tiers are used to store copies of that object, and the number of copies of that object that must be stored on each tier.

Storage for HCP systems

An HCP system includes multiple nodes that are networked together, where each node is either an individual server, a blade in a blade server, or a virtual machine. Each physical node can have multiple internal drives that can connect to SAN storage. Each virtual node emulates a server that has only internal drives.

The physical storage that is managed by the nodes in the HCP system is called *primary storage*. By default, primary storage consists entirely of running storage, which is storage on continuously spinning disks. However, an HCP with SAN-attached storage system can be configured to use SAN storage that includes both running storage and *spindown storage*, which is storage on disks that can be spun up or spun down, as needed. If primary spindown storage is enabled on an HCP with SAN-attached storage system, you can configure HCP to use that storage for tiering purposes.

You can also add S Series Nodes to your HCP system. These nodes can be used as an alternative to primary running storage or for tiering purposes. The number of objects you can write to an S Series Node is limited to the total storage capacity of the node. If you want more storage capacity, you need to purchase more S Series Nodes. The HCP system communicates with the S Series Nodes through the S3 compatible and management APIs.

You can also configure any HCP system to use *extended storage* for tiering purposes. Extended storage is additional storage that is managed by devices outside of the HCP system.

Unless you are writing directly to HCP S Series storage, HCP initially stores each object in a repository on primary running storage. By default, throughout the lifecycle of an object, HCP continues to store all copies of the data and metadata for that object only on primary running storage. However, you can configure HCP to offload object content from primary running storage and store that content on primary spindown storage, HCP S Series storage, or any of the supported types of extended storage that you have configured HCP to access and use.

Using primary spindown storage to store object content that is accessed infrequently saves energy, thereby reducing the cost of storage. While all copies of the data, custom metadata, ACL, and secondary metadata for an object can be moved onto primary spindown storage, all copies of the primary metadata for an object must always remain on primary running storage. Similarly, while all the data for an object can be written directly to S Series storage or later moved off primary running storage and stored on HCP S Series or extended storage, at least one copy of the system metadata, custom metadata, and ACL for that object must always remain on primary running storage.

HCP moves object content from primary running storage onto one or more other types of storage according to rules specified in service plans.

Each namespace has a service plan that defines one or more tiers of storage that can be used to store objects in that namespace. For each object in a namespace, at any point in the object lifecycle, the service plan specifies the criteria that determine which storage tiers must be used to store copies of that object and the number of copies of that object that must be stored on each tier.

You can set the HCP initial storage tier, called the *ingest tier*, to either primary running storage or to HCP S Series storage. When a service plan is first created, it defines only the ingest tier, so HCP stores all objects in a given namespace on the designated ingest tier throughout the entire object lifecycle.

Primary running storage is designed to provide both high data availability and high performance for object data storage and retrieval operations. To optimize data storage price/performance for the objects in a namespace, you can configure the service plan for that namespace to define a storage tiering strategy that specifies multiple storage tiers.

About storage components

HCP uses storage components to represent the storage available to it for storing objects.

A storage component is a set of one or more access points (buckets, containers, or mount points) that share a common endpoint. An endpoint is either a specific type of HCP storage (primary running or primary spindown) or a specific externally addressable storage device or storage service such as an S Series Node or Amazon S3. Each storage component has a specific set of data availability, price, and performance characteristics.

HCP uses storage components to provide you with an interface to:

- Configure HCP to provide the information that HCP needs to access specific extended storage devices and cloud storage service endpoints.
- Configure HCP to monitor, manage, and use all of the storage that is represented by one or more storage components of the same type as a single storage pool.
- Monitor the health, availability, capacity, and usage of the storage that is represented by each component (primary running storage, primary spindown storage, HCP S Series storage, and each extended storage device and cloud service endpoint) and appropriately provision storage.
- Retire HCP S Series or extended storage that is represented by a single storage component, or retire all of the storage that is represented by the components in a single storage pool.

Primary storage components

Every HCP system has a preconfigured storage component for each type of primary storage that the system is configured to use. The primary running storage component represents all continuously spinning disks that are currently managed by the HCP nodes. For HCP with SAN-attached storage systems with spindown storage, the primary spindown storage component represents all spindown-capable disks that are currently managed by the HCP nodes.

In the System Management Console, you can use the Storage page to perform the following actions:

- View information about the current hardware configuration, health status, availability, capacity, and use of the storage that is represented by each primary storage component.
- View current and historical storage usage statistics for each primary storage component.
- View a comparison of the current and historical storage capacity usage statistics for all components that are defined on the HCP system, including the two primary storage components.
- Monitor the health and use of each type of primary storage.
- Determine when you need to add primary storage or replace storage devices that are used for primary running storage or primary spindown storage.

Note: You cannot modify a primary storage component for the purpose of adding, retiring, or upgrading primary running storage or primary spindown storage. To add primary storage to an HCP system either to increase primary storage capacity or to replace one or more retired storage devices, contact your authorized HCP service provider for help.

On a HCP with internal storage or HCP with SAN-attached storage system, you can use either the Storage page or the Migration page in the System Management Console to retire one or more primary storage devices. When you retire primary storage, HCP automatically updates each primary storage component, as needed, to reflect the changes in the total

storage capacity and the total number of disks represented by each primary storage component.

HCP S Series storage components

HCP can use HCP S Series Nodes as an alternative to primary storage or for tiering purposes.

To connect the S Series Nodes to the HCP system, you need to add them to the HCP system on the Hardware page of the System Management Console.

You can configure HCP to write directly to S Series Nodes by changing the ingest tier of a service plan. This does not remove the need for primary storage. Primary running storage still keeps all custom metadata of objects tiered to HCP S Series storage.

After an HCP S Series storage component is added, you can use the Storage page to view its health status, availability, capacity, and current and historical storage usage statistics.

S Series Nodes have a storage capacity limit. You can use the Storage page to monitor the health and usage of HCP S Series storage components and determine when you need to add more S Series Nodes to the HCP system.

Extended storage components

HCP supports several types of extended storage. To enable HCP to use a specific type of extended storage, you first create and configure one or more storage components of the applicable type.

You can configure HCP to access and store object data on the following types of extended storage:

NFS
: Volumes that are accessed on physical storage devices using NFS mount points

Amazon S3
: Cloud storage that is accessed using an Amazon Web Services user account

Google Cloud
: Cloud storage that is accessed using a Google Cloud Platform user account

Microsoft Azure
: Cloud storage that is accessed using a Microsoft Azure user account

S3 compatible
: Any physical storage device or cloud storage service that is accessed using a protocol that is compatible with the Amazon S3 access protocol

ThinkOn cloud
: S3 compatible cloud storage that is accessed using a ThinkOn cloud user account

Important: Extended storage is intended to increase the amount of storage that's available to HCP. Extended storage does not function as backup storage. You should secure, back up, and monitor the health and availability of each extended storage device and cloud storage service that you use to store data in an HCP repository.

About storage pools

HCP uses *storage pools* to represent logical groups of storage components that can be used as storage tiers. Each storage pool consists of one or more storage components that are used to access the same type of storage.

Each storage tier typically consists of only one storage pool, but a tier can be configured to use multiple storage pools. To store objects on a given tier, HCP uses all of the storage that's accessed using the storage components that are contained in the storage pools that are configured for the storage tier. Therefore, the capacity of a given storage pool is the total amount of space that's associated with all the physical storage devices or all of the cloud storage service endpoints represented by the storage components in the pool. You can add storage components to a pool at any time, thereby increasing the capacity of the pool.

You should size extended storage pools to accommodate the amount of data you expect to be written to them. In making this calculation, you need to account for multiple namespaces using the same service plan as well as for multiple service plans specifying the same target storage pool.

Primary storage pools

Every HCP system has a pre-configured storage pool for each type of primary storage that the system is configured to use. The primary running storage pool contains the pre-configured primary running storage component, which represents all continuously spinning disks that are currently managed by the HCP nodes. For HCP with SAN-attached storage systems with spindown storage, the primary spindown storage pool contains the pre-configured primary spindown storage component, which represents all spindown-capable disks that are currently managed by the HCP nodes.

In the System Management Console, you can use the Storage page to view information about the current hardware configuration, health status, availability, capacity, and usage of the storage that's represented by each primary storage pool.

You can also use the Storage page to view current and historical storage usage statistics for each individual primary storage pool, and you can view a comparison of the current and historical storage capacity usage statistics for all storage pools that are defined on the HCP system, including the two primary storage pools.

You can use the information that you can view on the Storage page to monitor the health and usage of each type of primary storage and determine when you need to add primary storage to an HCP system or replace storage devices that are used for primary running storage or primary spindown storage.

Note:

You cannot modify a primary storage pool in order to add, retire, or upgrade primary running storage or primary spindown storage.

To add primary storage to an HCP system either to increase primary storage capacity or to replace one or more retired storage devices, contact your authorized HCP service provider for help.

On a HCP with internal storage or HCP with SAN-attached storage system, you can use either the Storage page or the Migration page in the System Management Console to retire one or more primary storage devices. When you retire primary storage, HCP automatically updates each primary storage pool as necessary to reflect the changes in the total storage capacity and in the total number of disks represented by each primary storage pool.

HCP S Series storage pools

HCP S Series Nodes use storage pools to group buckets together. A storage pool can contain multiple buckets from different S Series Nodes, but a bucket cannot belong to multiple storage pools.

If you add an S Series Node to the HCP system, a storage pool needs to already exist or be created. To create a storage pool you must specify the following information:

- The storage pool name.
- Whether you want HCP to compress object data that's stored on the storage that's allocated to the buckets in the storage pool.

- Whether you want HCP to encrypt object data that's stored on the storage that's allocated to the buckets in the storage pool. If encryption is disabled for the system, this option is not visible.
- For each bucket you want to include in the storage pool:
  - The account to which the bucket is assigned
  - The name of the bucket

Note: At any given time, a bucket can be included in only one storage pool.

Each bucket you add to a new storage pool must be empty or have only HCP data in it.

A storage pool is compliant only if all of the buckets in the pool are associated with compliant storage components.

When you deselect a component, HCP disables write operations to that component. However, you can still perform read and delete operations on the component until it is retired.

Extended storage pools

HCP supports the use of several different types of extended storage. To enable HCP to use a specific type of extended storage, you need to create and configure one or more storage pools of the applicable type.

For each storage pool, you need to specify the name of the pool, the type of extended storage that's represented by the pool, and the storage components that are contained in the pool.

The next sections describe each type of extended storage pool and describe the information you need to specify to enable HCP access the storage that's represented by each type of storage pool.

Storing objects on extended storage tiers

Each extended storage pool consists of one or more extended storage component access points (mount points, buckets, or containers) that are used to access the same type of extended storage. To store objects in a given extended storage pool, HCP uses all of the storage that's accessed using all of the extended storage component access points that are contained in that pool. You can add access points to an extended storage pool at any time, thereby increasing the capacity of the pool.

The service plan for a namespace defines one or more storage tiers for that namespace, and specifies the rules that determine which tier is used to store each object in that namespace at any given point in the object lifecycle. Each extended storage tier that's defined for a namespace typically consists of only one extended storage pool, but a tier can be configured to use multiple storage pools. To store objects on a given extended storage tier, HCP uses all of the storage that's accessed using the extended storage component access points contained in the storage pools that are configured for that tier.

Considerations for tiering objects from primary storage to HCP S Series or extended storage

When moving an object to a storage tier that includes only HCP S Series or extended storage pools, the Storage Tiering service moves only the object data onto the HCP S Series or extended storage that is used for the new tier.

Note: For the purpose of storage tiering, HCP treats parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of multipart objects as individual objects.

HCP keeps all metadata, including custom metadata, for an object on primary running storage. The system metadata for an object points to each specific NFS volume and each specific S Series or extended storage bucket or container that is used to store the data for that object. Primary storage keeps metadata even if S Series storage is used as an ingest tier alternative to running storage instead of as a storage tier.

All objects added to a namespace are first written to the ingest tier defined in their namespace service plan. However, HCP can read the data for an object directly from any storage component the object may later be tiered to.

The service plan for a given namespace defines one or more storage tiers for that namespace and specifies a separate DPL setting for each tier, including the ingest tier. When an object is moved from one storage tier to another, all copies of the object data are removed from the previous tier, and the object is then stored only on the new tier. The DPL for the new tier is the total number of copies of the object data that must be stored on that tier. The DPL is also the total number of copies of the object data that must be stored in the HCP repository. (For a metadata-only tier, the DPL is zero.)

When the Storage Tiering service moves an object in a given namespace from a storage tier that includes only ingest tier storage pools to a tier that includes only extended storage pools, the Storage Tiering service removes all existing copies of the data for that object from the ingest tier storage and stores the specified number of copies of the object data only on the extended storage that is represented by the pools that are configured for the new storage tier.

The Storage Tiering service moves all copies of the data for an object to HCP S Series or extended storage only if all of these are true:

- The cryptographic hash algorithm for the object has been stored in both the primary and secondary metadata for the object
- The object is not still open for write.
- The object is not a part of an in-progress multipart upload.
- If the namespace containing the object is being replicated and the target tier is extended storage, the object has already been replicated. The Storage Tiering service can move objects to HCP S Series storage before the objects are replicated.
- The namespace containing the object has a service plan that defines a storage tier that includes only HCP S Series or extended storage pools, and the object meets the criteria for being moved to that tier.

An HCP system can have a full copy of the data for an object that is subject to erasure coding but that has not yet been erasure coded. The Storage Tiering service can tier the data for such an object to HCP S Series or spindown storage but not to extended storage.

While the data for an object is stored only on HCP S Series or extended storage:

- If the object is deleted, the data that is on HCP S Series or extended storage is also deleted
- If the object is an old version that is pruned, the version data that is stored on HCP S Series or extended storage is also deleted
- If the object is shredded, the data that is stored on HCP S Series or extended storage is not shredded

Encryption and compression of objects in storage pools

The configuration of an HCP S Series or extended storage pool specifies whether the object data should be encrypted and/or compressed when it is stored on the storage that is used for that pool. Encryption can be enabled only if it was enabled when HCP was first installed. If encryption was not enabled during installation, the System Management Console does not have an option to encrypt data.

If the encryption option is selected for an HCP S Series or extended storage pool, the Storage Tiering service encrypts object data before writing it to the storage that is used for that pool. When reading encrypted data from an HCP S Series or extended storage pool, HCP automatically decrypts the data.

If an extended storage tier contains multiple external storage pools, HCP evenly distributes object data that is stored on that tier across all of those pools. For this reason, each storage pool that is configured for a given extended storage tier should be configured to use the same encryption setting (enabled or disabled).

To encrypt object data for S Series or extended storage, the Storage Tiering service uses the currently active PGP encryption key.

If compression is selected for an HCP S Series or extended storage pool, the Storage Tiering service compresses the object data before writing it to the storage that is used for that pool. When reading compressed data from an HCP S Series or extended storage pool, HCP automatically decompresses the data.

This compression activity is separate from the activity of the Compression/Encryption service. If an HCP object has been compressed by the Compression/Encryption service, HCP must decompress it before the Storage Tiering service can compress the object data and write it to HCP S Series or extended storage.

If you select compression and/or encryption for an HCP S Series used as an ingest tier, the object data is compressed and/or encrypted when it is written to the HCP S Series. When you read compressed and/or encrypted data from an HCP S Series, HCP automatically decompresses/decrypts the data. This compression/encryption activity is separate from the regular compression/encryption service.

If an extended storage tier contains multiple storage pools, HCP evenly distributes object data that is stored on that tier across all of those pools. For this reason, each extended storage pool that is configured for a given storage tier should be configured to use the same compression setting (enabled or disabled).

If you change the encryption or compression setting for a given HCP S Series or extended storage pool, the change affects only the data that is stored after you make the change. HCP does not change the data that is already stored on the storage that is used for the pool. As a result, an HCP S Series or extended storage pool may contain both encrypted and unencrypted data and both compressed and uncompressed data at the same time.

Downloading an encryption key

You use the Storage Certificates & Keys page of the System Management Console to download an encryption key.

1. In the System Management Console, click the Storage tab at the top of the page.

   The Storage Overview page opens.

2. On the side pane, click the Certificates & Keys tab. The Storage Certificates & Keys page opens.
3. In the Encryption Keys pane, click the Download Key ( ) next to the key that you want to download.

   For an encryption key, the download requires you to specify a password. HCP uses this password to encrypt the key before downloading it.

   The Download Encryption Key dialog box opens.

4. In the Secret Key password field, type a password for the key. The password can contain any valid UTF-8 characters, including white space.
5. In the Confirm Password field, type the password again. Then click Download.
6. Save the key file.

Uploading an encryption key

You use the Storage Certificates & Keys page of the System Management Console to upload a storage encryption key. This operation is available only if the cluster does not contain any objects. The operation is used for disaster recovery.

1. In the System Management Console, click the Storage tab at the top of the page.
   The Storage Overview page opens.
2. On the side pane, click the Certificates & Keys tab.

   The Storage Certificates & Keys page opens.

3. In the Encryption Keys pane, click Upload Key. The Upload Key dialog box opens.
   a. In the Secret Key Password field, enter the password for the key.
   b. For the Key File field, click Browse and select the PGP private key file that you want to upload.
   c. Click Upload Key.

      The dialog box closes. At the top of the Storage Certificates & Keys page, a success or error message appears.

Working with HCP S Series storage components

HCP uses HCP S Series storage components to:

- Monitor the general health, read permissions, and write permissions of the storage
- Manage node settings
- Add buckets and accounts
- Suspend or abandon the HCP S Series storage
- Configure advanced settings

Add an S Series Node to your HCP system

When you add an HCP S Series Node to your HCP system, HCP automatically creates a storage component, a storage pool (if an HCP S Series storage pool does not already exist), and a bucket. A user account is also created. The user account is granted permission to manage buckets and storage pools.

Bucket creation

The bucket that HCP creates when you add an S Series Node is available only to that HCP system. The name of this bucket is:

`hcpsrv-`*`hcp-system-name`*

If a bucket with that name already exists, which can happen if the S Series Node is added to the HCP system a second time, HCP creates a new bucket named:

`hcpsrv-`*`hcp-system-name0`*

Subsequently, each time HCP automatically creates a new bucket on the S Series Node, HCP either increments the numeric suffix on the bucket name by one or reuses an earlier name from a deleted HCP software-created bucket.

User account creation

The user account that HCP creates when you add an S Series Node is:

`hcpsrv-`*`hcp-system-name`*

If a user account with that username already exists, HCP creates a new user account:

`hcpsrv-`*`hcp-system-name0`*

Subsequently, each time HCP creates a new user account on the S Series Node, HCP either increments the numeric suffix on the user name by one or reuses an earlier user name from a deleted HCP software-created account.

Creating an HCP S Series storage component

To create an HCP S Series storage component, you need to add an S Series Node to the HCP system.

You must have the HCP administrator role to create an S Series Node storage component.
Note: Adding an S Series Node using a virtual IP address affects the ability of HCP to load balance traffic across Server Modules of the S Series Node.
Distributing the HCP load across the two Server Modules in the S Series Node requires the following:

- A properly set up DNS with a link to the detail setup instructions.
- Use the virtual IP addresses in the DNS configuration for the S Series Node FQDN.
- Use the correct FQDN for the S Series Node specified in the DNS.

Note: Using a virtual IP address instead of a static IP address is critical for high availability in case one of the Server Modules in the S Series Node becomes temporary unavailable.

1. On the Hardware > Nodes page, click Add Node.

   The Add Node wizard is displayed.

2. In the Username field, type a user name for an S Series Node user account with the administrator and security roles.
3. In the Password field, type the password for the userrname that you specified in step 2.
4. In the Domain Name field, type the fully qualified domain or virtual IP address of the S Series Node.

   If you receive an `invalid connection information` error message and you are connecting to the S Series Node through an IP address, disable HTTPS in step 7.

5. Optional: If Virtual network management is enabled and the Storage Network field is displayed, select the network that you want HCP to use to communicate with the S Series Node.

   If Virtual network management is not enabled, the field does not exist.

6. Optional: To use HTTP with SSL security for S Series Node management requests, select Use HTTPS for Management.
7. Optional: To display additional configuration options, click Advanced.
   a. To use HTTP with SSL security for data access requests, select Use HTTPS.
   b. In the HTTPS Port field, type the port you want to use to connect to the end point. Default value: 443.
   c. In the HTTP Port field, type the port you want to use to connect to the S Series Node. Default value: 80.
   d. Optional: To connect to the endpoint, select Use proxy .
   e. In the Proxy Host field, type the hostname or IP address of the proxy server.
   f. In the Proxy Port number field, type the number of the proxy server. Default value: 0.
   g. In the Proxy Username field, type the user name of the proxy server.
   h. In the Proxy Password field, type the password of the proxy server.
   i. In the Proxy Domain field, type the AD domain of the proxy server.
8. Click Next.
9. In the Name field, type a name for the S Series Node.
10. Optional: In the Description field, type a description for the S Series Node.
11. Click Next.
12. If the storage represented by the storage component is compliant with the terms and conditions of your service plan, select Compliant.
13. Perform one of the following actions.

    To create a new storage pool and attach the S Series Node to it:

    a. Select Add to new storage pool.
    b. In the Add to new storage pool field, type a name for the new storage pool.
    c. Optional: If you want to compress data in the new HCP S Series storage pool, select Compress Data at Rest.
    d. Optional: If you want to encrypt data on the new HCP S Series storage pool, select Encrypt Data at Rest.
    e. Optional: If you want the Content Verification service to run on the new HCP S Series storage pool, select Content Verification.

    To add the S Series Node to an existing storage pool:

    a. Select Add to existing storage pool.
    b. From the Name field, select the existing storage pool.
    c. Optional: To enable the HCP S Series Balancing service when there are multiple HCP S Series components in a pool, select Enable balancing for this pool.
14. Click Next.
15. On the Review page, ensure that the S Series Node is configured to your specifications.
16. Click Finish.

    If HCP cannot add the S Series Node to the system, the Console displays an error message.

    If the operation failed because the S Series Node user account does not have the administrator or security role, the following message is displayed:

    ```
    Unable to create S Series Node. An unexpected error occurred. Please contact your HCP system administrator.
    ```

Modifying an HCP S Series storage component

After an S Series Node is added to an HCP system, its storage component is displayed on the Storage > Components page. Use the System Management Console to manage and update the S Series Node settings.

Modifying basic component settings

The Settings tab of the S Series Storage Components page shows the name, type, description, storage network (if enabled) and endpoint of the S Series Node. You can modify most of the information on the page.

1. In the HCP System Management Console, open the Storage > Components page and select an S Series Node.
   The Storage Node page opens.
2. Click the Settings tab.
3. In the Name field, type a new name for the S Series Node.
4. In the Description field, type a new description for the S Series Node.
5. If the Storage Network field is visible, select a network for tiering.
6. In the Domain Name or Virtual IP field, type the new domain or virtual IP address of the S Series Node.
7. If the S Series Node meets the compliancy expectations of your service plan, select the Compliant checkbox.
8. Click Update Settings.

Modifying advanced component settings

1. Go to the Storage > Components page.
2. Click an S Series Node.
3. On the Storage > Node page that opens, click the Advanced tab.
4. Configure the following options:

   Use HTTPS

   To use HTTP with SSL security for data access requests, select Use HTTPS.

   HTTPS Port
   In the HTTPS Port field, type the port you want to use to connect to the S Series Node with SSL requests. The default is 443.

   HTTP Port
   In the HTTP Port field, type the port you want to use to connect to the S Series Node. The default is 80.

   Use proxy
   Optionally, select Use proxy to connect to the S Series Node. If you select Use proxy:

   Proxy Host
   In the Proxy Host field, type the hostname or IP address of the proxy server.

   Proxy Port
   In the Proxy Port number field, type the number of the proxy server. The default is 0.

   Proxy Username
   In the Proxy Username field, type the user name of the proxy server.

   Proxy Password
   In the Proxy Password field, type the password of the proxy server.

   Proxy Domain
   In the Proxy Domain field, type the AD domain of the proxy server.

   Connection Timeout (ms)
   In the Connection Timeout (ms) field, type the wait time you want to permit a connection to respond before the connection times out.

   Socket Timeout (ms)
   In the Socket Timeout (ms) field, type the amount of time you want to wait for data to be transferred over an open connection before the connection closes.

   Max Connections
   In the Max Connections field, type the max connection pool size.

   Max Error Retries
   In the Max Error Retries field, type the maximum allowable error retries.

   User Agent
   In the User Agent field, type the user agent.

   TCP Send Buffer Size Hint
   In the TCP Send Buffer Size Hint field, type the optional size hint (in bytes) for the low-level TCP send buffers.

   TCP Receive Buffer Size Hint
   In the TCP Receive Buffer Size Hint field, type the optional size hint (in bytes) for the low-level TCP receive buffers.

   Enable additional data integrity validation
   Select this option if you want the S Series Node to check the md5 hash of every object it receives against the hash generated by HCP when writing the object. If the hashes do not match, the object fails to tier.

   Maximum object size (GB)
   In the Maximum object size (GB) field, type the maximum allowable object size.

   Enable multipart object uploads
   Allows HCP to write objects to the S Series Node using multipart object upload. Starting with release 2.0 of the S Series Node, multipart upload is automatically disabled by the system and, under normal circumstances, should not be enabled. If you choose to configure Enable multipart object uploads:

   Multipart object upload size threshold (MB)
   In the Multipart object upload size threshold (MB) field, type the object size threshold you want HCP to use to determine when to employ a multipart upload.

   Multipart object upload part size (MB)
   In the Multipart object upload part size (MB) field, type the part size of a single part of a multipart object upload.

   Support Metadata
   Whether the extended storage component supports S3 metadata on objects. If you are unsure whether S3 metadata is supported, contact your service provider.

   Max metadata size
   In the Max metadata size field, type the maximum size (in bytes) of S3 metadata files that will be attached to objects written to S Series Nodes. S Series Nodes permit a maximum size of 6,144 bytes.
   Note:

   Support Metadata and Max metadata size options only work for S Series Nodes release 2.0 or later. When you upgrade an S Series Node to release 2.0 or later, the metadata settings take effect within twenty-four hours.

5. After you are finished, perform one of the following actions:
   - If you want to save your configuration, click Update Settings.
   - If you want to restore the page to its default settings, click Reset Advanced Settings.

Pausing and resuming an HCP S Series storage component

When an HCP S Series storage component is in use, you can pause it at any time. Pausing the component makes it inaccessible for all read and write operations and for storage tiering. After you resume the component, it becomes available again for read and write operations and for tiering.

1. Go to the Storage > Components page.
2. Click an S Series Node.
   The Storage > Node page opens.
3. Click the Manage tab.
4. Click Pause Component.

   After the storage component is paused, the button is replaced with Resume Component.

5. To resume communication between HCP and the storage component, click Resume Component.

Deleting an HCP S Series storage component

If the storage represented by an HCP S Series storage component is not being used to store objects in any namespaces defined on the HCP system, you can safely delete that storage component.

1. Retire the storage component.
2. On the Storage > Retirement page, click the retired S Series Node.
3. Click Delete Volume. If the node is not successfully retired, the Delete Volume button is inaccessible.

Abandoning an HCP S Series storage component

Abandoning an HCP S Series storage component removes the associated S Series Node from the HCP system. This can be done regardless of whether data is tiered to the S Series Node. If you abandon an S Series Node without retiring its data, that data becomes inaccessible even if you add the S Series Node to the system again. As a general rule, you should retire and delete a component instead of abandoning it.

1. Go to the Storage > Components page.
2. Click an S Series Node.
3. On the Storage > Node page that opens, click the Manage tab.
4. Click Abandon Component.
5. In the Confirm: Abandon Component window, type `Yes` in the text field.
6. Click Abandon.

Working with buckets and accounts on an HCP S Series storage component

The Buckets tab of an S Series Node on the Storage > Components page shows the buckets defined on the S Series Node and the S Series Node user accounts to which they are assigned. Each bucket shows how many bytes of data it's currently storing, whether it's in use, and alerts. Once you add an S Series Node to the HCP system, a bucket and user account are automatically created. More buckets can be created manually through the storage component.

Creating a bucket

1. Go to the Storage > Components page.
2. Click an S Series Node.
3. On the Storage > Node page, click the Buckets tab.
4. Click Add Buckets.
5. In the Select Account section that opens, select the account you want to own the bucket.
6. Click Go.
7. Click Bucket Actions.
8. Select Create new in the Action field.
9. Type the name of the new bucket in the Bucket Name text box.

   A bucket name must be at least three and no more than 63 characters long. Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and dashes. Each label must start and end with a lowercase letter or a number. Bucket names must not be formatted as an IP address.

10. Click Go.
11. Click Finish.

Deleting a bucket

1. Go to the Storage > Components page.
2. Click an S Series Node.
3. On the Storage > Node page, click the Buckets tab.
4. Click the delete control on the right side of the bucket.

   A Confirm: Delete window appears.

5. Click Delete.

Adding an existing bucket to an HCP S Series storage component

Buckets can be created and not added to their respective account. When this occurs, the buckets are not displayed on the Buckets tab and cannot have objects tiered to them from the HCP system.

1. On the Buckets tab, click Add Buckets.

   A Select Account drop down menu appears.

2. Select the account to which the bucket is assigned and click Continue.

   All buckets assigned to the account appear in the Available Buckets field. Buckets that are already added to the account are selected.

3. Select the buckets you want to add from the Available Buckets field.
4. Click Finish.

Adding an existing S Series Node user account

Aside from the S Series Node user account that's automatically generated when an S Series Node is added to your HCP system, S Series Node user accounts are created on the HCP S Series Management Console. The accounts are independent of the HCP system and can exist without appearing on the HCP System Management Console. If you want user accounts to appear on the HCP system, they need to be manually added.

To add an S Series Node user account to HCP, you need an access key and secret key. For more information about these keys, see the HCP S Series Node Help.

Tip:

After multiple user accounts have been added to the HCP system, you can change the owner of a bucket by clicking the gear beside a bucket on the Storage > Components page and selecting the new owner.

1. On the Buckets tab of an S Series Node, click Accounts.
2. Click Add Accounts.

   An Add Account wizard opens.

3. In the Account Label field, type the name you want to give the S Series Node user account on HCP.
4. In the Access Key field, type your account access key.
5. In the Secret Key field, type your account secret key.
6. Optionally, if you want custom request headers:
   a. Click Custom Request Headers.
   b. Type the header name in the blank text field.
   c. Click Add.
   d. In the Value field, type the header value.
7. Click Finish.

Updating the owner of a bucket

Before you update the owner of a bucket, make sure you have created an additional S Series Node user account.

1. Go to the Storage > Components page.
2. Click an S Series Node.
3. On the Storage > Node page, click the Buckets tab.
4. Click the bucket that you have created and want to update.
5. In the Select Account section that opens, select the account that you want to own the bucket.
6. Click Continue.

Deleting an S Series Node user account

Except for the S Series Node user account that's automatically created when you add the S Series Node to the HCP system, all other accounts can be deleted. Deleting an S Series Node user account does not delete it permanently, but rather removes the account from the HCP system. The account still exists and can be added back to the HCP system. An account can be removed only after all buckets on the account have been deleted.

1. On the Buckets tab of an S Series Node, click Accounts.
2. Click the garbage can icon beside the account you want to delete.
3. In the warning message that appears, type `Yes`.
4. Click Delete.

Working with extended storage components

HCP uses extended storage components to provide you with an interface to use, manage, and monitor extended storage devices and cloud storage service endpoints.

Using the System Management Console, you can perform the following actions on extended storage components:

- Configure HCP to access specific extended storage devices and cloud storage service endpoints.
- Configure HCP to monitor, manage, and use all of the extended storage that is accessed using one or more extended storage components of the same type as a single storage pool.
- Monitor the health, availability, capacity, and usage of the extended storage that is represented by each component, and appropriately provision storage.
- Pause (suspend), retire, or abandon extended storage that is represented by a single storage component, or retire all of the extended storage that is represented by the components in a single storage pool.

Creating an extended storage component

Use the Add Component wizard on the Storage page to create and configure an extended storage component.

Each time you use the Storage page to access the Add Component wizard, you are prompted to select the type of extended storage component that you want to create. The System Management Console then dynamically builds the pages in the Add Component wizard to present only the fields you need to use to configure HCP to access and use the specified type of extended storage component.

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click Add Component.

   The Get Started wizard opens.

3. In the wizard, click the arrow and select the type of component that you want to create.
   Note:

   To create a ThinkOn cloud storage component, select ThinkOn as the type of component to configure. Then follow the same procedure as you do to configure other S3 compatible storage components.

4. Click Go.

The Get Started wizard exits and the System Management Console opens the applicable Add Component wizard.

5. Specify the information that HCP needs to use to access and use the extended storage component:
   - To create an Amazon S3 storage component, use the Amazon S3 storage component settings. Then return to this procedure.
   - To create a Google Cloud storage component, use the Google Cloud storage component settings. Then return to this procedure.
   - To create a Microsoft Azure storage component, use the Microsoft Azure storage component settings. Then return to this procedure.
   - To create an S3 compatible storage component, including a ThinkOn cloud storage component, use the S3 compatible storage component settings. Then return to this procedure.
   - To create an NFS storage component, use the NFS storage component settings. Then return to this procedure.
6. Click Next to save the information you entered and advance to the last page of the wizard.
7. On the Review page, take one of these actions:
   - If the extended storage component configuration information that you entered is correct, click Finish.
   - If the extended storage component configuration information is not correct, use the Previous and Next buttons to navigate through the pages in the wizard and change any settings that are not correct. Then navigate to the Review page and click Finish.

   The wizard closes and the System Management Console displays the Components panel on the Storage page

You created and configured the extended storage component.

HCP can use the storage that is represented by a given component only if at least one of its access points (a mount point, bucket, or container) is contained in a storage pool that's included in at least one storage tier that is defined for a namespace by its service plan.

Amazon S3 storage component settings

Each Amazon S3 component represents a single endpoint that's used to access cloud storage using one or more Amazon S3 Web Services user accounts.

To enable HCP to access the storage that's represented by an Amazon S3 storage component, when you create that component, specify the following information:

- The component name.
- Optionally, a description of the component.
- Optionally, the network you want HCP to use for communication with storage component. This field is only visible if Virtual network management is enabled.
- Whether you want HCP to use the default endpoint, s3.amazonaws.com, to connect to Amazon S3 Web Services, and if not, the fully qualified domain name (FQDN) of the endpoint that you want HCP to use instead of the default.
- Optionally, you may choose any of these advanced configuration settings:
  - Whether you want HCP to use HTTPS to access the endpoint, and if so, the HTTPS port you want to use to connect to the endpoint (default is 443).
  - The HTTP port you want to use to connect to the endpoint (default is 80).
  - Whether you want to use a proxy server to connect to the endpoint, and if so, the following information about the proxy server:
    - The hostname or IP address of the proxy server.
    - The port number you want to use to connect to the proxy server (default is 0).
    - The user name, password, and AD domain of the user account that HCP needs to use to access the proxy server.
  - Whether you want HCP to use path-style URLs to access the storage that's represented by the storage component, and if so, the region that includes the Amazon S3 Web Services datacenter that hosts the storage that's represented by this component. If you select this option, you need to specify a region-specific endpoint instead of using the default endpoint.
  - The region that includes the Amazon S3 Web Services datacenter that hosts the storage that's represented by this component (default is us-east-1).

    For faster access to storage located in a particular region, you should specify a region-specific endpoint instead of using the default endpoint.
  - Whether the extended storage component supports S3 metadata on objects. If you are unsure whether S3 metadata is supported, contact your service provider.
  - In the Max metadata size field, type the maximum size (in bytes) of the S3 metadata that will be attached to objects tiered to the storage component. Each extended storage service provider permits a different maximum size. Contact your service provider to learn the maximum size.
- Whether the storage that's represented by this component is considered to be compliant.
- The account label that you want to associate with the initial Amazon S3 Web Services user account that you want HCP to use to access the storage that's represented by the component. In the System Management Console, HCP uses the account label to represent the user account with the specified credentials.
- The authentication type you want to use to authenticate all requests sent from HCP to the storage component.
- The access key and secret key for the Amazon S3 Web Services user account that you want HCP to use to access the storage that's represented by the component. After you create an Amazon S3 storage component, you can modify it to specify credentials for one or more additional user accounts.
- If you are using AWS STS or CAP authentication, the authentication endpoint text field appears. This is the endpoint to which you send your credentials in order to generate an AWS STS authentication token.
- If you are using CAP authentication, the following additional fields are displayed:
  - Authentication port field. Enter the port of your CAP endpoint.
  - Authentication certificate drop down menu. Select the account certificate that connects HCP to the CAP authentication endpoint. To see the account certificate in the dropdown field, it must already exist in the HCP system.
- Optionally, any custom request headers that you want HCP to include in the access request URLs that are sent to Amazon S3 Web Services to request read or write access to the storage associated with the specified user account.
- Whether you want to access existing buckets associated with the specified user account. If yes, enter the name of each existing bucket to access.

  At any given time, a bucket can be associated with only one storage component.

  You can add an existing bucket to an Amazon S3 storage component only if that bucket is empty or has only HCP data in it.
- Whether you want to create any new buckets for the specified user account. If yes, enter the name of each new bucket to create.
  Note: By default, the Add Component wizard displays a list of the existing buckets that HCP can access using the specified user account credentials. However, the wizard does not display the controls required to create a new bucket. To create a new bucket, you must click Bucket Actions, select Create new from the dropdown list, and specify the name of the bucket you want to create.

Google Cloud storage component settings

Each Google Cloud component represents a single endpoint that's used to access cloud storage using one or more Google Cloud Platform user accounts.

To enable HCP to access the storage that's represented by a Google Cloud storage component, when you create that component, you specify the following information:

- The component name.

- Optionally, a description of the component.
- Optionally, the network you want communicating with the storage component. This field is only visible if Virtual network management is enabled.
- Whether you want HCP to use the default endpoint, storage.googleapis.com, to connect to Google Cloud Platform, and if not, the fully qualified domain name (FQDN) of the endpoint that you want HCP to use instead of the default.
- Optionally, any of these advanced configuration settings:
  - Whether you want HCP to use HTTPS to access the endpoint, and if so, the HTTPS port you want to use to connect to the endpoint (default is 443).
  - The HTTP port you want to use to connect to the endpoint (default is 80).
  - Whether you want to use a proxy server to connect to the endpoint, and if so, the following information about the proxy server:
    - The hostname or IP address of the proxy server.
    - The port number you want to use to connect to the proxy server (default is 0).
    - The user name, password, and AD domain of the user account that HCP needs to use to access the proxy server.
  - Whether you want HCP to use path-style URLs to access the storage that's represented by the storage component
  - Whether the extended storage component supports S3 metadata on objects. If you are unsure whether S3 metadata is supported, contact your service provider.
  - In the Max metadata size field, type the maximum size (in bytes) of the S3 metadata that will be attached to objects tiered to the storage component. Each extended storage service provider permits a different maximum size. Contact your service provider to learn the maximum size.
- Whether the storage that's represented by this component is considered to be compliant.
- The account label that you want to associate with the initial Google Cloud Platform user account that you want HCP to use to access the storage that's represented by the component. In the System Management Console, HCP uses the account label to represent the user account with the specified credentials.
- The access key and secret key for the Google Cloud Platform user account that you want HCP to use to access the storage that's represented by the component.

  After you create a Google Cloud storage component, you can modify it to specify credentials for one or more additional user accounts.

- Optionally, any custom request headers that you want HCP to include in the access request URLs that are sent to Google Cloud Platform to request read or write access to the storage associated with the specified user account.
- Whether you want to access existing buckets associated with the specified user account, and if so, the name of each existing bucket you want to access.

  At any given time, a bucket can be associated with only one storage component.

  You can add an existing bucket to a Google Cloud storage component only if that bucket is empty or has only HCP data in it.

- Whether you want to create any new buckets for the specified user account, and if so, the name of each new bucket you want to create.
  Note: By default, the Add Component wizard displays a list of the existing buckets that HCP is able to access using the specified user account credentials, but the wizard does not display the controls required to create a new bucket. To create a new bucket, you need to click Bucket Actions, then select Create new from the dropdown list, then specify the name of the bucket you want to create.

Microsoft Azure storage component settings

Each Microsoft Azure component represents a single endpoint that's used to access cloud storage using one or more Microsoft Azure user accounts.

To enable HCP to access the storage that's represented by a Microsoft Azure storage component, when you create that component, you specify the following information:

- The component name.
- Optionally, a description of the component.
- Optionally, the network you want communicating with the storage component. This field is only visible if Virtual network management is enabled.
- Whether you want HCP to use the default endpoint, blob.core.windows.net, to connect to Windows Azure, and if not, the fully qualified domain name (FQDN) of the endpoint that you want HCP to use instead of the default.
- Optionally, you may choose any of these advanced configuration settings:
  - You can display an advanced option that lets you specify whether to connect to Microsoft Azure using HTTPS. This option is enabled by default.
  - Whether you want to use a proxy server to connect to the endpoint, and if so, the following information about the proxy server:
    - The hostname or IP address of the proxy server.
    - The port number you want to use to connect to the proxy server (default is 0).
  - Whether the extended storage component supports S3 metadata on objects. If you are unsure whether S3 metadata is supported, contact your service provider.
  - In the Max metadata size field, type the maximum size (in bytes) of the S3 metadata that will be attached to objects tiered to the storage component. Each extended storage service provider permits a different maximum size. Contact your service provider to learn the maximum size.
- Whether the storage that's represented by this component is considered to be compliant.
- The account label that you want to associate with the initial Microsoft Azure user account that you want HCP to use to access the storage that's represented by the component. In the System Management Console, HCP uses the account label to represent the user account with the specified credentials.
- The access key and secret key for the Microsoft Azure user account that you want HCP to use to access the storage that's represented by the component.

  After you create a Microsoft Azure storage component, you can modify it to specify credentials for one or more additional user accounts.

- Optionally, any custom request headers that you want HCP to include in the access request URLs that are sent to Microsoft Azure to request read or write access to the storage associated with the specified user account.
- Whether you want to access existing containers associated with the specified user account, and if so, the name of each existing container you want to access.

  At any given time, a container can be associated with only one storage component.

  You can add an existing container to a Microsoft Azure storage component only if that container is empty or has only HCP data in it.

- Whether you want to create any new containers for the specified user account, and if so, the name of each new container you want to create.
  Note: By default, the Add Component wizard displays a list of the existing containers that HCP is able to access using the specified user account credentials, but the wizard does not display the controls required to create a new container. To create a new container, you need to click Container Actions, then select Create new from the dropdown list, then specify the name of the container you want to create.

S3 compatible storage component settings

Each S3 compatible component represents a single physical storage device or cloud storage service that's used to access storage using a protocol that's compatible with the Amazon S3 access protocol.

To enable HCP to access the storage that's represented by an S3 compatible storage component, when you create that component, you specify the following information:

- Optionally, the network you want communicating with the storage component. This field is only visible if Virtual network management is enabled.
- The endpoint that HCP needs to use to access the physical device or cloud storage service that manages the storage that's represented by this component.
- Optionally, you can choose any of these advanced configuration settings:
  - Whether you want HCP to use HTTPS to access the endpoint, and if so, the HTTPS port you want to use to connect to the endpoint (default is 443).
  - The HTTP port you want to use to connect to the endpoint (default is 80).
  - Whether you want to use a proxy server to connect to the endpoint, and if so, the following information about the proxy server:

        - The host name or IP address of the proxy server.
        - The port number you want to use to connect to the proxy server (default is 0).
        - The user name, password, and AD domain of the user account that HCP needs to use to access the proxy server.
    - Whether you want HCP to use path-style URLs to access the storage that's represented by the storage component.
    - Whether the extended storage component supports S3 metadata on objects. If you are unsure whether S3 metadata is supported, contact your service provider.
    - In the Max metadata size field, type the maximum size (in bytes) of the S3 metadata that will be attached to objects tiered to the storage component. Each extended storage service provider permits a different maximum size. Contact your service provider to learn the maximum size.
- Whether the storage that's represented by this component is considered to be compliant.
- The account label that you want to associate with the initial user account that you want HCP to use to access the storage that's represented by the component. In the System Management Console, HCP uses the account label to represent the user account with the specified credentials.
- The authentication type you want to use to authenticate all requests sent from HCP to the storage component.
- The access key and secret key for the user account that you want HCP to use to access the storage that's represented by the component.

  After you create an S3 compatible storage component, you can modify it to specify credentials for one or more additional user accounts.

- If you are using AWS STS or AWS STS V4 authentication, the authentication endpoint text field appears. This is the endpoint to which you send your credentials, in order to generate an authentication token.
- Optionally, any custom request headers that you want HCP to include in the access request URLs that are sent to the target storage device or cloud service to request read or write access to the storage associated with the specified user account.
- Whether you want to access existing buckets associated with the specified user account, and if so, the name of each existing bucket you want to access.

  At any given time, a bucket can be associated with only one storage component.

  You can add an existing bucket to an S3 compatible storage component only if that bucket is empty or has only HCP data in it.

- Whether you want to create any new buckets for the specified user account, and if so, the name of each new bucket you want to create.
  Note: By default, the Add Component wizard displays a list of the existing buckets that HCP is able to access using the specified user account credentials, but the wizard does not display the controls required to create a new bucket. To create a new bucket, you need to click Bucket Actions, then select Create new from the dropdown list, then specify the name of the bucket you want to create.

NFS storage component settings

Each NFS storage component represents a single physical storage device on which one or more volumes are accessed using NFS mount points.

When you create an NFS storage component, you provide HCP with the information that it needs to create an NFS mount point for each volume that you want to access on the device that's represented by the NFS storage component. However, HCP creates an NFS mount point that's associated with a given storage component only when that mount point is added to an NFS storage pool.

When an HCP system is upgraded from release 6.x to release 7.0 or later, HCP automatically creates an NFS storage component and an NFS storage pool for each external volume that was configured on the HCP system before it was upgraded, and defines each NFS storage pool as a storage tier. For each namespace that was configured to use NFS storage before the upgrade, HCP automatically configures the service plan for that namespace to define the applicable NFS storage pool as a storage tier.

On the Hardware page of the System Management Console, HCP uses an external volume (also called an NFS volume) to represent the storage that's accessed using a single NFS mount point that's contained in an NFS storage pool. You can use the Storage page to view information about all NFS volumes stored on a single physical storage device that's represented by an NFS storage component.

Creating NFS shares on a physical storage device

Before you can create an NFS storage component, you need to create and configure the NFS shares for the volumes you want to access on the physical storage device that's represented by the component.

The main steps for creating NFS shares on a physical storage device for which you want to create an NFS storage component are:

1. On the physical storage device, create the directories you want to share.
2. Export each directory as an NFS share.

Exports and required NFS component settings

Directories for export

For each storage volume you want to access on the physical storage device that's represented by an NFS storage component, you need to create a directory on that physical storage device. For each directory, you need to set the permissions to allow read, write, and execute access to all users.

For example, on Linux systems, each directory you want to share must have its permissions set to 777.

Exported shares

Each directory that you want to mount as an NFS volume on an HCP node must be exported as an NFS share on the physical storage device that's represented by the NFS storage component you want to create. To ensure that other systems and applications cannot mount the same storage, you should export each share exclusively to the HCP system. You can identify each the HCP system in one of three ways:

- Using the fully-qualified domain name (FQDN) of the domain that's associated with the [hcp_system] network, preceded by admin (for example, admin.hcp.example.com). This option is available only if the HCP system is using DNS.
- By the CIDR notation for any IPv4 or IPv6 gateway that's defined for the [hcp_system] network.
- By the node IP addresses that the extended storage device needs to use to communicate with the [hcp_system] network. In this case, you need to export the share to the applicable IPv4 or IPv6 addresses for all the HCP nodes.

  You need to export each share to all nodes because you cannot predict with which node HCP will associate the NFS storage volume you create for a share. If you omit a node and HCP associates a volume with that node, HCP has no access to the share for that volume.

  If you use node IP addresses to identify the HCP system and you subsequently change any of those IP addresses in the [hcp_system] network, you need to update the export specification for the share with the new addresses. Then you need to export the share again.

The method you use to export the shares and the export options you specify depend on the type of storage device for which you want to create an NFS storage component. Minimally, the exported share must allow read and write access by the HCP system.

The following information on exporting shares on Linux systems is included for explanatory purposes only. The extended storage devices that are represented by NFS storage components should be enterprise-class, purpose-built appliances. The storage volumes that are accessed using NFS mount points should be on storage that's RAID-protected,

secure, and monitored closely for its health.

The extended devices that are represented by the NFS storage component must support the Linux file naming scheme. When using a non-Linux OS, you need to reconfigure mapping on the NFS storage device.

On Linux systems, you specify the shares to be exported in the /etc/exports file. To ensure that HCP correctly uses the NFS volumes that you make available to it, the specification of each exported share must minimally include these options:

```
rw,sync,no_wdelay
```

For example, to export the share named /hcp_shares/share1 to the HCP system with the domain name hcp.example.com, you would add this line to the /etc/exports file:

```
/hcp_shares/share1 admin.hcp.example.com(rw,sync,no_wdelay)
```

The export options in each line in the /etc/exports file must directly follow the system identifier with no space between them.

After you've specified the shares to exported, you use this command to export them:

```
exportfs -a
```

For information about how to export shares on non-Linux storage devices, see the device-specific documentation.

Required NFS storage component configuration settings

To enable HCP to access the storage that's represented by an NFS storage component, when you create that component, you specify the following information:

- The IP address or hostname that HCP needs to use to connect to the physical storage device on which you want to access storage volumes using NFS mount points.
- The mount command options that you want HCP to use when it creates NFS mount points to access NFS shares on the device that's represented by the component.

  To ensure that NFS volumes are mounted correctly, HCP always uses these options to the mount command:

  ```
  rw,sync,soft,nodev,nfsvers=3
  ```

  HCP uses the options that you specify in addition to the above options. The additional options that you can specify are:

  ```
  lookupcache=none
  noatime
  nodiratime
  nosuid
  port=n
  retrans=n
  rsize=n
  tcp
  proto=tcp6
  timeo=n
  wsize=n
  ```

  Other mount command options are not supported.

  If the [hcp_system] network is currently configured to use both IPv4 and IPv6 addresses, you need to specify tcp or proto=tcp6 to indicate which type of IP address you want HCP to use to connect to the NFS storage component.

- The full pathname of each directory that you want to access using an NFS mount point.
  Note: At any given time, a mount point can be associated with only one NFS storage component.

  By default, the Add Component wizard displays a list of the existing mount points that HCP is able to access using the specified user account credentials, but the wizard does not display the controls required to specify the pathname for an existing NFS share. To specify a directory that does not appear in the list, you need to click Mount Point Actions, then specify the full path name of the directory for which you want to create an NFS mount point.

Modifying an extended storage component

You can use the Components panel on the Storage page to view and modify the configuration of any extended storage component. To display this panel, click the Components tab on the left side of the Storage page.

You can modify the following items associated with an extended storage component:

- Change one or more of the configuration settings that are specified when the component is first created.
- Modify one or more of the default values for the advanced settings used for the extended storage component. Each type of extended storage component has slightly different advanced settings.

  Typically, you do not need to change any of the default values that are used for the advanced settings for an extended storage component.

- Add a new access point (a mount point, bucket, or container) to an existing storage component.
- Delete any access point that's not currently in use.
- For all types of extended storage components except NFS:
  - Configure a new user account to be used to access the cloud storage service endpoint or S3 compatible storage device endpoint that's represented by the component.
  - Delete any user account that's not currently in use.

Modifying the configuration settings that are specified for an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component that you want to modify.
3. At the top of the panel that opens, click the Settings tab.
4. On the panel that opens, use the fields to change any of the settings that are currently used for the component.
5. Click Update Settings.

Modifying the advanced configuration settings that are used for an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component that you want to modify.
3. At the top of the panel that opens, click the Advanced tab.
4. On the panel that opens, use the fields to change any of the settings that are currently used for the component or click Reset Advanced Settings to change all advanced settings to use the default values.
5. Click Update Settings.

Adding access points to an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component for which you want to configure one or more new access points.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's used for the component (Mount Points, Buckets, or Containers).
4. At the bottom of the panel that opens, click Add *AccessPointType*.
5. For every type of extended storage except NFS, in the window that opens, use the dropdown list to select the account label that's associated with the user account that's used to access the bucket or container you want to add, and click Go. The window does not appear if you're adding a mount point to an NFS storage component.

   The Add AccessPointType wizard opens, displaying a table that contains a list of existing access points (mount points, buckets, or containers) that are available for use, along with a check box that corresponds to each access point in the list.

6. Click *AccessPointType* Actions.
7. Take either or both of these actions:

   To add existing access points to the storage component:

   a. In the *AccessPointType* Actions section, in the Action field, select Add existing.

      When you first expand the *AccessPointType* Actions section, Add existing is selected by default.

   b. Use the check boxes in the left column in the table to select each existing access point that you want to add to the storage component configuration.
   c. Click Go.

   To create one or more new buckets or containers for use by the specified user account or to create one or more mount points:

   a. In the *AccessPointType* Actions section, in the Action field, select Create new.
   b. In the *AccessPointType*Name field, for each new access point you want to create, type a name for the new access point, and click Go.

      Each new access point you create is added to the list of existing access points, and its checkbox is automatically selected.

      Note: You can delete any new access point from the list before you actually create the new access point on the extended storage device. To do this, click the delete control ( ) in the row that corresponds to the access point name.
   c. When you're finished creating new access points, in the Action field, select Add existing, and then click Go.
8. When you're finished adding both new and existing access points to the extended storage components, click Finish at the bottom of the panel.

   When you click Finish, the Add AccessPointType wizard exits, and the *AccessPointType* panel (Mount Points, Buckets, or Containers) for the storage component you've modified appears, showing the list of access points that are currently configured for the component and the current status of each access point. All of the new and existing access points you've just added are included in the list.

Configuring a new user account for access to an extended storage endpoint

You can configure a new user account to be used to access any cloud storage service endpoint or S3 compatible storage device endpoint that's represented by an extended storage component.

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component for which you want to configure a new user account.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's used for the component (Buckets or Containers).
4. At the top of the Buckets or Containers panel, click the Accounts tab.
5. At the bottom of the Accounts panel, click Add Account.

   The Add Account wizard opens.

6. In the Add Account wizard, specify the following information to configure the new user account:
   - The account label that you want HCP to use to identify the user account in the System Management Console
   - The access key and secret key that HCP needs to use to access the new user account
   - For S3 compatible storage components, the authentication type you want to use to authenticate all requests sent from HCP to the storage component
   - Optionally, any custom request headers that you want HCP to include in the access request URLs that are sent to the cloud storage service or storage device that's represented by the storage component in order to request read or write access to the storage associated with the new user account
7. Click Finish.

   When you click Finish, the Add Account wizard exits, and the AccessPointType panel (Buckets or Containers) for the storage component you've modified appears, showing the list of user accounts that are currently configured for the component and the current status of each account. The new and user account you've just added is included in the list.

Updating the owner of a bucket in an extended storage component

Before you update the owner of a bucket or container in an extended storage component, make sure you have configured a new user account for access to any cloud storage service endpoint or S3 compatible storage device endpoint represented by an extended storage component. This procedure is not applicable to NFS components.

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. Click the component you want.
3. Click the tab for the applicable type of access point (Buckets or Containers).
4. Click the Buckets or Containers tab, as applicable.
5. Click the bucket or container that you have created and want to update.
6. In the Select Account section that opens, select the account that you want to own the bucket.
7. Click Continue.

Deleting an unused access point from an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component from which you want to delete an unused access point.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's used for the component (Mount Points, Buckets, or Containers).

   The AccessPointType panel opens, showing a list of access points that are currently configured for the component. A delete control ( ) appears in the row for each unused access point.

4. Click the delete control for any access point to delete it from the component.

Deleting an unused user account from an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component from which you want to delete an unused user account.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's used for the component (Buckets or Containers).
4. At the top of the Buckets or Containers panel, click the Accounts tab.

   The Accounts panel opens, showing a list of user accounts that are currently configured for the component. A delete control ( ) appears in the row for each unused user account.

5. Click the delete control for any user account to delete it from the component.

Uploading an account certificate for CAP authentication

The C2S CAP server acts as an intermediary between HCP and AWS STS authentication. CAP looks up the user's S3 credentials based off HCP account credentials sent to CAP. If the check passes, CAP then sends the S3 credentials to a predefined AWS STS endpoint. STS, in turn, issues a temporary token which CAP sends back to HCP.

C2S CAP authentication can only be used with the S3 compatible component. In order to use C2S CAP authentication you need to provide an account certificate.

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the Storage > Certificates & Keys page, under the Account Certificates panel, click Browse and navigate to the location of your C2S CAP authentication certificate.
2. Click Upload Certificate.
3. Click Next.
4. Review your certificate information.
5. Click Finish.
   Note: To upload an account certificate, you need the administrator role.

Pausing and resuming an extended storage component

When an extended storage component is in use, you can pause all read and write operations on the associated extended storage at any time.

In certain situations, the storage that is represented by an extended storage component might become temporarily inaccessible. Reasons for the temporary inaccessibility can include scheduled maintenance or an unforeseen problem with an extended storage device or cloud-storage-service endpoint. If this situation occurs, you might need to temporarily pause all read and write operations on the storage component.

While a storage component is paused, the associated extended storage is unavailable for storage tiering and does not attempt to communicate with that device or service. Any alerts that would normally be generated by attempts to communicate with the inaccessible extended storage device or cloud-storage-service endpoint are not displayed when the component is paused. When an extended storage component is resumed, the associated storage becomes available for storage tiering, and HCP resumes attempting to communicate with the extended storage device or cloud storage endpoint. If such attempts fail, HCP displays the applicable alerts on the Components panel on the Storage page.

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component that you want to pause or resume.
3. At the top of the panel that opens, click the Manage tab.
4. On the Manage panel, take one of these actions:
   - To pause a component, click Pause Component. HCP pauses the component, and the panel displays Resume Component.
   - To resume a component that is currently paused, click Resume Component. HCP attempts to resume communications with the component, and the panel displays Pause Component.

Deleting or abandoning an extended storage component

If the storage that's represented by an extended storage component is not currently being used to store objects in any namespaces defined on the HCP system, you can safely delete that storage component.

If, however, the storage that's represented by an extended storage component is currently being used to store object data, you cannot delete that component. Instead you need to either retire that component or abandon it.

When you retire an extended storage component, HCP migrates the data off that component and then deletes that component from the system.

When you abandon an extended storage component, HCP deletes that component from the system without attempting to migrate any of the stored data off the extended storage component. This operation is not recommended because it may result in data loss. If the only existing copies of the data for a given object are stored on a single extended storage component, when you abandon that component, the object data becomes permanently inaccessible to HCP.

Retiring and deleting a component is a much safer alternative to abandoning that component, as retiring a component ensures that the data stored on that component remains protected at the applicable levels. You should consider abandoning an extended storage component only as a last resort and only after you've taken the necessary steps to ensure that the data stored on the component exists elsewhere in the HCP system.

Deleting an unused extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component that you want to delete.
3. At the top of the panel that opens, click the Manage tab.
4. On the Manage panel, click Delete Component.

Abandoning an extended storage component

To view the Storage page, you need the monitor or administrator role. To create, modify, or delete extended storage components and extended storage pools, you need the administrator role.

1. On the left side of the Storage page, click the Components tab.
2. On the Components panel, click the table row that contains the name of the component that you want to abandon.
3. At the top of the panel that opens, click the Manage tab.
4. On the Manage panel, click Abandon Component.

Working with HCP S Series storage pools

HCP uses HCP S Series storage pools to represent logical groups of storage components that can be used as storage tiers. Each storage pool consists of one or more storage components that are used to access the same type of storage.

When storing objects on S Series Nodes, HCP uses all the storage in all the S Series Nodes that are contained in the storage pools. The total capacity of a given storage pool is the total amount of space remaining in all S Series Nodes connected to the HCP system.

You use the Storage section of the System Management Console to create, modify, manage, delete, and retire HCP S Series storage pools. You also use the Storage section to monitor the health, availability, capacity, and usage of all the S Series Nodes associated with the storage pool.

Creating an HCP S Series storage pool

Use the Create Pool wizard on the Storage page to create and configure a storage pool.

To create an HCP S Series storage pool, you need the administrator role.

1. In the top-level menu of the System Management Console, select Storage.

   The Storage page opens to the Overview tab.

2. Click the Pools tab, and then click Create Pool

   The Get Started wizard opens.

3. In the Pools field, select HCP S Series.
4. Click Go.

   The Create Pool wizard opens.

5. In the Name field, type a name for the storage pool.
6. Optional: In the Description field, type a description for the storage pool, and then click Next.

   The Allocation page opens.

7. Select all the storage components that you want to allocate to the pool.
8. To compress object data that is stored in the buckets in the storage pool, select Compress data at rest.
9. Optional: If you want the Content Verification service to run on the new HCP S Series storage pool, select Content Verification, and then click Next.
10. Take one of these actions from the Review page:

    - If the HCP S Series storage pool configuration information is correct, click Finish.
    - If the HCP S Series storage pool configuration information is not correct:

      a. Use the Previous and Next buttons to navigate through the wizard and change any incorrect settings.
      b. When you are finished making changes, navigate back to the Review page and click Finish.

Modifying an HCP S Series storage pool

Use the Storage Pools page to view and modify the configuration of any HCP S Series storage pool.

Use the Storage Pools page to perform the following tasks:

- Change one or more configuration settings that were specified when the pool was created.
- Add one or more storage component buckets to an HCP S Series storage pool.
- Delete one or more buckets from an HCP S Series storage pool.

Modifying the settings of an HCP S Series storage pool

Use the Storage Pools page to modify the configuration settings of an HCP S Series storage pool.

To modify an HCP S Series storage pool, you need the administrator role.

1. Click Storage > Pools.

   The Pools page opens.

2. Click the table row corresponding to the name of the pool that you want to modify.
   Note:

   To enable balancing on an HCP S Series storage pool, you must choose a pool that has multiple HCP S Series storage components.

   The Overview page opens for the selected pool.

3. Click the Setting tab.
4. Modify the pool settings.
5. Click Update Settings.

Adding buckets to an HCP S Series storage pool

Use the Storage Pools page to add buckets to an existing HCP S Series storage pool.

To add buckets to an HCP S Series storage pool, you need the administrator role.

1. On the Storage > Pools page, click the table row corresponding to the name of the pool to which you want to add one or more buckets.

   The Overview page opens for the selected pool.

2. Click the Buckets tab.
3. Select the buckets that you want to add to the storage pool.

   You cannot select buckets that are used by other storage pools.

4. Click Update Settings.

Removing buckets from an HCP S Series storage pool

Use the Storage Pools page to delete buckets from an HCP S Series storage pool.

Deleting buckets from an HCP S Series storage pool does not remove them from the HCP system. S Series Node buckets that are not associated with a pool can be added to a pool.

To delete buckets from an HCP S Series storage pool, you need the administrator role.

1. On the Storage > Pools, click the table row corresponding to the name of the pool from which you want to delete buckets.

   The Overview page opens for the selected pool.

2. Click the Buckets tab.
3. Click to clear the checkboxes for the buckets you want to remove from the storage pool.
4. Click Update Settings.

Deleting an HCP S Series storage pool

If the storage represented by an HCP S Series storage pool is not used to store objects in any namespaces defined on the HCP system, you can delete the storage pool.

In contrast, if the storage represented by an HCP S Series storage pool is used to store object data, you must first retire the storage pool by migrating all the data to another location.

1. In the System Management Console, click Storage > Pools.
   The Storage Pools page opens.
2. Click the delete control beside the unused storage pool that you want to delete.

   The Confirm: Delete dialog box opens.

3. Click Delete.

Working with extended storage pools

HCP uses *extended storage pools* to represent logical groups of storage components that can be used as storage tiers.

Each extended storage pool consists of one or more extended storage components that are used to access the same type of storage. A storage pool contains one or more extended storage component access points (mount points, buckets, or containers).

Each storage tier that is defined for a namespace by its service plan typically consists of only one storage pool; however, a tier can be configured to use multiple storage pools. To store objects on an extended storage tier, HCP uses all of the storage that is allocated to all of the extended storage component access points (mount points, buckets, or containers) that are contained in the storage pools that are configured for the storage tier. Therefore, the capacity of a given extended storage pool is the total amount of space that can be accessed using the extended storage component access points included in the pool. You can add access points to an extended storage pool at any time, thereby increasing the capacity of the pool.

Each extended storage component provides HCP with the information it needs to use one or more mount points, buckets, or containers to access and use the storage that’s represented by that extended storage component. However, HCP can actually use the storage that is represented by a given extended storage component only if at least one of its access points is contained in a storage pool that is included in at least one storage tier that is defined for a namespace by its service plan.

Creating an extended storage pool

Use the Create Pool wizard on the Storage page to create and configure an extended storage pool.

Each time you use the Storage page to access the Create Pool wizard, you are prompted to select the type of extended storage pool that you want to create. The System Management Console then dynamically builds the pages in the Create Pool wizard to present only the fields you need to use to configure HCP to access and use the specified type of extended storage pool.

1. On the left side of the Storage page, click the Pools tab.
2. On the Pools panel, click Create Pool.

   The Get Started wizard opens.

3. In the Get Started wizard, click the arrow to display a list of supported extended storage pools, and select the type of pool that you want to create.
   Note:

   To create a ThinkOn cloud storage pool, select ThinkOn as the type of pool to configure. Then follow the same procedure as you do to configure other S3 compatible storage pools.

4. Click Go.

   The Get Started wizard exits and the System Management Console opens the Create Pool wizard for the type of extended storage pool that you selected.

5. Use the fields on each page of the Create Pool wizard to specify the extended storage component access points that you want to include in the pool:
   - To create an Amazon S3 storage pool, specify the configuration information that is described in Amazon S3 and S3 compatible storage pools. Then return to this procedure.
   - To create a Google Cloud storage pool, specify the configuration information that is described in Google Cloud storage pools. Then return to this procedure.
   - To create a Microsoft Azure storage pool, specify the configuration information that is described in Microsoft Azure storage pools. Then return to this procedure.
   - To create a S3 compatible storage pool, including a ThinkOn cloud storage pool, specify the configuration information that is described in S3 compatible storage pools. Then return to this procedure.
   - To create an NFS storage pool, specify the configuration information that is described in NFS storage pools. Then return to this procedure.
6. Click Next to save the information you entered and advance to the last page of the wizard.
7. On the Review page, take one of these actions:

   - If the extended storage pool configuration information that you entered is correct, click Finish at the bottom of the page.

   - If the extended storage pool configuration information is not correct, use the Previous and Next buttons at the bottom of each page to navigate through the pages in the wizard and change any settings that are not correct.

8. When you are finished making changes to the storage pool configuration settings, navigate to the Review page and click Finish.

   The wizard closes. The System Management Console displays the Pools panel on the Storage page. This panel displays a list of all of the primary storage pools and extended storage pools that exist on the HCP system and provides information about the current status of each pool, including the one you just created.

You created and configured the extended storage pool.

Each extended storage pool provides HCP with the information it needs to access and use the storage that is represented by that pool. However, HCP can use the storage that is represented by a given pool only if it is included in at least one storage tier that is defined for a namespace by its service plan.

Amazon S3 and S3 compatible storage pools

Each Amazon S3 or S3 compatible storage pool contains one or more buckets that are associated with specific Amazon S3 or S3 compatible storage components. Each storage pool includes all of the storage that is allocated to all of the buckets in the pool.

To enable HCP to access the storage that is represented by the storage pool, you specify the following information when you create the component:

- The storage pool name.
- Optionally, a description of the pool.
- Whether you want HCP to compress object data that's stored on the storage that's allocated to the buckets in the storage pool.
- Whether you want HCP to encrypt object data that's stored on the storage that's allocated to the buckets in the storage pool. If encryption is disabled for the system, this option is not visible.
- For each bucket you want to include in the storage pool:
  - The name of the Amazon S3 or S3 compatible storage component that represents the endpoint that's used to access the bucket
  - The account label used to identify the Amazon S3 Web Services user account that's used to access the storage associated with the bucket
  - The name of the bucket

Note: At any given time, a bucket can be included in only one storage pool.

Each bucket you add to a new Amazon S3 or S3 compatible storage pool must be empty or have only HCP data in it.

A storage pool is compliant only if all of the buckets in the pool are associated with compliant Amazon S3 or S3 compatible storage components.

Google Cloud storage pools

Each Google Cloud storage pool contains one or more buckets that are associated with specific Google Cloud storage components. Each Google Cloud storage pool includes all of the storage that's allocated to all of the buckets in the pool.

To enable HCP to access the storage that's represented by a Google Cloud storage pool, when you create that component, you specify the following information:

- The storage pool name.
- Optionally, a description of the pool.
- Whether you want HCP to compress object data that's stored on the storage that's allocated to the buckets in the storage pool.
- Whether you want HCP to encrypt object data that's stored on the storage that's allocated to the buckets in the storage pool. If encryption is disabled for the system, this option is not visible.
- For each bucket you want to include in the storage pool:
  - The name of the Google Cloud storage component that represents the Google Cloud Platform endpoint that's used to access the bucket
  - The account label used to identify the Google Cloud Platform user account that's used to access the storage associated with the bucket
  - The name of the bucket

Note: At any given time, a bucket can be included in only one storage pool.

Each bucket you add to a new Google Cloud storage pool must be empty or have only HCP data in it.

A storage pool is compliant only if all of the buckets in the pool are associated with compliant Google Cloud storage components.

Microsoft Azure storage pools

Each Microsoft Azure storage pool contains one or more containers that are associated with specific Microsoft Azure storage components. Each Microsoft Azure storage pool includes all of the storage that is allocated to all of the containers in the pool

To enable HCP to access the storage that is represented by a Microsoft Azure storage pool, when you create that component, you specify the following information:

- The storage pool name.
- Optionally, a description of the pool.
- Whether you want HCP to compress object data that is stored on the storage that is allocated to the containers in the storage pool.
- Whether you want HCP to encrypt object data that is stored on the storage that is allocated to the containers in the storage pool. If encryption is disabled for the system, this option is not visible.
- For each container you want to include in the storage pool:
    - The name of the Microsoft Azure storage component that represents the Microsoft Azure endpoint that is used to access the container
    - The account label used to identify the Microsoft Azure user account that is used to access the storage associated with the container
    - The name of the container

Note: At any given time, a container can be included in only one storage pool.

Each container you add to a new Microsoft Azure storage pool must be empty or have only HCP data in it.

A storage pool is compliant only if all of the containers in the pool are associated with compliant Microsoft Azure storage components.

NFS storage pools

Each NFS storage pool contains one or more mount points that are associated with specific NFS storage components. Each NFS storage pool includes all of the storage that's accessed using the NFS mount points included in the pool.

To enable HCP to access the storage that's represented by an NFS storage pool, when you create that component, you specify the following information:

- The storage pool name.
- Optionally, a description of the pool.
- Whether you want HCP to compress object data that's stored on the storage that's accessed using the NFS mount points in the storage pool.
- Whether you want HCP to encrypt object data that's stored on the storage that's accessed using the NFS mount points in the storage pool. If encryption is disabled for the system, this option is not visible.
- For each NFS mount point you want to include in the storage pool:
    - The name of the NFS storage component that represents the physical storage device that's accessed using the NFS mount point
    - The full path name of the directory that you want to access using the NFS mount point

Note: At any given time, an NFS mount point can be included in only one storage pool.

An NFS storage pool is compliant only if all of the NFS mount points in the pool are associated with compliant NFS storage components.

When you add an NFS mount point to a new or existing NFS storage pool, HCP creates that mount point and mounts the applicable storage volume (called an NFS volume or an external storage volume) on a node in the HCP system. HCP then adds that NFS volume to the NFS storage pool.

HCP uses a round-robin algorithm to determine which node to associate with each new NFS volume that's added to an NFS storage pool. This method of assigning NFS volumes to the nodes in the HCP system ensures that the volumes are distributed evenly among the nodes.

If the node with which an NFS storage volume is associated becomes unavailable, that volume also becomes unavailable. HCP does not reassign the volume to a different node. When the node returns to service, the volume becomes available again.

In the HCP System Management Console, you can use the Hardware and Storage Node pages to view information about the NFS storage volumes (called external storage volumes) that are associated with each node in the HCP system.

Considerations for using NFS volumes

These considerations apply to using NFS volumes with HCP:

- HCP can use multiple NFS shares from a single device that's represented by an NFS storage component. Keep in mind, however, that the larger the number of shares HCP uses, the greater the I/O load on the device.
- Typically, you specify export options for a share according to the standards for your site. However, if HCP is unable to mount the extended storage volume that you created as an NFS share, you may need to change the export options. After changing the export options, you need to export the NFS share again.
- For each NFS mount point that's associated with an NFS storage component, you can specify more mount options than the required ones. You might do this, for example, to set the network block size for read or write requests to the optimal size for the storage device that's represented by the NFS storage component. However, if HCP is unable to mount the extended storage volume that you created as an NFS share, you may need to change the additional mount options that you specified.
- If the share for an NFS volume becomes unavailable (for example, because the extended storage device that's hosting the share is inaccessible), HCP tries periodically to remount the volume. If, after the share is available again, the remount fails, you can try to manually remount the NFS volume.

Manually remount the NFS volume

1. On the left side of the Storage page, click Components.
2. In the components list, click the name of the NFS storage component that is associated with the NFS volume that you want to remount.
3. At the top of the panel that opens, click the Mount Points tab.
4. On the Mount Points panel, in the table row that contains the NFS mount point that corresponds to the NFS volume you want to remount, click the remount control ( ).

   HCP attempts to remount the NFS volume. If the remount fails, contact your authorized HCP service provider for help.

   To see which node the NFS volume is associated with, hover your cursor over the status icon for the mount point on the Mount Points panel.

Considerations for using NFS volumes (cont.)

- You cannot move an NFS volume from one NFS storage pool to another.
- You cannot control which NFS volume HCP writes data to within an NFS storage pool.
- When HCP creates a mount point for a specific NFS volume, HCP stores a file named .__hcp_uuid__ in the shared directory on the device that's represented by the NFS storage component associated with that mount point. This file uniquely associates the NFS shared directory with the NFS volume. As a result:

- HCP creates only one NFS storage volume for any given exported share.
- If you delete an NFS mount point from an NFS storage component, the associated exported share cannot be reused as is. This means that any data remaining in the NFS volume associated with the mount point becomes permanently inaccessible to HCP.
- To reuse an exported share after the associated NFS mount point is deleted from HCP, you first need to delete any remaining files from the shared directory, including the .__hcp_uuid__ file.
- If you inadvertently delete the .__hcp_uuid__ file from an NFS shared directory that contains other HCP data, HCP can no longer use the exported share. Contact your authorized HCP service provider for help in recreating the file.
- When you back up an NFS shared directory that's associated with an NFS volume, you need to ensure that the .__hcp_uuid__ file is included in the backup operation. This ensures that the file still exists in the directory after a restore operation.

Reusing the exported share

A situation can occur in which HCP can access an exported share but cannot mount the associated NFS volume. In this case, if the .__hcp_uuid__ file is the only file in the shared directory on the extended storage device on which the data in the NFS volume is stored, you can reuse the exported share.

1. Delete the mount point that's associated with the NFS volume from the NFS storage component that represents the device on which the NFS volume is stored.
2. Delete the .__hcp_uuid__ file from the shared directory.
3. Create a new NFS mount point for the share on the same NFS storage component from which you deleted the mount point in step 1.

Manually remounting the NFS volume

If an NFS volume becomes inaccessible due to a disk failure on the extended storage device on which the data in the NFS volume is stored, you need to replace the disk, restore the data from backup, and then export the NFS share again.

In this case, the NFS volume needs to be remounted. If HCP doesn't remount the volume automatically, you can try to manually remount the NFS volume.

1. On the left side of the Storage page, click Components.
2. In the components list, click the name of the NFS storage component that's associated with the NFS volume that you want to remount.
3. At the top of the panel that opens, click the Mount Points tab.
4. On the Mount Points panel, in the table row that contains the NFS mount point that corresponds to the NFS volume you want to remount, click the remount control ( ).

   If the manual remount fails, try restarting the node with which the NFS volume is associated. To see which node the NFS volume is associated with, hover over the status icon for the mount point on the Mount Points panel.

Considerations for using NFS volumes (last part)

- You can restore an NFS shared directory to a different location from where it was originally. If you do this, you need to modify the configuration of the associated NFS mount point to point to the new location.
- If HCP cannot create, mount, or use an NFS volume and you've already determined that the permissions for the shared directory, the export options for the share, the mount point configuration on the associated NFS storage component in HCP, and the mount options for the mount point are all correct, the problem may exist on the extended storage device that's represented by the NFS storage component on which you configured the mount point. To resolve such problems:
  - Ensure that the NFS share has been exported on the device.
  - Ensure that the NFS server is running on the device.
  - Ensure that any NFS security software on the device is not blocking access by any of the HCP nodes.
  - Check the system log file on the device for messages indicating device errors. Then correct those errors.

If HCP still cannot create, mount, or use the volume, contact your authorized HCP service provider for help.

Modifying an extended storage pool

You can use the Pools panel on the Storage page to view and modify the configuration of any extended storage pool. To display this panel, click the Pools tab on the left side of the Storage page.

You can use the Pools panel to modify the configuration of any extended storage pool in any of the following ways:

- Change one or more of the configuration settings that are specified when the pool is first created:
  - Amazon S3 and S3 compatible storage pools configuration settings
  - Google Cloud storage pools configuration settings
  - Microsoft Azure storage pools configuration settings
  - Amazon S3 and S3 compatible storage pools configuration settings
  - NFS storage pools configuration settings
- Add one or more storage component access points (mount points, buckets, or containers) to an extended storage pool.
- Delete one or more storage component access points from an extended storage pool.

Modifying the configuration settings used for an extended storage pool

1. On the left side of the Storage page, click the Pools tab.
2. On the Pools panel, click the table row that contains the name of the pool that you want to modify.
3. At the top of the panel that opens, click the Settings tab.
4. On the panel that opens, use the fields to change any of the settings that are currently used for the pool.
5. Click Update Settings.

Adding access points to an extended storage pool

You can add one or more access points (mount points, buckets, or containers) to an existing extended storage pool.

1. On the left side of the Storage page, click the Pools tab.
2. On the Pools panel, click the table row that contains the name of the pool to which you want to add one or more access points.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's contained in the pool (Mount Points, Buckets, or Containers).

   The *AccessPointType* panel opens, displaying a table that contains a list of existing access points (mount points, buckets, or containers) that can be included in the type of storage pool that you're currently configuring. The access points that are currently included in the pool are selected.

4. Select each existing access point that you want to add to the storage pool.
5. Click Update Settings.

Deleting access points from an extended storage pool

You can delete one or more unused access points (mount points, buckets, or containers) from an existing extended storage pool.

1. On the left side of the Storage page, click the Pools tab.
2. On the Pools panel, click the table row that contains the name of the pool from which you want to delete one or more access points.
3. At the top of the panel that opens, click the tab that corresponds to the type of access point that's contained in the pool (Mount Points, Buckets, or Containers).

   The *AccessPointType* panel opens, displaying a table that contains a list of existing access points (mount points, buckets, or containers) that can be included in the type of storage pool that you're currently configuring. The access points that are currently included in the pool are selected.

4. Deselect each existing access point that you want to delete from the storage pool.
   Note:

   After you store data on an NFS volume, you cannot delete it from its NFS storage pool. Also, you cannot delete all of the access points in a storage pool if that pool is currently used for a storage tier that's defined for a namespace by its service plan.

5. Click Update Settings.

Remounting an NFS volume

If an NFS volume is experiencing problems, you can manually try to remount that NFS volume. Before doing that, however, you should ensure that the device hosting the NFS volume and the network connection to that device are functioning properly. You should also ensure that the exported share that corresponds to the NFS volume is configured correctly on the host device.

HCP can take up to a minute to respond to a remount request.

1. On the left side of the Storage page, click Components.
2. In the components list, click the name of the NFS storage component that's associated with the NFS volume that you want to remount.
3. At the top of the panel that opens, click the Mount Points tab.
4. On the Mount Points panel, in the table row that contains the NFS mount point that corresponds to the NFS volume you want to remount, click the remount control ( ).

If the manual remount fails, try restarting the node with which the NFS volume is associated. To see which node the NFS volume is associated with, hover your cursor over the status icon for the mount point on the Mount Points panel.

Deleting an extended storage pool

If the storage that is represented by an extended storage pool is not currently being used to store objects in any namespaces defined on the HCP system, you can safely delete that storage pool.

If, however, the storage that is represented by an extended storage pool is currently being used to store object data, you cannot delete that pool. Before you can delete a storage pool, you need to first remove the extended storage pool from all storage tiers that currently include that pool and then retire the storage pool by migrating all of the data off it.

When you retire an extended storage pool, HCP migrates the data off that pool and then deletes that pool from the system.

1. On the left side of the Storage page, click the Pools tab.

   The Pools pane opens, showing a list of storage pools that are currently defined on the HCP system. A delete control ( ) appears in the row for each unused storage pool.
2. Click the delete control for any unused extended storage pool to delete it from the HCP system.

Retiring storage

You can use the Storage > Retirement page in the System Management Console to retire primary storage devices, HCP S Series storage pools, HCP S Series storage components, HCP S Series storage volumes (buckets), extended storage pools, extended storage components, and extended storage volumes that are associated with specific access points (mount points, buckets, and containers).

Retiring primary storage devices

You can use either the Migration page or the Storage page in the System Management Console to migrate data off selected storage nodes in either an HCP with internal storage or HCP with SAN-attached storage system or off selected storage systems in an HCP with SAN-attached storage system in preparation for retiring those devices.

The Migration service is not available for HCP VM systems.

During a data migration, the Migration service copies objects and, if applicable, the metadata query engine index from the selected devices to free storage on the remaining devices. Before you start a data migration, you need to ensure that those devices have enough unused capacity to hold the data to be migrated.

After copying an object, the Migration service deletes the object from the source device. After the migration is complete, you can submit a request to your authorized HCP service provider to finalize the migration and remove the retired devices from the system.

Important:

After the migration of data off a storage node in an HCP with internal storage system is finalized, the system can never again include a node with the same fourth octet in its back-end IP address as that node had.

Retiring a node is not part of the normal procedure for replacing a node that has failed or for upgrading to newer hardware. In these cases, the new node can use the same back-end IP address as the one being replaced.

The Migration service runs only when you explicitly start a data migration. When the migration is complete, the service stops automatically.

When you start a data migration, the selected nodes or storage systems automatically become read-only (except for allowing the Migration service to delete objects). After the migration is complete, they remain read-only.

When you start a migration of data off selected nodes in a HCP with internal storage system, HCP automatically removes any NFS volumes from those nodes and associates those volumes with other nodes in the system.

Important:

To prevent data loss in namespaces that are not being replicated and that have service plans that set the ingest tier DPL to 1, always migrate data off a device before submitting a request to your authorized HCP service provider to remove the device from the HCP system.

Before starting a primary storage retirement

Typically, for a HCP with internal storage system, before starting a data migration, you submit a request to your authorized HCP service provider to add new nodes to the HCP system in order to maintain (or increase) the system storage capacity. However, if the nodes not selected for migration have sufficient free space to accommodate all the data to be migrated, adding new nodes before the data migration is not required.

For a HCP with SAN-attached storage system, before starting a data migration, your SAN storage administrator, working in conjunction with your authorized HCP service provider, needs to add logical volumes (LUNs) from new or existing storage systems to any nodes on which all the existing LUNs on all the existing arrays are being retired. Migrated data, however, can be written to any node, and does not necessarily have to be written to the same node from which the data is being migrated.

The HCP system cannot be upgraded while a data migration is in progress. Before the system can be upgraded, you need to either allow the migration to finish or cancel the migration. If you cancel the migration, you can configure a new migration of data off the same devices after the system is upgraded.

Using the Retire Primary Storage wizard to perform a data migration

Important: This section describes how to use the Retire Primary Storage wizard to migrate data off one or more primary storage devices, but it does not provide a detailed description of the entire data migration process.

To retire one or more primary storage devices, you can use the Retire Primary Storage wizard on the Retirement panel to specify the devices you want to retire and then configure and run a data migration to move all the data off the storage devices you want to retire and onto one or more other primary storage devices.

When configuring a data migration on an HCP with internal storage system, you select nodes to be retired. When configuring a data migration on an HCP with SAN-attached storage system, you can either retire an entire storage system or individual nodes.

You can use the Storage page to perform a data migration in preparation for retiring primary storage.

1. On the left side of the Storage page, click Retirement.
2. On the Retirement panel, click Retire Storage.

   The Get Started wizard opens. You use this wizard to select the type of storage you want to retire. After you select a type of storage, the System Management Console dynamically builds either the Retire Primary Storage wizard or the Retire Extended Storage wizard, depending on the type of storage you selected.

3. In the Get Started wizard, click the arrow and select Primary Storage from the dropdown list.
4. Click Go.

   The Get Started wizard exits, and the Retire Primary Storage wizard opens.

5. On the Select page of the Retire Primary Storage wizard, in the Select Hardware for Retirement section, select the HCP with internal storage system storage nodes you want to retire. If you're retiring an HCP with SAN-attached storage system, either select Retire Entire Array and select the storage systems you want to retire or select Retire Specific Hardware Nodes and select the nodes you want to retire.

   To clear your selections and start over, click Cancel.

6. Click Next.
   The Review page of the Retire Primary Storage wizard opens, displaying step two of the migration configuration process (Review configuration summary and confirm). The Configuration Summary section on this page in the wizard indicates whether the migration configuration is acceptable.
   - When you click Next, HCP checks that the system is in a valid state to perform the migration. This includes checking for degraded RAID groups. This check can take up to 90 seconds.
   - Certain hardware errors, such as a degraded RAID group on a source or target node, prevent you from configuring a data migration. In such cases, you need to fix the problem before you can continue.

   If the configuration is not acceptable, you can click view details in the Configuration Summary section to display the specific reasons why. You can also click Configuration Report to download the configuration summary and details to a file. The default name for this file is Configuration-Report.txt.

   The Configuration Details section on the Review page in the Retire Primary Storage wizard lists the HCP with internal storage system nodes or the HCP with SAN-attached storage system storage systems that are selected for migration

7. Take one of these actions:

   - To change the list of selected nodes or storage arrays, click Previous to return to the Select page in the wizard. Use this page to change your selections. Then click Next to return to the Review page in the wizard.

   - To cancel the migration and exit the wizard, click Cancel.

   - If the list of selected storage devices is correct, and you want to perform the data migration, continue on to step 8.

8. Optionally, add a description of the data migration and/or change the performance level for the Migration service:
   a. To add a description, click Add description.
      In the text box that opens, type a description of the migration. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
   b. To change the performance level, in the Performance Level field, select Low, Medium, or High. The higher the performance level, the greater the load on the HCP system.
9. Click Finish.

   The Migration service begins the data migration process, and the wizard exits. The Migration service reports its progress on the Retirement panel on the Storage page. You can refresh this page at any time to view the current status of the data migration.

   If any nodes become unavailable while the Migration service is running, the service stops migrating data. When those nodes become available, the service automatically starts migrating data again.

   You can use the Retirement panel on the Storage page to manage the Migration service throughout the entire data migration process. At any time during the migration, you can click Retirement Settings to change the performance level of the retirement process.

   You can also click Primary running to display the controls that you can use to change the performance level of the migration, pause and resume the migration as needed, or cancel the migration.

   You can use the applicable field in the Overview panel on the Migration page to modify the migration description at any time (for example, to record when and how long the migration was paused).

10. When the data migration is complete (that is, the migration status is Migrated), if a migration report is available, review it.

This report identifies tenants that own namespaces containing unacknowledged irreparable objects. For the default tenant and for HCP tenants that are configured to allow system-level users to manage them, the report also lists the unacknowledged irreparable objects in those namespaces.

If the Migration service encounters one or more objects that it cannot migrate, it marks those objects as irreparable (if they weren't already marked that way).

If the data migration statistics show that not all objects were migrated, contact your authorized service provider for help.

11. Submit a request to your authorized service provider to finalize the migration and remove the retired hardware.

Retiring HCP S Series and extended storage pools, components, and volumes

You can use the Storage > Retirement page in the System Management Console to retire both HCP S Series and extended storage pools, storage components, and storage volumes that are associated with storage component access points (buckets, containers, or NFS volumes). If you are retiring HCP S Series components and pools that are selected as the ingest tier of a service plan, their replacements are limited to other HCP S Series components and pools.

Before retiring an HCP S Series or extended storage, you must remove the bucket(s) associated with the component, storage pool, or volume being retired from the storage pool. To do this, clear the checkbox associated with the bucket(s) in the storage pool. Clearing the checkbox renders the bucket read-only. While HCP can still read data from the bucket, it cannot write to it. HCP does not automatically remove the bucket from the storage pool marked for retirement.

When you retire an HCP S Series or extended storage that's associated with a specific storage pool, component, or volume, HCP migrates all the data off that storage and moves it to the replacement storage that you specify.

You can use the Storage > Retirement page to retire an HCP S Series or extended storage pool, component, or volume.

1. On the Storage > Retirement page, click Retire Storage.

   The Get Started wizard opens. You use this wizard to select the type of storage you want to retire. After you select a type of storage, the System Management Console dynamically builds either the Retire S Series Storage, or the Retire Extended Storage wizard, depending on the type of storage you selected.

2. In the Get Started wizard, click the arrow and select either S Series Storage or Extended Storage from the dropdown list.
3. Click Go.
4. On the Select page of the Retire S Series Storage or Retire Extended Storage wizard, use the fields to specify the S Series or extended storage pool, component, or volume that you want to retire:

   In the What do you want to retire? field, select the applicable option to indicate whether you want to retire a storage pool, component, or volume.

   Depending on your selection, the wizard displays up to three different fields: Pool, Component, and Volume.

   Use the Pool, Component, or Volume field to select the specific storage pool, component, or volume you want to retire.

   If multiple fields appear, you can use the Pool field to filter the lists of components and volumes, and you can use the Component field to filter the list of volumes.

5. Click Finish to exit the wizard and start the retirement process.

   The Migration service checks to see whether the selected pool, component, or volume is eligible for retirement.

   If the storage is not eligible for retirement, the Migration service reports the problem on the Retirement tab. If this happens, you need to fix the problem and then restart the storage retirement process.

   If the storage is eligible for retirement, the Migration service starts the retirement process:

   - If the storage does not have any data on it, the Migration service simply deletes the selected pool, component, or volume.
   - If a selected storage pool has data on it, the service migrates all object data off that pool and onto the replacement pool you selected. The service then deletes the storage pool you selected for retirement.
   - If a selected storage component has data on it, the service migrates all of the data off that component. The service moves this data onto one or more of the other components that are contained in the same storage pool as the component you're retiring. The service then deletes the storage you selected for retirement.
   - If a selected storage volume has data on it, the service moves all of the data off that volume. The service moves that data onto one or more of the other volumes that are stored on the same storage component as the one you're retiring. The service then deletes the volume you selected for retirement.

   The Migration service reports the progress of the HCP S Series or extended storage retirement on the Storage > Retirement page. You can refresh this page at any time to view the current status of the HCP S Series or extended storage pool, component, or volume retirement.

   If you're retiring HCP S Series or extended storage that has data on it, you can use the Storage > Retirement page to manage the Migration service throughout the entire data migration process. At any time during the migration, you can click Retirement Settings to display the controls that you can use to change the performance level of the migration, pause and resume the migration as needed, or cancel the migration (and the retirement). You can also use the applicable field in the Retirement Settings section to modify the retirement description at any time (for example, to record when and how long the data migration was paused).

About service plans

Each namespace has a service plan that defines both a storage tiering strategy and a data protection strategy for the objects in that namespace. At any given point in the lifecycle of an object, its storage tiering strategy specifies the types of storage on which copies of that object must be stored, and its data protection strategy specifies the number of object copies that must be stored on each type of storage.

For the purposes of storage tiering and data protection, HCP treats these as individual objects:

- Parts of multipart objects
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

The service plan for a given namespace defines one or more tiers of storage that can be used to store objects in that namespace. For each object in the namespace, at any given point in the object lifecycle, the service plan specifies the criteria that determine which storage tiers must be used to store copies of that object and the number of copies of that object that must be stored on each tier.

Primary running storage is designed to provide both high data availability and high performance for object data storage and retrieval operations. To optimize data storage price/performance for the objects in a namespace, you can configure the service plan for that namespace to define S Series storage as the ingest tier or create a storage tiering strategy that specifies multiple storage tiers.

By default, HCP stores every object on primary running storage, so every service plan automatically defines primary running storage as the initial storage tier, called the *ingest tier*. If the HCP system is using HCP S Series storage, this storage can be used as the ingest tier instead of primary running storage. This causes object data to be written directly to the S Series Nodes. Even if you set HCP S Series storage as the ingest tier, metadata is stored on primary running storage.

Storage tiers

The service plan for a given namespace defines one or more storage tiers for that namespace. For each storage tier, the service plan specifies the data protection level (DPL) and the primary running storage metadata protection level (MPL) for each storage tier:

- The *DPL* for a given storage tier is the number of copies of the object data that HCP must maintain for each object that's stored on that tier.
- The *MPL* for a given storage tier is the number of copies of the object metadata that HCP must maintain on primary running storage for each object that's stored on the tier.

For any given storage tier, the primary running storage MPL must be equal to or greater than the DPL.

Note: For the purpose of storage tiering, HCP treats parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of multipart objects as individual objects.

Every service plan initially defines primary running storage as the initial storage tier, called the *ingest tier*, and specifies a DPL setting and an MPL setting for that tier. If the HCP system is using HCP S Series storage, you can define HCP S Series storage as a service plan ingest tier to be used as an alternative to primary running storage. If an HCP S Series pool, or pools, is selected as the ingest tier, DPL copies of objects are written directly to HCP S Series storage. MPL copies of object metadata are written to primary running storage.

Tiering objects that are subject to erasure coding

HCP does not tier objects that are subject to erasure coding but not yet erasure coded unless the target tier is primary running storage, an S Series Node, or primary spindown storage. Instead, on any given system in an erasure coding topology, if the system initially receives a full copy of the data for an object that's subject to erasure coding, HCP waits to tier the object until the full copy of the data has been reduced to a chunk.

After the system has a chunk for the object, HCP can move the chunk to the applicable tier, according to the tiering strategy in the service plan associated with the namespace that contains the object. If the object was due to be tiered before the full copy of the data was reduced to chunk, HCP immediately moves the chunk to the applicable tier.

If a system initially receives a chunk for an object, that chunk is immediately subject to the tiering strategy in the applicable service plan.

On any given storage tier, for an object that's subject to erasure coding, HCP keeps DPL copies of the full object data or the chunk for the object, as applicable, where DPL is the DPL specified for that storage tier.

DPL settings for objects and default-namespace directories

Objects have a DPL setting as part of their metadata. This setting is the DPL for the tier where the object data currently should be stored, according the service plan associated with the namespace that contains the object. If the object is not yet on that tier or if the DPL for the tier changes while the object is on that tier, the actual number of copies of the object data may not immediately match the DPL setting for the object.

Directories in the default namespace also have a DPL setting as part of their metadata. This setting is the DPL for the ingest tier in the service plan associated with the default namespace.

Users and applications can see, but not modify, the DPL setting for an object or directory.

Default ingest tier DPL setting

Each HCP system has a default service plan that's automatically created and configured during the HCP software installation. The default service plan is applied to each tenant and namespace for which another service plan is not explicitly selected.

For any given HCP system, the ingest tier DPL setting that's initially configured for the default service plan is used as the default ingest tier DPL setting for each new service plan that's created on the HCP system. When you create a new service plan, you can choose to use the default ingest tier DPL setting or select a different setting. You can also modify any service plan, including the default service plan, to change the ingest tier DPL setting. However, changing the ingest tier DPL setting used for the default service plan does not change the default ingest tier DPL setting that's used for new service plans.

Typically, the default ingest tier DPL setting used for service plans created on an HCP system is the optimal setting for the type of physical storage that the HCP system uses. For HCP with internal storage systems, the default ingest tier DPL is two. For HCP with SAN-attached storage systems, for which SAN arrays provide a high level of data protection, and for VM systems, for which the virtual environment provides node failover capabilities, the default ingest tier DPL is one.

The default ingest tier DPL setting used for all service plans that are created on an HCP system is the optimal setting for the type of storage used by that system. However, the optimal ingest tier DPL setting that's configured for the service plan that's assigned to a specific tenant or namespace is subject to considerations such as whether the tenant or namespace is being replicated and whether the HCP system owner or the tenant administrator has any particular data protection needs.

On HCP with internal storage systems, by default, service plans can be configured to set the ingest tier DPL to two, three, or four. To enable HCP with internal storage system administrators to configure service plans to set the ingest tier DPL to one, contact your authorized HCP service provider.

Storage tier properties specified in service plans

For each storage tier, including the ingest tier, that's defined for a given namespace, the service plan specifies:

- The storage pools that are used to store copies of object data or chunks for erasure-coded objects on the tier. Each *storage pool* consists of one or more storage components. Each *storage component* represents a type of primary storage (running or spindown), HCP S Series storage, an extended storage device, or a cloud storage service endpoint.
- For each object that's stored on the tier, the number of copies of the object data or of the chunk for an erasure-coded object that HCP must maintain on each storage pool (that is, the DPL).
- For each object that's stored on the tier, the number of copies of the object metadata that HCP must maintain on the ingest tier (that is, the MPL).
- The transition criteria for each tier except for the ingest tier. The *transition criteria* for a storage tier are the rules that determine when one or more copies of each object in the namespace must be stored on the tier:
  - The object age (number of days since ingest) at which one or more copies of the object data must be moved from the previous tier to this tier.

    The age of an object created by a multipart upload is counted from the time the multipart upload was completed.

  - For service plans that define exactly two tiers, including the ingest tier, whether a threshold will be applied to the second tier, and if so, the percentage of ingest tier storage capacity that must be used (the *threshold*) before object data can be moved to the second storage tier.
  - For HCP systems with replication enabled, whether objects must be fully replicated before they can be transitioned from the previous tier onto this tier. If replication is disabled for the HCP system, this transition criterion does not appear in the HCP System Management Console.
- For a namespace that's currently being replicated to another system, whether the copies of the object that are stored on the tier are to be made metadata-only.

  Regardless of the transition criteria that are specified for a metadata-only tier, objects are moved to such a tier only after they are replicated. When a replicated object is moved to a metadata-only tier, all existing copies of the object data are deleted from the current tier and the ingest tier, and HCP stores the specified number of copies of the

object metadata on primary running storage.

Erasure-coded objects never become metadata-only on any systems in the applicable erasure coding topology. If an erasure-coded object reaches a point in its lifecycle where the object should move to a metadata-only tier, the chunk for the object remains on the last tier before the metadata-only tier, and the DPL for that tier still applies to the chunk.

- Whether the data for each object stored on the tier is *rehydrated* (that is, restored on the ingest tier) upon being read from the tier, and if so, the number of days HCP is required to keep a rehydrated copy of object data on the ingest tier.

  Rehydration does not apply to erasure-coded objects. Instead, if the applicable erasure coding topology specifies a restore period, after an erasure-coded object is read, the chunk for the object is restored to a full copy on the ingest tier on the system from which the object was read.

How HCP uses the information in service plans

If the service plan for a given namespace defines only the ingest tier, for each object in that namespace, the Protection service works to ensure that:

- The correct number of copies of the object data are always stored on the ingest tier, which can be primary running storage or HCP S Series storage
- The correct number of copies of the object metadata are always stored on primary running storage

If the service plan for a given namespace defines multiple storage tiers, the Storage Tiering service works to ensure that each object in that namespace is stored on the correct tier and the correct number of copies of the object are stored on each tier.

For each object in that namespace, the Storage Tiering service:

- Moves copies of the object data among the storage tiers that are defined for the namespace to satisfy the transition criteria that are defined for each storage tier
- Upon moving all existing copies of the data for an object from one tier to another:
  - If the new tier has a different DPL from the previous tier, creates or deletes copies of the object data as required to satisfy the DPL setting for the new tier
  - If the new tier has a different primary running storage metadata protection level (MPL) from the previous tier, creates or deletes copies of object metadata as required to satisfy the MPL setting for the new tier
- Upon moving a replicated object to a metadata-only tier, deletes all copies of the object data from the previous tier, and if the previous tier is not the ingest tier, deletes any copies of the object data that exist on the ingest tier (primary running storage or HCP S Series storage)
- Checks to see whether the object data has been read from a data storage tier for which rehydration is enabled, and if so, creates an extra copy of the object data on the ingest tier
- After moving a replicated object to a metadata-only tier for which rehydration is enabled and making that object metadata-only, checks to see whether that object has been read from a remote system, and if so, restores the data to each copy of the object that's stored on the ingest tier (primary running storage or HCP S Series storage)

Metadata-only storage tiers

When the Storage Tiering service moves an object off the ingest tier and onto another storage tier, the service removes all copies of the object data from ingest tier and stores the specified number of copies of the object data on the new storage tier. However, at least one copy of the object metadata must always remain on primary running storage. For each storage tier that's defined for a given namespace, the service plan specifies the number of copies of object data that must be stored on the tier and the number of copies of object metadata that must be stored on primary running storage.

A service plan can include a metadata-only storage tier. For each object that's stored on a metadata-only tier, the service plan specifies the number of copies of the object metadata that must be stored on primary running storage, but the service plan also specifies that no copies of the data for that object can be stored on any storage tier, including the ingest tier.

Each service plan can be configured to define only one metadata-only storage tier. Additionally, that tier must be the last storage tier that's defined by the service plan. After objects in a namespace are moved to the metadata-only tier that's defined for that namespace, the data for those objects is removed from all storage tiers defined for the namespace.

The Storage Tiering service makes an object metadata-only only when all of these conditions are true:

- The service plan for the namespace that contains the object defines a metadata-only storage tier.
- The object is on the storage tier that immediately precedes the metadata-only tier defined in the namespace service plan, and the object meets the transition criteria specified for the metadata-only storage tier.
- A copy of the data for the object exists on at least one other HCP system in the replication topology in which the current system participates. (This is possible because service plans with the same name can have different definitions on different systems.)

When all these conditions are true, the Storage Tiering service deletes all copies of the data for the object from the preceding storage tier. If the preceding storage tier is not the ingest tier, the Storage Tiering service also deletes any copies of the object data that exist on the ingest tier. After deleting all copies of the data for the object, the Storage Tiering service creates or deletes copies of the object metadata on primary running storage, as necessary, to satisfy the primary running storage MPL that's specified for the metadata-only storage tier.

For the purpose of making objects metadata-only, the Storage Tiering service treats each part of a multipart object as a separate object. The applicable number of copies of the metadata for the part are stored on primary running storage, and no data for the part is stored on any storage tier.

Erasure-coded objects are never made metadata-only on any system in the applicable erasure coding topology. If an erasure-coded object is due to move to a metadata-only storage tier, the chunk for the object remains on the previous tier.

On the other hand, an object that is subject to erasure coding but not yet erasure coded can be made metadata-only on a system if all of these are true:

- The system does not have a chunk for the object.
- The erasure coding delay has not yet expired for the object.
- The object is due to be made metadata-only on that system.
- At least one other available system in the erasure coding topology has a full copy of the object data.

If rehydration is enabled for a metadata-only storage tier, when rehydrating a replicated object that's been read from the ingest tier on a remote system, the Storage Tiering service rehydrates all copies of that object on the ingest tier of the local system.

When replicating an object in a namespace to a system on which objects in that namespace can be made metadata-only, HCP replicates only the object metadata if the object is larger than one MB. If the object is smaller than one MB, HCP replicates both the data and metadata.

Here's a scenario that shows how allowing metadata-only objects can be used to advantage:

- You have a many-to-one replication topology in which the HCP systems at the outlying sites are much smaller than the central HCP system to which they all replicate. To optimize the use of storage on the outlying systems, you allow the namespaces on those systems to have metadata-only objects while requiring the central system to have the object data. The outlying systems respond to client requests for object data by reading the data from the central system.

In this scenario, the replication topology should include a disaster recovery system (that is, a replica of the central system) to protect against data loss in case of a catastrophic failure of the central system.

Important: HCP does not prevent you from removing a namespace from a replication topology even if the namespace contains metadata-only objects on one or more systems in that topology. This can result in data for objects in that namespace being permanently inaccessible from those systems. In most cases, HCP warns you if the modification you're making to a replication link would cause this condition to occur.

Rehydration

HCP reads objects most efficiently from the ingest tier, which can be either primary running storage or HCP S Series storage, on the system that's the target of the read request. If you anticipate frequent reads of the same objects in a namespace while the objects are stored on a specific extended storage tier, consider reconfiguring the service plan used by the namespace to enable rehydration on the applicable tier. Similarly, if you anticipate frequent reads of the same objects in a namespace that contains metadata-only objects or remote cloud storage, consider configuring the service plan used by the namespace to enable rehydration on the tier.

When you use rehydration, the rehydration days time period is started or restarted with reads over a day since the last read. The rehydration days time period can even be started before the object tiers. If an object tiers with a rehydration days time period in effect, the copy on primary storage will not be deleted. As long as the rehydration days time period remains in effect with additional reads, the copy on primary storage will not be deleted.

Default service plan configuration settings

Each HCP system has a service plan named Default that's automatically created and configured during the HCP software installation. The Default service plan is applied to each tenant and namespace for which another service plan is not explicitly selected.

When the HCP system is first installed, the Default service plan defines primary running storage (the ingest tier) as the only storage tier. On HCP with SAN-attached storage and VM systems, by default, the ingest tier DPL and MPL are both set to one. On HCP with internal storage systems, by default, the ingest tier DPL and MPL are both set to two.

You can modify the Default service plan at any time to define one or more additional storage tiers or to change the ingest tier DPL and MPL settings.

General considerations for namespace service plans

Initially, when you add an object to a namespace, HCP creates and stores the data on the ingest tier and metadata for the object on primary running storage. For each object that's stored in a namespace:

1. HCP creates *primary metadata* for it. This metadata consists of information HCP already knows, such as the creation date, and, for objects only, the data size, hash algorithm, and cryptographic hash value generated by that algorithm. It also includes metadata that was either inherited or specified in the write request, such as retention setting, UID, and GID.
2. HCP creates the number of additional copies of the primary metadata required to satisfy the ingest tier metadata protection level (MPL) that's set for the namespace by its service plan. HCP then distributes all copies of the primary metadata among the HCP storage nodes.
3. HCP creates the number of copies of the object data required to satisfy the ingest tier data protection level (DPL) that's set for the namespace by its service plan. HCP then distributes all copies of the object data either among the HCP storage nodes or HCP S Series Nodes, depending on the ingest tier.

   Each copy of the primary metadata for the object points to all copies of the object data. However, the object data is not necessarily stored on the same node as the primary metadata for the object.

4. HCP stores a copy of the metadata with each copy of the object data. Each copy, called the *secondary metadata*, lets HCP reconstruct the primary metadata should that become necessary.

Object content stored on different types of storage

When the Storage Tiering service moves an object off the ingest tier and onto another storage tier, the service removes all copies of the object data from the ingest tier and stores the specified number of copies of the object data on the new storage tier. However, at least one copy of the object metadata must always remain on primary running storage. For each storage tier that's defined for a given namespace, the service plan specifies the number of copies of object data that must be stored on the tier and the number of copies of object metadata that must be stored on primary running storage.

For each object in a given namespace, the Storage Tiering service always moves copies of the data for that object among the storage tiers that are defined for the namespace by its service plan. However, the Storage Tiering service does not move all of the other content for an object to each storage tier that's defined for a namespace.

For each copy of an object that's stored on primary spindown storage, only the data, custom metadata, ACL, and secondary metadata for that object are actually stored on primary spindown storage. All copies of the primary metadata for an object must always remain on primary running storage.

Note:

Objects moved from primary running storage to primary spindown storage are always kept on the same storage node.

For each copy of an object that's moved to S Series or extended storage, only the data for that object is actually stored on primary running storage. All copies of the object metadata must always remain on primary running storage.

Storage allocation for objects on an HCP S Series or extended storage tier

Each HCP S Series or extended storage tier can be configured to use one or more storage pools. Each storage pool can be configured to include one or more access points (mount points, buckets, or containers) that can be associated with one or more storage components.

If a service plan defines an HCP S Series or extended storage tier that contains more than one storage pool and the DPL for that storage tier is greater than one, HCP uses different storage pools to store duplicate copies of the data for each object on that tier. Similarly, if a storage pool that's used for a given storage tier contains more than one HCP S Series or extended storage component access point, HCP uses the storage that's associated with different access points to store any duplicate copies of object data that are stored on the tier that contains the storage pool.

When HCP stores a single copy for each object on a given HCP S Series or extended storage tier, HCP still distributes the object data storage evenly across all of the storage component access points contained in all storage pools configured for a given HCP S Series or extended storage tier.

This ensures that data that's stored on a given tier is protected as much as possible and the storage that's used for a given tier is allocated as efficiently as possible.

Service plans and read requests

When creating service plans, you should keep in mind how HCP handles read requests.

In response to a read request, HCP tries to retrieve the data for an object from these sources, in the order specified below:

1. Primary running storage
2. HCP S Series storage
3. Primary spindown storage
4. NFS storage
5. Cloud storage
6. Primary storage on a remote system to which the object has been replicated

In response to a read request, HCP tries to retrieve the metadata for an object from these sources, in the order specified below:

1. Primary running storage
2. Primary spindown storage
3. Primary running storage on a remote system to which the object has been replicated

Service plans for tenants and namespaces

When you create an HCP tenant, you have the option of associating a service plan with it. This plan then applies to each of the tenants namespaces. Alternatively, you can allow HCP tenant administrators to associate service plans with their individual namespaces. In this case, the tenant administrator can choose from any of the service plans that are defined at the system level (including Default).

When you create the default tenant and namespace, you associate a service plan with the default namespace. The default tenant administrator can choose a different service plan for the default namespace at any time.

You can change the service plan that's associated with an HCP tenant at any time. However, if you switch to allowing the tenant to associate service plans with individual namespaces, you can no longer associate a service plan with the tenant.

When allowed to choose service plans for individual namespaces, tenant administrators see only the service plan names and descriptions, and not service plan rules. The names and descriptions can indicate the namespace usage patterns and properties with which the service plans are intended to work. Thus, tenant administrators do not need to be aware of the HCP system storage in order to associate service plans with namespaces.

Service plans and replication

HCP replicates the associations between service plan names and tenants or namespace but does not replicate the service plans themselves. If you change the associations between service plan names and tenants on namespaces on a replica HCP system, the change is replicated to the rest of the HCP systems in the replication topology, ensuring that the service plan name associated with a tenant or namespace remains the same.

HCP does not replicate service plans. This means that replicated tenants or namespaces can be associated with the same service plan name on the two systems involved in a replication link, but the service plan configuration settings on the two systems can be entirely different. For example, a service plan named External Storage can tier to Amazon storage from system A and to HCP S Series storage on system B.

You need to configure the service plans on each system in the replication topology. If you do not configure the service plans, the replicated namespaces and tenants use the Default service plan settings.

Working with service plans

Each namespace has a service plan that defines both a storage tiering strategy and a data protection strategy for the objects in that namespace. At any point in the lifecycle of an object, its storage tiering strategy specifies the types of storage on which copies of that object must be stored, and its data protection strategy specifies the number of object copies that must be stored on each type of storage.

A service plan is a named specification of HCP service behavior that determines how HCP manages the storage of the data and metadata for objects in a given namespace. For example, the service plan for a namespace could specify that the Storage Tiering service should move objects from primary running storage to primary spindown storage 30 days after they're stored and specify that the Protection service should ensure that HCP maintains two copies of the data for each object that exists on primary spindown storage. Service plans enable you to tailor a storage tiering strategy and a data protection strategy for each tenant and its namespaces based on specific storage usage patterns or business needs.

You can create any number of service plans on an HCP system and configure each plan to use up to four different storage tiers, including the ingest tier (primary running storage or HCP S Series storage). You can then offer a wide variety of service plans to tenant administrators in order to meet the business needs of each tenant.

You can use the Storage page in the System Management Console to create, modify, retire, and delete service plans. You can also use the Storage page to monitor the usage of all primary spindown storage and extended storage tiers that are defined by any given service plan.

To display the Storage page, in the top-level menu of the System Management Console, click Storage.

Note:

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

Creating a service plan

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. At the top of the Service Plans panel, click Create Service Plan.

   The Create Service Plan wizard opens.

3. On the Name page, use the applicable fields to specify a name for the new service plan and, optionally, a description for the service plan and then click Next.

   A service plan name must be up to 64 characters long, can contain only alphanumeric characters, hyphens (-), and underscores (_), and is not case sensitive.

   A service plan description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

4. On the Import page, you can import an existing service plan configuration and create a new service plan with it. If you want to import an existing service plan configuration into the new service plan you're creating, check the box next the existing service plan you want to import and then click Next.
   When you import an existing service plan configuration, the storage tiers that are configured for that plan are automatically defined in the new plan. You can use the imported service plan configuration as a starting point to configure each of the tiers you want to define in the service plan.

   If you want to import the configuration for an existing service plan into the new service plan you're creating, check the box next the existing service plan you want to import.

5. Click Next.
   On the **Encrypt Cloud Pools** page, you can select the method for encrypting the data. You can use either local key or a key management server (KM Server).
   a. To not to use encryption, select **None**.
   b. To encrypt all the cloud pools, select **All** and then select the KM Server from the **Encryption** drop down. To manage keys locally, select Use local key management.
   c. To use imported service plan settings, select **Selected** and then select the **KM server** from the drop down. Click Next.
6. On the Review page, review the information.
7. Take one of these actions:
   - If the information you entered is correct, click Finish.
   - If the information is incorrect, use the Previous and Next buttons to navigate through the pages of the wizard and change any settings that are not correct. When you are satisfied with the configuration settings you've entered, click Finish.

   When you click Finish, the wizard exits, and the Storage page displays the Tiers panel on the service plan configuration page for the service plan that you just created.

   You can use the Tiers panel to add one or more new tiers to the service plan configuration. If you chose to import the configuration from another service plan into the new plan you created, you can delete or modify any of the existing tiers that were imported from that plan.
8. If you're satisfied with the storage tiers that are configured for the new service plan, you can click the Tenants tab at the top of the page and use the Tenants panel to assign the service plan to one or more tenants.

Assign the service plan to one or more tenants in the Tenants tab.

Modifying a service plan

You can use the Service Plans panel on the Storage page to view and modify the configuration of any existing service plan. At any time, you can modify any service plan to:

- Change the service plan name or description. If you change the name, the original name remains associated with any applicable tenants and namespaces. The result is that these tenants and namespaces are associated with an undefined service plan, and HCP uses the Default service plan for them. If you subsequently create a new service plan with the original name, the plan then applies to those tenants and namespaces.
- Change the ingest tier.
- Add one or more new storage tiers to the storage tiering strategy defined in the service plan.
- Delete one or more existing storage tiers from the plan.
- Change any configuration settings used for any storage tier defined in the service plan.

  If you change the storage tiering strategy or the data protection strategy defined in a service plan, objects that complied with the original service plan requirements might not be in compliance with the new ones. The next time the Storage Tiering service processes such an object, the service moves, copies, deletes, or changes the object as needed to comply with the new storage tiering strategy and/or the new data protection plan.
- Change the encryption settings to either use local encryption or a specific KM Server for encryption.
- Assign the service plan to one or more tenants.

Note: If you assign a service plan to an existing tenant, that service plan replaces the one that was previously in effect for the tenant. Similar to a change in the configuration for an existing service plan for a namespace, if you change the service plan that's assigned to a tenant, the new storage tiering strategy and data protection strategy do not take effect until the next time the Storage Tiering service runs.

Modifying basic configuration settings for a service plan

You can modify the basic configuration settings for any service plan to change either the name or the description that's used for the service plan.

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Settings tab.
4. On the Settings panel, you can change the Encrypt Cloud Pools settings.
   If you are upgrading from an older version, the default encryption settings will be based on the earlier encryption settings cloud storage pools:
   - If all the cloud storage pools are encrypted, the default is All.
   - If some cloud storage pools are encrypted, the default is Selected.
   - If none of the cloud storage pools is encrypted, the default is None
   a. To not to use encryption, select **None**.
   b. To use a KM Server, select All and then select the KM server from the dropdown.
   c. To retire the service plan, select Retired.
5. At the bottom of the page, click Update Settings.

Adding a storage tier to a service plan

You configure any storage plan to define up to four different storage tiers, including the ingest tier.

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Tiers tab.
4. On the Tiers panel, click Add Tier.

   The Add Tier wizard opens.
5. On the Transition page in the wizard, use the appropriate fields to set these transition criteria:
   - The object age (number of days since ingest) at which one or more copies of the object data must be moved from the previous tier onto this tier.
   - For service plans that define two tiers only, including the ingest tier, select whether a threshold will be applied to the second tier. If it is applied, the percentage of primary running storage capacity that must be used (the threshold) before object data can be moved to the second storage tier.
   - For HCP systems with replication enabled, whether objects must be fully replicated before they can be transitioned from the previous tier onto this tier. If replication is disabled for the HCP system, this transition criterion does not appear in the HCP System Management Console.
6. Click Next.

7. On the Options page in the wizard, use the applicable fields to specify:
    - Whether to enable rehydration for the new storage tier, and if so, the number of days an object must remain on the ingest tier after it's rehydrated.
    - Whether to make this storage tier metadata-only.
8. Click Next.
9. Take one of these actions:
    - If in step 7 above, you did not select the option to make this tier metadata-only, on the Storage Pools page:
        - The wizard displays a table containing a list of all of the storage pools that you can include in the storage tier, along with a check box that corresponds to each storage pool in the list. Use the checkboxes in the left column in the table to select one or more storage pools to be included in the tier.
        - A dropdown list box appears next to the name of each storage pool you select. Use these fields to specify the number of copies of object data that HCP must maintain on each storage pool for each object that's moved to the storage tier you're configuring. The total number of copies of object data that must be stored on each pool is the DPL for the storage tier.
        - In the Metadata Copies on Primary Storage field, specify the primary running storage MPL for the new tier. This is the number of copies of the object metadata that HCP must maintain on primary running storage for each object that's moved to the new storage tier.
        - At the bottom of the page, select I Understand to indicate that you understand the consequences of moving all copies of the object data to the new tier.
    - If in step 7 above, you selected the option to make this tier metadata-only, on the Storage Pools page:
        - In the Metadata Copies on Primary Running Storage field, specify the primary running storage MPL for the new tier. This is the number of copies of the object metadata that HCP must maintain on primary running storage for each object that's moved to the new storage tier.
        - Select I Understand to indicate that you understand the consequences of moving all copies of the object data to the new tier. In this case, this statement means that you understand that the DPL of the new tier is zero, so all copies of the object data will be deleted for each object that's moved to the new tier.
10. Click Next.
11. On the Review page in the wizard, review the storage tier configuration settings that you specified in the wizard.
12. Take one of the following actions:
    - If the information you entered is correct, click Finish.
    - If the information is incorrect, use the Previous and Next buttons to navigate through the pages of the wizard and make the changes you want. When you're satisfied with the configuration settings you've entered, click Finish.

When you click Finish, the wizard exits, and the Storage page displays the Tiers panel on the service plan configuration page for the service plan for which you've just created a new storage tier.

Removing one or more storage tiers from a service plan

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Tiers tab.
4. The Tiers panel opens, showing a list of storage tiers that are currently configured for the service plan. A delete control ( ) appears in the row for each storage tier except for the ingest tier.
5. Click the delete control for any storage tier to delete it from the service plan.

Choose the ingest tier

The default ingest tier for HCP is primary running storage. If you have HCP S Series Node on your HCP system, you can select HCP S Series storage pools as the ingest tier of a service plan. This means that all objects ingested through namespaces under that service plan are written directly to S Series Nodes rather than primary running storage. Regardless of the ingest tier, HCP keeps all object metadata on primary running storage.

If one or more namespaces on the service plan have ingested data through CIFS, NFS, or WebDAV, the service plan ingest tier cannot be changed to HCP HCP S Series. Likewise, NFS, CIFS, and WebDAV cannot be enabled on namespaces that have HCP HCP S Series set as the ingest tier.

Note:

The following services do not process objects ingested or tiered to HCP S Series storage: Content Verification, Duplicate Elimination, Shredding, hardware encryption, Capacity Balancing, and Scavenging.

Selecting primary running storage as the ingest tier

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Tiers tab.
4. On the Tiers panel, click the tier you want to modify.

   The Edit Tier wizard opens.

5. Select Primary running as the ingest tier.

   Selecting Primary running as the ingest tier deselects all HCP S Series options. You cannot have both Primary running and HCP S Series as the ingest tier.

6. In the Data field, select the number of data copies you want to have in your ingest tier at all times.
7. In the Metadata Copies on Primary Storage field, select the number of object metadata copies you want to keep on primary running storage at all times.
8. Click Next.
9. On the Review page in the wizard, review the storage tier configuration settings that you specified in the wizard.
10. Choose one of the following options:
    - If the information you entered is correct, click Finish.
    - If the information you entered is incorrect, use the Previous and Next buttons to navigate through the pages of the wizard and make the changes you want. When you're satisfied with the configuration settings you've entered, click Finish.

Selecting HCP S Series storage pools as your ingest tier

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Tiers tab.
4. On the Tiers panel, click the tier you want to modify.

   The Edit Tier wizard opens.

5. Select the HCP S Series pools you want to target as the ingest tier.
   Note:

   Selecting HCP S Series as the ingest tier deselects Primary running. You cannot have both primary running storage and HCP S Series storage as the ingest tier. If you have the CIFS, NFS, WebDAV, or SMTP protocol enabled on any namespace that's using the service plan, you cannot select HCP S Series as the ingest tier.

6. From the Data drop down field, select the number of copies you want to have in your ingest tier at all times. You can have a different number of copies for each pool.
7. Click to select Encrypted if you want to encrypt the pool.
8. From the Primary Storage panel, choose one of the following steps:
   - If you want to remove all data existing on primary running storage prior to the change in ingest tier and move it to your HCP S Series storage, deselect Keep current data on primary.
   - If you want to keep all data existing on primary running storage prior to the change in ingest tier on primary running storage, leave Keep current data on primary selected and select the number of copies of object data you want to keep of that data on primary running storage at all times.
9. From the Primary Storage panel Metadata dropdown field, select the number of copies of object metadata you want to keep on primary running storage at all times.
10. Click Next.
11. On the Review page in the wizard, review the storage tier configuration settings that you specified in the wizard.
12. Choose one of the following options:
    - If the information you entered is correct, click Finish.
    - If the information you entered is incorrect, use the Previous and Next buttons to navigate through the pages of the wizard and make the changes you want. When you're satisfied with the configuration settings you've entered, click Finish.

Assigning a service plan to one or more tenants

You can configure the service plan for a namespace to assign that service plan to any existing tenant. When you assign a particular service plan to a tenant, that service plan replaces the one that was previously assigned to the tenant.

Similar to a change in the configuration for an existing service plan for a namespace, when you change the service plan that’s assigned to a tenant, the new storage tiering strategy and data protection strategy do not take effect until the next time the Storage Tiering service runs.

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Tenants tab.
4. The Tenants panel, in the Tenants assigned other service plans section, use the checkboxes in the left column in the table to select the tenants to which you want to assign the service plan.
   Note:

   You can also use the checkboxes in the Tenants assigned service plan name field to deselect one or more tenants in order to delete those service plan assignments. However, if you do this, the deselected tenants will have no service plan assigned to them, so you’ll have assign new service plans to them. If you want to change the service plan that’s assigned to a specific tenant, you should modify the configuration for that tenant or modify the configuration of the new service plan to assign it to the tenant.

5. At the bottom of the page, click Update Settings.

Retiring a service plan

You can retire a service plan at any time. When you retire a service plan, the plan remains in effect for all namespaces and tenants to which it is currently assigned. However, a retired service plan is no longer available to be assigned to any new or existing tenants or namespaces.

You can also reactivate a retired service plan at any time to make that service plan available to be assigned to tenants and namespaces once again.

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.
2. On the Service Plans panel, click the table row that corresponds to the service plan for which you want to configure a new storage tier.
3. At the top of the panel that opens, click the Settings tab.
4. On the Settings tab, in the Retire service plan section, take one of these actions:
   - If you want to retire the service plan, select Retire.
   - If you want to reactivate the service plan, deselect Retire.
5. At the bottom of the page, click Update Settings.

Deleting a service plan

You can delete any service plan except the Default service plan at any time. However, in order to delete a service plan that’s assigned to one or more tenants or namespaces, you need to specify a replacement service plan for those tenants and namespaces.

When you delete a service plan, objects to which that plan applied must now comply with the replacement service plan that you specified when you deleted the plan. The next time the Storage Tiering service processes such an object, the service moves or changes the object as needed to comply with the specified replacement service plan.

To view existing service plans and monitor storage usage for storage tiers defined for one or more service plans, you need the monitor or administrator role. To create, modify, retire, and delete service plans, you need the administrator role.

1. On the left side of the Storage page, click the Service Plans tab.

   The Service Plans panel displays a list of service plans that are currently configured on the HCP system. A delete control ( ) appears next to each service plan that's not currently assigned to any tenants or namespaces.
2. Take one of these actions:

   - If the service plan you want to delete is not currently assigned to any namespaces or service plans, on the Service Plans panel:

     a. Click the delete control ( ) in the table row that corresponds to the service plan you want to delete.
     b. In response to the confirming message, click Delete.

   - If the service plan is associated with one or more tenants or namespaces, on the Service Plans panel:

     a. Click the table row that corresponds to the service plan that you want to delete.
     b. At the top of the panel that opens, click the Manage tab.
     c. On the Manage panel, in the Delete service plan section in the Replacement Service Plan field, select the service plan that you want to assign to all namespaces and tenants that are currently assigned to the service plan you want to delete.
     d. Click Delete Service Plan.

HCP deletes the service plan from the system and assigns the specified replacement service plan to each tenant and namespace to which the deleted service plan was assigned.

Monitoring storage

In the HCP System Management Console, you can monitor the status and usage of storage components, storage pools, buckets, containers, mount points, and service plans.

Several System Management Console pages and reports display storage status and usage information:

- The Storage > Overview shows storage and service plan usage statistics in various formats.
- The details pages for these items show overall usage statistics for the applicable component or pool:
  - Primary running storage component
  - Primary running storage pool
  - Primary spindown storage component
  - Primary spindown storage pool
- The Storage > Components page lists all storage components and shows status and high-level usage information for them.
- The details page for an HCP S Series or extended storage component shows detailed usage information for that component.
- The Storage > Pools page lists all storage pools and shows status and high-level usage information for them.
- The details page for an S Series or extended storage pool shows detailed usage statistics for that pool.
- The Storage > Service Plans page lists all service plans and shows status and high-level usage information for them.
- The details page for a service plan shows detailed usage information for that service plan.
- The Storage > Reports page lets you generate reports that show current and historical usage statistics for storage components, storage pools, and service plans.

About the storage Overview page

The storage Overview page provides a high-level view of storage component, storage pool, and service plan usage. To display this page, in the top-level menu of the HCP System Management Console, click Storage.

The top part of the storage Overview page has these sections:

Extended and S Series Storage Statistics
: Displays the following storage statistics::

  - The total number of objects and object parts stored on HCP S Series or extended storage. This number includes objects that are in the process of being created by multipart uploads.
  - The total number of bytes used to store objects and object parts on HCP S Series or extended storage. This number includes the parts of in-progress multipart uploads that have already been written to primary running storage or HCP S Series storage, as applicable. This number does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

Erasure Coding Statistics
: Displays the total number of erasure-coded objects and object parts stored on the HCP system

Metadata-only Statistics
: Displays the following metadata statistics::

  - The total number of objects for which the HCP system stores only metadata.
  - The total number of bytes not used for storing data for metadata-only objects. This number does not take compression or duplicate elimination into consideration.

    If you have an active/active replication link, the metadata-only statistics fluctuate during object replication.

The Component Usage By Capacity section of the storage Overview page contains:

- A bar graph showing the number of bytes used to store objects on storage represented by each storage component defined on the HCP system. Hover your cursor over a bar to see the name of the applicable component and the number of used bytes for that component.
- A pie chart showing the number of bytes used to store objects on storage represented by each storage component defined on the HCP system. Hover your cursor over a segment to see, for the applicable component:
  - The amount of used storage for the component as a percent of the total amount of used storage for all storage components defined on the HCP system
  - The component name
  - The number of used bytes for the component
- A legend for the bar graph and pie chart. The legend shows the color used for each storage component and the number of bytes used to store objects on storage represented by the component.

  For an NFS storage component, the number of bytes shown is the total number of bytes used on the NFS storage in the component, including bytes used for the OS, non-HCP files, and system overhead.

The Pool Usage By Capacity section of the storage Overview page contains:

- A bar graph showing the number of bytes used to store objects on storage represented by each storage pool defined on the HCP system. Hover your cursor over a bar to see the name of the applicable pool and the number of used bytes for that pool.
- A pie chart showing the number of bytes used to store objects on storage represented by each storage pool defined on the HCP system. Hover your cursor over a segment to see, for the applicable pool:
  - The amount of used storage for the pool as a percent of the total amount of used storage for all storage pools defined on the HCP system
  - The pool name
  - The number of used bytes for the pool
- A legend for the bar graph and pie chart. The legend shows the color used for each storage pool and the number of bytes used to store objects on storage represented by the pool.

  For an NFS storage pool, the number of bytes shown is the total number of bytes used on the NFS storage in the pool, including bytes used for the OS, non-HCP files, and system overhead.

The Service Plan Usage section of the storage Overview page displays service plan usage statistics for tenants or for namespaces. To display the statistics you want, click Tenants or Namespaces, as applicable, in the top right corner of the section.

The Service Plan Usage section contains:

- A bar graph for each service plan defined on the HCP system:
  - In the tenant view, the number of tenants with one or more namespaces that use that service plan. Hover your cursor over a bar to see the name of the applicable service plan and the number of tenants with namespaces using that plan.
  - In the namespace view, the number of namespaces that use that service plan. Hover your cursor over a bar to see the name of the applicable service plan and the number of namespaces using that plan.
- A pie chart for each service plan defined on the HCP system:
  - In the tenant view, the number of tenants with one or more namespaces that use that service plan. Hover your cursor over a segment to see, for the applicable service plan:
    - The percent of tenants defined on the HCP system that have namespaces using the service plan
    - The service plan name
    - The number of tenants with namespaces using the service plan
  - In the namespace view, the number of namespaces that use that service plan. Hover your cursor over a bar to see, for the applicable service plan:
    - The percent of namespaces defined on the HCP system that use the service plan
    - The service plan name
    - The number of namespaces using the service plan

If no namespaces are defined on the HCP system, the Service Plan Usage section does not appear on the storage Overview page.

Understanding the storage component list

The Components page in the HCP System Management Console lists all storage components currently defined on the HCP system. You can display this page.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Components.

   For each listed component, the Components page shows:

   Name
   : The component name.

   Type
   : The component type, which can be:
     - Amazon S3
     - Google Cloud
     - HCP HCP S Series
     - Microsoft Azure
     - NFS
     - Primary running
     - Primary spindown
     - S3 Compatible

   Status
   : The component status:

     Active
     : The component is not paused, retiring, or retired.

     Paused
     : A user paused the component. While a component is paused, HCP cannot write to or read from the storage represented by the component.

     Retired
     : A user retired the component. All objects have been moved off the storage represented by the component.

     Retiring
     : A user retired the component. HCP is in the process of moving objects off the storage represented by the component.

   Usage
   : The number of bytes currently used to store objects, parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of objects on storage represented by the component.

     For primary running and HCP S Series storage components, the number of bytes includes storage occupied by the parts of in-progress multipart uploads that have already been written to storage represented by the component. The number of bytes does not include storage occupied by replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

     Note: For an NFS storage component, the number of bytes shown is the total number of bytes used on the NFS storage in the component, including bytes used for the OS, non-HCP files, and system overhead.

   Compliant
   : Whether the component is marked compliant. A green checkmark indicates that the component is marked compliant.

     If a storage pool includes at least one component that's marked compliant, that pool is considered compliant. A service plan is considered compliant if each tier in the plan includes at least one compliant storage pool. Only compliant service plans can be associated with namespaces that are in compliance mode.

   In Use

Whether any buckets, containers, or mount points associated with the component are assigned to a storage pool. A green checkmark indicates that the component includes items that are assigned to a pool.

Alerts
: If an issue exists with the component, either a warning icon ( ) or an error icon ( ), depending on the severity of the issue.

If the problem is with the storage network associated with the component, the page also displays an icon that indicates the type of problem.

To view text describing the condition that's causing an alert, hover over the alert icon.

Understanding component and pool details for primary storage

The details pages for the primary running storage component or pool and the primary spindown storage component or pool show overall usage statistics for the applicable component or pool. You can display one of these pages.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Components or Pools, as applicable.
3. In the list of components or pools, click Primary running or Primary spindown, as applicable.

The details page for a primary storage component or pool has a single panel, Overview. The Usage Statistics graph in this panel shows the total storage capacity and amount of used storage for primary running storage or primary spindown storage, as applicable, during the past 30 days (or since HCP was installed if that was less than 30 days ago).

The x-axis in the Usage Statistics graph marks the passage of time. The y-axis measures the storage in gigabytes, terabytes, or petabytes, depending on the storage capacity. As the total storage capacity increases, the intervals on the y-axis get larger. The graph heading indicates the current measurement unit (gigabytes (GB), terabytes (TB), or petabytes (PB)).

The legend below the Usage Statistics graph shows:

- The total storage capacity of the applicable type, excluding the space required for system overhead and the operating system, as applicable.
- The amount of used storage of the applicable type.

  The used storage value is the total amount of storage occupied by object data, system and custom metadata, the metadata query engine index, and any redundant data required to satisfy data protection level and metadata protection level settings in service plans.

  Used storage includes storage occupied by the parts of in-progress multipart uploads that have already been written to the repository. Used storage does not include storage occupied by replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

- The number of logical volumes of the applicable type that are defined on the HCP system.

Understanding component details for HCP S Series and extended storage

The details page for an HCP S Series or extended storage component lets you view and modify information about that component. You can display this page for a component.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Components.
3. In the component list, click the HCP S Series or extended storage component you want.

   The details page for HCP S Series and extended storage components has five tabs:

   Overview
   : Displays read and write information for the component.

   Settings
   : Displays the basic settings for the component and lets you change some of them.

   Buckets, Containers, or Mount Points
   : Has two subtabs:

     Buckets, Containers, or Mount Points
     : Lists the buckets, containers, or mount points included in the component and shows usage information for each item. This tab also lets you add items of the applicable type to the component and remove existing items of the applicable type from the component.

     Accounts
     : Lists the accounts associated with the component and shows usage information for each account. This tab also lets you associate additional accounts with the component and remove existing accounts from the component.

       The Accounts tab is not present for NFS storage components.

   Manage
   : Lets you pause, resume, delete, or abandon the component.

   Advanced
   : Shows the advanced settings for the component and lets you change them.

HCP S Series and extended storage component reads and writes

The Overview tab on the details page for an HCP S Series or extended storage component contains four graphs. These graphs show information about the use of storage represented by the component during the past 30 days (or since the component was added to the HCP system if that was less than 30 days ago).

The graphs are:

Writes (bytes)
: Shows the number of bytes of data written to storage represented by the component.

  For an HCP S Series storage component, this number includes:

  - Bytes written both with the component included in a storage pool in the ingest tier and with the component included in a storage pool in a non-ingest tier.
  - Bytes written for all parts of multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Writes (operations)
: Shows the number of successful write operations that targeted storage represented by the component.

  Each write of a part of a multipart object counts as a separate write operation.

For an HCP S Series storage component:

- This number includes write operations both with the component included in a pool in the ingest tier and with the component included in a pool in a non-ingest tier.
- Each write of a part of a multipart upload counts as a separate write operation. This applies even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Reads (bytes)
: Shows the number of bytes of data read from storage represented by the component.

Reads (operations)
: Shows the number of read operations that successfully retrieved data from storage represented by the component.

Each read of a part of a multipart object counts as a separate read operation.

Bucket, container, or mount point list for HCP S Series and extended storage components

The Buckets, Containers, or Mount Points subtab on the details page for an HCP S Series or extended storage component lists the items of the applicable type that are included in the component. For each listed item, this tab shows:

Name
: The name of the bucket, container, or mount point.

Account
: The label for the account associated with the bucket or container. NFS mount points are not associated with accounts.

Usage
: The number of bytes currently used to store objects, parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of objects in the bucket, container, or mount point.

For an S Series Node bucket, the number of bytes includes storage occupied by the parts of in-progress multipart uploads that have already been written to the bucket. The number of bytes does not include storage occupied by replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

Note: For an NFS mount point, the number of bytes shown is the total number of bytes used on the NFS mount point, including bytes used for non-HCP files and system overhead.

In Use
: Whether the bucket, container, or mount point is assigned to a storage pool. A green checkmark indicates that the item is assigned to a pool.

Alerts
: If an issue exists with the bucket, container, or mount point, either a warning icon ( ) or an error icon ( ), depending on the severity of the issue.

To view text describing the condition that's causing an alert, hover over the alert icon.

Account list

The Accounts subtab on the details page for an HCP S Series or extended storage component lists the buckets or containers included in the component, as applicable. For each listed item, this tab shows:

Name
: The account label.

In Use
: Whether the account is associated with at least one bucket or container. A green checkmark indicates that the account is associated with a bucket or container.

Understanding the storage pool list

The Pools page in the HCP System Management Console lists all storage pools currently defined on the HCP system. You can display this page.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Pools.

For each listed pool, the Pools page shows:

Name
: The pool name.

Type
: The pool type, which can be:
  - Amazon S3
  - Google Cloud
  - HCP HCP S Series
  - Microsoft Azure
  - NFS
  - Primary running
  - Primary spindown
  - S3 Compatible

Usage
: The number of bytes currently used to store objects, parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of objects on storage represented by the pool.

For primary running and HCP S Series storage pools, the number of bytes includes storage occupied by the parts of in-progress multipart uploads that have already been written to the storage represented by the component. The number of bytes does not include storage occupied by replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

Note: For an NFS storage pool, the number of bytes shown is the total number of bytes used on the NFS storage in the pool, including bytes used for the OS, non-HCP files, and system overhead.

Compliant
: Whether the pool is compliant. A green checkmark indicates that the pool is compliant.

A storage pool is considered compliant if it includes at least one compliant component. A service plan is considered compliant if each tier in the plan includes at least one compliant storage pool. Only compliant service plans can be associated with namespaces that are in compliance mode.

In Use
: Whether the pool is included in any storage tiers defined a service plan. A green checkmark indicates that the pool is included in at least one tier.

Alerts
: If an issue exists with the pool, either a warning icon ( ) or an error icon ( ), depending on the severity of the issue.

  To view text describing the condition that's causing an alert, hover over the alert icon.

Understanding pool details for HCP S Series and extended storage

The details page for an HCP S Series or extended storage pool lets you view and modify information about that pool. You can display this page for a component.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Pools.
3. In the pool list, click the HCP S Series or extended storage pool you want.

   The details page for HCP S Series and extended storage pools has three tabs:

   Overview
   : Shows read and write information for the pool.

   Settings
   : Shows the pool settings and lets you change some of them.

   Buckets, Containers, or Mount Points
   : Lists the buckets, containers, or mount points included in the storage components that are of the same type as the storage pool. This tab shows which of these items are currently assigned to the pool. On this tab, you can assign additional items to the pool and remove items from the pool.

HCP S Series and extended storage pool reads and writes

The Overview tab on the details page for an HCP S Series or extended storage pool contains four graphs. These graphs show information about the use of storage represented by the pool during the past 30 days (or since the pool was added to the HCP system if that was less than 30 days ago).

The graphs are:

Writes (bytes)
: Displays the number of bytes of data written to storage represented by the pool.

  For an HCP S Series storage pool, this number includes:

  - Bytes written both with the pool included in the ingest tier and with the pool included in a non-ingest tier.
  - Bytes written for all parts of multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Writes (operations)
: Displays the number of successful write operations that targeted storage represented by the pool.

  Each write of a part of a multipart object counts as a separate write operation.

  For an HCP S Series storage component:

  - This number includes write operations both with the pool included in the ingest tier and with the pool included in a non-ingest tier.
  - Each write of a part of a multipart upload counts as a separate write operation. This applies even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Reads (bytes)
: Displays the number of bytes of data read from storage represented by the pool.

Reads (operations)
: Displays the number of read operations that successfully retrieved data from storage represented by the pool.

  Each read of a part of a multipart object counts as a separate read operation.

Bucket, container, or mount point list for HCP S Series and extended storage pools

The Buckets, Containers, or Mount Points tab on the details page for an HCP S Series or extended storage pool lists the items of the applicable type that are included in storage components that are of the same type as the pool. The list is ordered alphabetically by the components that include the listed items. For each listed item, this tab shows:

A checkbox
: Whether the bucket, container, or mount point is assigned to a storage pool. A checkmark in the box indicates that the item is assigned to a pool.

Component
: The name of the component that includes the bucket, container, or mount point.

Account
: The account label associated with the component that includes the bucket or container. This column is not present for NFS mount points.

Bucket, Container, or Mount Point
: The name of the bucket, container, or mount point.

Compliant
: Whether the component that includes the bucket, container, or mount point is marked compliant. A green checkmark indicates that the component is marked compliant.

Alerts
: If an issue exists with the bucket, container, or mount point, either a warning icon ( ) or an error icon ( ), will appear depending on the severity of the issue.

  To view text describing the condition that is causing an alert, hover your cursor over the alert icon.

Understanding the service plan list

The Service Plans page in the HCP System Management Console lists all service plans currently defined on the HCP system. You can display this page.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Service Plans.

   For each listed service plan, the storage Service Plans page shows:

   Name
   : The service plan name.

   Tenants

The number of tenants with one or more namespaces that use the service plan.

Namespaces
: The number of namespaces that use the service plan.

Status
: The service plan status:

  Active
  : The service plan is not retired.

  Retired
  : A user retired the service plan. While a service plan is retired, it cannot be associated with any additional tenants or namespaces. However, the plan is still being used by the namespaces that were already using it.

Compliant
: Whether the service plan is compliant. A green checkmark indicates that the service plan is compliant.

  A service plan is considered compliant if each tier in the plan includes at least one compliant storage pool. A storage pool is considered compliant if it includes at least one compliant component. Only compliant service plans can be associated with namespaces that are in compliance mode.

Understanding service plan usage details

The Overview tab on the details page for a service plan shows usage information for the plan. You can display the details page.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Service Plans.
3. In the service plan list, click the service plan you want.

The Overview tab contains four graphs. These graphs show information about the use of HCP S Series and extended storage because of the service plan. The graphs cover the past 30 days (or since the plan was added to the HCP system if that was less than 30 days ago).

The graphs are:

Writes (bytes)
: Shows the number of bytes of data written to HCP S Series and extended storage because of the service plan.

  This number includes:

  - Bytes written to HCP S Series storage both with the storage included in a storage pool in the ingest tier and with the storage included in a storage pool in a non-ingest tier.
  - Bytes written for all parts of multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Writes (operations)
: Shows the number of successful write operations that targeted HCP S Series and extended storage because of the service plan.

  Each write of a part of a multipart object counts as a separate write operation.

  This number includes:

  - Write operations that targeted HCP S Series storage both with the storage included in the ingest tier and with the storage included in a non-ingest tier.
  - Each write of a part of a multipart upload. The write operation counts even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Reads (bytes)
: Shows the number of bytes of data read from HCP S Series and extended storage, where the data was on that storage due to the service plan.

Reads (operations)
: Shows the number of read operations that successfully retrieved data from HCP S Series and extended storage, where the data was on that storage because of the service plan.

  Each read of a part of a multipart object counts as a separate read operation.

About storage reports

Storage reports contain statistics about the use of HCP S Series, extended storage, and service plans over time. These reports are a good source of information for storage analysis, enabling you to monitor storage usage patterns at either the component, pool, or service plan level.

Each storage report covers one of these:

- A single storage component, single storage pool, or single service plan
- All storage components, all storage pools, or all service plans
- All storage components, storage pools, and service plans

Storage reports do not include statistics for components and pools representing primary storage.

You generate storage reports from the HCP System Management Console. For each report, you specify the start and end dates of the *report period*, which is the time period covered by the report. You also specify the *reporting interval*, which determines whether HCP generates hourly, daily, or total values for the report period.

Storage reports contain aggregated namespace statistics for each tenant that's defined on the HCP system, including the default tenant. For example, for a given tenant and a given storage component, the number of read operations shown for a specific reporting interval is the total number of read operations that:

- Targeted storage represented by the component
- Occurred during the reporting interval
- Targeted objects in the tenant's namespaces

Storage reports also contain aggregated tenant statistics for the HCP system as a whole. Additionally, for an HCP tenant that has granted system-level administrative access to itself, storage reports contain statistics for the individual namespaces owned by that tenant.

HCP generates storage reports in CSV format. Each line in a report contains the values for one namespace, for one tenant, or for the entire HCP system during a specific reporting interval (that is, during a specific hour, during a specific day, or during the entire report period).

Generating a storage report

When generating a storage report, you need to specify what the report is for, the report period, and the reporting interval. A report can be for one or all components, pools, or service plans or for all components, pools, and service plans.

To specify the *report period*, you select start and end dates. The report period starts at 12:00:00 a.m. on the start date (shown as 00:00:00) and ends at 11:59:59 p.m. on the end date.

The earliest start date you can specify is either 30 days earlier than the current date or the date when the HCP system was installed (if the system was installed less than 30 days ago). The latest end date you can specify is the current date.

You can use the same date as the start date and the end date for a report period. In this case, the report period starts at 12:00:00 a.m. on the specified date and ends at 11:59:59 p.m. on that date.

The *reporting interval* you select determines whether the report contains hourly, daily, or total statistics:

- An *hourly report* contains one set of statistics for each hour in the report period for which statistics are available.

  If the report period starts on the day when the HCP system was installed, the first set of statistics in the report covers the time the system first came online through the end of the last minute in that hour. For example, if the system came online at 2:30:20 p.m. on July 25th and the report period starts on July 25th, the first set of statistics in the report covers 2:30:20 p.m. through 2:59:59 p.m. on July 25th.

  If the report period ends on the current day, the last set of statistics in the report covers the time from the start of the current hour to the time when you requested the report. For example, if you request an hourly report at 2:30:15 p.m., the last set of statistics in the report covers 2:00:00 p.m. through 2:30:15 p.m. on the current day.

- A *daily report* contains one set of statistics for each day in the report period, where a day is defined as the period from 12:00:00 a.m. through 11:59:59 p.m. on a given date.

  If the report period starts on the day when the HCP system was installed, the first set of statistics in the report covers the time the system first came online through the end of the last minute on that day. For example, if the system came online at 2:30:20 p.m. on July 25th and the report period starts on July 25th, the first set of statistics in the report covers 2:30:20 p.m. through 11:59:59 p.m. on July 25th.

  If the report period ends on the current day, the last set of statistics in the report covers 12:00:00 a.m. on the current day to the time when you requested the report. For example, if you request a daily report at 2:30:15 p.m., the last set of statistics in the report covers 12:00:00 a.m. through 2:30:15 p.m. on the current day.

- A *total report* contains one set of statistics for the entire report period.

  If the report period starts on the day when the HCP system was installed, the statistics in the report cover the time the system first came online either through 11:59:59 p.m. on the last day of the report period or through the time when you requested the report on the current day.

  For example, if the system came online at 2:30:20 p.m. on July 25th and, at 2:50:25 p.m. on August 7th, you request a total report with a start date of July 25th and an end date of August 7th, the statistics in the report cover 2:30:20 p.m. on July 25th through 2:50:25 p.m. on August 7th.

  Note: Statistics collected for the current hour may not include some reads and writes that have already occurred during the hour. After the hour is over, however, the statistics collected for it are complete.

To generate a chargeback report, you need the monitor or administrator role.

1. In the top-level menu of the HCP System Management Console, click Storage.
2. On the left side of the Storage page, click Reports.
3. On the Reports page:
   a. In the Report For field, select Component, Pool, Service Plan, or Everything to choose what you want to report on.

      Then, in the field next to the Report For field, if you selected Component, Pool, or Service Plan, select the specific component, pool, or service plan you want, or select All to report on all components, pools, or service plans.

   b. In the Reporting Interval field, select Hour, Day, or Total to generate an hourly, daily, or total report.
   c. In the Start Date field, take one of these actions to specify the start date for the report period:
      - Click the calendar icon ( ) to display a calendar. In the calendar, use the arrows at the top to navigate to the month containing the date you want. Then click the date.
      - Type the date in the text field in mm/dd/yyyy format.
   d. In the End Date field, specify the end date for the report period by selecting the date from the calendar or typing the date in the field.
4. Click Download Report.
5. Select the option to open or save the report file.

   By default, the name of the report file is report.csv.

Storage report content

The first line of a storage report contains identifiers for the values in the subsequent lines. The table below describes each of these values.

Identifier	Value
bytesRead	For a storage component or storage pool, the total number of bytes of data read from storage represented by the component or pool during the reporting interval, where the requested object was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For a service plan, the number of bytes of data read from HCP S Series and extended storage, where the requested object was on that storage because of the service plan and was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system.
bytesWritten	For a storage component or storage pool, the number of bytes of data written to storage represented by the component or pool during the reporting interval, where the writes targeted the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For a service plan, the number of bytes of data written to HCP S Series and extended storage because of the service plan during the reporting interval, where the writes targeted the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For HCP S Series storage, this number includes: • Bytes written both with the targeted storage included in the ingest tier and with the targeted storage included in a non-ingest tier.

Identifier	Value
	• Bytes written for all parts of multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.
deleted	One of the following: • true — The namespace or tenant was deleted after the statistics in the set were collected. • false — The namespace or tenant currently exists. • included — For a tenant or the HCP system, the statistics in the set include values for one or more namespaces that were subsequently deleted.
deletes	For a storage component or storage pool, the number of successful delete operations that targeted storage represented by the component or pool during the reporting interval, where the deleted object was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For a service plan, the number of successful delete operations that targeted HCP S Series and extended storage because of the service plan during the reporting interval, where the deleted object was on that storage due to the service plan and was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. A delete of a multipart object counts as a single delete operation.
endTime	The end time of the reporting interval for the set of statistics in the line, in the same format as is used for the startTime value.
namespaceName	The name of the namespace to which the set of statistics in the line applies. In lines that contain tenant or systemwide statistics, this field has no value.
reads	For a storage component or storage pool, the number of read operations that targeted storage represented by the component or pool during the reporting interval, where the requested object was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For a service plan, the number of read operations that successfully retrieved data from HCP S Series or extended storage during the reporting interval, where the requested object was on that storage due to the service plan and was in the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. Each read of a part of a multipart object counts as a separate read operation.
startTime	The start time of the reporting interval for the set of statistics in the line, in this format: yyyy-MM-dd hh:mm:ss hh is hours on a 24-hour clock. For example: 2017-10-07 14:32:47
systemName	One of the following: • The name of the domain associated with the data access network for the tenant that owns the namespace to which the set of statistics in the line applies • The name of the domain associated with the data access network for the tenant to which the set of aggregated statistics in the line applies • The name of the domain associated with the [hcp_system] network for the HCP system to which the set of aggregated statistics in the line applies
target	The storage component, storage pool, or service plan to which the set of statistics in the line applies.
tenantName	Either: • The name of the tenant that owns the namespace to which the set of statistics in the line applies • The name of the tenant to which the set of statistics in the line applies In lines that contain systemwide statistics, this field has no value.
valid	The status of the set of statistics in the line. Possible values are: • true — HCP successfully collected all statistics in the set. • false — The statistics in the set do not reflect all the activity that occurred during the reporting interval. This may be due, for example, to one or more nodes being unavailable during that time, to a network failure, or to other hardware issues.
writes	For a storage component or storage pool, the number of successful write operations that targeted storage represented by the component or pool during the reporting interval, where the data was written to the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. For a service plan, the number of successful write operations that targeted HCP S Series and extended storage due to the service plan during the reporting interval, where the data was written to the given namespace, any of the namespaces owned by the given tenant, or any of the HCP namespaces in the HCP system. Each write of a part of a multipart object counts as a separate write operation. For HCP S Series storage: • This number includes write operations both with the targeted storage included in the ingest tier and with the targeted storage included in a non-ingest tier.

Identifier	Value
	• Each write of a part of a multipart upload counts as a separate write operation. This applies even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Sample storage report

Here's an example of a daily storage report for the Amazon-Comp-1 component, where the report period is March 5, 2018, through March 6, 2018, and the report was requested at 11:55 a.m. on March 6th. The report shows statistics for the canada and europe tenants. Because system-level users have administrative access to the europe tenant, the report also shows statistics for the individual namespaces owned by the europe tenant. The report is shown as it would appear in a spreadsheet.

systemName	tenantName	namespaceName	target	startTime	endTime	bytesWritten	bytesRead	writes	reads	deletes	deleted	valid
hcp.example.com	canada		Amazon-Comp-1	3/5/2018 0:00:00	3/5/2018 23:59:59	206315331	247634	15	6	0	FALSE	TRUE
hcp.example.com	canada		Amazon-Comp-1	3/6/2018 0:00:00	3/6/2018 11:55:59	91476093	64387	27	2	0	FALSE	TRUE
hcp.example.com	europe	finance	Amazon-Comp-1	3/5/2018 0:00:00	3/5/2018 23:59:59	123986263	87561	10	1	0	FALSE	TRUE
hcp.example.com	europe	finance	Amazon-Comp-1	3/6/2018 0:00:00	3/6/2018 11:55:59	52253026	0	12	0	0	FALSE	TRUE
hcp.example.com	europe	hr	Amazon-Comp-1	3/5/2018 0:00:00	3/5/2018 23:59:59	9609368	0	7	0	0	FALSE	TRUE
hcp.example.com	europe	hr	Amazon-Comp-1	3/6/2018 0:00:00	3/6/2018 11:55:59	10098019	0	8	0	0	FALSE	TRUE
hcp.example.com	europe		Amazon-Comp-1	3/5/2018 0:00:00	3/5/2018 23:59:59	133595631	0	17	0	0	FALSE	TRUE
hcp.example.com	europe		Amazon-Comp-1	3/6/2018 0:00:00	3/6/2018 11:55:59	62351045	0	20	0	0	FALSE	TRUE
hcp.example.com			Amazon-Comp-1	3/5/2018 0:00:00	3/5/2018 23:59:59	339910962	335195	32	7	0	FALSE	TRUE
hcp.example.com			Amazon-Comp-1	3/6/2018 0:00:00	3/6/2018 11:55:59	153827138	64387	47	2	0	FALSE	TRUE

Network administration

An HCP system can be configured to support virtual networking. Virtual networking enables the segregation of network traffic between clients and different HCP tenants, between management and data access functions, and between system-level and tenant-level traffic. This segregation enhances the privacy and security of communications over the HCP front-end network.

To implement virtual networking on a system that is configured to support it, you define one or more networks. You then configure the system to use specific networks for specific functions.

This help section assumes that you already have a solid understanding of network virtualization and experience with configuring physical and logical network components.

HCP networks

HCP has two networks that are created during system installation: [hcp_system] and [hcp_backend]. The [hcp_system] network is used for front-end communication with the system. The [hcp_backend] network is used for communication between the nodes in the HCP system. Modifying the [hcp_system] and [hcp_backend] networks requires the service role and should be done only by authorized HCP service providers.

With certain HCP system hardware configurations, an [hcp_management] network is created during installation and can be enabled once the system is running. The [hcp_management] network needs to be enabled by a system administrator. The management network segregates system and tenant administration, management API, SNMP, syslog, outgoing SMTP, and SSH traffic from the [hcp_system] network.

IP modes

The *IP mode* for a front-end network determines whether that network can be configured to use IPv4 addresses, IPv6 addresses, or both. HCP has a system-level IP mode setting that determines which types of front-end network IP addresses are supported.

If the system supports both IPv4 and IPv6 addresses (that is, the IP mode is set to Dual), the [hcp_system] networks can be configured to use either or both types of IP addresses. If the HCP system is configured to support the [hcp_management] network, the [hcp_management] network can use IPv4 or IPv6 regardless of the IP mode set for front-end network.

The IP mode of a front-end network determines the types of IP addresses that can be used for communication between HCP and other devices over that network. For example, if the [hcp_system] network is configured to use only IPv6 addresses, all devices that need to use that network to communicate with HCP must be configured to use IPv6 addresses (or both IPv4 and IPv6 addresses).

If HCP is not currently configured to support a specific type of IP address that is required for communication between HCP and other devices, contact your authorized HCP service provider to request a change to the system configuration.

About virtual networking with HCP

Virtual networking is a technology that enables the overlay of multiple logical network configurations onto a single physical network. For virtual networking to work, the physical network must include VLAN-capable devices.

HCP supports virtual networking only for the front-end network through which clients communicate with the system and through which different HCP systems communicate with each other. HCP does not support virtual networking for the back-end network through which the HCP nodes communicate with each other.

In HCP, logical network configurations are referred to simply as *networks*. Each network has a name, an IP mode (IPv4, IPv6, or Dual), one or more subnets defined for the network, IP addresses defined on each subnet for none, some, or all of the nodes in the HCP system, and some other settings.

You can create and configure user-defined networks for communication with HCP over the front-end network. In order to create networks the Virtual network management must be enabled. You can then configure the system to use the specific networks for specific functions.

You can also create network aliases for user-defined networks. Aliases are pointers to actual networks.

At any given time, the total number of user-defined networks and network aliases together cannot exceed 200.

Front-end network usage

The [hcp_system] network is always used for:

- Access to the HCP System Management Console
- Access to the Tenant Management Console for the default tenant
- Access to the HCP management API using a system-level URL
- Syslog functions at the system and tenant levels
- SNMP functions at the system and tenant levels
- Access to the default namespace using the namespace access protocols
- Access to the HCP metadata query API using a system-level URL
- Access to the HCP Search Console using a system-level URL
- Communication between HCP and Active Directory for configuration and for user authentication at the system and tenant levels
- Communication between HCP and RADIUS servers for user authentication at the system and tenant levels
- For HCP with SAN-attached storage systems, communication between HCP and the storage systems
- Communication between HCP and any external storage components configured for the system
- Communication between HCP and Hitachi Tiered Storage Manager
- Communication between HCP and Hitachi Device Manager(HDvM)
- Communication between HCP and Hitachi Remote Ops®
- Access to the HCP system through interfaces reserved for authorized service providers

You can choose to use [hcp_system] or any user-defined network for the following purposes:

- Management of a given HCP tenant, including:
  - Access to the Tenant Management Console for the tenant
  - Access to the HCP management API using a URL for the tenant

  You select the network for this purpose when you create or modify the tenant.

- Access to the namespaces owned by a given HCP tenant, including access through:
  - Namespace access protocols
  - Namespace Browser
  - HCP metadata query API using a URL for the tenant
  - HCP Search Console using a URL for the tenant
- Communication with other HCP systems in a replication topology.

You can use the same network for multiple purposes. If you don't choose a network for a purpose, HCP uses [hcp_system] by default.

When you select a network for a given purpose, you need to ensure that your networking infrastructure is configured to allow client requests for that purpose to be routed to that network. HCP responds to each client request on the same network as the one on which the request arrived. Therefore, clients do not need to be on the same subnet as the network they are using to access the system, but they do need to be configured to use at least one IPv4 or IPv6 address that is routable from that network.

Network properties

A user-defined network has the following properties:

- A name
- Optionally, a description
- Optionally, a VLAN ID
- A domain
- A maximum transmission unit (MTU). The MTU is the largest packet size supported for data sent on the network.

  The MTU for a network can be 1,500 or, if supported by the networking infrastructure, 9,000. The larger MTU reduces overhead and increases network throughput.

- Whether the network is enabled or disabled. If a network is disabled, HCP does not accept communications routed on that network.

  When first created, networks are enabled by default.

- A total number of tenant references. This is the number of tenants that are configured to use the network for management, data access, or both. HCP derives this number from the tenant configurations defined on the system.
- If the network is assigned to one or more tenants, a list of tenant references. This list contains the names of the tenants that are configured to use the network and the purpose for which each tenant uses the network (management, data access, or both). HCP obtains this information from the tenant configurations defined on the system.
- A total number of alias references. This is the number of network aliases that are defined for the network. HCP derives this number from the network alias configurations defined on the system.
- If one or more aliases are defined for the network, a list of alias references. This list contains the names of the network aliases that are defined for the network. HCP obtains this information from the network alias configurations defined on the system.
- Whether HCP should hide the IP addresses of its primary name servers from clients using the network and allow client access to HCP over the network only through specified downstream DNS servers.
- Whether HCP should notify specified downstream DNS servers about changes to the zone definition for the network.
- The rate at which the downstream DNS servers should query HCP for updates to the zone definition for the network domain.
- If the [hcp_system] network is also configured to use a specific type of IP address, a user-defined network can have that IP address.
- Whether the network supports IPv4 addresses, IPv6 addresses, or both:
  - If the network supports IPv4 addresses, the network has these properties:
    - An IPv4 gateway. This is the IPv4 address from which system-initiated communications are sent over the network.
    - An IPv4 subnet mask.
    - An IPv4 subnet. HCP derives the IPv4 subnet for the network from the IPv4 gateway and subnet mask that you specify.
    - Optionally, assignments of IPv4 addresses to storage nodes. The IPv4 addresses for a given network must all be on the IPv4 subnet defined for that network.

Note: If a node has any IP addresses assigned to it for a given network, that node must have an IP address assigned to it on each IPv4 and IPv6 subnet defined for the network.

- If the network supports IPv6 addresses, it has primary IPv6 address settings and, optionally, secondary IPv6 address settings. For each type of IPv6 address settings, the network has these properties:
  - An IPv6 gateway. This is the IPv6 address from which system-initiated communications are sent over the network.
    Note: Each IPv6 gateway defined for the network can be a global address, a unique local address (ULA), or a link local address (LLA). However, if two IPv6 gateways are defined for the network, you cannot use ULAs for both gateways, and the two gateways must be on separate, non-overlapping IPv6 subnets.
  - An IPv6 address prefix length.
  - An IPv6 subnet. HCP derives the IPv6 subnet for the network from the IPv6 gateway and IPv6 address prefix length that you specify.
  - Optionally, assignments of IPv6 addresses to storage nodes. The IPv6 addresses for the network must all be on the IPv6 subnet defined for that network.

  Each network, including the [hcp_system] and [hcp_backend], must use separate, non-overlapping subnets for IPv4 addresses, primary IPv6 addresses, and secondary IPv6 addresses.

- A zone definition. This is the DNS zone definition that is currently used for the network domain. HCP automatically creates and maintains a DNS zone definition for each network defined on the system.

Tagged and untagged networks

A *tagged network* is one that has a specified VLAN ID. The VLAN ID is an identifier that's attached to each packet routed to HCP over that network. This function is performed by the switches in the physical network.

The routing tables in the switches that route requests to the HCP front end must include each VLAN ID you assign to a network. The routing tables associate the VLAN IDs with the network subnets.

A network carries only the packets that have its VLAN ID and ignores all other packets, thereby segregating the traffic on each tagged network from the traffic on other networks.

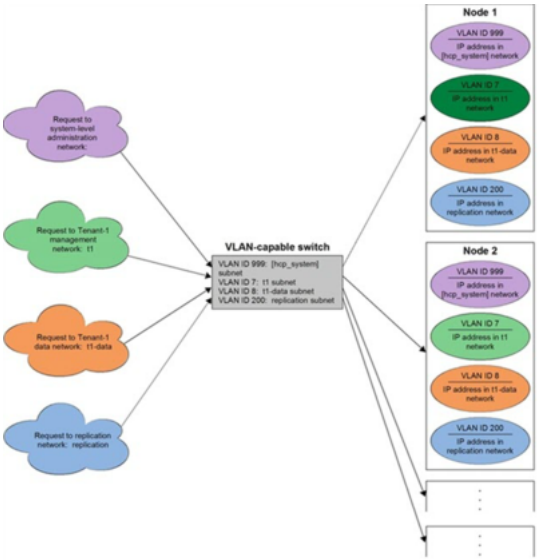
An *untagged network* is one for which you don't specify a VLAN ID. An untagged network ignores all packets that have VLAN IDs.

HCP can have at most one untagged front-end network, including the [hcp_system] network. All other networks must have a VLAN ID.

An untagged network uses the bond0 front-end network interface. When you assign a VLAN ID to a network, HCP creates a logical network interface for the network. This interface is named bond0.*xxxx*, where xxxx is the VLAN ID, with leading zeroes added if needed to create a four-digit number.

The following figure shows a configuration in which:

- HCP uses the [hcp_system] network with VLAN ID 999 for system-level management purposes
- The tenant named Tenant-1 uses a network named t1 with VLAN ID 7 for tenant management purposes and a network named t1-data with VLAN ID 8 for data access purposes
- HCP uses a network named replication with VLAN ID 200 for replication traffic



Network domains

Each network you create must be associated with a domain. The domain can be unique to the network or can be shared among networks. For example, you may want to configure different tenants to use networks associated with different domains, but you may want to configure a single tenant to use management and data networks associated with the same domain.

Clients use network domain names in the URLs that provide access to the HCP system. By associating different domains with different networks, you can brand the system for different customers. For example, the networks you associate with the tenants you create for Customer-1 could all have the domain named object-store.cust1.com.

Assigning different domains to different networks enhances network security because each domain uses a separate certificate to authenticate access requests. If two different networks have two different domains assigned to them, a client cannot use the same credentials to access HCP over both networks. In addition, when a client request uses a domain name for access to HCP, the client making that request has visibility only into the networks that use the specified domain. Thus, a client can retrieve IP addresses only for the networks that it's authorized to use to access the HCP system.

Downstream DNS configuration settings for networks

At any time after you create a network, you can change its downstream DNS configuration settings to:

- Enable hidden primary for one or more downstream DNS servers

- Enable notify for one or more downstream DNS servers
- Change the DNS refresh rate for all the downstream DNS servers

A *downstream DNS server* is a DNS server through which client requests are routed to HCP. An *upstream DNS server* is a DNS server to which HCP routes the outbound communications it initiates (for example, for sending log messages to syslog servers or for communicating with Active Directory). The downstream and upstream DNS servers can be the same servers.

Hidden primary

Hidden primary is an HCP DNS configuration that's used to hide the IP addresses of the HCP nodes configured as primary name servers from users accessing HCP over a specific network. In a hidden primary configuration, the specified downstream DNS servers become the authoritative primary for the zone defined for the network domain. Additionally, in the zone definition that HCP sends, the name server records contain the IP addresses of the downstream DNS servers, and not the IP addresses of the HCP nodes configured as primary name servers.

Notify

Notify is a network configuration option that, when enabled for a network, tells HCP to notify only the specified downstream DNS servers whenever any of the network properties changes (including the description). In response to this notification, each specified DNS server sends a request to HCP to get the updated zone definition for the network domain.

Zone definitions with hidden primary or notify enabled

When hidden primary or notify is enabled for a network, the domain associated with that network must be defined as a secondary zone, and not as a stub zone, on the specified downstream DNS servers. If a network domain is defined as a stub zone and:

- You enable hidden primary for the network, client requests routed to any of the specified DNS servers fail
- You enable notify for the network, the specified DNS servers do not receive the notify messages

If a stub zone is already defined for a domain associated with a network, and you plan to enable hidden primary or notify for that network, change the DNS zone definition type for the domain to secondary before you modify the network.

When hidden primary or notify is enabled for a network that's configured to use a secondary IPv6 subnet, each IPv6 address that's specified in the downstream DNS server list must either be on the secondary IPv6 subnet or be routable from the primary IPv6 gateway that's defined for the network.

Refresh rate

The *refresh rate* for a network is the frequency with which the downstream DNS servers poll HCP to check whether the zone definition for the network domain has changed. If the definition has changed, the servers then ask HCP for the updated definition.

The refresh rate always applies to all the downstream DNS servers that have a zone definition for the network domain and is used regardless of whether that zone definition has a type of secondary or stub.

By default, the refresh rate is three hours. If you enable notify and specify all the applicable DNS servers, consider increasing the refresh rate to a much higher value.

Notify does not work with stub zones. Therefore, if the domain is defined as a stub zone, consider decreasing the refresh rate. If DNS failover occurs, the shorter refresh rate may allow clients targeting a failed system over the network to be more quickly redirected to another system in the replication topology.

You specify the refresh rate for a network as any combination of weeks (W), days (D), hours (H), minutes (M), and seconds (S), using this syntax:

```
#W#D#H#M#S
```

These considerations apply:

- In each case, # must be an integer greater than or equal to one.
- If an integer is specified without a time unit, the time unit is assumed to be seconds.
- Time units can be specified in any order.
- Any given time unit can be specified only once.
- Time units are not case-sensitive.
- The total time specified must be in the range one through 2,147,483,647 seconds.

Advanced downstream DNS configuration

A system administrator can activate advanced downstream DNS configuration mode through the HCP management API.

Advanced downstream DNS configuration mode offers more control over the HCP system downstream DNS configuration for an individual network than using the Network View page of the System Management Console. This configuration enables you to work directly with the HCP DNS management files.

Important: Unless you have an extensive background in networking, using advanced downstream DNS configuration mode is not recommended.

Downstream DNS configuration supports 32 downstream DNS servers.

Network aliases

A *network alias* is a named pointer to another network. You can select a network alias for any purpose for which you can select a network. When a network alias is selected for a particular purpose, HCP uses the network the alias points to for that purpose.

For example, suppose you have a network alias named t1-mng that points to a network named tenant-1. If you select t1-mng as the management network for a given tenant, HCP uses the tenant-1 network as the management network for that tenant.

Network aliases are useful in the context of replication, particularly in situations where the network topologies differ between the two systems involved in a given replication link. The two systems, for example:

- May not have the same number of nodes
- May not both have a VLAN-capable networking environment

Because network topologies can differ, HCP doesn't replicate the definitions of networks and network aliases from one system to another. However, when replicating a tenant, HCP does replicate the names of the networks or aliases associated with that tenant. For the tenant and its namespaces to be accessible on the target system, networks or aliases with those names must be defined on that system.

Here are two replication scenarios that illustrate the use of network aliases:

- One of the HCP systems involved in a given replication link makes extensive use of virtual networking, with each tenant having its own networks for management and data access purposes. None of these networks is [hcp_system]. The other system involved in the link is in a networking environment that is not VLAN capable. As a result, the only front-end network defined on that system is [hcp_system].

  To support replication of the tenants on the first system to the second system, for each network used by a tenant on the first system, you create a network alias with the same name on the second system. You define each of these aliases to point to the [hcp_system] network.

- One of the HCP systems involved in a given replication link has networks named t1-mng, t1-data, t2-mng, t2-data, and so forth selected as the management and data access networks for Tenant-1, Tenant-2, and so forth. The other system involved in the link is used exclusively for data access. Therefore, on that system, the segregation of tenant management networks is not important.

  On the second system, you want to have a single network for the management of all tenants and a separate network for data access for each tenant. To do this and still support replication of all the tenants from the first system to the second system, on the second system:

  - For tenant management, you create a single network named tenant-mng. You also create network aliases named t1-mng, t2-mng, and so forth that all point to the tenant-mng network.
  - For data access, you create networks named t1-data, t2-data, and so forth.

HCP does not require that the networks and network aliases defined on one system in a replication pair directly correspond to networks and network aliases on the other system. That is, the name of a network on one system can be the name of an alias on the other system.

These considerations apply to network aliases:

- The target network for a network alias can be a user-defined network or the [hcp_system] network. A network alias cannot point to another network alias.
- A network alias can point to only one network. However, multiple aliases can point to the same network.

Network states

To be used most effectively, a network should have IP addresses defined for each node in the HCP system. This enables HCP to spread the processing load across all nodes for clients using that network.

If a node doesn't have IP addresses for a given network, that node does not receive communications that come into the system on that network. However, a network is usable as long as at least one available node is assigned IP addresses for the IPv4 and IPv6 subnets defined for that network.

Depending on the number of nodes that have IP addresses for a network, the network can be in any of these states:

Fully defined
: A network is fully defined if all nodes in the system have IP addresses defined for the network.

Partial
: A network is partial if at least two nodes have IP addresses defined for the network and at least one node does not have any IP addresses defined for the network.

Degraded
: A network is degraded if exactly one node has IP addresses defined for that network

  A degraded network presents a single point of failure for clients using that network for system access.

Empty
: A network is empty if no nodes have IP addresses defined for the network. An empty network is not usable.

You cannot select an empty network for tenant management or data access purposes. You cannot select an empty, degraded, or partial network for use with replication.

Isolating networks for storage tiering

A network can be reserved for exclusive communication between an HCP system and an HCP S Series Node or an HCP supported external storage device. This increases tiering security by segregating data tiering to individual networks instead of having all data tiered over one network.

The total amount of virtual networks that can tier to individual storage components is 200. In order to designate an individual network to a storage component, you need the administrator role. Users with the monitor role can see which storage components are tiering through which networks.

If a network is assigned to a storage tier, it can still be used for Tenant data management, Tenant network management, and replication.

In order to give storage components individual networks, Virtual network management must be enabled.

A network is only accepted for an individual storage component if each node that belongs to the network has its IP address defined on HCP.

Considerations for virtual networking

The following considerations apply to virtual networking with HCP.

- The IP mode of a front-end network determines the type of IP addresses that can be used to communicate with HCP over that network. Before selecting a specific network for a specific purpose, you need to ensure that all devices that need to communicate with HCP for that purpose are configured to use at least one type of IP address supported by that network.
- HCP accepts communications from Active Directory only on the [hcp_system] network. Therefore, if a tenant is configured to use AD for user authentication, that tenant must also be configured to use either the [hcp_system] network or an alias for that network for both management and data access purposes. In addition, each Active Directory domain controller used for HCP user authentication must have at least one IPv4 or IPv6 address that is routable from the [hcp_system] network.
- After HCP is upgraded from release 6.x to release 7.0 or later, by default, the HCP system is configured to support only IPv4 addresses for front-end networks. If you need to use IPv6 addresses for communication between HCP and other devices over the [hcp_system] network or any user-defined network, you need to ensure that when the upgrade is complete, your authorized HCP service provider configures HCP to enable support for IPv6 addresses and then configures the [hcp_system] network to use IPv6 addresses.
- When a new node is added to the HCP system, it automatically has IP addresses on each subnet defined for the [hcp_system] network. However, it does not have any IP addresses for any user-defined front-end networks. Those networks, therefore, become partial networks. You can assign IP addresses to the new node for each of those networks at any time.

About the Networks page

To work with networks and network aliases, you use the Networks page in the HCP System Management Console.

The Networks page has four sections:

Network View
: Lets you view, create, modify, and delete networks and network aliases, and monitor the health of individual networks.

Node View
: Lets you view, add, modify, and delete the IP addresses assigned to each node for each network. Both the Network View panel and the Node View panel let you view and modify node IP addresses. However, the Network View panel shows the node IP addresses defined for each network, while the Node View panel shows the IP addresses assigned to each node for all networks in which it participates. The Node View panel is particularly useful for assigning IP addresses to nodes that are added to the HCP system after you've defined multiple networks.

All Zone Definitions
: Lets you view the DNS zone definitions that HCP uses for all network domains that are currently defined on the HCP system.

  You cannot filter the list of DNS zone definitions that are displayed on the All Zone Definitions panel. However, you can use the Network View panel to display all properties of any specific network, including the zone definition information for that network.

Advanced Settings
: Lets you enable IP address configurations for the nodes in your networks and enable virtual network management.

To display the Networks page, in the top-level menu, select Configuration > Networks.

The System Management Console opens the Networks > Network View page.

Note: To view the Networks page, you need the monitor, administrator or service role. To create, modify, and delete user-defined networks and network aliases, you need the administrator role. To modify the [hcp_system] or [hcp_backend] network, you need the service role.

When you use the Configuration menu to access the Networks page, the Networks > Network View is displayed by default. You can then use the tabs on the left side of the page to navigate between sections.

About the Network View page

The Networks > Network View page lets you view, create, modify, and delete networks and network aliases, and monitor the health of individual networks. This panel displays a list of existing networks and network aliases defined for the HCP system and shows basic configuration information and alerts for each network and network alias.

Understanding the network list

The Networks > Network View contains a list of existing networks and network aliases. For each network, this list shows:

- The network name.
- The IP mode currently used for the network. The IP mode for a network indicates the types of IP addresses that the network is configured to use for each node that participates in the network.

  If the IP mode for a network is:

  - IPv4, the network is configured to use only IPv4 addresses
  - IPv6, the network is configured to use only IPv6 addresses
  - IPv4/IPv6, the network is configured to use both IPv4 and IPv6 addresses
- All IPv4 and IPv6 subnets that are defined for the network, shown in CIDR format.
- The name of the network domain.
- None, one, or more alert icons representing problems with the network. To see the text that accompanies an icon, hover your cursor over the icon.

For each network alias, the list shows:

- The alias name
- The IP mode, IPv4 and IPv6 subnets, and domain name used for the target network
- The alerts that apply to the target network

Additionally, the network list displays this icon in the table row that corresponds to the network or alias that's currently selected as the replication network:

To view more information about a specific network or network alias, or to modify the configuration settings used for that network or network alias, click its name in the network list.

Managing the network list

By default, the network list on the Networks > Network View page includes all existing networks and network aliases. The networks and aliases are listed 20 at a time in ascending order by network or alias name.

You can page through, sort, and filter the list of networks and aliases. The Networks > Network View page indicates which networks and aliases are shown out of the total number of networks and aliases in the current list.

Paging

You can change the number of networks and aliases that appear on each page of the network list on the Networks > Network View page. To do this, in the Items per page field, select the number of networks and aliases you want to display on each page in the network list. The options are 10, 20, and 50.

To page forward or backward through the network list, click the next ( ) or back ( ) control, respectively.

To view the Networks page, you need the monitor, administrator or service role. To create, modify, and delete user-defined networks and network aliases, you need the administrator role. To modify the [hcp_system] or [hcp_backend] network, you need the service role.

1. In the Page field, type the page number that corresponds to the network list page you want to view.
2. Press Enter.

Sorting

You can sort the networks and aliases in the network list in ascending or descending order by network name or by domain name. To sort the list, click the column heading for the property by which you want to sort. Each time you click the column heading, the sort order switches between ascending and descending.

Filtering the list by network name

You can use the fields and controls that appear above the network list to filter the items in the list by network name or by network IP mode.

When filtered by network name, the list includes only those networks and aliases that have a name that begins with or is the same as a specified text string.

To view the Networks page, you need the monitor, administrator or service role. To create, modify, and delete user-defined networks and network aliases, you need the administrator role. To modify the [hcp_system] or [hcp_backend] network, you need the service role.

1. Select Name from the drop-down list above the network list.
2. In the text field, type the text string that you want to use as a filter. This string can be up to 64 characters long, can contain any valid UTF-8 characters except commas (,), and is not case sensitive. White space is allowed.
3. Click the find control ( ).

   When filtered by network IP mode, the list includes only those networks and network aliases that have the specified IP mode (IPv4, IPv6, or IPv4/IPv6).

Filtering the list by IP mode

To view the Networks page, you need the monitor, administrator or service role. To create, modify, and delete user-defined networks and network aliases, you need the administrator role. To modify the [hcp_system] or [hcp_backend] network, you need the service role.

1. Select IP Mode from the drop-down list above the network list.
2. In the text field, type the text string that corresponds to the IP mode that you want to use as a filter:
   a. Type IPv4 to filter the list to show the networks and network aliases that are configured to use only IPv4 addresses.
   b. Type IPv6 to filter the list to show the networks and network aliases that are configured to use only IPv6 addresses.
   c. Type IPv4/IPv6 to filter the list to show the networks and network aliases that are configured to use both IPv4 and IPv6 addresses.
3. Click the find control ( ).

About the Node View page

The Networks > Node View page lets you view and modify the IP address assignments for the nodes in the HCP system.

Note:

To view the Networks > Node View page, you need the administrator, service, or monitor role. To change the IP address assignments for user-defined networks, you need the administrator role. You cannot modify IP addresses for the [hcp_system] or [hcp_backend] networks on the Networks > Node View page

Understanding the node list

The Networks > Node View page contains a list of all nodes in the HCP system. For each node, the list shows:

- The node number (node ID).
- The back-end IP address for the node.
- The node status, either OK or Unavailable. You can change the IP addresses for a node regardless of its status.

To view the network IP address assignments for an individual node, click the node number. In the list of networks that appears, the networks for which the node has IP addresses are listed first, in ascending order by network name. These are followed by the networks for which the node doesn't have IP addresses, also listed in ascending order by network name.

Managing the node list

By default, the nodes in the node list are listed 20 at a time in ascending order by node number. You can page through and sort the node list. The Networks > Node View page indicates which nodes are shown out of the total number of nodes in the current list.

Paging

You can change the number of nodes displayed on each page of the node list shown on the Networks > Node View page. To do this, in the Items per page field, select the number of nodes that you want to display on each page of the node list. The options are 10, 20, and 50.

To page forward or backward through the node list, click the next ( ) or back ( ) control, respectively.

To view the Networks > Node View page, you need the administrator, service, or monitor role. To change the IP address assignments for user-defined networks, you need the administrator role. You cannot modify IP addresses for the [hcp_system] or [hcp_backend] networks on the Networks > Node View page

1. In the Page field, type the page number that corresponds to the node list page that you want to view.
2. Press Enter.

Sorting the node list

You can sort the node list in ascending or descending order by node number. To change the sort order, click the Node ID column heading. Each time you click the column heading, the sort order switches between ascending and descending.

Filtering the list by node number

You can use the fields and controls that appear above the node list to filter the items in the list by node number or by node status.

When filtered by node number, the list displays only the node with the specified node number.

To view the Networks > Node View page, you need the administrator, service, or monitor role. To change the IP address assignments for user-defined networks, you need the administrator role. You cannot modify IP addresses for the [hcp_system] or [hcp_backend] networks on the Networks > Node View page

1. Select Node ID from the drop-down list above the node list.
2. In the text field, type the node number for the node you want to display in the node list.
3. Click the find control ( ).

Filtering the list by node status

When filtered by node status, the list includes only those nodes that have the specified node status (ok or unavailable).

To view the Networks > Node View page, you need the administrator, service, or monitor role. To change the IP address assignments for user-defined networks, you need the administrator role. You cannot modify IP addresses for the [hcp_system] or [hcp_backend] networks on the Networks > Node View page

1. Select Status from the drop-down list above the node list.
2. In the text field, type the text string that corresponds to the node status that you want to use as a filter:

   a. Type ok to filter the list to show the nodes that have a status of ok.
   b. Type unavailable to filter the list to show the nodes that have a status of unavailable.
3. Click the find control ( ).

About the All Zone Definitions pages

The Networks > All Zone Definitions page lists the zone definitions of all network domains used for each network defined on the system. If you have a network alias, the zone definition displayed is the DNS zone definition that HCP uses for the network that the alias points to.

About the Advanced Setting panel

The Networks > Advanced Settings page is used for enabling network creation, configuring network versions for your nodes, and enabling the management network if the system is configured for the management network.

Enabling IPv4 and IPv6 addresses

IPv4 addresses are automatically permitted on all nodes in your networks.

You can permit IPv6 addresses on all nodes in your networks.

On the Networks > Advanced Settings page, select Enable IPv6.

Disabling IPv6 addresses

IPv4 addresses are automatically permitted on all nodes in your networks.

You can enable or disable IPv6 addresses on all nodes in your networks.

On the Networks > Advanced Settings page, clear the Enable IPv6 checkbox.

Enabling and configuring the management network

Allowing management network configuration lets users with the system administrator role to segregate system management traffic to the [hcp_management] network.

1. On the Networks > Advanced Settings page, select Allow Management Network Configuration.
   Note:

   If the Allow Management Network Configuration is visible but grayed out on the Advanced Settings page, it means that [hcp_management] network is enabled. If you want to disable Allow Management Network Configuration, you first need to set the [hcp_management] Network status to disable.

2. Click Update Settings.
3. On the Networks > Network View page, confirm that the [hcp_management] network is listed.
4. Click the [hcp_management] network, then click the IP Configuration tab.
5. Assign the management network IP, gateway, netmask, and subnet information.

   Make sure the subnet is different from your front-end and back-end networks.

6. Click the Settings tab.
7. For Network status, select Enable.
8. Click Update Settings.

To permit users with the system administrator role to create networks, on the Networks > Advanced Settings page, select Enable virtual network management.

These networks can be created with the Create Network wizard from the Networks > Network View page.

Virtual network management also permits a system administrator to use the network per storage component tiering.

Creating a network

You use the Create Network wizard on the Networks > Network View page to create a new network on the HCP system. In order to use the wizard, a system administrator needs to have enabled Virtual network management.

When you create a new network with the wizard:

- The network is enabled by default, but it is initially empty. To make the new network usable, you need to modify the initial network configuration to assign IP addresses to one or more nodes.
- The network is configured to use the default downstream DNS configuration settings: hidden primary is disabled, notify is disabled, and the refresh rate is set to three hours.

1. Click Create Network above the network list to open the Create Network wizard.
2. On the Settings page in the wizard:
   a. In the Network Name field, type a unique name for the network. User-defined network names:
      - Must be from one through 63 characters long.
      - Can contain only characters that are valid in DNS hostnames. In English, valid hostnames can contain only alphanumeric characters and hyphens (-).
      - Cannot start or end with a hyphen.
      - Cannot contain white space.
      - Are not case-sensitive.

      Additionally, the following words are reserved and cannot be used as network names: none, [hcp_system], and [hcp_backend].

   b. Optionally, in the Description field, type a description of the network. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
   c. Take one of these actions:
      - To create an untagged network, select Make untagged network. This option is hidden if an untagged network already exists.
      - To create a tagged network, in the VLAN ID field, type a VLAN ID for the network. Valid values are integers in the range one through 4,094.

        The VLAN ID field is grayed while Make untagged network is selected.

d. In the MTU field, select 1500 or 9000.

If an untagged network exists, the MTU that you select cannot be larger than the MTU for the untagged network. If you're creating an untagged network and an existing network has an MTU of 9,000, the network you're creating must have an MTU of 9,000.

e. In the Domain field, select a domain for the network. The dropdown list does not include domains that have only a certificate signing request (CSR) and no SSL server certificates.

3. Click Next.
4. On the IP Configuration page in the Create Network wizard, take one of these actions:
   - If HCP is configured to support only one type of IP address, the wizard automatically selects the supported IP mode for the new network and displays the fields that you need to use to specify IPv4 or IPv6 configuration settings for the network. If the wizard displays the IPv4 Configuration section or the IPv6 Configuration section, go to step 5.
   - If HCP is configured to support both IPv4 and IPv6 addresses, and the [hcp_system] network is configured to use both IPv4 and IPv6 addresses, you can configure the network to use either or both types of IP addresses.

     If the wizard displays the IP Mode section, and does not display any warning messages, select one or both options to set the IP mode for the network:

     - To configure the network to use only IPv4 addresses, select only IPv4. When you select this option, the wizard displays the IPv4 Configuration section.
     - To configure the network to use only IPv6 addresses, select only IPv6. When you select this option, the wizard displays the IPv6 Configuration section.
     - To configure the network to use both IPv4 and IPv6 addresses, select both options.
   - If HCP is configured to support both IPv4 and IPv6 addresses, but the [hcp_system] network is configured to use only one type of IP address, you need to configure the new network to use only the type of IP address that the [hcp_system] network uses.

     If the wizard displays the IP Mode section, but it also displays a warning message to inform you that the [hcp_system] network is configured to use only one type of IP address, select only the option that corresponds to that type of IP address.

     Note: If the wizard displays this warning message, only the supported IP Mode option is selectable. However, you still need to select this option before you can continue specifying configuration settings for the new network.
5. Take either or both of these actions:
   - If the HCP system supports only IPv4 addresses or if you selected IPv4 in step 4 above, in the IPv4 Configuration section:
     - In the Gateway field, type the IP address of the gateway that you want to use for the IPv4 subnet.
     - In the Subnet Mask field, type the subnet mask that you want to use for the IPv4 subnet.
   - If the HCP system supports only IPv6 addresses or if you selected IPv6 in step 4 above, in the IPv6 Configuration section:
     - Under IPv6 Address Settings:
       - In the Gateway field, type the IP address of the gateway that you want to use for the primary IPv6 subnet.
       - In the Prefix Length field, type the IPv6 address prefix length that you want to use for the primary IPv6 subnet.
     - Optionally, to configure a secondary IPv6 subnet for the network, under Secondary IPv6 Address Settings:
       - In the Gateway field, type the IP address of the gateway that you want to use for the secondary IPv6 subnet.
       - In the Prefix Length field, type the IPv6 address prefix length that you want to use for the secondary IPv6 subnet.
6. Click Next.
7. On the Review page in the Create Network wizard, review the network configuration settings that you entered.
8. Take one of these actions:
   - If the configuration settings that you entered are incorrect:
     - Use the Previous and Next buttons to navigate through the wizard and modify your entries on each page, as necessary.
     - When you have corrected all the configuration errors, use the Next button to navigate to the Review page.
     - Click Finish to exit the wizard and create an empty network with the specified configuration.
   - If the configuration settings that you entered are correct, click Finish to exit the wizard and create an empty network with the specified configuration settings.

When you exit the wizard, the Network View panel displays the IP Configuration panel for the new network, showing the IPv4 and IPv6 subnet configuration information that you entered in the Create Network wizard.

You can use the IP Configuration panel to assign IP addresses to one or more nodes for the new network.

Optionally, from the IP Configuration panel, you can click the applicable tab to display the Settings panel, and then use the Settings panel to change the default downstream DNS settings for the network.

Assigning IP addresses to nodes for a network

You can use either the Networks > Network View page or the Networks > Node View page to assign IP addresses to one or more nodes for each network defined on the HCP system:

- Use the Networks > Network View page to configure node IP addresses for a specific network.
- Use the Networks > Node View page to assign IP addresses to each node for one or more networks.

The next two sections provide instructions for assigning IP addresses to nodes for a network using the Networks > Network View page and using the Networks > Node View page, respectively.

Using the Network View page to configure node IP addresses for a network

1. On the Networks > Network View page, in the network list, click the name of the network that you want to configure.
2. In the panel that opens, click the IP Configuration tab.
3. On the IP Configuration panel, in the node IP addresses table at the bottom of the page, specify the IPv4 and IPv6 addresses that you want to assign to each node included in the network:
   a. To assign an IPv4 address to a node, in the row for that node, in the text field in the IPv4 Address column, type the IP address that you want to assign to the node on the IPv4 subnet.
   b. To assign a primary IPv6 address to a node, in the row for that node, in the text field in the IPv6 Address column, type the IP address that you want to assign to the node on the primary IPv6 subnet.
   c. To automatically generate a primary IPv6 address for each node in the HCP system, click Calculate Primary.

If any node already has a primary IPv6 address for the network, the generated primary IPv6 address overwrites the existing address.

You can use Calculate Primary to generate primary IPv6 addresses only if the primary IPv6 address prefix length is 64 or greater.

d. To assign a secondary IPv6 address to a node, in the row for that node, in the text field in the IPv6 Address column, type the IP address that you want to assign to the node on the secondary IPv6 subnet.
e. To automatically generate a secondary IPv6 address for each node in the HCP system, click Calculate Secondary.

If any node already has a secondary IPv6 address for the network, the generated secondary IPv6 address overwrites the existing address.

You can use Calculate Secondary to generate secondary IPv6 addresses only if the secondary IPv6 address prefix length is 64 or greater.

Note:

Fields and buttons used to assign IPv4 and IPv6 addresses to nodes appear only when the applicable IP Mode options are selected on the IP Configuration panel. The IPv4 Address column in the node list table appears only when IPv4 is selected. The IPv6 Address and Secondary IP Address columns in the node list table and Calculate Primary and Calculate Secondary under the node list table appear only when IPv6 is selected.

4. Click Update Settings.

A warning message appears asking you to confirm the changes you've made to the IP configuration settings for the network.

5. In the field in the message window, type `YES`. This is case-sensitive.
6. Click Update Settings.

Using the Node View page to assign network IP addresses to a node

1. On the Networks > Node View page, in the node list, click the number of the node to which you want to assign network IP addresses.
2. On the panel that opens, in the Network Settings table, specify the IP addresses that you want to assign to the node for each network in which you want to include that node:
   a. To assign an IPv4 address to a node for a network, in the row for that network, in the IP field, type the IP address that you want to assign to the node on the IPv4 subnet defined for the network.
   b. To assign a primary IPv6 address to a node for a network, in the row for that network, in the Primary IP field, type the IP address that you want to assign to the node on the primary IPv6 subnet defined for the network.
   c. To automatically generate a primary IPv6 address for the node for each network that is configured to use a primary IPv6 subnet:
      - At the top of the panel, click Calculate IPv6 Addresses.
      - In the Calculate IPv6 Addresses section, click Calculate Primary.

        If any node already has a primary IPv6 address for the network, the generated primary IPv6 address overwrites the existing address.

        You can use Calculate Primary to generate primary IPv6 addresses only if the primary IPv6 address prefix length is 64 or greater.

   d. To assign a secondary IPv6 address to a node for a network, in the row for that network, in the Secondary IP field, type the IP address that you want to assign to the node on the secondary IPv6 subnet defined for the network.
   e. To automatically generate a secondary IPv6 address for the node for each network that is configured to use a secondary IPv6 subnet:
      - At the top of the panel, click Calculate IPv6 Addresses.
      - In the Calculate IPv6 Addresses section, click Calculate Secondary.

        If any node already has a secondary IPv6 address for the network, the generated secondary IPv6 address overwrites the existing address.

        You can use Calculate Secondary to generate secondary IPv6 addresses only if the secondary IPv6 address prefix length is 64 or greater.

3. At the bottom of the page, click Update Settings.

A warning message appears asking you to confirm the changes you've made to the networks for which you've assigned IP addresses to the node.

4. In the field in the message window, type `YES`.

This is case-sensitive.

5. Click Update Settings.

Changing the default downstream DNS configuration settings for a network

When you create a new network with the Create Network wizard, the network is configured to use these default downstream DNS configuration options:

- Hidden primary is disabled
- Notify is disabled
- The refresh rate is three hours

After you have created a new network, at any time, you can use the Networks > Network View page to change these default settings.

1. On the Networks > Network View page, click the name of the network for which you want to change the default downstream DNS configuration settings.
2. Take one of these actions:

   - If the Settings panel opens, go to step 4.

   - If the IP Configuration panel opens, click the Settings tab at the top of the panel to display the Settings panel.

3. On the Settings panel, click Downstream DNS Configuration to view the downstream DNS configuration settings.
4. In the Downstream DNS Configuration section:
   a. To enable hidden primary, select Enable hidden primary.
   b. To enable notify, select Enable notify.
   c. If you are enabling hidden primary or notify, in the Downstream DNS Servers field, type a comma-separated list of between one and ten downstream DNS server IP addresses.

   Spaces are not allowed.

   Note:

   If a secondary IPv6 subnet is defined for the network, then each IPv6 address that you specify in the downstream DNS server list must either be on the secondary IPv6 subnet or be routable from the primary IPv6 gateway that's defined for the network.

d. To change the refresh rate, in the Refresh Rate field, type the new refresh rate.

Changing the advanced downstream DNS configuration settings for a network

If advanced downstream DNS configuration mode is enabled and you have the service role, you can use the Networks > Network View page to directly access the UNIX IP address management for any forward facing network you created, including [hcp_system].

Changes made in advanced downstream DNS configuration mode need to be manually applied to all nodes added to the system. HCP generates a system log message that alerts you if you need to add new nodes to the zone file. If your changes are compatible with new system versions, all modifications carry over through future system upgrades.

1. On the Networks > Network View page, click the network for which you want to change the advanced downstream DNS configuration settings.
2. In the Zone Entry field, make all of your necessary changes.
3. In the Forward Zone field, make all of the your necessary changes.
4. Perform one of the following actions:
   - If you want to discard your changes, click Reset Zone Entry and File. This resets the network to its default downstream DNS configuration settings.
   - If you want to keep your changes, click Update Settings.

   After you click Update, HCP performs a syntax validation check and administers your changes to the HCP system. Before they can take effect however, a system reboot is required.

   During the reboot, if the HCP system finds any issues with your DNS configuration, it reverts all forward facing networks to their default downstream DNS configuration value. If this occurs, advanced downstream DNS configuration mode remains enabled but your changes are not saved.

After your HCP system reboots, it's recommended that you test your DNS access to HCP. If you do not want to keep your changes, click Reset Zone Entry and File in the Advanced DNS Downstream Configuration panel.

Creating a network alias

1. Click Create Network Alias above the network list to open the Create Network Alias wizard.
2. On the Settings page in the wizard:
   a. In the Network Name field, type a unique name for the network alias. Alias names follow the same rules as network names.
   b. In the Aliased Network field, select the network for which you're creating the alias.
3. Click Next.
4. On the Review page in the Create Network Alias wizard, review the network alias configuration settings that you entered.
5. Take one of these actions:
   - If the configuration settings that you entered are incorrect:
     a. Click Previous to return to the Settings page of the wizard and modify your entries as necessary.
     b. When you have corrected all the configuration errors, click Next to return to the Review page.
     c. Click Finish to exit the wizard and create the specified alias for the specified network.
   - If the configuration settings that you entered are correct, click Finish to exit the wizard and create the specified alias for the specified network.

Viewing and modifying properties of a network or network alias

You can use the Networks > Network View page to view all properties of a network or network alias. You can also use this panel to modify any configurable properties of a network or network alias.

You can use the Networks > Network View page to view the network name, IPv4 and IPv6 subnets, and node IP address assignments that are defined for each existing network on the HCP system. You can also use this panel to modify the network IP address assignments that are defined for each node for each existing network on the HCP system.

You can use either the Networks > All Zone Definitions page or the Networks > Network View page to view the DNS zone definition that HCP uses for a network:

- Use the Networks > Network View page to view the DNS zone definition that HCP uses for a specific network.
- Use the Networks > All Zone Definitions page to view the DNS zone definitions that HCP uses for all existing networks.

Viewing properties of a network or network alias on the Network View page

To use the Networks > Network View page to view the properties of a network or network alias, click its name in the network list. The properties of the network or network alias are displayed on three separate panels: Settings, IP Configuration, and Zone Definitions.

If there are no alerts associated with a network or network alias, when you click its name to view its properties, the Settings panel opens. If an alert is associated with a network or network alias, when you click its name to view its properties, the panel that opens is the one used to display the configuration settings that you need to change to fix the problem indicated by the alert.

You can use the tabs at the top of each panel to navigate between the three panels. To display a specific panel, click the corresponding tab.

The next three sections list the network and network alias properties that are displayed on the Settings, IP Configuration, and Zone Definitions panels, respectively.

Network and network alias properties displayed on the Settings panel

The Settings panel displays different properties for networks and network aliases.

For a network, the Settings panel displays these properties:

- The name of the network.
- Whether the network is enabled or disabled.
- The network description (if configured).
- The maximum transmission unit (MTU) used for the network.
- The domain associated with the network.
- The total number of tenant references defined for the network or network alias. This is the number of tenants that are configured to use the network for data access, management, or both purposes.

- The tenant reference list for the network or network alias. This list contains the names of the tenants that are configured to use the network and the purpose for which each tenant uses the network (data access, management, or both purposes).
- The total number of alias references defined for the network. This is the total number of aliases that point to the network.
- The alias reference list for the network. This list contains the names of the network aliases that have been defined for the network.
- The downstream DNS configuration settings for the network.
- The advanced Downstream DNS Configuration settings for the network, if the mode is enabled.

For a network alias, the Settings panel displays these properties:

- The name of the network alias.
- The name of the targeted network. This is the network that the alias points to.
- The total number of tenant references defined for the network alias. This is the number of tenants for which the alias is selected as the data access network, the management network, or both networks.
- The tenant reference list for the network alias. This list contains the names of the tenants for which the alias is selected as the data access network, the management network, or both networks.
- The following properties of the targeted network:
  - The network description (if configured).
  - The maximum transmission unit (MTU) used for the network.
  - The domain associated with the network.
  - The total number of alias references defined for the network. This is the total number of aliases that point to the network.
  - The alias reference list for the network. This list contains the names of the network aliases that have been defined for the network.
  - The downstream DNS configuration settings for the network.

Network and network alias properties displayed on the IP Configuration panel

When you click the name of a network in the network list, the IP Configuration panel displays the IP configuration properties defined for that network.

When you click the name of a network alias in the network list, the IP Configuration panel displays the IP configuration properties defined for the targeted network (that is, the IP configuration properties defined for the network that the alias points to).

The IP Configuration panel displays these properties for a network or for the targeted network of an alias:

- The IP Mode settings that are used for the network. These settings determine whether the network supports IPv4 addresses, IPv6 addresses, or both.
- In the IP Mode section on the panel, if IPv4 is selected, then the network supports IPv4 addresses, and the IP Configuration panel displays these properties:
  - The IPv4 gateway and subnet mask that are defined for the network.
  - The IPv4 subnet that is defined for the network. HCP derives the IPv4 subnet from the IPv4 gateway and subnet mask that are configured for the network.
  - The IPv4 addresses that are assigned to the nodes that are included in the network (if any). These addresses must be on the IPv4 subnet defined for the network.
- If IPv6 is selected, indicating that the network supports IPv6 addresses, the IP Configuration panel displays these properties:
  - The primary IPv6 gateway and the primary IPv6 address prefix length that are defined for the network.
  - The primary IPv6 subnet that is defined for the network. HCP derives the primary IPv6 subnet for the network from the IPv6 gateway and IPv6 address prefix length that are configured for the network.
  - The primary IPv6 addresses that are assigned to the nodes that are included in the network (if any). These addresses must be on the primary IPv6 subnet defined for the network.
  - Whether or not a secondary IPv6 subnet is defined for the network.
  - If a secondary IPv6 subnet is defined for the network, the IP Configuration panel displays these additional properties:
    - The secondary IPv6 gateway and the secondary IPv6 address prefix length that are defined for the network.
    - The secondary IPv6 subnet that is defined for the network. HCP derives the secondary IPv6 subnet for the network from the IPv6 gateway and IPv6 address prefix length that are configured for the network.
    - The secondary IPv6 addresses that are assigned to the nodes that are included in the network. These addresses must be on the secondary IPv6 subnet defined for the network.
- A list of nodes that do not have any IPv4 or IPv6 addresses assigned to them for the network. These nodes are not included in the network.

Network and network alias properties displayed on the Zone Definitions panel

HCP automatically creates and maintains a DNS zone definition for the network domain used for each network defined on the system.

When you click the name of a network in the network list, the Zone Definitions panel displays the DNS zone definition that HCP uses for that network.

When you click the name of a network alias in the network list, the Zone Definitions panel displays the DNS zone definition that HCP uses for the targeted network (that is, the DNS zone definition that HCP uses for the network that the alias points to).

Viewing properties of a network on the Node View page

To use the Networks > Network View page to view the properties of a network or network alias, click its name in the network list. The properties of the network or network alias are displayed on three separate panels: Settings, IP Configuration, and Zone Definitions.

If there are no alerts associated with a network or network alias, when you click its name to view its properties, the Settings panel opens. If an alert is associated with a network or network alias, when you click its name to view its properties, the panel that opens is the one used to display the configuration settings that you need to change to fix the problem indicated by the alert.

You can use the tabs at the top of each panel to navigate between the three panels. To display a specific panel, click the corresponding tab.

The next three sections list the network and network alias properties that are displayed on the Settings, IP Configuration, and Zone Definitions panels, respectively.

Viewing the DNS zone definition for a network domain

If you're using DNS for domain name resolution, you need to add each domain you associate with a network to your DNS. If the domain for the network you're using for replication is shared with other networks, you need to add this additional domain to the DNS:

`replication.admin.`*`replicaton-network-domain-name`*

You can use either the Networks > All Zone Definitions page or the Networks > Network View page to view the DNS zone definition that HCP uses for a network:

- Use the Networks > Network View page to view the DNS zone definition that HCP uses for a specific network.
- Use the Networks > All Zone Definitions page to view the DNS zone definitions that HCP uses for all existing networks.

The DNS zone definition for each network domain is displayed in the format used for DNS zone definitions on Unix DNS servers. To add a network domain to your DNS, you can copy its DNS zone definition directly from the HCP System Management Console into your DNS.

If hidden primary or notify is enabled for a network, the domain associated with that network is defined as a secondary zone. Otherwise, the network domain is defined as a stub zone.

Viewing the DNS zone definition for a specific network

To display the DNS zone definition for the domain associated with a specific network:

1. On the Networks > Network View page, in the network list, click the name of the network for which you want to display the DNS zone definition, or click the name of an alias that points to that network.
2. At the top of the panel that opens, click the Zone Definitions tab.

   The Zone Definitions panel opens. This panel shows the secondary or stub zone definition that HCP uses for the network domain, formatted as shown in this example:

```
# net5 Network for Customer-1
zone "object-store.cust1.com" IN {
    type slave;
    file "/var/named/slave/object-store.cust1.com";
    masters {
         192.168.10.101;
         2001:0db8::101 ;
         192.168.10.102;
         2001:0db8::102;
         192.168.10.103;
         2001:0db8::103;
         192.168.10.104;
         2001:0db8::104;
     };
};
```

   Tip: You can use the Zone Definition link on the Replication page to show the zone definition for a user-defined network that's selected for replication.

Viewing the DNS zone definitions for all existing networks

To display the DNS zone definitions for all network domains defined on the HCP system, go to the Networks > All Zone Definitions page.

The Networks > All Zone Definitions page shows the DNS zone definitions that HCP uses for all existing network domains.

Considerations for modifying properties of networks and network aliases

The following considerations apply to modifying properties of networks and network aliases:

- You can modify only the configurable properties of a network or network alias. You cannot modify any property that has a value that's generated or derived by HCP.
- You cannot change the name of a network while that network is associated with a tenant or referenced by an alias. You cannot change the name of an alias while that alias is associated with a tenant.
- You cannot change a network to an alias or an alias to a network.
- When you take any of these actions for a network, communication on that network is temporarily disrupted:
  - Modify the VLAN ID or MTU. However, in the case of MTU, applications may not notice the disruption.
  - Modify the IPv4 gateway or netmask (if defined)
  - Modify the primary or secondary IPv6 gateway or IPv6 address prefix length (if defined)
  - Add or remove all settings for the secondary IPv6 configuration, including the gateway, prefix length, and node IP addresses
  - Disable support for IPv4 addresses, which automatically removes all IPv4 configuration settings, including the gateway, subnet mask, and node IP addresses. (Removing all these settings automatically disables support for IPv4 addresses.)
  - Disable support for IPv6 addresses, which automatically removes all IPv6 configuration settings, including the gateway, prefix length, and node IP addresses for the primary IPv6 subnet and, if defined, for the secondary IPv6 subnet. (Removing all these settings automatically disables support for IPv6 addresses.)
  - Add or remove the IP address assignments for one or more nodes
- The following considerations apply to modifying the IP Configuration settings for a network:
  - The [hcp_system] network IP mode determines the IP modes that are supported for user-defined networks:
    - You can configure a network to use a specific type of IP address (IPv4 or IPv6) only if the [hcp_system] network is also configured to use that type of IP address. However, If the [hcp_system] network is configured to use both IPv4 and IPv6 addresses, you can configure a network to use only IPv4 addresses, only IPv6 addresses, or both types of IP addresses.
    - If the [hcp_system] network is configured to use IPv6 addresses, you can configure a network to use a primary IPv6 subnet and, optionally, a secondary IPv6 subnet. The number of IPv6 subnets that are defined for the [hcp_system] network does not affect the number of IPv6 gateways that can be defined for a user-defined network.
  - To configure a network to use an IPv4 subnet, you need to define both the gateway and the subnet mask for that IPv4 subnet.
  - You can assign IPv4 addresses to nodes for a network only if an IPv4 subnet is defined for that network. All IPv4 addresses defined for a network must be on the IPv4 subnet defined for that network.
  - To configure a network to use an IPv6 subnet (whether it's a primary or secondary IPv6 subnet), you need to define both the gateway and the prefix length for that subnet.
  - A secondary IPv6 subnet can be defined for a network only if a primary IPv6 subnet is also defined for that network.
  - When hidden primary or notify is enabled for a network, if you configure that network to use a secondary IPv6 subnet, you also need to review and, if necessary, modify the list of downstream DNS server IP addresses configured for that network to ensure that each IPv6 address either is on the secondary IPv6 subnet or is routable from the primary IPv6 gateway that's defined for the network.
  - You can assign primary IPv6 addresses to nodes for a network only if a primary IPv6 subnet is defined for that network. All primary IPv6 addresses defined for a network must be on the primary IPv6 subnet defined for that network.
  - You can assign secondary IPv6 addresses to nodes for a network only if a secondary IPv6 subnet is defined for that network. All secondary IPv6 addresses defined for a network must be on the secondary IPv6 subnet defined for that network.
  - To include a node in a network, you need to assign a separate IP address to that node on each IPv4 and IPv6 subnet that is defined for the network.
    Note: To configure a partial network, you need to ensure that each node in the HCP system either has no IP addresses for the network or has an IP address on every IPv4 and IPv6 subnet that is defined for the network.
- Selecting a different domain for a network has no effect on requests currently being serviced over that network. However, in subsequent requests, clients using that network need to specify the new domain name in the request URL.

- If the HCP system is configured for DNS and you select a different domain for a network, make sure you change the domain name in the DNS to specify the name of the new domain for the network.
- After you select a different domain for a network that's being used for tenant management, any clients connected to the Tenant Management Console for the applicable tenants at the time of the change need to close all browser windows to clear cookies so they can access the Console using the new domain name.
- If you select a different domain for the network that's used for replication and the other system in the replication pair identifies the current system by its domain name, you need to modify the domain name in the definition of the replication link. Similarly, if you change the node IP addresses for the network that's used for replication and the other system in the replication pair identifies the current system by its IP addresses, you need to modify the IP addresses in the definition of the replication link.
- For the network that's currently selected for replication, all nodes must have IP addresses. You can change but cannot remove IP addresses for that network.
- You can disable or reenable a network at any time. If you disable the network that's currently selected for replication, the status of all replication links in which the HCP system participates changes to broken, and replication or recovery, as applicable, stops on those links. If you then reenable the network, replication or recovery resumes automatically on those links.

Modifying a network

You can use the Networks > Network View page to view and modify any configurable properties of a network or network alias.

You can use the Networks > Node View page to modify the network IP address assignments that are defined for each node for each existing network on the HCP system.

The next two sections provide instructions for modifying a network using the Networks > Network View page and using the Networks > Node View page, respectively.

Modifying a network on the Network View panel

1. On the Networks > Network View page, in the network list, click the name of the network that you want to modify.

   The properties of the network are displayed on three separate panels: Settings, IP Configuration, and DNS Zone Definitions.

   If there are no alerts associated with a network, when you click its name in the network list, the Settings panel opens.

   If an alert is associated with a network, when you click its name in the network list, the panel that opens is the one used to display the network configuration settings that you need to change to fix the problem indicated by the alert.

2. On the panel that opens, either change the settings displayed on the panel or click the applicable navigation tab to display the panel that has the settings you want to change:
   a. On the Settings panel, you can:
      - Enable or disable the network. To do this, select the applicable option in the Network Status field in the top right corner of the panel.
        Note: If you enable or disable the [hcp_management] network, the HCP system restarts.
      - Use the fields that are displayed by default to change any of these general network configuration settings: network name, description, domain, and MTU.
      - If Downstream DNS Configuration basic mode is enabled, display the applicable fields and change the Downstream DNS Configuration settings for the network.
      - If the advanced downstream DNS configuration mode is enabled, display the applicable fields and change the downstream DNS configuration settings for the network.

   b. On the IP Configuration panel, you can:
      - Use the Make untagged network and VLAN ID fields to specify whether the network is tagged or untagged and to specify the VLAN ID for a tagged network, respectively.
      - If HCP is configured to support both IPv4 and IPv6 addresses for user-defined networks, use the fields in the IP Mode section to change the IP mode for the network.

        If you select an IP Mode option that was not previously selected, the IP Configuration panel displays the fields that you need to use to configure the network to use the specified type of IP addresses. If you deselect an option that was previously unselected, the panel hides all IP configuration settings associated with that option.

      - Depending on the IP mode selected for the network, use the fields in the IPv4 Configuration section, the IPv6 Configuration section, or both sections to specify the IPv4 gateway and subnet mask for the IPv4 subnet and to specify the IPv6 gateway and prefix length for each IPv6 subnet, respectively.
      - At the bottom of the IP Configuration panel, use the fields in the node IP addresses table, and optionally, use Calculate Primary and Calculate Secondary below the table to assign IP addresses to each node included in the network.

   You cannot use the Zone Definitions panel to change any network configuration settings.

3. When you finish modifying settings on the selected panel, click Update Settings at the bottom of the page.

   A warning message appears asking you to confirm the changes you've made.

4. In the field in the message window, type `YES`. This is case-sensitive.
5. Click Update Settings.
6. Optionally, to change additional network configuration settings on another panel, click the applicable navigation tab to display that panel. Then, repeat steps 3-6 above to make the additional changes to the network configuration.
7. After your finish making changes in the network configuration section, go to the Networks > Network View page to return to the network list.

Modifying network IP address assignments for a node on the Node View page

You can use the Networks > Node View page to modify the network IP address assignments that are defined for each node for each existing network on the HCP system.

1. On the Networks > Node View page, in the node list, click the number of one of the nodes for which you want to modify network IP address assignments.
2. On the panel that opens, use the fields in the Network Settings table, and optionally, use the buttons in the Calculate IPv6 Addresses section above the table to assign IP addresses to the node for each network in which you want to include that node.
3. When you finish modifying the network IP address assignments for the node, click Update Settings at the bottom of the page.

   A warning message appears asking you to confirm the changes you've made.

4. In the field in the message window, type `YES`. This is case-sensitive.
5. Click Update Settings.

Modifying a network alias

You can use the Networks > Network View page to change the name of the alias or to select a different targeted network for the alias (that is, configure the alias to point to a different network.

Note: When you click the name of a network alias in the network list, you can view the configuration settings used for the targeted network, but you cannot change them.

1. On the Networks > Network View page, in the network list, click the name of the network alias that you want to modify.
2. Take one of these actions:
   - If the Settings panel opens, go to step 4.
   - If the IP Configuration panel opens, click the Settings tab at the top of the panel to display the Settings panel.
3. On the Settings panel, take one or both of these actions:
   - To change the name of the alias, edit the text in the Network Alias Name field.
   - To change the targeted network for the alias:
     a. Select Switch targeted network.

     The panel displays the Aliased Network field, showing the name of the network that the alias currently points to.

     b. In the Aliased Network field, select the new targeted network for the alias.
4. Click Update Settings.

   A warning message appears asking you to confirm the changes you've made.

5. In the field in the message window, type `YES`. This is case-sensitive.
6. Click Update Settings.

Restarting a network

If a tagged network is enabled but traffic on it is not reaching the HCP system, the cause may be that the network interface cannot be found. In this case, both the Overview and Networks pages in the HCP System Management Console display an alert about the condition.

To resolve this issue, you can restart the network. Restarting a network causes HCP to recreate the network interface that corresponds to the network VLAN ID.

You should not restart a network for which the network interface is functioning properly. Restarting a working network temporarily stops communications on that network from reaching HCP.

Note:

Before restarting a network, ensure that the physical network is functioning properly.

1. On the Networks > Network View page, in the network list, click the name of the network that you want to restart.
2. At the bottom of the panel that opens, click Restart Network.

   A warning message appears asking you to confirm the action.

3. In the field in the message window, type `YES`. This is case-sensitive.
4. Click Update Settings.

Deleting a network or network alias

You can delete a user-defined network or network alias only if it's not currently selected for use for any purpose. Additionally, you cannot delete a network that is currently the target of a network alias.

You cannot delete the [hcp_system] or [hcp_backend] network.

1. On the Networks > Network View page, in the network list, click the delete control ( ) for the network or network alias that you want to delete.
2. In response to the confirming message, take one of these actions:
   - If you're sure you want to delete the network or network alias, click Delete.
   - If you decide not to delete the network or network alias, click Cancel.

Tenant administration

Tenants are the administrative entities that own and manage namespaces. When an HCP system is first installed, no tenants exist. You use the HCP System Management Console to create them as needed.

Tenant-level administrators create HCP namespaces in the Tenant Management Console. When you create the default tenant, HCP automatically creates the default namespace.

After creating a tenant, you can modify only some of its properties. You can delete a tenant only if it has no namespaces.

This section of the help contains information about:

- The information displayed for tenants
- Creating, modifying, and deleting tenants
- Accessing the Tenant Management Console for a tenant
- Resetting tenant security (HCP tenants only)
- Changing the product branding that's exposed to tenants
- Selecting the protocol optimization option you want for the tenant

About the Tenants page

To view, create, and manage tenants, you use the Tenants page in the HCP System Management Console. To display this page, in the top-level menu, click Tenants.

The Create Tenant bar on the Tenants page shows:

- The total amount of storage currently used by all namespaces in the HCP system
- The total amount of storage still available out of the total storage capacity for the HCP system

The Tenants page also lists the existing tenants.

Note: To view the Tenants page, you need the monitor or administrator role.

Understanding the tenant list

The Tenants page contains a list of existing tenants. For each tenant, the list shows:

- The tenant name.
- In an HCP system that uses virtual networking, the network assigned to the tenant for management purposes.
- In an HCP system that uses virtual networking, the network assigned to the tenant for data access purposes.
- Icons for any current alerts that apply to the tenant. Alerts indicate conditions that may need your attention. To see the text that accompanies an alert icon, hover your cursor over the icon.
- The total amount of storage currently used by all the tenant's namespaces.
- For HCP tenants only, a graphical representation of the amount of storage used out of the hard quota for the tenant.
- For HCP tenants only, the hard quota for the tenant.
- For the default tenant and for each HCP tenant that has been configured to allow system-level users to manage it and search its namespaces, an icon ( ) that you can click to open the Tenant Management Console for the tenant.

To view additional information about an individual tenant, click the tenant name.

Managing the tenant list

By default, the tenant list on the Tenants page includes all existing tenants. The tenants are listed 20 at a time in ascending order by tenant name.

You can page through, sort, and filter the list of tenants. The Tenants page indicates which tenants are shown out of the total number of tenants in the current list.

Paging

You can change the number of tenants shown at a time on the Tenants page. To do this, in the Items per page field, select the number of tenants you want. The options are 10, 20, and 50.

To page forward or backward through the tenant list, click the next ( ) or back ( ) control, respectively.

To view the Tenants page, you need the monitor or administrator role.

1. In the Page field, type the page number you want.
2. Press Enter.

Sorting

You can sort the tenant list in ascending or descending order by tenant name, management network, data access network, or hard quota. To sort the list, click the column heading for the property you want to sort by. Each time you click the column heading, the sort order switches between ascending and descending.

Filtering

You can filter the tenant list by tenant name, management network, data access network, or tag. The filtered list includes only those tenants with a name, management network, data access network, or tag, as applicable, that begins with or is the same as a specified text string.

You can filter the tenant list by using the fields above the list. You can also filter the list by tag using the tag control.

To view the Tenants page, you need the monitor or administrator role.

1. In the field above the Name column, select the property you want to filter by.
2. In the next field, type the text string you want to use as a filter. This string can be up to 64 characters long, can contain any valid UTF-8 characters except commas (,), and is not case sensitive. White space is allowed.
3. Click the find control ( ).
4. To redisplay the entire list of tenants after filtering it, click the clear filter control ( ).

Filter the tenant list by tag using the tag control

1. Click the tag control ( ) on the right above the tenant list.
   The Tags window opens. This window lists all the tags currently associated with the existing tenants. For each tag, the window shows the number of associated tenants.
2. Click the tenant-count icon ( ) for the tag you want.
   The tenant list shows only the tenants that have the selected tag, and the fields above the Name column show the filter criteria.

About the tenant Overview panel

The tenant Overview panel shows the current status of any given tenant. You can display this panel for a tenant.

To view the Tenants page, you need the monitor or administrator role. To view the tenant Overview panel, you need the monitor or administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. In the list of tenants, click the name of the tenant that you want to examine.
3. To return to the tenant Overview panel from the tenant Settings panel, click Overview in the row of tabs below the tenant name.

Tenant URL

The top of the tenant Overview panel shows the URL for access to the Tenant Management Console for the tenant. The URL has this format:

`https://tenant-url-name.hcp-domain-name:8000`

In this format, *hcp-domain-name* is the name of the domain associated with the management network for the tenant.

For example, the URL for access to the Tenant Management Console for the tenant named Finance in the HCP system named hcp-ma.example.com is:

`https://finance.hcp-ma.example.com:8000`

Clicking a tenant URL opens either the Overview page or the login page for the Tenant Management Console for that tenant:

- If a tenant is configured to allow system-level users to manage it, clicking the URL for that tenant opens its Tenant Management Console Overview page. For an HCP tenant, the Overview page opens only if at least one of your client IP addresses is allowed access to the Tenant Management Console for the tenant.
- If the tenant is not configured to allow system-level users to manage it, clicking the URL for that tenant opens its Tenant Management Console login page.

You can also use the access control ( ) for a tenant to click through to the Tenant Management Console.

Tenant description

The tenant Overview panel shows the tenant description, if any, below the tenant URL. This is optional text that you can specify when creating or modifying the tenant.

Features Enabled section

The Features Enabled section of the tenant Overview panel lists the features that are enabled for the tenant. Possibilities are:

Replication
: The tenant is eligible for replication.

Retention Mode Selection

- An HCP tenant administrator can create namespaces in either enterprise or compliance mode. Additionally, a tenant administrator can change the retention mode of a namespace from enterprise to compliance.

  Without this feature, tenant administrators can create namespaces only in enterprise mode and cannot subsequently change the retention mode.

- The default tenant administrator can change the retention mode of the default namespace from enterprise mode to compliance mode (if the namespace was originally in enterprise mode).

Search
: Tenant administrators can enable and disable search in the namespaces that the tenant owns.

Service Plan Selection
: Tenant administrators can associate service plans with the namespaces that the tenant owns.

  If the tenant does not have this feature, the HCP system administrator chooses the service plan for the tenant, and that service plan applies to all namespaces owned by that tenant.

Versioning
: Tenant administrators can enable and disable versioning in the namespaces that the tenant owns. This feature is available only for HCP tenants.

Namespaces section

For HCP tenants only, the Namespaces section of the tenant Overview panel shows:

Quota
: The number of namespaces that HCP reserves for the tenant out of the total number of namespaces that the system can have. This is also the maximum number of namespaces that the tenant can own at any given time. If the tenant doesn't have a namespace quota, this field displays No Quota.

Used
: The number of namespaces the tenant currently owns.

Available
: If the tenant has a quota, this is the number of additional namespaces that the tenant can own. If the tenant has no quota, this is the number of unallocated namespaces out of the total number of namespaces the system can have, minus the number of existing namespaces owned by tenants that don't have quotas.

When calculating the number of available namespaces for a tenant with no quota, HCP considers only locally created namespaces and not namespaces that were replicated to the system from another system

Objects section

The Objects section of the tenant Overview panel shows:

Ingested
: The total number of objects currently stored in all the tenant's namespaces. Each version of an object counts as a separate object. However, the object count does not include *delete markers* or *delete records*. When you delete an object from a versioning-enabled namespace, a delete marker is created to indicate that the object has been deleted. A delete marker has a version ID but does not have any data or metadata. For more information on delete markers and delete records please see *Enabling delete markers* section in Versioning.

  Multipart objects are each counted as a single object. Objects that are in the process of being created by a multipart upload are not included in the object count.

Indexed
: The total number of indexed objects currently stored in all the tenant's namespaces. This item appears only if the tenant has the search feature and a search facility is currently selected for use with the Search Console.

Erasure coded
: The total number of erasure-coded objects in all the tenant's namespaces. An object is counted as erasure coded if a chunk for it is stored on the current system.

  Each multipart object counts as one object even though the parts of a multipart object are erasure coded independently of each other.

Storage section

For HCP tenants only, the Overview panel includes a Storage section. This section shows:

Quota
: The total amount of storage available to the tenant for allocation to its namespaces.

Used
: The total amount of storage currently used by all the tenant's namespaces to store object data, system and custom metadata, and any redundant data required to satisfy data protection level and metadata protection level settings in service plans.

  Used storage includes storage occupied by the parts of in-progress multipart uploads that have already been written to the repository. Used storage does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

  Note: The size of the data for an object created by a completed multipart upload may be slightly less than the total size of the parts before the multipart upload was completed.

Available
: The amount of unused storage still available to the tenant.

Creating a tenant

The information you provide when creating the default tenant differs from the information you provide for HCP tenants. This is because:

- When you create the default tenant, HCP automatically creates the default namespace as well
- HCP administers storage usage differently for the default tenant

This section contains separate procedures for creating the two types of tenants.

Note: To create an HCP tenant or the default tenant and namespace, you need the administrator role.

You can create the default tenant and namespace only if allowed to do so by the system configuration.

Creating an HCP tenant

You create HCP tenants in the System Management Console. After an HCP tenant exists, tenant administrators can use the Tenant Management Console to create namespaces for the tenant.

HCP tenant properties

You specify a set of properties when you create a tenant.

You can specify the following tenant properties:

- A *name* for the tenant. This name determines the URL for the tenant.

  When naming tenants, keep in mind that each tenant name must be unique within an HCP system. For example, you cannot create a tenant named finance for each of two different customers. You could, however, create a tenant named cust1-finance for Customer 1 and another tenant named cust2-finance for Customer 2.

  Also, keep in mind that you cannot replicate a tenant to another HCP system that already has a different tenant with the same name.

  You can change the tenant name at any time after you create the tenant, except while the CIFS or NFS protocol is enabled for any of the tenant's namespaces. However, keep in mind that when you change the tenant name, you are also changing the URLs for the tenant and its namespaces.

  Be sure to notify the tenant contact when you change the name of a tenant.

- Optionally, a *description* of the tenant. For example, you can use a description to specify the name of the organization for which you're creating the tenant.

  You can change this description at any time after you create the tenant.

- In an HCP system that uses virtual networking and has the management network enabled at the System Management Console, a management network for the tenant. Clients use this network to access the Tenant Management Console and HCP management API for the tenant. Clients use the domain name associated with this network when sending access requests to the management interfaces (Tenant Management Console and HCP management API) for the tenant.

  You need to ensure that requests for access to the Tenant Management Console and HCP management API for the tenant are routable from the clients to the HCP system over the management network that you specify.

  If the tenant is configured to allow system-level users to manage it, those users can access its Tenant Management Console directly from the System Management Console even if the tenant management network is not [hcp_system].

  You can select a different management network for a tenant at any time. However, when you change the management network, you also change:

  - The IP addresses used to route access requests from clients to the management interfaces (Tenant Management Console and HCP management interface) for the tenant
  - The management network domain name included in the tenant URL.

    Be sure to notify the tenant contact when you select a different management network for a tenant.

- In an HCP system that utilizes virtual networking, a data access network is provided for the tenant. Clients use this network to access the contents of namespaces that the tenant owns. Clients use the domain name associated with this network when sending namespace data access requests to the tenant.

  You need to ensure that requests for access to the contents of the namespaces that the tenant owns are routable from the clients to the HCP system over the data access network that you specify.

  You can select a different data access network for a tenant at any time. However, when you change the data access network, you also change:

  - The IP addresses used to route namespace data access requests from clients to the tenant
  - The domain name included in the URLs for the namespaces that the tenant owns

  Changing the IP addresses and domain name used to access the namespaces that a tenant owns causes all CIFS and NFS mounts of those namespaces to be disconnected from HCP.

  Be sure to notify the tenant contact when you select a different data access network for a tenant.

- A *hard quota* for the tenant. This is the total amount of storage available to the tenant. The tenant allocates this storage to the namespaces it owns by setting a hard quota for each namespace.

  You can allocate more total space to your tenants than is actually available for storing objects. HCP warns you when the space used by all tenants is approaching the system storage capacity.

  You can change this quota at any time after you create the tenant. However, you cannot specify a quota that is less than the total amount of storage that the tenant has already allocated to its namespaces.

  HCP checks the amount of data stored in a namespace against the namespace hard quota hourly. If large amounts of data are added rapidly to a namespace, the namespace can store substantially more data than its hard quota allows.

  Each namespace managed by a tenant can exceed its hard quota in this way. As a result, the total amount of storage used by all namespaces owned by a tenant can exceed the hard quota for that tenant.

- A *soft quota* for the tenant. This is the percentage point at which HCP should notify tenant administrators that the storage available to the tenant is running low on free space.

  You can change this quota any time after you create the tenant.

- A *namespace quota* for the tenant. This is the number of namespaces that HCP reserves for the tenant out of the total number of namespaces that the system can have (10,000).

  You cannot overallocate namespaces. That is, the maximum number of namespaces that you can allocate to tenants is 10,000, or 9,999 if the system includes the default namespace.

  You can create tenants that do not have quotas. The total number of namespaces that these tenants can own is equal to the number of unallocated namespaces in the HCP system. If you allocate a total of 10,000 namespaces to other tenants, the tenants that do not have quotas cannot create any namespaces.

  You can change the namespace quota for a tenant at any time after you create the tenant, as long as the new quota is not less than the number of namespaces that the tenant currently owns.

  While an active/passive replication link that includes a given HCP tenant is failed over to the replica, you cannot change the namespace quota for that tenant on the replica.

- The authentication methods allowed for the tenant. At least one of these authentication methods must be enabled:

  Local
  : The tenant supports internal authentication by HCP. To be authenticated, a user must have a locally authenticated HCP user account.

  RADIUS
  : The tenant supports remote authentication by RADIUS. To be authenticated, a user must have a RADIUS-authenticated HCP user account.

    A tenant that supports RADIUS authentication must also support local authentication, Active Directory authentication, or both.

  Active Directory
  : The tenant supports remote authentication by AD. To be authenticated, a user must have an AD user account.
    Tip: To help ensure that AD authentication is available for those tenants that need to support it, enable AD only for those tenants.

    For RADIUS or Active Directory authentication to work for the tenant to access the Tenant Management Console and HCP management API, the tenant management network must be [hcp_system]. Similarly, for RADIUS or Active Directory authentication to work for the tenant to access the content of the tenant's namespaces, the tenant data access network must be [hcp_system].

    You can change the allowed authentication methods at any time after you create the tenant. However, you cannot disable local authentication if the only tenant-level account with the security role is a locally authenticated HCP user account. Similarly, you cannot disable AD authentication if the only tenant-level account with the security role is a group account.

    If you disable AD authentication for a tenant after the tenant has created group accounts, those accounts continue to exist but are not visible to the tenant. If you subsequently reenable AD authentication for the tenant, the group accounts become visible again.

- An *initial security account* for the tenant. This can be a locally authenticated HCP user account or an HCP group account, depending on which authentication methods are allowed for the tenant:
  - For a locally authenticated user account, you specify the account username and password. When HCP creates the tenant, it also creates a tenant-level user account with the specified username and password. This account has only the security role and no data access permissions.
  - For an HCP group account, you select an AD group. When HCP creates the tenant, it also creates a tenant-level group account that corresponds to that AD group. This group account has only the security role and no data access permissions.

    For the initial security account to be a group account, Active Directory must be selected as an authentication method for the tenant, HCP must be configured to support AD, and HCP must be able to communicate with AD.

  After creating the tenant, you cannot modify the initial security account configuration from the System Management Console. However, tenant administrators can modify the initial security account configuration in the Tenant Management Console.

- Optionally, *contact information* for the tenant. For example, you can specify contact information for the primary person responsible for administering the tenant.

  You can change this information at any time after you create the tenant. Tenant-level administrators can also change this information from the Tenant Management Console.

- Optionally, *tags* for the tenant. A tag is an arbitrary text string associated with an HCP tenant. You can associate up to ten tags with any given tenant, and you can use the same tags for multiple tenants.

  You can use tags to group tenants and filter tenant lists. For example, if you've created multiple tenants for a company named ABC Corporation, you could associate the tag ABC with each of those tenants. Then you could filter a list of tenants to display only the tenants with that tag.

  Tags exist only as long as they are associated with at least one tenant. If you remove a tag from the last tenant with which it's associated, the tag no longer exists.

  You can change the tags associated with the tenant at any time after you create the tenant.

- Whether the tenant can be *replicated*.

  After creating the tenant, you can change this setting from not allowing replication to allowing replication. However, you cannot do the reverse.

- If the tenant can be replicated, whether tenant administrators can choose which cloud-optimized namespaces allow *erasure coding*. If tenant administrators are not allowed to do this, all cloud-optimized namespaces owned by the tenant allow erasure coding.

  After creating the tenant, you can change this setting from having all cloud-optimized namespaces allow erasure coding to allowing tenant administrators to choose which cloud-optimized namespaces allow erasure coding. However, you cannot do the reverse.

  When HCP is upgraded to release 8.0 or later, preexisting tenants are configured such that tenant administrators cannot select erasure coding for namespaces.

- Whether tenant administrators can select the *retention mode* for the namespaces that the tenant owns. If this is not allowed, tenant administrators can create namespaces only in enterprise mode.

  After creating the tenant, you can change this setting from not allowing tenant administrators to select the retention mode to allowing it. However, you cannot do the reverse.

- Whether tenant administrators can enable *search* for the namespaces that the tenant owns.

  After creating the tenant, you can change this setting from not allowing tenant administrators to enable search for the namespaces that the tenant to allowing it. However, you cannot do the reverse.

- Whether tenant administrators can associate *service plans* with the namespaces that the tenant owns. If tenant administrators are not allowed to do this, you need to specify a service plan for the tenant. This specification is not visible in the Tenant Management Console.

  After creating the tenant, you can change this setting from not allowing tenant administrators to associate service plans with the namespaces that the tenant owns to allowing it. However, you cannot do the reverse.

- Whether tenant administrators can enable *versioning* for the namespaces that the tenant owns.

  After creating the tenant, you can change this setting from not allowing tenant administrators to enable versioning for the namespaces that the tenant owns to allowing it. However, you cannot do the reverse.

HCP tenant creation procedure

To create an HCP tenant or the default tenant and namespace, you need the administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. On the Tenants page, click Create Tenant.
3. In the Create Tenant panel:
   a. If the Make default tenant/namespace option is present, leave it unselected. This option does not appear if the default tenant already exists or if the system does not support creation of the default tenant.
   b. In the Tenant Name field, type a unique name for the tenant. HCP derives the host name for the tenant from this name. The host name is used in URLs for access to the tenant and its namespaces.

      In English, the name you specify for a tenant must be from one through 63 characters long, can contain only alphanumeric characters and hyphens (-), and cannot start or end with a hyphen. In other languages, because the derived English hostname cannot be more than 63 characters long, the name that you specify can be limited to fewer than 63 characters.

      Tenant names cannot contain special characters other than hyphens and are not case sensitive. White space is not allowed.

      Tenant names cannot start with xn-- (that is, the characters x and n followed by two hyphens).

      You can reuse tenant names that are not currently in use. So, for example, if you delete a tenant, you can create a new tenant with the same name that you originally assigned to the deleted tenant.

      The following words are reserved and cannot be used as tenant names: admin, cifs, default, fcfs, nfs, scavenging, search, search-api, smb, smtp, snmp, and www.

   c. Optionally, in the Description field, type a description of the tenant. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
   d. In the Management Network field, select the management network for the tenant. The dropdown list of networks does not include empty networks.

      The Management Network field is present only if the HCP system is configured to support virtual networking or has the [hcp_management] network enabled.

   e. In the Data Network field, select the data access network for the tenant. The dropdown list of networks does not include empty networks.

      The Data Network field is present only if the HCP system is configured to support virtual networking.

   f. In the Hard Quota field, type the number of gigabytes (GB) or terabytes (TB) of storage to make available to the tenant and select either GB or TB to indicate the measurement unit. Valid values are decimal numbers with up to two places after the period. The minimum is 1 (one) for GB and .01 for TB.
   g. In the Soft Quota field, type the percentage point at which you want HCP to notify tenant administrators that free storage space is running low. Valid values are integers in the range 0 (zero) through 100.
   h. Take one of these actions:
      - To specify a namespace quota for the tenant, in the Namespace Quota field, type an integer in the range 1 (one) through the current number of namespaces available for allocation.

        The number of available namespaces is displayed below the Namespace Quota field. This number is equal to 10,000 minus the number of namespaces currently allocated to HCP tenants, minus the number of namespaces currently owned by HCP tenants that do not have quotas, minus one for the default namespace, if it exists. If any tenants are above their quotas, the number of excess namespaces is also subtracted from the number of available namespaces.

      - To create the tenant without giving it a namespace quota, select No quota.
   i. In the Authentication Methods section, select one or more of these authentication methods for the tenant: Local, RADIUS, and Active Directory. If you select RADIUS, you also need to select one or both of these RADIUS authentication methods: Local or Active Directory.
   j. In the Initial Security Account section, select Local or Active Directory to specify the type of initial security account that you want to create for the tenant. Then:
      - If you selected Local, specify the user name and password for the initial HCP user account that you want to create for the tenant:
        - In the Username field, type a name for the initial HCP user account for the tenant. Usernames must be from one through 64 characters long, can contain any valid UTF-8 characters, and cannot start with an opening square bracket ([). White space is allowed.

          User names are not case-sensitive.

        - In the Password field, type a password for the initial HCP user account. Passwords can be up to 64 characters long, are case-sensitive, and can contain any valid UTF-8 characters, including white space. The minimum length for the password for the initial user account is six characters.

          To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

        - In the Confirm Password field, type the password again.
      - If you selected Active Directory, in the Group field, specify the name of the AD group account whose credentials you want to use for the initial HCP group account that you want to create for the tenant.
   k. Optionally, specify contact information for the tenant:
      i. Click Contact Information.
      ii. In the Contact Information panel, fill in the contact information. The table below describes the values that you can specify. Except as indicated, all fields are optional.

Field	Description
First Name	First name of the tenant contact. First names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Last Name	The last name of the tenant contact. Last names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Email	A valid email address for the tenant contact. Email addresses cannot be more than 254 characters long.

Field	Description
Confirm Email	A repeat of the email address for the tenant contact. This field is required if you specify an email address in the Email field.
Phone	A telephone number for the tenant contact. Do not include a telephone number extension. Instead, put the extension, if any, in the Extension field. Telephone numbers can contain only numbers, parentheses, hyphens (-), periods (.), plus signs (+), and spaces and can be up to 24 characters long (for example, (800) 123-4567).
Extension	A telephone number extension for the tenant contact. Telephone number extensions can contain only numbers and can be up to five characters long.
Address Line 1	The first line of an address for the tenant contact. Address lines can be up to 100 characters long and can contain any valid UTF-8 characters, including white space.
Address Line 2	The second line of an address for the tenant contact.
City	The city for the tenant contact. City names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
State/Province	The state or province for the tenant contact. State and province names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Postal Code	The postal code for the tenant contact. Postal codes can be up to 64 characters long and can contain only alphanumeric characters and hyphens (-).
Country	The country for the tenant contact. Country names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.

l. Optionally, associate tags with the tenant:
   i. Click Tags.
   ii. For each tag you want to associate with the tenant:
      1. In the field in the Tags section, type a text string to be used as a tag. Tags must be from one through 64 characters long, can contain any valid UTF-8 characters except commas (,), and are not case sensitive. White space is allowed.
      2. Click Add Tag.

         To remove a new tag, click the delete control ( ) for the tag.

m. Optionally, select Replication to allow the tenant to be replicated. This option is present only if the HCP system supports replication.

   If you select Replication, take one of these actions:

   - To have all cloud-optimized namespaces that the tenant owns allow erasure coding, select All cloud-optimized namespaces.
   - To allow tenant administrators to choose which cloud-optimized namespaces allow, select Selected namespaces.

n. Optionally, select Retention Mode Selection to allow tenant administrators to select the retention mode for the namespaces that the tenant owns.
o. Optionally, select Search to allow tenant administrators to enable search for the namespaces that the tenant owns.
p. Take one of these actions:
   - To allow tenant administrators to associate service plans with the namespaces that the tenant owns, select Service Plan Selection.
   - To associate a service plan with the tenant, leave Service Plan Selection unselected. Then either type the name of an existing service plan in the accompanying field or click the arrow control ( ) for the field. If you click the arrow control:
      i. In the Service Plans window, select the service plan that you want to assign to the tenant.
      ii. Click Apply Service Plan.
q. Optionally, select Versioning to allow tenant administrators to enable versioning for the namespaces that the tenant owns.

4. Click Create Tenant.

Creating the default tenant and namespace

You create the default tenant and namespace in a single operation in the HCP System Management Console. The name of the default tenant is always *Default*. Similarly, the name of the default namespace is always *Default*.

You can create the default tenant and namespace only if allowed to do so by the HCP system configuration.

Default tenant and namespace properties

When creating the default tenant and namespace, you specify:

- Optionally, a description of the tenant. For example, you can use a description to specify the purpose of the tenant.

  You can change this description at any time after you create the tenant and namespace.

- Optionally, contact information for the tenant. For example, you can specify contact information for the primary person responsible for administering the default tenant and namespace.

  You can change this information at any time after you create the tenant and namespace. You can change it either from the System Management Console or from the Tenant Management Console for the default tenant.

- The cryptographic hash algorithm used to calculate the hash value for each object in the namespace. After creating the tenant and namespace, you cannot change the hash algorithm.
- The retention mode for the namespace — either enterprise or compliance. Tenant administrators can use the Tenant Management Console to change this setting from enterprise to compliance. However, they cannot do the reverse.
- Whether the namespace is search-enabled. Tenant administrators can use the Tenant Management Console to change this setting at any time.
- The service plan for the namespace. Tenant administrators can change use the Tenant Management Console to change this setting at any time.

Default tenant and namespace creation procedure

To create an HCP tenant or the default tenant and namespace, you need the administrator role.

1. In the top-level menu of the System Management Console, click Tenants.

2. On the Tenants page, click Create Tenant.
   The Create Tenant panel opens.
3. In the Create Tenant panel, select Make default tenant/namespace.
   The Create Tenant panel changes to show the applicable options for the default tenant.
4. In the Create Tenant panel:
   a. Optionally, in the Description field, type a description of the tenant.

      The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

   b. Optionally, specify contact information for the tenant:
      i. Click Contact Information.
      ii. In the Contact Information panel, fill in the contact information. The table below describes the values that you can specify. Except as indicated, all fields are optional.

Field	Description
First Name	First name of the tenant contact. First names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Last Name	The last name of the tenant contact. Last names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Email	A valid email address for the tenant contact. Email addresses cannot be more than 254 characters long.
Confirm Email	A repeat of the email address for the tenant contact. This field is required if you specify an email address in the Email field.
Phone	A telephone number for the tenant contact. Do not include a telephone number extension. Instead, put the extension, if any, in the Extension field. Telephone numbers can contain only numbers, parentheses, hyphens (-), periods (.), plus signs (+), and spaces and can be up to 24 characters long (for example, (800) 123-4567).
Extension	A telephone number extension for the tenant contact. Telephone number extensions can contain only numbers and can be up to five characters long.
Address Line 1	The first line of an address for the tenant contact. Address lines can be up to 100 characters long and can contain any valid UTF-8 characters, including white space.
Address Line 2	The second line of an address for the tenant contact.
City	The city for the tenant contact. City names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
State/Province	The state or province for the tenant contact. State and province names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
Postal Code	The postal code for the tenant contact. Postal codes can be up to 64 characters long and can contain only alphanumeric characters and hyphens (-).
Country	The country for the tenant contact. Country names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.

   c. In the Hash Algorithm field, select the cryptographic hash algorithm for the default namespace.
   d. For Retention Mode, select either Enterprise or Compliance to set the retention mode of the default namespace.
   e. Optionally, select Enable Search to enable search for the default namespace.
   f. In the Service Plan field, specify the service plan for the default namespace. To do this, either type the name of an existing service plan in the accompanying field or click the arrow control ( ) for the field. If you click the arrow control:
      i. In the Service Plans window, select the service plan that you want to assign to the default namespace.
      ii. Click Apply Service Plan.
5. Click Create Tenant.

Accessing the Tenant Management Console for a tenant

If a tenant is configured to allow system-level users to manage it, you can open the Tenant Management Console for that tenant directly from the HCP System Management Console. You can use this method to access the Tenant Management Console for an HCP tenant only if at least one of your client IP addresses is allowed access to the Tenant Management Console for that tenant.

To access the Tenant Management Console directly from the System Management Console, you need the monitor or administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. Take one of these actions:
   - In the list of tenants, click the access control ( ) for the tenant that you want to access.
   - In the list of tenants, click the name of the tenant that you want to access. Then click the tenant URL in the tenant Overview panel.

   The browser window switches to the tenant Overview page in the Tenant Management Console.
3. To return to the System Management Console from the Tenant Management Console, click the return control ( ) in the top right corner of the Tenant Management Console window.
   Note: After opening a Tenant Management Console from the System Management Console, do not use the browser back button to return to the System Management Console. Doing so can have unpredictable results.

Modifying a tenant

After creating a tenant, you can modify some of its properties. You do this by using the Settings and Security panels on the Tenants tab for the tenant.

Note: To view the Settings and Tenants panels, you need the monitor or administrator role. To modify a tenant, you need the administrator role.

These considerations apply to modifying HCP tenants:

- You can enable AD authentication for a tenant only while HCP can communicate with AD.
- When you rename a tenant for which AD authentication is enabled, AD authentication is automatically disabled for that tenant. After the operation is complete, you need to manually reenable AD authentication for the tenant.
- You cannot rename a tenant while the only account with the security role defined for the tenant is a group account.
- You cannot rename a tenant while the CIFS or NFS protocol is enabled for any namespaces owned by that tenant.
- When you select a different management network for an HCP tenant while any given user is logged in to the Tenant Management Console for that tenant, HCP denies any subsequent requests made within the same Console session. To continue using the Console, you must start a new session so that the client can use the new management network to access the Console for the tenant.
- When you select a different data access network for an HCP tenant, HCP denies any client requests for access to namespaces owned by that tenant that arrive over the previously selected network.
- When a tenant is replicated from one system to a second system, if the management or data access network selected for the tenant on the first system does not exist on the second system, the applicable field in the tenant Settings panel on the second system shows the network name enclosed in angle brackets (for example, <ten1_data>). This network is not included in the dropdown list for the field, so if you select a different network in that field, you cannot then select the undefined network.
- You can change the service plan that's assigned to a specific tenant by modifying the tenant to select the new service plan or by modifying the new service plan to assign it to the tenant. You can also modify a service plan to assign it to multiple tenants at the same time.

  To modify the configuration settings for an individual tenant, including selecting a new service plan for that tenant, follow the procedure outlined below.

Modifying tenant properties

You can modify some properties for a tenant by using the Settings panel for the tenant.

To view the Settings panel, you need the monitor or administrator role. To modify a tenant, you need the administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. In the list of tenants, click the name of the tenant that you want to modify.
3. In the row of tabs below the tenant name, click Settings.
4. In the Settings panel, make the changes you want.

   To remove a tag from an HCP tenant, in the Tags section in the Settings panel, click the delete control ( ) for the tag. The row with the tag turns red. To revert the removal before submitting your changes, click again on the delete control.

5. Click Update Settings.
   If all of these are true, a confirming message appears:
   - You changed the name of the tenant.
   - The tenant supports AD authentication.
   - HCP cannot communicate with AD.

In response to the confirming message, click Update Settings.

Tenant-level CORS rules configuration

You can configure CORS rules at the tenant level to serve as the default configuration for all namespaces owned by a tenant. This practice is useful in deployments where a large number of namespaces support the same CORS configuration.

To configure the default CORS settings for all namespaces owned by a tenant, use either the System Management Console or the HCP management API.

- If a namespace managed by the tenant does not have a CORS configuration, the namespace inherits the tenant-level configuration.
- If a namespace has its own CORS configuration, the namespace-level configuration overrides the tenant-level configuration.

This section describes how to use the System Management Console to configure the default CORS configuration for all namespaces owned by a tenant.

Request elements (CORS rules)

A CORS rules configuration uses the request elements described in the following table. Some of the request elements are optional.

Request elements for CORS rules configuration

Element	Description
CORSConfiguration	Container for CORSRules elements. • Type: Container • Children: CORSRules • Ancestor: None **Note:** A CORS rules configuration in HCP can have any number of CORSRule, AllowedMethod, AllowedOrigin, and AllowedHeader elements. However, the maximum size of the CORS configuration cannot exceed 2.5 MB.
CORSRule	A set of origins and methods that you want to allow to access a resource. • Type: Container • Children: AllowedMethod, AllowedOrigin, AllowedHeader, MaxAgeSeconds, ExposeHeader • Ancestor: CORSConfiguration
Id	Optional. A unique identifier for the rule. The Id value assists you in finding a rule in the CORS configuration. • Type: String • Ancestor: CORSRule
AllowedMethod	HTTP methods that you want to allow the origin to execute. Each CORSRule must identify at least one origin and one method.

Element	Description
	• Type: Enum (GET, PUT, HEAD, POST, DELETE) • Ancestor: CORSRule
AllowedOrigin	Origins that you want to allow cross-origin requests from. Each CORSRule must identify at least one origin and one method. The origin value can include at most one wildcard character "*", for example, http://*.example.com. Alternatively, you can specify the wildcard character by itself to enable all origins to send cross-origin requests. • Type: String • Ancestor: CORSRule
AllowedHeader	Optional. List of headers that are allowed in a preflight OPTIONS request through the Access-Control-Request-Headers header. This element can contain at most one wildcard character "*". Each header name in the Access-Control-Request-Headers header must have a corresponding entry in the CORSRule. The server will send only the allowed headers that were requested in a response. • Type: String • Ancestor: CORSRule
MaxAgeSeconds	Optional. Maximum time, in seconds, that the browser can cache a preflight OPTIONS response for a specified resource. By caching the response, the browser does not have to send preflight requests to the server within the MaxAgeSeconds time window if repeated requests (same origin, HTTP method, and resource) are issued. A CORSRule can have at most one MaxAgeSeconds element. • Type: Integer (seconds) • Ancestor: CORSRule
ExposeHeader	Optional. One or more response headers that customers can access from their applications, for example, from a JavaScript XMLHttpRequest object. You add one ExposeHeader element in the rule for each header. This element restricts the response headers that are accessible by the client. • Type: String • Ancestor: CORSRule

CORS configuration template

Here is a sample XML template for setting a CORS rules configuration.

CORS rules configuration template

```
<CORSConfiguration>
     <CORSRule>
          <Id>Optional: Unique string value that identifies the rule</Id>
          <AllowedOrigin>Origin that you want to allow cross-origin requests from</AllowedOrigin>
          <AllowedOrigin>A single wildcard is allowed</AllowedOrigin>
          <AllowedMethod>HTTP method</AllowedMethod>
          <AllowedMethod>HTTP method</AllowedMethod>
          <MaxAgeSeconds>Optional: Time, in seconds, the browser can cache the preflight OPTIONS response for a resource</MaxAgeSeconds>
          <AllowedHeader>Optional: Header that you want the browser to send. A single wildcard is allowed.</AllowedHeader>
          <AllowedHeader>...</AllowedHeader>     <!-- Optional -->
          <ExposeHeader>Optional: Response header that you want accessible from the browser </ExposeHeader>
          <ExposeHeader>...</ExposeHeader>     <!-- Optional -->
     </CORSRule>
     <CORSRule>
          ...
     </CORSRule>
     <CORSRule>
          ...
     </CORSRule>
</CORSConfiguration>
```

Configuring CORS rules at the tenant-level

You can use the System Management Console to configure the default CORS settings for all namespaces owned by a tenant.

To view a tenant, you need the monitor or administrator role. To modify a tenant, you need the administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. On the Tenants page, in the Name column, click the right arrow next to the tenant for which you want to configure CORS settings.
   The tenant Overview panel is displayed.
3. Click the Security tab.
   The Security panel opens to the CORS tab on the left.
4. In the CORS Configuration field, enter the default CORS settings to use for all namespaces that are owned by the tenant.
5. Click Update Settings.
   You are returned to the Overview panel for the tenant. A message is displayed at the top of the page indicating whether the update was successful. If a success message is displayed, your configuration is saved and persists in HCP.
6. To view, update, or delete the saved configuration, click Security to display the Security panel.

   CORS configuration

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CORSConfiguration>
     <CORSRule>
          <AllowedOrigin>http://www.example.com</AllowedOrigin>
          <AllowedMethod>PUT</AllowedMethod>
          <AllowedHeader>*</AllowedHeader>
          <ExposeHeader>ETag</ExposeHeader>
          <MaxAgeSeconds>3000</MaxAgeSeconds>
     </CORSRule>
     <CORSRule>
          <AllowedOrigin>*</AllowedOrigin>
          <AllowedMethod>GET</AllowedMethod>
          <AllowedHeader>*</AllowedHeader>
     </CORSRule>
...
```

Notice that the HCP software added the following XML header at the top of the CORS configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

7. If a failure message is displayed, for example, if your configuration had a syntax error, return to the Security panel to make the necessary corrections.
8. Click Update Settings.

You configured the default CORS settings for all namespaces owned by the tenant.

Protocol optimization

HCP namespace access protocols are categorized as either cloud protocols or noncloud protocols. The cloud protocols are the HTTP and S3 compatible. The noncloud protocols are WebDAV, CIFS, and NFS.

Protocol optimization improves namespace ingest performance. You can optimize namespaces for all protocols, which provides balanced performance across both cloud protocols and noncloud protocols. Alternatively, you can optimize namespaces for cloud protocols only. Cloud-only optimization improves the ingest rate of namespaces using cloud protocols. Cloud protocols, themselves, are further optimized for improved ingest performance.

A namespace that is optimized only for cloud protocols is said to be *cloud optimized*. Clients can use only cloud protocols to access cloud-optimized namespaces. For clients to use noncloud protocols to access a namespace, the namespace must be optimized for all protocols.

Only cloud-optimized namespaces support multipart uploads and the management of multipart objects. Additionally, only cloud-optimized namespaces support erasure coding as their protection type.

To benefit most from optimization, you should increase system memory. Results are most apparent on systems with high object and directory counts. If you want to upgrade system memory, contact your HCP sales representative.

At the system level, the default configuration setting for new namespaces is optimize for all namespace access protocols. You can change this to optimize for cloud protocols only. You can also change all existing namespaces for which no noncloud protocols are enabled to be cloud-optimized.

Note: You cannot make protocol optimization changes while an HCP system upgrade is in progress.

Setting the default protocol optimization option and directory usage for new namespaces

Namespaces can be optimized for cloud protocols only or for all protocols and can be configured for either balanced or unbalanced directory usage. You can specify the type of protocol optimization and directory usage to be selected by default for new namespaces across all tenants. Tenant administrators can use these defaults or can override them by specifying a different default. Additionally, when creating a namespace, the tenant administrator can override the default by changing the setting for that namespace.

To view the default protocol optimization and directory usage settings for new namespaces, you need the monitor or administrator role. To change the default protocol optimization and directory settings for new namespaces, you need the administrator role.

1. In the top-level menu of the System Management Console, select Configuration > Protocol Optimization.
2. On the Protocol Optimization and Directory Usage page, under Protocol Optimization take either of these actions:
   - To set the default to cloud optimized, select Default new namespaces to optimize for cloud protocols only.
   - To set the default to optimized for all protocols, select Default new namespaces to optimize for all protocols.
3. On the Protocol Optimization and Directory Usage page, under Directory Usage take either of these actions:
   - To set the default to Balanced, select Default new namespaces to balanced directory usage.
   - To set the default to Unbalanced, select Default new namespaces to unbalanced directory usage.
4. Click Update Settings.

Cloud-optimizing existing namespaces

You can use a single operation to optimize all existing eligible namespaces for cloud protocols only. Eligible namespaces are those for which no noncloud protocols are enabled.

Note: A cloud-optimized namespace that contains objects cannot be changed to be optimized for all namespace access protocols.
To cloud-optimize existing namespaces, you need the administrator role.

1. In the top-level menu of the System Management Console, select Configuration > Protocol Optimization.
2. On the Protocol Optimization page, click Optimize for Cloud Only.
3. In the Confirm: Optimize Existing Namespaces for Cloud Protocols Only window that appears, type `YES` in the text box.
4. Click Optimize Namespaces.

Resetting HCP tenant security

HCP ensures that each HCP tenant always has at least one:

- Locally authenticated HCP user account with the security role
- Group account with the security role

For a given tenant, it is highly improbable that all locally authenticated users with the security role will forget their passwords at the same time. However, should this happen, if the tenant does not have a group account with the security role, the tenant would have no administrators who could manage user and group accounts.

To resolve this issue, you can use the System Management Console to restore access to the tenant for locally authenticated users with the security role. You can do this in one of two ways:

- Reset the passwords for all locally authenticated user accounts with the security role. When you do this, you specify a single password for all affected accounts.
- Grant the security role to a new or existing group account. A new group account will have only the security role and no data access permissions. An existing group account will have the security role plus whatever roles and data access permissions it currently has.

  You can grant the security role to a group account only if the tenant is configured to support AD authentication, HCP is configured to support AD, and HCP is to communicate with AD.

Note: To reset security for an HCP tenant, you need the administrator role.

Resetting security for an HCP tenant

To reset security for an HCP tenant, you need the administrator role.

1. In the top-level menu of the System Management Console, click Tenants.
2. In the list of tenants, click the name of the tenant for which you want to reset security.
3. In the row of tabs below the tenant name, click Settings.
4. In the Settings panel, click Reset Security.
5. In the Reset Security window, select Local to reset the passwords of all locally authenticated HCP user accounts with the security role, or select Active Directory to grant the security role to a new or existing group account.

   If you selected Local:

   - In the Password field, type a new password for the locally authenticated user accounts with the security role. Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters, including white space. The minimum length for a password is the tenant-specific minimum password length.

     To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.
   - In the Confirm Password field, type the password again.

   If you selected Active Directory:

   - In the Group field, enter the name of the AD group account that corresponds to the new HCP group account that you want to create or the existing HCP group to which you want to grant the security role.
6. Click Reset Security.

Deleting a tenant

You can delete an HCP tenant only if it doesn't currently own any namespaces. You cannot delete the default tenant.

To delete a tenant, you need the administrator role.

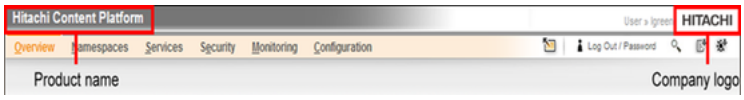
1. In the top-level menu of the System Management Console, click Tenants.
2. In the list of tenants, click the delete control ( ) for the tenant that you want to delete.
3. In response to the confirming message, click Delete.

Changing the product branding

By default, the graphical user interfaces that HCP provides for tenant and namespace access are branded for the company Hitachi and the product Hitachi Content Platform. The elements that show this are:

- In the Tenant Management Console and Namespace Browser:
  - The company logo that appears in the top right corner of each page except the login page
  - The product name that appears:
    - In the title bar of the browser window for all pages
    - In the top portion of the login page
    - Above the top-level menu on every page except the login page
  - The product name abbreviation that appears before the product name in the title bar of the browser window for the login page

  The following figure highlights the branding elements that appear on each page of the Tenant Management Console except the login page.



- In the HCP Search Console:
  - The company logo that appears in the top right corner of every page except the login page
  - The product name that appears:
    - In the title bar of the browser window for the login page
    - In the top portion of the login page

You can change these elements to show your own company logo and product name. You can also reset them to show the Hitachi and HCP branding.

For the company logo, HCP supports BMP, GIF, JPEG, JPG, and PNG images that are no larger than two MB. For best results, the logo should be 77 pixels wide by 19 pixels high and should have a transparent background. Logos with other dimensions are resized to fit in the available space.

The logo for the Tenant Management Console and Namespace Browser appears on a white background, so text on a transparent background should use a dark color. The logo for the Search Console appears on a medium gray background, so text on a transparent background should use either a very light color or a very dark color.

To view and change the branding settings for an HCP system, you use the Branding Settings page in the HCP System Management Console. To display this page, in the top-level menu, select Configuration > Branding.

Note: To view branding settings, you need the monitor or administrator role. To change branding settings, you need the administrator role.

Changing the product name and abbreviation

To view branding settings, you need the monitor or administrator role. To change branding settings, you need the administrator role.

1. On the Branding Settings page, in the Product Settings section:
   a. Optionally, in the Product Name field, type a new product name.

      Product names must be at least one character long and can contain any valid UTF-8 characters. White space is allowed.

      Product name length is limited by the width of the area in which the name is displayed on the login pages. This width is 440 pixels.

   b. Optionally, in the Product Abbreviation field, type a new product name abbreviation.

      Product name abbreviations must be from one to ten characters long and can contain any valid UTF-8 characters. White space is allowed.
2. Click Update Settings.

Changing the company logo

You can change the company logo for the Tenant Management Console and Namespace Browser or for the HCP Search Console, on the Branding Settings page.

To view branding settings, you need the monitor or administrator role. To change branding settings, you need the administrator role.

1. In the Company Logo section, click the applicable Browse button.

   Use the button on the left side to select a new logo for the Tenant Management Console and Namespace Browser. Use the button on the right side to select a new logo for the HCP Search Console. Then select the image file the contains the logo that you want to use.

   The logo appears in the sample display.
2. Click Apply Logo.

Resetting the branding

You can restore the Hitachi and Hitachi Content Platform branding, on the Branding Settings page.

To view branding settings, you need the monitor or administrator role. To change branding settings, you need the administrator role.

1. Click Reset Brand Settings.
   A confirming message appears.
2. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
3. Click Reset Brand Settings.

Search administration

HCP supports two search facilities: the metadata query engine .

The metadata query engine is always available in the HCP system.

Configuring search

The Search page in the HCP System Management Console lets you configure the supported search facilities and select a search facility for use with the HCP Search Console. It also shows the current status of each facility.

To display the Search page, in the top-level menu of the System Management Console, select Services > Search.

Note: To view the Search page, you need the monitor or administrator role. To configure search, you need the administrator role.

Metadata query engine

The metadata query engine is one of the search facilities supported by HCP. In addition to supporting the HCP Search Console, the metadata query engine supports the metadata query API.

About the metadata query engine

The metadata query engine uses an index to find results for object-based queries issued through the metadata query API and for searches performed in the HCP Search Console. You can configure metadata query engine indexing and control the use of the metadata query API.

Metadata query engine index

The metadata query engine index resides on the Hitachi Content Platform (HCP) storage nodes. The engine builds and maintains this index by reading objects in the search-enabled namespaces that also have indexing enabled. The engine indexes system metadata, custom metadata (optional), and ACLs. In HCP namespaces that support versioning, it indexes only the most recent version of each object.

The System Management Console shows how current the metadata query engine index is by displaying the date and time before the objects that are guaranteed to be indexed.

Index protection level

HCP can store one or two copies of the metadata query engine index. The number of copies stored is called the *index protection level*.

Storing one copy of the index uses less storage than storing two copies. However, storing two copies helps to ensure the availability of the index in the case of node unavailability. With an index protection level of one, if one or more nodes in a HCP with internal storage or VM system are unavailable, the index is unavailable.

In HCP with SAN-attached storage systems without an all-SSD configuration that have an index protection level of one, single-node unavailability does not cause the index to be unavailable because of zero-copy failover. However, if multiple nodes are unavailable, the index might be unavailable depending on which nodes are involved.

In contrast, in HCP G10 and G11 all-SSD HCP with SAN-attached storage systems with an index protection level of one, if a node is unavailable, the index is unavailable because it is stored on an internal volume. For this reason, in HCP G10 and G11 all-SSD HCP with SAN-attached storage systems, it is a best practice to set an index protection level of two.

While the metadata query engine index is unavailable:

- The metadata query engine does not update the index.
- The metadata query API does not support object-based queries.
- If the metadata query engine is selected for the Search Console, searches in the Console return an error.

Enabling and disabling indexing

You can enable and disable metadata query engine indexing. While indexing is enabled, the engine continuously processes objects in order based on the time of their last metadata changes. For new objects, this is the time they were added to the repository.

If indexing is disabled after being enabled, the metadata query engine stops all indexing activity. However, it does not delete the existing index, and that index remains available. When indexing is reenabled after being disabled, the engine updates the index with all the object additions and metadata changes that occurred while indexing was disabled.

When the HCP system is installed or is upgraded from an earlier release, metadata query engine indexing is disabled by default.

Custom metadata indexing

You can choose whether to allow the metadata query engine to index custom metadata. If you allow this, tenant administrators can choose whether to index custom metadata in each of their namespaces. If you disallow custom metadata indexing, custom metadata cannot be indexed in any namespaces.

By default, when custom metadata indexing is enabled for a namespace, the metadata query engine indexes the content properties for that namespace and not the full text of custom metadata. If the namespace doesn't have any associated content properties, no custom metadata is indexed.

Tenant administrators can choose to have the metadata query engine index the full text of custom metadata. If they enable this option, the metadata query engine indexes both content properties, if any exist, and the full text of custom metadata.

Custom metadata can take up a significant amount of the space in the metadata query engine index. Disallowing custom metadata indexing can save space but also means that searches based on custom metadata do not find any objects.

If you disable custom metadata indexing after it has been enabled, the custom metadata that has already been indexed is not removed from the index.

Index size

HCP stores the metadata query engine index on predetermined logical volumes on storage nodes. Depending on the type of system (HCP with internal storage, HCP with SAN-attached storage, or VM) and volume configuration, the index shares or does not share the space on these volumes with object data:

- In HCP with internal storage or VM systems, one logical volume on each node is index enabled and can store both the index and object data (that is, it's a shared volume).
- In HCP with SAN-attached storage systems without an all-SSD configuration, logical volumes with numbers in the range of 64 through 95 store only the index. Furthermore, one additional volume on each node is a shared volume.
  Note: In HCP G10 and G11 all-SSD HCP with SAN-attached storage configurations, logical volumes with numbers in the range of 64 through 95 are not supported.

In the System Management Console, you specify the maximum amount of space the index can occupy on shared volumes as a percent of the total space on those volumes. You can increase or decrease this percent at any time. However, you cannot decrease it to less than the percent of space already used for the index on those volumes.

HCP does not reserve the amount of space you specify as the maximum for the index on shared volumes. As a result, as additional data is stored, the space available for the index on those volumes may actually be less than the maximum amount of space allowed.

HCP notifies you when the size of the index reaches 50 percent of the combination of the space on the index-only volumes with either the maximum amount of space allowed for the index on the shared volumes or the actual space available on the shared volumes, whichever is less. At this point, HCP can no longer optimize the space used by the index. As a result, the index grows faster, and responses to metadata query engine API requests become slower, as do responses to searches in the Search Console when that Console is using the metadata query engine.

When the size of the index reaches 100 percent of the same combination, indexing is disabled. To start indexing again, you must increase the maximum index size and then reenable indexing. If sufficient space is not available to increase the maximum size, you must add index-enabled storage to the HCP system so that the index can continue to grow.

The System Management Console can show the following information about storage usage on the index-enabled logical volumes:

- The total amount of storage space allowed for the index across all shared volumes in the system. This includes both used and unused space.
- The total amount of storage space on all index-only volumes in the system. This includes both used and unused space.
- The amount of space currently occupied by the index on all index-enabled volumes (that is, both index-only volumes and shared volumes).
- The total amount of space currently occupied by other data on all shared volumes.
- The total amount of space currently available for storing more of the index across all index-only and shared volumes in the system.

Objects that cannot be indexed

HCP reports objects that the metadata query engine cannot index in the applicable tenant-level log. The short description of the logged event is

`Object indexing failed.`

Metadata query engine management

From the HCP System Management Console, you can:

- Enable or disable the ability to use the metadata query API. Disabling the use of the metadata query API has no effect on the use of the metadata query engine with the Search Console.
- Enable or disable the indexing of new objects and metadata changes across all namespaces.
- Enable or disable indexing of custom metadata.
- Change the maximum size of the metadata query engine index.
- Change the index protection level. To change the index protection level, you first need to disable indexing.
- Display information about storage usage on index-enabled logical volumes.

- Delete the metadata query engine index. You might delete the index, for example, to save space in a system in which no namespaces have clients using the metadata query API or Search Console.

  To delete the index, you first need to disable indexing and then wait for indexing to completely stop.

Configuring the metadata query engine

On the left side of the Search Facility Settings section on the Search page, click MQE.

In the MQE panel:

- To enable or disable use of the metadata query API, select or deselect, respectively, Enable metadata query API.
- To enable or disable metadata query engine indexing, select or deselect, respectively, Enable indexing.
- To enable or disable indexing of custom metadata, select or deselect, respectively, Enable indexing of custom metadata. You can enable this option only while metadata query engine indexing is enabled.
- To change the maximum amount of space allowed for the metadata query engine index on shared volumes, in the Maximum Allowed Size on Shared Volumes field, type the maximum percent of shared storage that can be used for the index. Valid values are integers in the range one through 100.
  Tip: Before changing the maximum index size, click Index storage details to view information about storage usage on the index-enabled logical volumes.
- To change the number of copies of the metadata query engine index, in the Index Protection Level field, select 1 or 2. You can change the index protection level only while indexing is disabled.

Click Update MQE Settings. If you changed the index protection level, a confirming message appears.

In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Settings.

Deleting the metadata query engine index

You can delete the metadata query engine index at any time while indexing is disabled and completely stopped. To rebuild the index after deleting it, you need to reenable indexing.

Note: To check the status of indexing, refresh the Search page.
To view the Search page, you need the monitor or administrator role. To configure search, you need the administrator role.

1. On the left side of the Search Facility Settings section on the Search page, click MQE.
2. In the MQE panel, click Delete Index.
   A confirming message appears.
3. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
4. Click Delete Index.

Search facility status

The Search page in the HCP System Management Console displays the current availability of each search facility and displays the current indexing status of the metadata query engine. To refresh this information without reloading the page, click Refresh Now below the Indexing Status column in the data table.

Search facility availability

The following table describes the possible values for search facility availability.

Search facility	Value	Description
Metadata query engine	Available	The metadata query engine is running on all HCP storage nodes.
	Partial	The metadata query engine is running on at least one but not all HCP storage nodes. This is most likely because one or more storage nodes are unavailable. If this value persists while all storage nodes are available, contact your authorized HCP service provider for help.
	Unavailable	The metadata query engine is not running on any storage nodes. If this value persists while at least one storage node is available, contact your authorized HCP service provider for help.

Metadata query engine indexing status

The following table describes the possible values for the indexing status of the metadata query engine.

Value	Description
Enabled, starting	Indexing is enabled and in the process of starting.
Enabled, running	Indexing is enabled and running.
Enabled, optimizing	Indexing is enabled but is temporarily not running because the metadata query engine is in the process of optimizing the index. When the optimization is complete, indexing automatically resumes.
Enabled, balancing	Indexing is enabled but is temporarily not running while HCP redistributes the index across the available storage. When the redistribution is complete, indexing automatically resumes.
Enabled, upgrading	Indexing is enabled but is temporarily not running while the HCP system is being upgraded. When the upgrade is complete, indexing automatically resumes.
Enabled, paused	Indexing is enabled but is currently paused. This status can appear, for example, when the metadata query engine experiences a temporary error. When the situation is resolved, indexing automatically resumes.
Enabled, stopped	Indexing is enabled but not running. This status can appear, for example, when the index has reached its maximum allowed size. When the situation is resolved, indexing automatically resumes.
Enabled, out of space	Indexing is enabled but not running because insufficient space is available on the index-enabled logical volumes. When more space becomes available, indexing automatically resumes.

Value	Description
Enabled, out of memory	Indexing is enabled but not running because insufficient memory is available for the metadata query engine to continue the indexing process. When more memory is added to the system (typically, by adding storage nodes), indexing automatically resumes.
Enabled, missing index segments	Indexing is enabled but not running because at least one part of the index is unavailable. This status can appear, for example, while an index-enabled logical volume is unavailable. When the situation is resolved, indexing automatically resumes.
Disabled, stopping	Indexing is disabled and in the process of stopping.
Disabled, stopped	Indexing is disabled and has completely stopped.

If indexing has stopped unexpectedly and does not automatically restart, contact your authorized HCP service provider for help.

Enabling or disabling the Search Console

To enable the HCP Search Console, you select a search facility to be used with it. If you do not select a search facility, users cannot access the Search Console at all.

Tenant administrators need to know which search facility, if any, is enabled at any given time. This is because the choice of search facility:

- Determines which index, if any, is used as the source of indexing statistics in the System Management Console and Tenant Management Console
- Affects namespace indexing options in the Tenant Management Console

Note: If the Search Console is currently enabled, before disabling it, you should notify your tenant contacts. You should notify them again when access to the Search Console is restored.

To enable or disable the Search Console, in the Search Console section on the Search page in the System Management Console:

To view the Search page, you need the monitor or administrator role. To configure search, you need the administrator role.

1. Take one of these actions:
   - To enable the Search Console, select Metadata Query Engine.
   - To disable the Search Console, select Disable Search Console.
2. Click Update Console Settings.

HCP policies

An HCP policy is one or more settings that influence how transactions and services work on objects in namespaces. Policies ensure that objects behave in expected ways.

HCP supports these policies:

- Retention
- Shredding
- Indexing
- Versioning
- Custom metadata XML checking

Retention policy

The retention policy determines how long an object must remain in the repository. Each object has its own retention policy settings. These settings are part of the object metadata.

The retention policy consists of two settings:

- A retention setting, which is one of these:

  A specific date and time
  : before which the object cannot be deleted.

  Deletion Allowed
  : which means that the object can be deleted at any time.

  Deletion Prohibited
  : which means that the object can never be deleted.

  Initial Unspecified
  : which means that the object has not yet been assigned one of the other possible retention settings. Objects with a setting of *Initial Unspecified* cannot be deleted.

  A retention class
  : which prevents an object from being deleted before a certain amount of time past its creation date. The specific amount of time is part of the retention class definition.

- A hold setting. An object is either on hold or not. An object that is on hold cannot be deleted through any mechanism under any circumstances. Objects can be placed on hold or released from hold at any time.

Users and applications can see and modify retention policy settings.

Note: If the namespace is in enterprise mode, the privileged delete function can be used to delete objects regardless of their retention setting, except when the objects are on hold.

Shredding policy

The shredding policy determines whether objects are shredded by the Shredding service when they're deleted. Each object has its own shredding policy setting that indicates whether or not the object should be shredded. This setting is part of the object metadata.

Users and applications can see and modify shredding policy settings.

Indexing policy

The indexing policy determines how the metadata query engine indexes objects. Each object has its own indexing policy setting that indicates whether the metadata query engine should index custom metadata for that object. This setting is part of the object metadata.

Note: For any given object, if custom metadata indexing is disabled for the HCP system or for the namespace that contains the object, the metadata query engine does not index custom metadata for that object, regardless of its indexing policy setting.

Every object has an individual indexing policy setting defined as part of its system metadata. HCP ignores this setting for an object when custom metadata indexing is disabled for its namespace. However, metadata query API requests can always use the individual indexing policy setting as a namespace search criterion. Additionally, third-party applications can use this setting for their own purposes.

Versioning policy

The versioning policy determines whether HCP can create multiple versions of objects. The policy is set at the namespace level and applies only to HCP namespaces.

The versioning policy consists of two settings:

- A versioning setting, which is either on or off. When versioning is on, an attempt to store an object that already exists in the target namespace results in the creation of a new version of the object. When versioning is off, an attempt to store such an object results in an error.
- A version pruning setting. This setting is the amount of time HCP should wait after a version is created before automatically deleting it. HCP automatically deletes only old versions of objects and never automatically deletes the most recent version.

If the effective permission mask for the namespace prohibits deletions, HCP does not automatically prune object versions.

Custom metadata XML checking policy

The custom metadata XML checking policy determines whether HCP allows custom metadata to be added to a namespace if it is not well-formed XML. This policy is set at the namespace level.

The XML checking policy can have a setting of enabled or disabled:

Enabled
: When custom metadata is added to or replaced in a namespace, HCP checks whether it's well-formed XML. If the XML is not well-formed, HCP rejects it.

Disabled
: HCP accepts any data submitted as custom metadata.

XML checking applies only when custom metadata is added to or replaced in a namespace. It does not apply to custom metadata already in the namespace.

HCP services

HCP services are responsible for optimizing the use of system resources and maintaining the integrity and availability of the stored data.

Each HCP service performs a specific function that contributes to the overall health and viability of the system. Services generally run without user intervention either according to a schedule or in response to certain events.

Using the HCP System Management Console, you can set the service schedule and control certain aspects of some services. You can also monitor the progress of certain services and review the use of primary spindown storage and extended storage. Additionally, you can configure and manage data migrations and replication.

About services

A service is a background process that performs a specific function that contributes to the continuous tuning of the HCP system. Services work across all namespaces in the repository.

In general, services run only while they are enabled. An exception is the Protection service, which runs in response to certain triggers even while it is disabled. Typically, services are disabled only by authorized HCP service providers during problem resolution.

The Overview page of the System Management Console shows the status of most services. HCP records information about service runs and irreparable violations in the system log.

Service types

A number of services contribute to the continuous tuning of the HCP system.

HCP implements the following services:

Capacity Balancing service
: Ensures that the percentage of space used remains roughly equivalent across the storage nodes in the HCP system.

Compression/Encryption service
: Compresses object data to make more efficient use of HCP storage.

Content Verification service
: Ensures that object data is not corrupted.

Disposition service
: Automatically deletes expired objects.

Duplicate Elimination service
: Merges duplicate data to free space in the HCP storage. You can monitor the activity of this service.

Fast Object Recovery service
: Ensures that unavailable objects have their status changed to available once they are recovered.

Garbage Collection service
: Deletes data and metadata left in the repository by incomplete operations, thereby freeing space for the storage of additional objects.

Geo-distributed Erasure Coding service
: Erasure codes full copies of object data in replicated namespaces that allow erasure coding.

Migration service
: Migrates data off selected nodes in an HCP with internal storage system or selected storage arrays in an HCP with SAN-attached storage system in preparation for retiring those devices.

Network Per Storage Component service
: Increases tiering performance from the HCP system to HCP S Series Nodes or external storage devices by isolating their communication to an individual forward-facing HCP network. Each HCP S Series Node or external device can use its own network to communicate with HCP.

Protection service
: Ensures that damaged or lost objects can be recovered.

Replication service
: Maintains selected tenants and namespaces on two or more HCP systems and manages the objects in the selected namespaces across those systems to ensure data availability and enable disaster recovery. You can configure, monitor, and control the activity of this service.

Replication Verification service
: Replicates objects that the Replication service missed replicating or was unable to replicate.

HCP S Series Balancing service
: Ensures that the percent of space used across S Series Nodes in a pool remains roughly equivalent.

Scavenging service
: Ensures that the metadata for each object exists and is not corrupted.

Shredding service
: Shreds deleted objects that are marked for shredding.

Storage Tiering service
: Moves objects among storage tiers, creates and deletes copies of objects on various storage tiers to ensure that each tier contains the correct number of copies of each object, and changes objects to metadata-only according to rules in service plans.

Service precedence

Some services take precedence over others.

- On any given node, the Capacity Balancing service takes precedence over the Scavenging service. If the Scavenging service is running when the Capacity Balancing service starts, the Scavenging service stops. When the Capacity Balancing service stops, the Scavenging service automatically restarts, providing that it is scheduled to run at that time.
- On any given node, the Migration service takes precedence over the Capacity Balancing service. If the Capacity Balancing service is running when the Migration service starts, the Capacity Balancing service stops. It does not restart automatically when the Migration service stops.
- On any given node, the Protection service takes precedence over the Compression/Encryption and Content Verification services. If either of these services is running when the Protection service starts, the service that was running stops. When the Protection service stops, each service that stopped automatically restarts, provided that the service is scheduled to run at that time.

Metadata storage

To fully understand how certain services work, you need to know how HCP manages metadata.

When you add an object, upload part of a multipart object, or add a directory or symbolic link to a namespace, the following events occur.

1. HCP creates primary metadata for the item being added. This metadata consists of information HCP already knows, such as the creation date, and for objects and parts only, the data size, hash algorithm, and cryptographic hash value generated by that algorithm. It also includes metadata that was either inherited or specified in the write request, such as retention setting, UID, and GID.
2. HCP creates a second copy of the primary metadata. HCP then distributes both copies of the primary metadata among the HCP general nodes.
3. For objects and parts of objects:
   - HCP creates the number of copies of the object data or part data required to satisfy the ingest tier data protection level (DPL) in the service plan associated with the namespace. If the ingest tier is primary running storage, HCP distributes all copies of the data among the HCP storage nodes. If the ingest tier is HCP S Series storage, HCP writes all copies of the data to that storage.

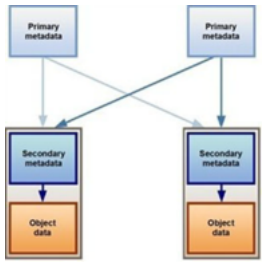
     Each copy of the primary metadata for the object or part points to all copies of the data for that object or part. However, object or part data in primary running storage is not necessarily stored on the same nodes as the primary metadata for the object or part.

   - In primary running storage, HCP stores the number of copies of the object or part metadata required to satisfy the ingest tier metadata protection level (MPL) in the service plan. These copies, called secondary metadata, let HCP reconstruct the primary metadata should that become necessary.

     If the ingest tier is primary running storage, the MPL is the same as the DPL.

   - HCP stores MPL copies of any custom metadata for the object in primary running storage. For multipart objects, HCP stores MPL copies of the custom metadata for the object as a whole instead of MPL copies for each part.
   - If the ingest tier is HCP S Series storage, HCP stores one copy of the secondary metadata along with each copy of the object data on that tier.

The following figure shows the data and primary and secondary metadata that result from storing an object in a namespace with a service plan that sets both the DPL and MPL for the ingest tier to 2. The figure assumes that the ingest tier is primary running storage.



When an object or part is moved from the ingest tier to another storage tier, HCP stores one copy of the secondary metadata along with each copy of the object or part data on that tier. Regardless of which tier the object or part data is on, HCP always keeps in primary running storage the number of copies of the secondary metadata and custom metadata required to satisfy the MPL for that tier.

Service scheduling

The Compression/Encryption, Content Verification, Disposition, Duplicate Elimination, Garbage Collection, Geo-distributed Erasure Coding, Protection, HCP S Series Balancing, Scavenging, and Storage Tiering services run according to a weekly schedule. The schedule controls when during the week each service runs and the performance level at which it runs.

Within a time period, each scheduled service has a performance level of low, medium, or high. The performance level determines the load the service puts on the HCP system. The higher the performance level, the greater the load.

The Replication service also runs according to a schedule, but this service has its own scheduling interface.

HCP comes with a predefined service schedule named HCP Default Schedule. This schedule cannot be modified or deleted.

HCP with SAN-attached storage systems with spindown storage come with an additional predefined schedule named HCP Spindown Schedule. This schedule is optimized for Storage Tiering service activity against spindown storage. The HCP Spindown Schedule is modifiable.

You can create as many other schedules as you want. However, only one schedule can be active at a time. At any time, you can change which schedule is active. For example, you could create two schedules: one that puts a very light load on the system, and one that puts a heavier load on the system. During periods of high system usage, you could activate the first schedule. During periods of low system usage, you could activate the second schedule.

After creating a service schedule, you can modify or delete it. You can modify a schedule regardless of whether it is active. You can delete a schedule only while it is inactive.

Note: Although you can modify or delete the HCP Spindown Schedule, doing this is not recommended because once the schedule is modified or deleted, you cannot restore it. Instead, create a new schedule based on the HCP Spindown Schedule and then modify the new one.

How scheduled services work

The Compression/Encryption, Content Verification, Disposition, Duplicate Elimination, Garbage Collection, Geo-distributed Erasure Coding, Protection, HCP S Series Balancing, Scavenging, and Storage Tiering services each examine objects one at a time, determine whether any action needs to be taken with the object, and if so, take the applicable action. These services, except Scavenging, start with the primary metadata and use that to find the object data. The Scavenging service starts with the secondary metadata, which is stored with the object data.

If the HCP system does not include any spindown storage, the services look at the object data for each object regardless of where the data is stored.

If the HCP system does include spindown storage, on most days, all scheduled services, except Duplicate Elimination, look at the object data on only a subset of the system nodes. Each day, these scheduled services look at the data on a different set of nodes. This prevents spindown volumes that are spun down from being spun up frequently or for long periods of time. Periodically, however, to address cases where the data for an object spans nodes in different sets, the services do not restrict the nodes they look at on a given day.

The Duplicate Elimination service always looks at object data regardless of which node the data is stored on because the service needs to correlate data from all locations. This can result in all spindown volumes being spun up at the same time. You should keep this in mind when scheduling the Duplicate Elimination service.

The length of time required for a service to examine every object in the repository depends on several factors, including the number of objects in the repository, how much time the service is scheduled to run each week, and the performance level at which the service runs.

If the HCP system includes spindown storage, services scheduled to run on only one day a week take a minimum of three-to-five weeks to examine all objects, depending on the number of system nodes. You can shorten this time by scheduling the services to run on more than one day a week.

Note: Services may examine some objects twice during a run. Rarely, this can result in the reported number of objects examined being larger than the number of objects in the repository. If an irreparable object is examined twice by the Protection or Content Verification service, that object is counted twice in the reported number of violations found.

About the Services Schedule page

You use the Services Schedule page in the HCP System Management Console to create, view, modify, activate, and delete service schedules, as well as view log messages about service activity.

The Service Schedule page has a service legend, a schedule grid, and a list of service events. On the schedule grid, each time period in which at least one service is scheduled to run is represented by a rectangle. These rectangles are numbered in the upper-left corner for ease of reference.

Note: To view service schedules and log messages about service activity, you need the monitor or administrator role. To create, modify, activate, and delete service schedules, you need the administrator role.

Services legend

The top part of the Services page has a legend that associates each service with an icon. These icons are used to identify services in the schedule grid.

The icons are:

- - Compression/Encryption service
- - Content Verification service
- - Disposition service
- - Duplicate Elimination service
- - Garbage collection service
- - Geo-distributed erasure coding service
- - Protection service
- - Scavenging service
- - Storage Tiering service
- - HCP S Series Balancing service

When you hover over a time period in the schedule grid:

- The legend heading shows the period reference number and the start and end times for the period
- The services scheduled in the time period are highlighted in the legend

Schedule grid

The schedule grid on the Schedule page shows the weekdays from Sunday through Saturday with each day each broken out into 24 hours. The time periods for a schedule are laid out on this grid.

The heading for each time period shows the period reference number and the start and end times for the period, if they fit in the width of the rectangle. Within each rectangle, either of these is displayed, depending on the size of the rectangle:

- For each scheduled service, the service icon with a bar under it indicating the performance level for the service:
  - Low:
  - Medium:
  - High:
- The number of services scheduled to run during the time period.

If a service in one time block conflicts with a service in an overlapping time block, the background color of the rectangle containing the service that does not take precedence is pink ( ). When you hover over the rectangle, the service that does not take precedence is highlighted in red in the service legend. Text below the legend tells you which service in the overlapping time block is involved in the conflict.

Displaying a service schedule

By default, when you open the Schedule page, the schedule grid shows the active schedule. To display a different schedule, select the schedule you want in the field on the left above the schedule grid.

If the displayed schedule is active, the word `Active` is displayed on a green background to the right of the schedule selection field.

Viewing the schedule for an individual service

By default, the schedule grid shows all scheduled services in the time periods for the displayed schedule. You can choose to show only a selected service in the scheduled time periods. To do this, select the service you want in the field on the right above the schedule grid.

To show all services again, select All services in the same field.

Service log messages

HCP writes messages about service activity to the system log. These messages are displayed in the Service Events section on the Schedule page as well as in other displays of the log.

The messages displayed depend on the selection in the field on the right above the schedule grid. If All services is selected, the list of messages includes all service-related messages. If a specific service is selected, the list includes only the messages related to that service.

Service schedule considerations

Before creating or modifying a service schedule, it is important to understand service schedule behavior.

These considerations apply to service schedules:

- You cannot modify or delete the service schedule named HCP Default Schedule.
- You cannot activate a service schedule that does not include the Garbage Collection service. Likewise, you cannot completely remove the Garbage Collection service from the currently active service schedule.
- If the HCP system includes spindown storage but the currently active service schedule does not include the Storage Tiering service, the Overview page in the System Management Console displays an alert indicating that this situation exists.
- If the HCP system is in an erasure coding topology but the currently active service schedule does not include the Geo-distributed Erasure Coding service, the Overview page in the System Management Console displays an alert indicating that this situation exists.

  While the Geo-distributed Erasure Coding service is not running, full copies of the data for objects that are subject to erasure coding are not reduced to chunks. These copies continue to occupy the full amount of storage required for the object data. How fast the amount of used storage on the system increases depends on:

  - The object ingest rate
  - The size of the objects being ingested
  - The Replication service schedule
  - Whether the erasure coding topology is configured for full-copy or chunk distribution.
- The minimum amount of time for a time period is two hours.
- Time periods can overlap. For example, on a given day, you can have a five-hour time period that starts at 1:00 a.m., a six-hour time period that starts at 1:00 a.m., and a three-hour time period that starts at 3:00 a.m.
- Overlapping time periods cannot include the same service.
- A service that is scheduled in contiguous time periods stops at the end of the first time period and restarts at the beginning of the next one.
- Time periods cannot span days. That is, you cannot create a single time period that starts before midnight on one day and continues after midnight on the next day. However, you can schedule the same service to run in one time period that ends at midnight and another that starts at the beginning of the next day.
- The recommended maximum number of services to schedule in a time period is half the number of hours in the time period, rounded down.
- The more services you schedule to run at the same time, the more the services compete for system resources.
- Each time a service runs, it picks up from where it left off the last time it ran.
- After a service completes a full run (that is, after it has examined every object in the repository), it does not start again for at least 24 hours regardless of the service schedule.
- When a service requires spindown volumes to be spun up, it waits while the volumes spin up. This uses up a small amount of time in the time period in which the service is running.
- When a service in one time period preempts a service in another time period, the preempted service stops. If the preempting service stops before the end of the time period containing the preempted service, the preempted service restarts only if at least ten minutes remain in the time period after HCP recognizes that the preempting service has stopped. HCP can take up to five minutes to recognize the stop.
- When you modify the active schedule, any service that is currently running stops. The service restarts only if the current time is in a time period in which the service is scheduled to run and only if at least ten minutes remain in that time period.

Creating a service schedule

You can create new service schedules from existing schedules. In this case, the new schedule is initially the same as the schedule from which you created it. After creating the schedule, you can modify it in any way you want.

Alternatively, you can create a new schedule by starting with a blank schedule grid.

Tip: To facilitate modification of a new schedule, create the schedule from the existing schedule that's the most similar to what you want the new schedule to be.

Optionally, if you're creating the new schedule from an existing schedule, in the field on the left above the schedule grid, select the existing schedule.

Click Create New Schedule.

In the Create New Schedule window, type a name for the new schedule. Schedule names must be from one through 64 characters long, can contain only alphanumeric characters, hyphens (-), underscores (_), periods (.), commas (,), and spaces, and are not case-sensitive.

You cannot use the name HCP Default Schedule or HCP Spindown Schedule for a schedule you create.

Select either From currently loaded schedule to create the schedule from the existing schedule you selected or From blank schedule to start with a blank schedule grid.

Click Save.

The schedule grid shows the new schedule. This schedule is not active.

Modifying a service schedule

To view service schedules and log messages about service activity, you need the monitor or administrator role. To create, modify, activate, and delete service schedules, you need the administrator role.

1. In the field on the left above the schedule grid, select the service schedule you want to modify.
2. Add, modify, or delete time periods in the schedule as needed.
3. Click Update Schedule.

Adding a time period

To add a time period to a service schedule:

1. In the field on the left above the schedule grid, select the service schedule to which you want to add the time period.
2. Take one of these actions in the schedule grid:
   - Click in the hour at which you want the time period to start. By default, this defines a two-hour time period. You can change the start and end times before saving the time period.
   - Click and drag from one hour (the start time) to another (the end time) in the same day. You can change the start and end times before saving the time period.
   - Click an existing time period.
   - Click the name of a weekday. This defines a 24-hour time period for that day. When you save this time period, all other time periods that are scheduled for that day are deleted.
   - Click All. This defines seven 24-hour time periods — one for each day of the week. When you save these time periods, all other time periods in the schedule are deleted.

     An Edit window appears. For a time period other than a weekday or all, the top of this window shows the number of hours in the time period and the start and end times.

     The Edit window lists the schedulable services. For each service, the window contains a Level field. The window also indicates the status of the service:

     Service not scheduled
     : The service is not scheduled in the time period you're editing or in any time period that overlaps the time period you're editing. The performance level is `Off`.

     Service scheduled
     : The service is scheduled in the time period you're editing. The performance level is `Low`, `Medium`, or `High`.

     Service already scheduled
     : The service is scheduled in a time period that overlaps the time period you're editing. No performance level is shown.

     Conflict with *service-name* service
     : The service cannot run at the same time as the named service, which is already scheduled to run in the time period you're editing. No performance level is shown.
3. Optionally, for a time period other than a weekday or all, select a different start time in the From field.
4. Optionally, for a time period other than a weekday or all, select a different end time in the To field.
5. For each service you want to run during the time period, select a performance level of Low, Medium, or High in the Level field. At least one service must be scheduled to run in the time period.

   For each service you don't want to run during the time period, select Off.
6. Take either of these actions:
   - If you started by clicking the grid, dragging, clicking a weekday, or clicking All, click Update Schedule.
   - If you started by clicking an existing time period, click Create New Period. This creates a new time period only if you scheduled a service that was not scheduled in the original time period.

Modifying a time period

To view service schedules and log messages about service activity, you need the monitor or administrator role. To create, modify, activate, and delete service schedules, you need the administrator role.

1. In the field on the left above the schedule grid, select the service schedule in which you want to modify the time period.
2. In the schedule grid, click the time period you want to modify.
3. In the Edit window, make the changes you want.
4. Click Update Schedule.

Deleting a time period

To delete an existing time period:

1. In the field on the left above the schedule grid, select the service schedule from which you want to delete the time period.
2. In the schedule grid, click the time period you want to delete.
3. In the Edit window, take either of these actions:
   - Click Delete Period.
   - Set the performance level for all services to Off. Then click Update Schedule.

Setting the active service schedule

To view service schedules and log messages about service activity, you need the monitor or administrator role. To create, modify, activate, and delete service schedules, you need the administrator role.

1. In the field on the left above the schedule grid, select the service schedule you want to make active.
   In the dropdown list for this field, the currently active service schedule is marked with an asterisk (*).
2. Click Activate Schedule.

   The Activate Schedule button is present only if the displayed schedule is not active.

Deleting a service schedule

To view service schedules and log messages about service activity, you need the monitor or administrator role. To create, modify, activate, and delete service schedules, you need the administrator role.

1. In the field on the left above the schedule grid, select the service schedule you want to delete.

   You cannot delete the active schedule. If the schedule you want to delete is currently active, activate a different schedule before you display the one you want to delete.

2. Click Delete Schedule.
3. In response to the confirming message, click Delete Schedule.
   HCP deletes the schedule, and the schedule grid displays the active schedule.

Capacity Balancing service

The Capacity Balancing service ensures that the percent of HCP storage space used on the storage nodes in the system remains roughly equivalent across the nodes when new nodes are added.

When the Capacity Balancing service runs, it evaluates the storage level for each node without regard to the individual logical volumes the node manages. If the storage levels for the nodes differ by a wide margin, the service moves objects around to bring the levels closer to a balanced state.

For the purpose of capacity balancing, HCP treats these items as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

The Capacity Balancing service runs only when it is started manually. Typically, an authorized HCP service provider starts this service after adding new storage nodes to the system.

Note: The Capacity Balancing service does not balance the storage space across nodes for data stored in namespaces that have HCP S Series storage set as the ingest tier.

Capacity Balancing service processing

The Capacity Balancing service detects and repairs imbalances in storage availability across nodes in an HCP system, except for nodes that have data stored in namespaces where HCP S Series storage is set as the ingest tier.

To detect imbalances in storage usage, the Capacity Balancing service compares node storage usage statistics. If the service determines that storage usage is imbalanced across nodes:

- The service determines whether the storage managed by each node is a source of objects to move or a target to move them to.
- From the storage for each source node, the service moves objects individually to storage managed by a target node provided the following conditions apply:
  - The percent of capacity used on the source node is less than or equal to the average percent of capacity used on all the nodes in the system.
  - The percent of capacity used on the target node is greater than the average percent of capacity used on all the nodes in the system.
  - The storage managed by the target node does not have a copy of the object to be moved.

    When selecting objects to move, the Capacity Balancing service considers the size of the object data and any custom metadata that the object includes.

At any point in time, HCP is unlikely to be in a perfectly balanced state for the following reasons:

- Object additions and deletions to and from the system do not trigger the Capacity Balancing service to run.
- When all the objects in a directory have been deleted, the empty directory remains in the namespace. Directories in the default namespace, whether empty or not, have metadata that takes up space.

Compression/Encryption service

The Compression/Encryption service compresses object data to make more efficient use of HCP storage space. The space reclaimed by compression can be used to store additional objects.

Depending on the types of objects stored, compression can provide a significant benefit. For example, email objects compress very well.

The Compression/Encryption service performs several tasks based on user settings in its interface. These tasks include:

- Rewriting objects to match the current compression or encryption settings of the storage pool. For example, if an object is uncompressed but compression has been enabled on its pool, then the service will compress the object data to match the pool's settings.
- Rewriting objects compressed prior to HCP release 8.2 to use the new compression method added in that release. This allows for efficient ranged-reads of the objects.
- Re-encrypting objects encrypted prior to HCP release 8.2 to use local or KM Server encryption on S Series Node and cloud storage.

The Compression/Encryption service runs according to the active service schedule.

Note:

The Compression/Encryption service does not compress object data if:

- The data is stored in a namespace that has HCP S Series storage set as the ingest tier.
- The data is stored on extended storage.

The Storage Tiering service manages the compression and encryption of object data on an S Series Node or other extended storage. For more information about data compression and encryption in storage pools, see Encryption and compression of objects in storage pools

Compression/Encryption service processing

When the Compression/Encryption service runs, it checks each object that's eligible for compression. If the object isn't already compressed, it compresses it. If compressing the object doesn't reduce its size (for example, because it's already in a compressed format), the Compression/Encryption service marks it as uncompressible and doesn't try to compress it again in future runs.

You control which objects are eligible for compression by setting criteria in the System Management Console.

In addition to compressing whole objects, the Compression/Encryption service can compress:

- Parts of multipart objects
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects
- Full copies of the data for objects and parts that are subject to erasure coding before those copies are reduced to chunks

For the purpose of compression:

- HCP treats parts of multipart objects as individual objects. Eligibility for compression is based on the individual part size, not on the size of the object as a whole.
- HCP treats chunks for erasure-coded objects and chunks for erasure-coded parts of multipart objects as individual objects. However, eligibility for compression is based on the size of the whole object or part before erasure coding.

By default, the Compression/Encryption service runs only on primary storage. However, you can configure HCP to run the Compression/Encryption service on extended storage as well.

If an object, part, or chunk that was not eligible for compression becomes eligible, the Compression/Encryption service compresses it on its next run. Similarly, if a compressed object, part, or chunk loses its eligibility for compression, the Compression/Encryption service decompresses it on its next run.

Note: Multiple objects, parts, or chunks merged by the Duplicate Elimination service may have differing eligibility for compression. If any one of the objects, parts, or chunks is eligible for compression, the merged object, part, or chunk data is compressed.

Understanding compression statistics

The Compression page in the HCP System Management Console displays statistics about the space saved by the Compression/Encryption service. It also lets you control various aspects of compression activity.

Note: To view the Compression page, you need the monitor or administrator role. To change compression settings, you need the administrator role.

To display the Compression page, in the top-level menu of the System Management Console, select Services > Compression.

The Compression page shows:

Total bytes saved by compression
: The current number of bytes of storage freed by compressed objects, object parts, and chunks for objects and object parts

Percent of storage saved
: The amount of storage space currently saved by compression, expressed as a percentage of the total space available for storing objects

Number of objects and object parts compressed
: The total number of these items currently compressed: objects, parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of multipart objects

The page also shows the current compression settings.

Changing compression settings

You can control which objects and object parts HCP compresses based on these properties:

Age
: You can compress only objects and parts that were added to the repository more than some number of days ago.

Size
: You can compress only objects and parts whose content is larger than a specified size. HCP compresses the parts of multipart objects individually based on the size of the part. HCP never compresses objects or parts smaller than seven KB.

Location
: You can exclude from compression objects and parts that are located in a specified directory or in any subdirectories of that directory, recursively.

Name
: You can exclude from compression objects and object parts where the object name matches a pattern you specify. For example, you might choose to exclude objects with names that match *.jpg because the data for this type of object is already highly compressed.

To be eligible for compression, an object or part must meet all the criteria you specify.

Chunks of erasure-coded objects and parts are compressed based on the eligibility of the applicable object or part.

Note:

The criteria you specify apply across all namespaces.

HCP always compresses old versions of objects, regardless of age, size, and any specified exclusion criteria.

HCP does not compress parts of in-progress multipart uploads, parts of a multipart upload that have been replaced, parts of an aborted multipart upload, or unused parts of completed multipart uploads.

How to change compression/encryption settings

To change the settings for the Compression/Encryption service, on the Compression page in the System Management Console:

- In the Compression Settings section, configure the settings that you want to use:
  - To compress only objects and parts added to a namespace more than a certain number of days ago, type the number of days in the Compress objects stored more than field. Valid values are integers in the range zero through 40,000.

    A value of zero tells the Compression/Encryption service not to use age as a criterion when selecting objects and parts to compress.

  - To compress only objects and parts larger than a certain size, type the size, in KB, in the Compress objects larger than field. Valid values are integers in the range zero though 104,857,600 (100 GB).

    A value of zero tells the Compression/Encryption service not to use size as a criterion when selecting objects and parts to compress.

- In the Other Compression/Encryption Settings section, change the settings to match the HCP system configuration of the following components:
  - **S Series node objects**

    Modify Compression/Encryption settings of HCP S Series Node objects.

  - **Legacy encrypted S Series node objects**

Re-encrypt objects that are encrypted earlier to HCP Release 8.2 to use either local encryption or KM Server encryption on HCP S Series Node objects.

- **Legacy encrypted cloud objects**

  Re-encrypt objects that are encrypted earlier to HCP Release 8.2 to use either local encryption or KM Server encryption on cloud objects.

Then click Update Settings.

If you change any of the Other Compression/Encryption Settings, a confirming message appears. In the field in the message window, type YES (this is case sensitive) to confirm that you understand the consequences of your action.

- To exclude objects and parts from compression based on location or name, specify the criteria for exclusion in the Exclude from Compression list:
  - To add a criterion to the list, type the criterion in the field above the list. Then click Add.
  - To remove a criterion from the list, click the delete control ( ) for that criterion.
  - To remove all criteria from the list, click Delete All.

Exclusion criteria

You can exclude objects and parts from compression based on location, name, or a combination of the two. Locations are paths relative to the namespace identification plus any protocol-specific identifiers, such as rest for HTTP or data for the CIFS protocol.

For object names, you can use patterns. The wildcard character for pattern matching is the asterisk (*), which matches any number of characters of any type, including none.

The format for criteria in the exclude list is:

`[/directory-path/]object-name-pattern`

The initial forward slash (/) is required with a directory path.

Here are some examples:

- Either of these excludes all objects and parts in the corporate/mktg/graphics directory, as well as all objects and parts in all subdirectories of that directory, recursively:

  `/corporate/mktg/graphics/*`

  `/corporate/mktg/graphics/*.*`

- This excludes all objects and parts with names ending in .jpg:

  `*.jpg`

- This excludes all objects and parts that have names ending in .ppt and that are in the /corporate/hr/benefits directory or any of its subdirectories, recursively:

  `/corporate/hr/benefits/*.ppt`

- This excludes all objects and parts that have names matching 21*_*.* (for example, 2198_John_Doe.doc) and that are in the corporate/hr/employees directory or any of its subdirectories, recursively:

  `/corporate/hr/employees/21*_*.*`

Content Verification service

When an object is created, HCP uses cryptographic hash algorithms to calculate various hash values for it. These values, which are generated based on the object data, system metadata, and custom metadata are stored with the primary metadata for the object.

One of the hash values that is generated only from the object data is also stored with the secondary metadata for the object. The cryptographic hash algorithm HCP uses to calculate this hash value is namespace dependent. It is set when the namespace is created. After set, it cannot be changed.

Users and applications can see, but not modify, hash values generated from object data and annotations. They cannot see any other hash values.

For the purpose of content verification, HCP treats the following items as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

The Content Verification service ensures the integrity of each object by:

- Checking that the object data, system metadata, and custom metadata still match the stored cryptographic hash values
- Ensuring that certain secondary metadata other than the hash value matches the primary metadata for the object

Note: The Content Verification service does not do a data check for objects that are stored in namespaces that use service plans with HCP S Series storage as the ingest tier, or for objects that are stored on extended storage.

The Content Verification service runs according to the active service schedule.

During HCP content verification, HCP attempts to repair any files that HCP S Series Nodes report as being irreparable.

Cryptographic hash algorithms

HCP supports these cryptographic hash algorithms for selection at the namespace level:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- RIPEMD-160

The more complex the hash algorithm, the greater the impact on performance when objects are stored or when services run.

Content Verification service processing

The Content Verification service has two main functions: detecting corrupted data and discrepancies in metadata, and repairing that data and metadata.

Detecting content verification violations

To detect corrupted data, the Content Verification service regenerates the cryptographic hash values for each object. After regenerating the hash values, the Content Verification service checks that these regenerated values match the corresponding values in the primary metadata.

The Content Verification service detects metadata discrepancies by checking that certain secondary metadata for each object matches the primary metadata for the object.

A violation occurs when either of the conditions described above is not true. Violations of the second type are not reported in the system log.

Note:

When an object is stored through the CIFS or NFS protocol, its primary metadata does not initially include cryptographic hash values that are based on the object data. HCP waits several minutes to ensure that the object content is complete before calculating these values. Large objects stored through these protocols may take longer to get hash values than smaller objects do.

If the Content Verification service encounters primary metadata without hash values, it adds the regenerated values to it.

Repairing content verification violations

If the Content Verification service finds a discrepancy between the cryptographic hash values it regenerates for the object and the corresponding hash value in the primary metadata, it creates a new copy of the object from an existing good copy and marks the corrupted copy for deletion.

If replication is in effect and the Content Verification service cannot find a good copy of the object in the current repository, it can repair the object by using a copy from another HCP system in the replication topology.

To repair a chunk for an erasure-coded object, the Content Verification service recalculates the chunk either by using a full copy of the object data, if one exists on another system in the replication topology, or by using the chunks for the object on all the other systems in the replication topology.

If the Content Verification service finds a discrepancy between other secondary metadata for the object and the corresponding primary metadata, it uses the primary metadata to replace the secondary metadata.

Unavailable, irretrievable, and irreparable objects

When the Content Verification service cannot repair a violation, it marks the object as unavailable, irretrievable or irreparable:

- An object is unavailable if all of these are true:
  - At least one copy of the object is unavailable because of a node, logical volume, or extended storage device being unavailable.
  - None of the available copies of the object is of good quality.
  - Either the namespace that contains the object is not being replicated, or all copies of the object data on other systems in the replication topology are either inaccessible or not good.
- An object is irretrievable if all of these are true:
  - The object or its part stored in the primary storage is corrupted or damaged.
  - Copies of the object located on secondary storage components such as AWS, Azure, S3 Compatible, HCP, HCP S Series, etc., are inaccessible.
  - Service attempts to repair the object fail due to the unavailability of a viable copy.

  Note:

  An object is marked as irretrievable if it meets all the criteria listed above for a duration of 24 hours or after the Content Verification (CV) service makes 3 unsuccessful repair attempts, whichever occurs first. These settings, the 24-hour timeframe and the limit of 3 repair attempts, are configurable. After either the 24-hour period elapses or the 3 repair attempts are exhausted, the object is flagged as irreparable.
- An object is irreparable if all of these are true:
  - All of the primary storage volumes, NFS volumes, and extended storage devices on which copies of the object data are stored are available.
  - None of the available copies of the object is of good quality.
  - Either the namespace that contains the object is not being replicated, or all copies of the object data on other systems in the replication topology are either inaccessible or not good.

Configuring the Content Verification service

The Content Verification service regenerates cryptographic hash values to detect object corruption. Under certain circumstances, you might want to modify or disable this function to reduce the load on the system.

Before you begin

The circumstances when you might want to modify or disable the Content Verification service from regenerating cryptographic hash values include:

- In a namespace that is not being replicated, has a service plan that sets the ingest tier DPL to 1, and does not define any additional storage tiers, only one copy of each object exists. Therefore, if the Content Verification service discovers a discrepancy in the cryptographic hash values for an object, it cannot repair the object from another copy.

  You can choose to have the Content Verification service regenerate hash values only for objects that it could repair, if needed. With this option, the service does not regenerate hash values for objects in a namespace if HCP is configured to maintain only one copy of each object in that namespace.

  Although the service cannot repair corrupt objects in this situation, it can report them. For this reason, if performance is not an issue, you might want to keep hash-value regeneration enabled for all objects.
- When the load on the system is high, temporarily disabling all hash-value regeneration can provide some relief.

Procedure

1. In the top-level menu of the System Management Console, click Services > Content Verification. The Content Verification page opens.
2. Select the applicable Content Verification Mode option:
   - To configure the Content Verification service to regenerate hash values for all objects stored in the repository, regardless of the number of copies of each object that HCP must maintain in the repository, select Check all objects and repair if needed.
   - To configure the Content Verification service to regenerate hash values for a given object only when HCP is required to maintain multiple copies of that object in the repository, select Check only objects that can be repaired and repair if needed.

- To disable the hash-value regeneration function, select Do not check and repair objects.

3. Click Update Settings.

   If you selected the second or third option in the previous step, a confirm message is displayed. To confirm that you understand the consequences of your actions, select I understand. Then click Update Settings.

Disposition service

The Disposition service automatically deletes expired objects.

An object is expired if either of these conditions is true:

- The object has a retention setting that's a specific date and time, and that date and time is in the past.
- The object has a retention setting that's a retention class, and the date and time calculated from the duration specified by the retention class is in the past. In this case, the Disposition service deletes the object only if the retention class has Disposition enabled.

The service deletes only the current version of a versioned object. It does not delete old versions.

The Disposition service is enabled or disabled both at the HCP system level and on a per-namespace basis. Enabling the service for a namespace has no effect if the service is disabled at the HCP system level.

By default, when the HCP system is first installed, the Disposition service is disabled at the system level.

The Disposition service runs according to the active service schedule. When the service runs, it checks each object to see whether the object is expired. If the object is expired, the service checks whether Disposition is enabled for the namespace that includes the object.

If an object is expired and in a namespace with Disposition enabled, the service hides the object data and metadata and marks the object for deletion. The Garbage Collection service then deletes the object through its normal processing. When applicable, the deletion triggers the Shredding service.

Duplicate Elimination service

Duplicate elimination is the process of merging the data associated with two or more identical objects. For objects to be identical, their data content must match exactly. By eliminating duplicates, HCP increases the amount of space available for storing additional objects.

For example, if the same document is added to several different directories, duplicate elimination ensures that each copy of the document content that HCP must maintain in the repository is stored in only one location. This saves the space that would have been used by the additional copies of the document.

For the purpose of duplicate elimination, HCP treats these as individual objects:

- Parts of multipart objects
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects
- Full copies of the data for objects and parts that are subject to erasure coding before those copies are reduced to chunks

The Duplicate Elimination service does not merge parts of in-progress multipart uploads, parts of a multipart upload that have been replaced, parts of an aborted multipart upload, or unused parts of completed multipart uploads.

The Duplicate Elimination service runs according to the active service schedule.

Note:

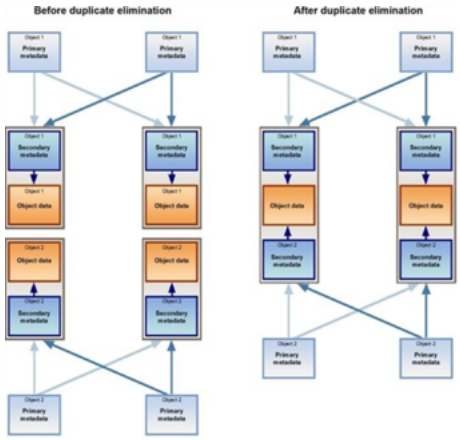
The Duplicate Elimination service does not eliminate duplicate objects stored in namespaces that use service plans that have HCP S Series storage devices set as the ingest tier.

Duplicate Elimination service processing

HCP performs duplicate elimination by first sorting objects, parts, and chunks according to their MD5 hash values. After sorting all the objects, parts, and chunks in the repository, the service checks for objects, parts, and chunks with the same hash value. If the service finds any, it compares the object, part, or chunk content. If the content is the same, the service merges the object, part, or chunk data but still maintains the required number of copies of the data that's specified in the service plan for the namespace that contains the object, part, or chunk.

The metadata for each merged object, part, or chunk points to the merged object, part, or chunk data. The Duplication Elimination service never deletes any of the metadata for duplicate objects, parts, or chunks.

The following figure shows duplicate elimination for two objects with the same content where the DPL is two.



These considerations apply:

- The Duplicate Elimination service does not merge objects, parts, and chunks smaller than seven KB.
- The Duplicate Elimination service does not merge the data for chunks with the data for objects and parts that are not erasure coded.
- If the Duplicate Elimination service merges the data for a whole object that is subject to erasure coding and then merges the data for applicable chunk after the object is erasure coded, only the merge of the whole object data is included in the duplicate elimination statistics.
- The Duplicate Elimination service does not merge data that is stored on extended storage.
- For objects, parts, and chunks stored on primary running storage, the Duplicate Elimination service generally merges objects, parts, and chunks from different namespaces only if the namespaces have the same ingest tier DPL.
- For objects, parts, and chunks stored on primary spindown storage, the Duplicate Elimination service generally merges objects, parts, and chunks from different namespaces only if the namespaces have the same primary spindown storage tier DPL.
- For the purpose of duplicate elimination, HCP considers an object, part, or chunk stored on extended storage to have a DPL that is one less than the ingest tier DPL that's specified in the service plan for the namespace that contains the object, part, or chunk. So, for example, the Duplicate Elimination service will merge objects, parts, and chunks stored on primary running storage in a namespace that has an ingest tier DPL of 1 with objects stored on extended storage in a namespace that has an ingest tier DPL of 2.
- The Duplicate Elimination service may bypass merging certain objects until it reprocesses them. This can happen with:
  - Objects stored with CIFS or NFS that are still open because of lazy close
  - Objects stored with CIFS or NFS that do not immediately have MD5 hash values

Understanding the Duplicate Elimination page

The Duplicate Elimination page in the HCP System Management Console shows statistics about duplicate-eliminated objects, parts, and chunks.

Note: To view the Duplication Elimination Status panel, you need the monitor or administrator role.

To display the Duplicate Elimination page, in the top-level menu of the System Management Console, select Services > Duplicate Elimination.

The Duplication Elimination page shows:

Total objects and object parts merged
: The total number of these items for which data was merged since HCP was installed: objects, parts of multipart objects, chunks for erasure-coded objects, and chunks for erasure-coded parts of multipart objects.

Total bytes saved from duplicate elimination
: The total number of bytes of storage freed due to duplicate elimination since HCP was installed.

  The amount of storage freed when you merge duplicates is the size of the data times one less than the number of objects, parts, and chunks merged, times the total number of copies that HCP needs to maintain on primary storage to comply with the ingest tier DPL and primary spindown storage DPL (if applicable) specified in the applicable service plans and to satisfy all protection set requirements.

HCP increases both of these numbers when duplicate data is deleted but does not subtract from these numbers when duplicate-eliminated objects are deleted from the repository.

Fast Object Recovery service

The Fast Object Recovery service checks unavailable objects and, if it finds that an object is available, changes the object status from unavailable to available. The service runs automatically if the Content Verification service is enabled. If the Content Verification service is disabled, the Fast Object Recovery service does not run.

While the Content Verification service is enabled, the Fast Object Recovery service runs once a day. Additionally, the Fast Object Recovery service runs in response to an availability event, such as an unavailable node becoming available. Although you cannot directly schedule the Fast Object Recovery service, you can effectively suspend running the service by disabling the Content Verification service.

Garbage collection service

The Garbage Collection service ensures that HCP storage does not fill up with data that is no longer needed.

The Garbage Collection service runs according to the active service schedule.

Garbage Collection service processing

The Garbage Collection service performs several functions, including object deletions and transaction log cleanup.

Object deletions

The Garbage Collection service performs object deletions according to the following scenarios:

- When a client or the Disposition service deletes an object, HCP hides the object data and metadata, marks the object for deletion, and if possible, immediately deletes it.
- When a client purges an object, HCP hides the data and metadata for all versions of the object, marks all these items for deletion, and if possible, immediately deletes the items.
- When HCP prunes a version of an object, HCP hides the data and metadata for that version, marks the version for deletion, and if possible, immediately deletes it.
- When a client replaces a part during a multipart upload, HCP hides the replaced part and marks the part for deletion.
- When a client aborts a multipart upload, HCP hides the parts of the multipart upload that have already been written and marks those parts for deletion.
- When a client completes a multipart upload, HCP hides any parts that were written for the multipart upload but not included in the completion and marks those parts for deletion.
- When the Garbage Collection service runs:
  - It looks for hidden objects and parts. If it finds such objects or parts marked for deletion, it deletes them.
  - It looks for objects and parts left by failed writes through HTTP, WebDAV, and SMTP. If it finds such objects or parts, it deletes them.
  - It looks for multipart uploads that should be automatically aborted. If it finds such a multipart upload, the Garbage Collection service hides the parts of the multipart upload that have already been written, marks those parts for deletion, and, on a subsequent run, deletes them.

In all cases, when applicable, object deletion triggers the Shredding service.

Note: If an object or part has been erasure coded, the Garbage Collection service works on the applicable chunk in the same way the service works on objects and parts that are not erasure coded.

Transaction log cleanup

HCP maintains a transaction log of all create, delete, purge, prune, and disposition operations performed on objects. HCP uses this log to respond to operation-based queries issued through the metadata query API.

HCP adds and deletes records in the transaction log according to the following scenarios:

- When a client creates an object, HCP adds a creation record to the log.
- When a client deletes an object from a namespace that has versioning enabled without specifying a version to be deleted, HCP adds a deletion record to the log but does not delete the creation record.
- When a client deletes a specified version of an object from a namespace that has versioning enabled, HCP deletes the applicable creation record from the log and adds a deletion record.
- When a client deletes an object from a namespace that does not have versioning enabled, HCP deletes the applicable creation record from the log and adds a deletion record.
- When a client purges an object, HCP deletes all the creation and deletion records for all versions of the object from the log and adds a purge record for the most recent version.
- When HCP prunes a version of an object, it deletes the applicable creation record from the log and adds a prune record.
- When the Disposition service deletes an object, HCP deletes the applicable creation record from the log and adds a disposition record.

Deletion, purge, prune, and disposition records contain only object metadata. You can configure the Garbage Collection service to delete these records after a specified amount of time. If you configure the service to delete these records, each time the service runs, it checks the log for records that are eligible for deletion and, if it finds any, deletes them.

If you do not configure the Garbage Collection service to delete deletion, purge, prune, and disposition records from the transaction log, they remain in the log indefinitely.

For any given namespace, the applicable tenant administrator can choose whether HCP should keep records of delete, purge, prune, and disposition operations if the namespace has ever had versioning enabled. If the tenant administrator chooses not to keep these records, they are immediately eligible to be deleted from the log regardless of the Garbage Collection service configuration.

While the transaction log contains any deletion, purge, prune, or disposition records for a namespace, the namespace cannot be deleted. If a tenant administrator cannot delete an apparently empty namespace, a possible reason is that the transaction log contains one or more of these records. In this case, have the tenant administrator disable the option to keep these records for that namespace.

Note: A namespace with versioning enabled can be cleared from replication while the owning tenant is included in an active/active replication link. In this situation, deletion, purge, prune, and disposition records for objects in the namespace are not deleted from the transaction log, regardless of the Garbage Collection service configuration, unless the namespace option to keep those records is disabled.

Other Garbage Collection service functions

The Garbage Collection service performs the following additional functions.

- Deletes data and metadata left in the repository by unsuccessful or interrupted write operations.
- Deletes extra copies of objects, parts, and chunks that are marked for deletion.

  For example, the following series of events could occur:

  1. A logical volume fails on primary running storage.
  2. The Protection service detects the failed volume and creates a new copy of each object, part, and chunk stored on that volume.
  3. The volume comes back online, so the extra object, part, and chunk copies that the Protection service created are no longer needed.
  4. The Protection service finds the extra copies that it created and marks them for deletion.
  5. The Garbage Collection service detects the object, part, and chunk copies marked for deletion, verifies that they are extra copies, and deletes them.

In all cases, when applicable, the deletion of an object, part, or chunk triggers the Shredding service.

Configuring the Garbage Collection service

The Garbage Collection page in the HCP System Management Console lets you set the length of time to keep deletion, purge, prune, and disposition records in the transaction log.

Note: To view the Garbage Collection page, you need the monitor or administrator role. To configure the Garbage Collection service, you need the administrator role.

Procedure

1. In the top-level menu of the System Management Console, click Services > Garbage Collection. The Garbage Collection page opens.
2. Take one of these actions:
   - To delete deletion, purge, prune, and disposition records from the transaction log after a set period of time:
     - Select Keep deletion records in the transaction log.
     - In the days field, type the number of days you want these records to remain in the transaction log. Valid values are integers in the range zero through 999. Zero means delete the records immediately.
   - To keep deletion, purge, prune, and disposition records in the transaction log indefinitely, select Keep deletion records in the transaction log forever.

     By default, the Garbage Collection service is configured to delete deletion, purge, prune, and disposition records from the transaction log after 90 days.
3. Click Update Settings.

Migration service

The Migration service migrates data off selected storage nodes in either an HCP with internal storage or HCP with SAN-attached storage system or off selected storage arrays in an HCP with SAN-attached storage system in preparation for retiring those devices. During a data migration, the service copies objects and, if applicable, the metadata query engine index from the selected devices to free storage on the remaining devices. Before you start a data migration, you need to ensure that those devices have enough unused capacity to hold the data to be migrated.

After copying an object, the service deletes it from the source device. Once the migration is complete, you can submit a request to your authorized HCP service provider to finalize the migration and remove the retired devices from the system.

For the purpose of data migration, HCP treats these as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

Important:

After a data migration off a storage node in an HCP system is finalized, the system can never again include a node with the same fourth octet in its back-end IP address as that node had.

Retiring a node is not part of the normal procedure for replacing a node that has failed or for upgrading to newer hardware. In these cases, the new node can use the same back-end IP address as the one being replaced.

The Migration service runs only when you explicitly start a data migration. When the migration is complete, the service stops automatically.

When you start a data migration, the selected nodes or storage arrays automatically become read-only (except for allowing the Migration service to delete objects). After the migration is complete, they remain read-only.

When you start a migration of data off selected nodes in an HCP system, HCP automatically removes any NFS volumes from those nodes and associates those volumes with other nodes in the system.

Typically, when migrating data off nodes, before starting a data migration, you submit a request to your authorized HCP service provider to add new nodes to the HCP system in order to maintain (or increase) the system storage capacity. However, if the nodes not selected for migration have sufficient free space to accommodate all the data to be migrated, adding new nodes before the data migration is not required.

For a HCP with SAN-attached storage system, before starting a data migration off storage arrays, your SAN storage administrator, working in conjunction with your authorized HCP service provider, needs to add logical volumes (LUNs) from new or existing storage arrays to any nodes on which all the existing LUNs on all the existing arrays are being retired. Migrated data, however, can be written to any node, and does not necessarily have to be written to the same node from which the data is being migrated.

The HCP system cannot be upgraded while a data migration is in progress. Before the system can be upgraded, you need to either allow the migration to finish or cancel the migration. If you cancel the migration, you can configure a new migration of data off the same devices after the system is upgraded.

Important: To prevent data loss in namespaces that are not being replicated and that have service plans that set the ingest tier DPL to 1, always migrate data off a device before submitting a request to your authorized HCP service provider to remove the device from the HCP system.

Considerations for migrations on HCP with internal storage systems

Using the Migration service to retire nodes in an HCP with internal storage system entails removing nodes from the system and, optionally, adding new nodes. After any new nodes are added to the HCP system but before you begin the data migration, you need to:

- For each combination of domain and network configured in the DNS, remove the IP addresses of the nodes being retired and add the IP addresses of any new nodes
- For each replication link that identifies the HCP system by its IP addresses, remove from the link configuration the IP addresses of the nodes that are being retired and add the IP addresses of any new nodes

Target storage requirements for HCP with SAN-attached storage systems

The information in this section is intended for your SAN storage administrator. It outlines storage requirements that, if not met, prevent a data migration from being started.

Each node in an HCP with SAN-attached storage system must have one OS LUN and at least two data LUNs. If a LUN being migrated is the OS LUN for a node, a replacement for that LUN must be added to the node before the data migration can occur. If the existing LUN is number zero, the new LUN must be number 128. If the existing LUN is number 128, the new LUN must be number zero. Additionally, the new LUN must have a capacity of at least 30 GB.

Migration procedure

The complete procedure for retiring a device is:

1. Take one of these actions:
   - Optionally, for a HCP with internal storage system, submit a request to your authorized HCP service provider to add one or more storage nodes to the system. After a data migration is finalized, the HCP system must still have at least four storage nodes.
   - For a HCP with SAN-attached storage system, either submit a request to your SAN storage administrator and your authorized service provider to add one or more storage nodes to the system or work together with your authorized service provider to add LUNs to the nodes on which all of the existing LUNs are on the storage arrays that you're retiring.
2. For a HCP with internal storage system, update the DNS and any replication links as needed.
3. Configure the data migration by selecting the devices to be retired. HCP can perform only one data migration at a time. Therefore, you should select all of the devices that you want to retire so that you don't have to run multiple sequential data migrations.

   Certain hardware errors, such as a degraded RAID group on a source or target node, prevent you from configuring a data migration. In such cases, you need to fix the problem before you can continue.

4. Review the configuration of the data migration.

   If the migration configuration is not acceptable, HCP provides detailed information about the problems.

5. Submit requests to your authorized HCP service provider and/or your SAN administrator (if you're migrating storage off a HCP with SAN-attached storage system), as necessary, to fix any reported problems.
6. Optionally, enter a description for the data migration and/or change the performance level for the Migration service.
7. Ensure that all of the nodes in the HCP system are running and healthy.
8. Start the data migration.

   If any nodes become unavailable while the Migration service is running, the service stops migrating data. When those nodes become available, the service automatically starts migrating data again.

9. Monitor the data migration and manage it by changing the performance level or pausing the migration, as needed. You can also modify the migration description at any time (for example, to record when and how long the migration was paused).
10. When the data migration is complete (that is, the migration status is Migrated):
    - If a migration report is available, review it. This report identifies tenants that own namespaces containing unacknowledged irreparable objects. For the default tenant and for HCP tenants that are configured to allow system-level users to manage them, the report also lists the unacknowledged irreparable objects in those namespaces.

      If the Migration service encounters one or more objects that it cannot migrate, it marks those objects as irreparable (if they weren't already marked that way).

    - If the data migration statistics show that not all objects were migrated, contact your authorized service provider for help.

Migration page

The Migration page in the HCP System Management Console lets you configure, monitor, and manage data migrations.

Note: To monitor data migrations, you need the monitor or administrator role. To configure and manage data migrations, you need the administrator role.

To display the Migration page, in the top-level menu of the System Management Console, select Services > Migration.

You can also perform a migration by using the Retire Primary Storage wizard. You can access the wizard from the Retirement pane on the Storage page in the System Management Console.

Configuring a data migration

When configuring a data migration on a HCP with internal storage system, you select nodes to be retired. When configuring a data migration on a HCP with SAN-attached storage system, you can either select nodes or storage arrays for retirement.

Configuring a migration on a HCP with internal storage system

To configure a data migration on a HCP with internal storage system:

1. On the left side of the Migration page, click Configuration.

   The Configuration panel displays step 1 (one) of the migration configuration (Choose items for migration). The Select Hardware for Retirement section lists the storage nodes in the HCP system.

2. Select the nodes from which you want to migrate the data.

   To clear your selections and start over, click Cancel.

3. Click Next.

   The Configuration panel displays step two of the migration configuration (Review configuration summary and confirm). The Configuration Summary section in this panel indicates whether the migration configuration is acceptable.

   Note: When you click Next, HCP checks that the system is in a valid state to perform the migration. This includes checking for degraded RAID groups. This check can take up to 90 seconds.

   If the configuration is not acceptable, you can click view details in the Configuration Summary section to display the specific reasons why. You can also click Configuration Report to download the configuration summary and details to a file. The default name for this file is Configuration-Report.txt.

   The Configuration Details section in the step-two panel lists the nodes selected for migration:

   - To change the migration configuration, click Modify Configuration. The Configuration panel redisplays step 1, which shows your current selections.
   - To restart the migration configuration, click Cancel. The Configuration panel redisplays step 1 with all selections cleared.
4. Optionally, add a description of the data migration and/or change the performance level for the Migration service:
   - To add a description:
     a. Click Add description.
     b. In the text box that opens, type a description of the migration. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
   - To change the performance level, in the Performance Level field, select Low, Medium, or High. The higher the performance level, the greater the load on the HCP system.
5. Click Start Migration.

   The Migration service begins preparing for the data migration, and the Migration page switches to the Overview panel.

Configuring a migration on a HCP with SAN-attached storage system

To configure a data migration on a HCP with SAN-attached storage system:

1. On the left side of the Migration page, click Configuration.

   The Configuration panel displays step 1 (one) of the migration configuration (Choose items for migration). From this panel you can select to either retire storage arrays or hardware nodes.

2. Take one of these actions:
   - Retire Storage Arrays:
     a. Select Retire Entire Array.

        The Select Hardware for Retirement section lists the storage systems used by the HCP system. Each array is assigned a number, starting from zero. Below this list, the section shows the number of LUNs currently selected for migration out of the total number of LUNs for each node.

        To view additional details about the LUNs, click in the row for the node you're interested in or click expand all to see details about the LUNs on all nodes. After displaying details for all the LUNs, you can click collapse all to hide the details.

        The details shown for each LUN are:

        - The number of the array the LUN comes from.
        - The LUN number.
        - The worldwide identification number (WWID) for the LUN.
        - The type of LUN (OS, data, or standby). Standby means that the LUN mapping provides zero-copy-failover support for a data LUN on a different node.
        - The LUN size.

     b. Select the storage arrays or storage nodes from which you want to migrate the data.

        When you select an array for migration, all HCP LUNs on the array are selected automatically. You cannot select or deselect the LUNs individually.

        To clear your selections and start over, click Cancel.
   - Retire Hardware Nodes:
     a. Select Retire Specific Hardware Nodes.
     b. Select the nodes from which you want to migrate the data.

        To clear your selections and start over, click Cancel.

3. Click Next.

   The Configuration panel displays step two of the migration configuration (Review configuration summary and confirm). The Configuration Summary section in this panel indicates whether the migration configuration is acceptable.

   Note: When you click Next, HCP checks that the system is in a valid state to perform the migration. This check can take up to 90 seconds.

   If the configuration is not acceptable, you can click view details in the Configuration Summary section to display the specific reasons why. You can also click Configuration Report to download the configuration summary and details to a file. The default name for this file is Configuration-Report.txt. You can send this file to your SAN storage administrator, who can then correct the problems.

   The Configuration Details section in the step-two panel lists the devices or nodes selected for migration. It also shows the number of LUNs currently selected for migration out of the total number of LUNs for each node. As in the step-1 panel, you can view details about the selected LUNs. In this case, the details have an additional column, Migration Status, that indicates whether the data on the LUN can (`Ready`) or cannot (`Not Ready`) be successfully migrated.

   To change the migration configuration, click Modify Configuration. The Configuration panel redisplays step 1, which shows your current selections.

   To restart the migration configuration, click Cancel. The Configuration panel redisplays step 1 with all selections cleared.

4. Optionally, add a description of the data migration and/or change the performance level for the Migration service:
   - To add a description:
     a. Click Add description.
     b. In the text box that opens, type a description of the migration. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
   - To change the performance level, in the Performance Level field, select Low, Medium, or High. The higher the performance level, the greater the load on the HCP system.
5. Click Start Migration.

   The Migration service begins preparing for the data migration, and the Migration page switches to the Overview panel.

Monitoring a data migration

To monitor a data migration, you use the Overview pane on the Migration page. This page shows information about the current data migration and the last completed or canceled data migration.

Information about the current data migration

The top of the Overview pane displays information about the current data migration and the Migration service.

- The current status of the Migration service:

  Not Migrating
  : The Migration service is not running. No migration is in progress.

  Starting Migration
  : The Migration service is preparing for the data migration. This includes determining the number of objects to be migrated and the size of the data to be migrated. It also includes changing the HCP system configuration to prevent data from being written to the selected devices.

  Migrating
  : The Migration service is actively migrating data off the selected devices.

  Paused
  : A data migration is in progress, but the Migration service is not actively migrating data at this time.

  Completing Migration
  : The Migration service is verifying that the migration was successful and waiting while HCP rebalances metadata.

  Migrated
  : The Migration service has finished migrating data off the selected devices and is no longer running.

    If the Overview panel displays a Migration Report link, click the link to download the migration report to a file. The default name for this file is Migration-number-Report.txt, where number is the number automatically assigned to the migration when the copying process started.

    Be sure to review the migration report before having your authorized service provider finalize the migration.

- The estimated amount of time remaining to complete the current data migration.
- The amount of time the Migration service has been running. This value does not include any time during which the service was paused.
- The time the Migration service started.
- The total number of items that have been migrated so far out of the total number of items to be migrated, along with a progress bar and text indicating the percent of items migrated. Items are any of these:
  - Whole objects
  - Parts of multipart objects
  - Parts of in-progress multipart uploads
  - Chunks for erasure-coded objects
  - Chunks for erasure-coded parts of multipart objects
- The amount of data migrated so far, in KB, out of the total amount of data to be migrated, along with a progress bar and text indicating the percent of data migrated.
- The current performance-level setting for the Migration service.
- The description of the current data migration.

  To modify the description:

  1. Click Edit description.
  2. In the text box that opens, edit the migration description.
  3. Click Submit.

To view the configuration of the current data migration:

1. Click View details.

   The Current Migration Details window opens. This window shows the same Configuration Summary and Configuration Details sections as step two of the Configuration pane.

2. After viewing the migration configuration, click Close.

Information about the last data migration

The Migration History section in the Overview pane displays information about the last completed or canceled data migration.

- The time at which the data migration was completed or canceled.
- The total amount of time the Migration service took to perform the data migration. This value does not include any time during which the service was paused.
- The number of items that were migrated out of the total number of these items that were to be migrated, along with a progress bar and text indicating the percent of items migrated. Items are any of these:
  - Whole objects
  - Parts of multipart objects
  - Parts of in-progress multipart uploads
  - Chunks for erasure-coded objects
  - Chunks for erasure-coded parts of multipart objects
- The amount of data migrated, in KB, out of the total amount of data that was to be migrated, along with a progress bar and text indicating the percent of data migrated.
- The description of the data migration.

  To modify the description:

  1. Click Edit description.
  2. In the text box that opens, edit the migration description.
  3. Click Submit.

To view the configuration of the data migration:

1. Click View details.

   The Previous Migration Details window opens. This window shows the same Configuration Summary and Configuration Details sections as step-two of the Configuration pane.

2. After reviewing the migration configuration, click Close.

Managing a data migration

While the Migration service is migrating data, you can use the Management panel on the Migration page to:

- Change the performance level of the Migration service
- Change the description of the data migration
- Pause or resume the data migration
- Cancel the data migration

Changing the performance level

The performance level determines how much load the Migration service puts on the HCP system. If the system load from other activities is heavy, you can lower the performance level for the Migration service to make more system resources available to those activities. If the system load from other activities is light, you can increase the performance level for the Migration service, thereby allowing the service to use more system resources.

You can change the performance level for the Migration service, in the Management panel.

To monitor data migrations, you need the monitor or administrator role. To configure and manage data migrations, you need the administrator role.

1. In the Performance Level field, select Low, Medium, or High.
2. Click Update Settings.
3. In response to the confirming message, click Update Settings.
   HCP pauses the data migration and changes the performance level.
4. Click Resume.

Pausing or resuming a migration

You can pause or resume the data migration at any time while the Migration service is copying objects. You would do this, for example, if you need to make changes to HCP networking or during periods of heavy namespace activity. While the migration is paused, the selected devices remain read-only.

To pause or resume a data migration, in the Management panel, click Pause or Resume, as applicable.

Canceling a migration

You can cancel the data migration at any time while the Migration service is copying objects or while the migration is paused. When you do this, the Migration service stops and the selected devices become read-write. Any data that was already migrated remains in its new location. Additionally, information about the data migration moves to the Migration History section in the Overview panel.

To monitor data migrations, you need the monitor or administrator role. To configure and manage data migrations, you need the administrator role.

1. Click Cancel.
2. In response to the confirming message, click Cancel Migration.

Protection service

The Protection service ensures the stability of the repository by maintaining a specified level of data redundancy, called the *data protection level* (*DPL*), for each object in the repository throughout the entire object lifecycle. The DPL for an object is the number of copies of the object data that HCP must maintain.

For the purpose of data protection, HCP treats these as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

Each namespace has a service plan that defines both a storage tiering strategy and a data protection strategy for the objects in that namespace. For all objects in a given namespace, the storage tiering strategy defines one or more types of storage as tiers. The data protection strategy specifies the DPL that’s applied to the objects that are stored on

each tier.

At any given point in the lifecycle of an object, the data protection strategy specifies the number of copies of the object that must exist in the HCP repository and the storage tier on which each copy must be stored.

HCP initially stores all object data in either primary running storage or HCP S Series storage and all metadata on primary running storage. Therefore, the service plan for a namespace must always define either primary running storage or HCP S Series storage as the initial storage tier, called the *ingest tier*, and must specify both the data protection level and the metadata protection level (MPL) for the that tier.

For each object in a given namespace, the *ingest tier DPL* is the number of copies of the object data that HCP must maintain on primary running storage or HCP S Series storage, as applicable, from the time the object is first stored in the repository until the time the object data is moved to another storage tier. The *ingest tier MPL* is the number of copies of the object metadata that HCP must maintain on primary running storage for as long as the object exists in the repository.

On HCP with SAN-attached storage and VM systems, by default, the ingest tier DPL and MPL are both set to one. On HCP with internal storage systems, by default, the ingest tier DPL and MPL are both set to two. At any time, you can modify the service plan for a namespace to set the ingest tier DPL and MPL for that namespace.

For any given namespace, you can assign a service plan that will give the namespace a DPL setting of one (supported on HCP with SAN-attached storage and VM systems only), two, three, or four. You can also set the ingest tier MPL to one, two, three, or four. However, the ingest tier MPL for a namespace must be equal to the ingest tier DPL for that namespace.

HCP uses the Protection service to maintain the correct number of copies of each object in the HCP repository. When the number of existing copies of an object goes below the number of object copies specified in the applicable service plan (for example, because of a logical volume failure), the Protection service automatically creates a new copy of that object in another location. When the number of existing copies of an object goes above the number of object copies specified in the applicable service plan, the Protection service automatically deletes all unnecessary copies of that object.

The Protection service runs according to the active service schedule and in response to certain events.

Ingest tier data protection level

Each namespace has a service plan that defines one or more storage tiers for that namespace and specifies the data protection level (DPL) that's applied to the objects that are stored on each tier.

Note: For the purpose of DPL, HCP treats parts of multipart objects, parts of multipart uploads, chunks for erasure-coded objects, and chunks for erasure-coded parts of multipart objects as individual objects.

Every service plan defines primary running storage or HCP S Series storage as the initial storage tier, called the *ingest tier*, and specifies a DPL setting and an MPL setting for that tier.

For each object in a given namespace, the *ingest tier DPL* is the number of copies of the object data that HCP must maintain on primary running storage or HCP S Series storage, as applicable, from the time the object is first stored in the repository until the time the object data is moved to one or more other storage tiers (if multiple storage tiers are defined for the namespace). The *ingest tier MPL* is the number of copies of the object metadata that HCP must maintain on primary running storage for as long as the object exists in the repository.

In the default namespace, each directory also has an ingest tier DPL setting. This setting is the same as the ingest tier DPL setting that's specified in the service plan that's assigned to the default namespace.

The ingest tier DPL for a namespace affects the amount of storage that's used when data is added to that namespace. With an ingest tier DPL of 1, HCP creates only one copy of the object data on primary running storage or HCP S Series storage, as applicable. With an ingest tier DPL of 2, HCP creates two copies, thereby using twice as much storage.

For both objects and directories, the ingest tier DPL setting is stored as metadata. Users and applications can see, but not modify, this metadata.

Note: When the ingest tier DPL of a namespace changes, for each object in that namespace that's stored on the ingest tier, HCP creates or deletes copies of the object data, as needed to satisfy the new ingest tier DPL. This can take some time, during which some objects have the old required number of copies and some have the new. When viewing object metadata, however, users and applications always see the intended number of copies (that is, the ingest tier DPL specified in the service plan for the namespace).

Protection sets

HCP groups storage nodes into *protection sets* with the same number of nodes in each set. To improve reliability in the case of multiple component failures, HCP tries to store all the copies of the data for an object that exist on primary running storage or primary spindown storage on nodes in a single protection set. Each copy is stored on a logical volume associated with a different node.

HCP creates protection sets for each possible ingest tier DPL setting that can be specified in a service plan. For example, if an HCP system has six nodes, it creates three groups of protection sets:

- One group of six protection sets with one node in each set (for DPL 1)
- One group of three protection sets with two nodes in each set (for DPL 2)
- One group of two protection sets with three nodes in each set (for DPL 3)

For each object in a given namespace, to store copies of the object data on primary running storage, HCP uses the group of protection sets that corresponds to the ingest tier DPL setting that's specified in the service plan for the namespace. To store copies of the object data on primary spindown storage (if it's used), HCP uses the group of protection sets that corresponds to the primary spindown storage tier DPL setting.

The nodes in a protection set are not necessarily all associated with the same amount of storage. If the total number of storage nodes in the system is not evenly divisible by a DPL setting, HCP can use the storage associated with the extra nodes as standby storage. At any time, HCP can add standby storage to any existing protection set that requires additional storage to balance available storage capacity among its nodes.

The Protection Service is responsible for checking and repairing protection sets. If a node in a protection set fails and the system includes an extra node, the service creates a new protection set that includes all the healthy nodes in the original protection set and the extra node.

Note: Regardless of whether HCP uses the storage associated with a node that's not in a protection set, the node itself runs all the HCP software and performs all the same functions as the nodes in protection sets.

Data availability

When HCP needs to maintain multiple copies of the data for an object on primary running storage or on primary spindown storage, HCP stores each copy of the object data on storage that's managed by a different node. All but one of these copies can become unavailable without affecting access to the object.

Copies of object data become unavailable on primary running storage or primary spindown storage when HCP detects an improperly functioning logical volume or corrupted or missing data. Copies of the object data also become unavailable if the nodes that provide access to those copies become unavailable. A *data outage* occurs when all the nodes that

provide access to all the copies of the data for an object fail.

Protection service processing

The Protection service has two main functions: detecting protection violations and repairing those violations.

Detecting protection violations

To detect protection violations, the Protection service checks that for each object in a given namespace, at any given point in the object lifecycle:

- The total number of existing copies of object data is equal to the total number of copies of object data that are currently required to exist on all of the storage tiers defined for the namespace by its service plan
- If copies of the object data are stored on primary running storage or primary spindown storage:
  - Each copy of the object data is stored on a different node
  - All copies of the object data are stored in the same protection set
  - Each copy of the object data is accessible

A violation occurs when any one of these conditions is not true.

Repairing protection violations

The Protection service can repair certain protection violations for an object, usually by relying on other good copies of the object data stored in the HCP repository.

For each object in a given namespace, at any given point in the object lifecycle:

- If the total number of existing copies of the object data is less than the total required number of copies that's specified in the namespace service plan (for example, because of a logical volume failure on primary running storage), then on each storage tier that's defined for the namespace, the Protection service creates the number of copies of the object data that's required to bring the object into compliance with the namespace service plan.
  - If one or more copies of the object data are supposed to be stored on a tier that's currently inaccessible (for example, due to a failed network connection), but rehydration is enabled for that tier, the Protection service creates an extra copy of the object data on primary running storage.
  - For objects stored on primary storage, if the repository contains fewer than the required number of copies of the object data for a set of duplicate-eliminated objects, then for each object, the Protection service creates enough additional copies of the object data on primary storage to:
    - Satisfy the ingest tier DPL and, if applicable, the primary spindown storage tier DPL specified in the service plan for the namespace that contains the object
    - Comply with the protection set requirements for the applicable ingest tier and primary spindown storage tier DPL settings

      The Duplicate Elimination service then merges the object data again the next time it runs.

- If the total number of existing copies of the object data is greater than the total required number of copies that's specified in the namespace service plan, then the Protection service deletes the correct number of copies of the object data from each storage tier in order to bring the object into compliance with the namespace service plan.

  An object can have an extra copy of its data if the object was rehydrated after a read from primary spindown storage (if it's used) or from any extended storage tier that's defined for the namespace that contains the object. Copies of objects on primary running storage that are supposed to be metadata-only can have data if they were rehydrated after a read from a remote system. The Protection service marks rehydrated object data for deletion only after the rehydration keep time has expired and only if another copy of the data exists.

  The Protection service may determine that it should mark object data on primary spindown storage or on extended storage for deletion when a rehydrated copy of that data exists on primary running storage. In this case, before marking the copy on primary spindown storage or extended storage for deletion, the Protection service checks the service plan for the applicable namespace to determine whether the object is supposed to be moved back onto the applicable storage tier. If the object is supposed to be moved back onto the applicable storage tier, the Protection service doesn't mark the copy that's currently on that storage tier for deletion.

- On primary storage, if two copies of the data for an object are stored on the same node, the Protection service creates a new copy on a different node and marks the extra one in the first location for deletion.
- On primary running storage, primary spindown storage, or NFS storage, if a logical volume has a copy of the secondary metadata for an object but no copy of the object data with that metadata, the Protection service creates a replacement copy of the object data on that volume.

  If replication is in effect and the Protection service cannot find a copy of the object data on the current system, it can repair the object by using a copy from another HCP system in the replication topology.

  To repair a chunk for an erasure-coded object, the Protection service recalculates the chunk either by using a full copy of the object data, if one exists on another system in the replication topology, or by using the chunks for the object on all the other systems in the replication topology.

- For an object that's stored on primary running storage or primary spindown storage, if fewer than the required number of copies of the object data are accessible on the nodes in a protection set, the Protection service first tries to increase the number of copies stored on those nodes. If the Protection service cannot create all the required copies of the object data on the nodes in the protection set (for example, because a node is unavailable), the service tries to put the required number of copies on the nodes in a different protection set. If the service cannot put all required copies of the object data on nodes in the same protection set, the service stores the copies on different nodes in different protection sets.

Unavailable and irreparable objects

When the Protection service cannot repair a violation, it marks the object as either unavailable or irreparable:

- An object is unavailable if all of these are true:
  - At least one copy of the object data is unavailable due to a node, logical volume, or extended storage device being unavailable.
  - None of the available copies of the object data are good.
  - Either the namespace that contains the object is not being replicated, or all copies of the object data on other systems in the replication topology are either inaccessible or not good.
- An object is irreparable if all of these are true:
  - All of the primary storage volumes, NFS volumes, and extended storage devices on which copies of the object data are stored are available.
  - None of the copies of the object data are good.
  - Either the namespace that contains the object is not being replicated, or all copies of the object data on other systems in the replication topology are either inaccessible or not good.

Protection service triggers

In addition to running according to the service schedule, the Protection service runs in response to certain events. In these cases, the service does a full run (that is, it examines every object in the repository regardless of the schedule and regardless of whether the object data is stored on primary running storage, primary spindown storage, or extended storage).

Events that trigger a Protection service run are:

Node shutdown
: When a node becomes unavailable, HCP triggers the Protection service after waiting 90 minutes to ensure that the node is not just temporarily unavailable.

Logical-volume failure
: When HCP determines that a local logical volume is broken, it triggers the Protection service after waiting one minute to ensure that the volume is not just temporarily unavailable.

Node removal
: When a node is removed from the HCP system, HCP triggers the Protection service after waiting ten minutes to ensure that the node removal is permanent.

Note: When the Protection service is disabled, its scheduled runs are canceled. However, the Protection service still runs in response to the triggers listed above unless all of these conditions are true:

- None of the tenants or namespaces on the HCP system are being replicated.
- All existing service plans are configured to set the ingest tier DPL to (1) one.
- If the HCP system is configured to use spindown storage, all existing service plans set the primary spindown storage tier DPL to 1 (one).

HCP S Series Balancing service

The HCP S Series Balancing service is a configurable service that balances object data across S Series Nodes in the same storage pool. The service ensures that the percent of space used across S Series Nodes in a pool remains roughly equivalent. The service is particularly useful when one or more S Series Nodes in the same storage pool is added to, removed from, or retired from an HCP system.

When the HCP S Series Balancing service runs, it evaluates the storage level of each node in a pool. If the levels differ by a wide margin, the service moves objects around to bring the levels closer to a balanced state.

For the purpose of HCP S Series balancing, HCP treats the following items as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

The HCP S Series Balancing service is included in the HCP Default Schedule. However, it remains idle until storage pools are configured to take advantage of the service.

To ensure optimal system performance in deployments with HCP S Series storage pools that include multiple S Series Nodes, you need to add the service to your active service schedule.

New installations and upgrades will benefit from the HCP S Series Balancing feature only when an HCP S Series pool with multiple S Series Nodes is configured to use the service.

HCP S Series Balancing service processing

The HCP S Series Balancing service detects and repairs imbalances in storage availability across S Series Nodes in the same storage pool by comparing storage usage statistics.

If the service determines that storage usage is imbalanced across S Series Nodes in the same pool:

- The service determines whether each S Series Node in the pool is a source of objects to move or a target to move them to.
- From the S Series Node source, the service moves objects individually to the S Series Node target provided the storage managed by the target node does not have a copy of the object to be moved.

  When selecting objects to move, the HCP S Series Balancing service considers the size of the object data and any custom metadata that the object includes, and the age of the object. If an S Series Node is retiring, the balancing service excludes the node in its balancing algorithm.

  At any point in time, HCP is unlikely to be in a perfectly balanced state for the following reasons:

  - The HCP S Series Balancing service is designed to stop balancing when the nodes are within a 10% difference threshold.
  - Object additions and deletions to and from the system do not trigger the HCP S Series Balancing service to run.
  - When all the objects in a directory have been deleted, the empty directory remains in the namespace. Directories in the default namespace, whether empty or not, have metadata that takes up space.

Best practices in configuring HCP S Series Balancing

The HCP S Series Balancing service balances object data across S Series Nodes in the same storage pool to spread the storage load.

When the HCP S Series Balancing service runs, balancing is initiated if S Series Nodes in the same storage pool have a percent-used disparity greater than 10%. Balancing is relative to the size of each storage node, that is, percent capacity.

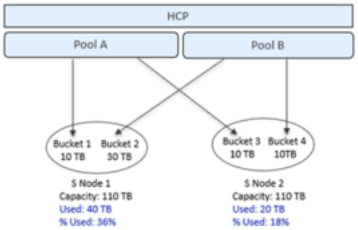
Best practices

To optimize balancing in a deployment with multiple attached S Series Nodes, if storage pools are sharing S Series Nodes, they should either share all their nodes with one another, or share none.

The practice of sharing all S Series Nodes allows data from any pool to be stored on any node, thereby maximizing the balancing algorithm and making use of all available storage capacity. Each pool must also have balancing enabled. If one pool does not enable balancing, balancing for the other pools might not complete.

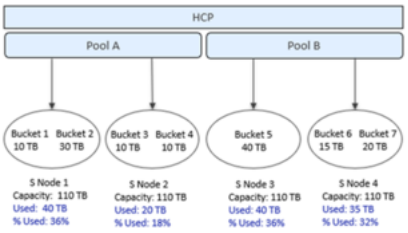
Similarly, the practice of pools sharing none of their S Series Nodes ensures that each pool that participates in balancing can always move data.

The following figure shows a best-practice configuration where Pools A and B share all the same S Series Nodes, in the example, Nodes 1 and 2.



Because there is a greater than 10% disparity in the used capacity between Nodes 1 and 2 (Node 1 = 36% used, Node 2 = 18% used), the HCP S Series Balancing service will have work to do. Each time the service runs, data will be moved from Node 1 to Node 2 until there is a less than 10% disparity in used capacity. For example, if Node 1 reaches 31% used capacity and Node 2 reaches 23% used capacity, the service will stop.

The following figure shows a best-practice configuration where Pools A and B each have their own set of S Series Nodes. There is no node sharing between the pools.

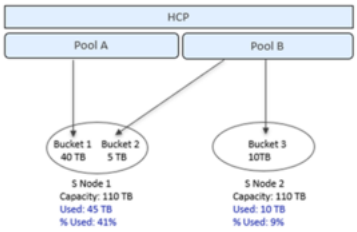


For Pool A, because there is a greater than 10% disparity in the used capacity between Nodes 1 and 2 (Note 1 = 36% used, Node 2 = 18% used), the S Series Balancing service will have work to do when it runs. For Pool B, because there is a less than 10% disparity in the used capacity between Nodes 3 and 4 (Node 3 = 36% used, Node 4 = 32% used), the HCP S Series Balancing service will not have any work to perform.

Poor practices

There are some configuration scenarios that can prevent the HCP S Series Balancing service from moving data, or can lead to less-than-optimal performance. When pools share some, but not all, of the same S Series Nodes, an object imbalance results across nodes. Data from any pool cannot be placed on any node, which prevents the HCP S Series Balancing service algorithm from using all available capacity. In some instances, capacity on one S Series Node in a pool should be moved to another node in the pool, but there is insufficient data to move to balance the nodes.

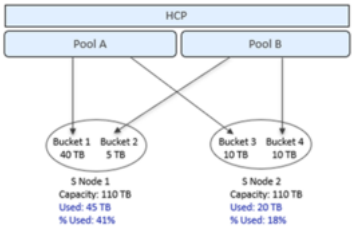
The following figure shows a configuration where Pools A and B share Node 1 but not Node 2.



Because there is a greater than 10% disparity in the used capacity between Nodes 1 and 2 (Node 1= 41% used, Node 2 = 9% used), the HCP S Series Balancing service has work to do for Pool B. When the service runs, data will be moved from Node 1 to Node 2. Data movement will occur each time the HCP S Series Balancing service is scheduled to run, or when the service is initiated manually from the Overview page of the System Management Console.

However, only the data available to Pool B (in Bucket 2) will be moved. As mentioned earlier, the HCP S Series Balancing service completes when there is a less than 10% disparity in the used capacity between the nodes that are participating in balancing. In this scenario, even after the 5 TB in Bucket 2 is moved from Node 1 to Node 2, there will still be a greater than 10% balance disparity. The HCP S Series Balancing service will continue to report that it has work to do, but it will be unable to address the disparity.

To correct this poorly performing configuration, you could create another bucket on Node 2, and add the bucket to Pool A.



HCP S Series Balancing service monitoring

The HCP System Management Console provides several ways to monitor various aspects of HCP S Series Balancing service processing.

- The System Events page in the Console displays HCP S Series Balancing service event status and metrics about each event. Metrics include the number of objects examined, the number of bytes examined, the number of objects moved to another S Series Node, and the number of bytes moved.
- The S Series Balancing page in the Console displays balancing status and metrics for each pool configured to use the service. Metrics include the pool balancing status (balanced, balancing, paused, unscheduled, or unavailable) and the percent balanced.
  Note: The HCP S Series Balancing service reports that a pool is balanced when the S Series Node in the pool have a percent-used disparity of less than 10%.
- The Overview, Services, and Monitoring System Events pages in the Console show HCP S Series Balancing service status.

Scavenging service

The Scavenging service ensures that objects in the repository have valid metadata. When the service runs, it verifies that both the primary metadata for each object and the secondary metadata are complete, valid, and in sync with each other.

For the purpose of scavenging, HCP treats these as individual objects:

- Parts of multipart objects
- Parts of in-progress multipart uploads
- Chunks for erasure-coded objects
- Chunks for erasure-coded parts of multipart objects

To correct violations it detects, the Scavenging service tries to rebuild or repair the problem metadata:

- If the primary metadata for an object is missing, the service reconstructs it from the secondary metadata. If a user or application changed any of the object metadata between when the violation occurred and the time of its repair, those changes may be overwritten with the previous settings.
- If the primary metadata is missing a pointer to a copy of the object data, the service reconstructs that pointer.
- If the secondary metadata for an object doesn't match any copies of the primary metadata, the object is considered irreparable, and the service moves it to the .lost+found directory, located under rest, data, or fcfs_data, as applicable,. At this point, you need to determine whether the object needs to be stored again and, if so, ensure that it happens.

  You can delete an object from the .lost+found directory only when it's not under retention.

In the default namespace, the Scavenging service detects and repairs violations in the metadata for directories only if the directory is associated with abandoned data (that is, data no longer associated with any metadata). If the service cannot recover the directory metadata, it rebuilds it from the metadata associated with the parent directory.

The Scavenging service runs according to the active service schedule.

Note: The Scavenging service does not ensure object metadata validity for objects stored in namespaces that use service plans that have HCP S Series storage set as the ingest tier.

Shredding service

Shredding, also called *secure deletion*, is the process of overwriting the places where all the copies of the data, secondary metadata, and custom metadata for an object were stored in such a way that the object cannot be reconstructed.

The Shredding service shreds deleted objects that are marked for shredding. If the object is a multipart object, the Shredding service shreds each part of the object. The Shredding service also shreds unused parts of multipart uploads that were initiated in namespaces where the default shred setting is true.

The primary metadata for a shredded object is deleted from HCP after all of these events have happened:

- The object is removed from the metadata query engine index, if applicable.
- The object deletion is replicated, if applicable.
- For old versions of objects, the version is pruned or purged.
- The deletion record for the object is deleted from the transaction log. If the Garbage Collection service is configured never to delete deletion records from the transaction log, the primary metadata for the object remains in the system indefinitely.

The shredding policy for each object determines whether that object is shredded.

Note: The Shredding service does not shred object data if:

- The data is stored in a namespace that uses a service plan that has HCP S Series storage set as the ingest tier.
- The data is stored on extended storage.

Shredding service processing

By default, the Shredding service uses three passes to overwrite the areas where the object data, secondary metadata, and custom metadata were stored. The three passes are applied to the entire object, repeating for each 128-KB block. Each pass has this pattern:

- Set to a specified value (write the 0xAA pattern to the file)
- Set to the complement of that value (write the 0x55 (~0xAA) pattern to the file)
- Set to a random value (write a random value to every byte of the entire file)
- Verify the value by reading it back

To use a different shredding algorithm, contact your authorized HCP service provider.

Sending shredding messages to syslog servers

HCP gives you the option of sending a log message for each shredded object or part to the syslog servers specified in the syslog logging configuration. This option takes effect only while syslog logging is enabled and the syslog logging level is set to `Notice`. The log message for a shredded object or part is sent to the syslog servers only after the primary metadata for the object is deleted.

Object shredding is a namespace-level event. Therefore, messages about shredded objects and parts are sent to the syslog servers only if syslog logging is enabled at the tenant level.

Log messages about shredded objects and parts do not appear in the System Management Console or Tenant Management Console regardless of whether those messages are sent to the syslog servers.

Note: HCP never sends messages about shredded objects and parts to the system log or SNMP managers.

Understanding shredding statistics

The Shredding page in the HCP System Management Console lets you monitor the amount of data waiting to be shredded. It also lets you control various aspects of shredding activity.

Note: To view the Shredding page, you need the monitor or administrator role. To change shredding settings, you need the administrator role.

To display the Shredding page, in the top-level menu of the System Management Console, select Services > Shredding.

The Shredding page shows:

Objects and object parts waiting to be shredded
: The total number of these items waiting to be shredded: objects, parts of multipart objects, replaced parts of multipart uploads, parts of aborted multipart uploads, unused parts of completed multipart uploads, and transient parts created during the processing of certain multipart upload operations

Total bytes to be shredded
: The total number of bytes of object and part data and metadata waiting to be shredded

These statistics include all objects and parts marked for shredding for which the primary metadata has not yet been deleted.

The panel also shows the current shredding settings.

Changing shredding settings

Depending on the system load, the HCP system can develop a backlog of objects and parts to be shredded. If the system load from other activities is light, you can increase the rate at which shredding occurs. If the load is heavy, you can lower the shredding rate.

To change the settings for the Shredding service:

1. On the Shredding page in the System Management Console, set the options you want:
   - To change the shredding rate, in the Shredding Rate field, select Low, Medium, or High. The higher the shredding rate, the greater the load on the HCP system.
   - To enable or disable sending log messages about shredded objects and parts to syslog servers, select or deselect, respectively, Log shredded objects and object parts to syslog.
2. Click Submit.

Duplicate elimination and shredding

Objects merged by the Duplicate Elimination service do not necessarily have the same shred settings.

When merged objects with different shred settings are deleted:

- If the last object deleted is not marked for shredding, the merged data is not shredded.
- If the last object deleted is marked for shredding, the merged data is shredded.

Erasure coding and shredding

For an object that's subject to both erasure coding and shredding:

- Each time a full copy of the data for the object is reduced to a chunk, the full copy must be shredded
- Each time a chunk for the object is restored to a full copy of the object data, the chunk must be shredded

As a result, shredding objects that are subject to erasure coding can put a significant load on all the systems in the replication topology across which the objects are erasure coded.

To minimize the load that the combination of erasure coding and shredding can put on an HCP system, take one of these actions:

- At the system level, do not enable erasure coding as an option for implementing replicaton.
- If you enable erasure coding as the replication method for all cloud-optimized namespaces, tell tenant administrators not to set shredding as the default for deleted objects in cloud-optimized namespaces that are selected for replication.
- If you allow tenant administrators to select erasure coding for their namespaces, tell the administrators not to do both of these for any given namespace:
  - Set shredding as the default for deleted objects
  - Allow erasure coding

Shredding service trigger

The Shredding service is event driven only, not scheduled. It is triggered by the deletion of an object that’s marked for shredding. The delete operation can be invoked by a user or application or by the Garbage Collection service.

Storage Tiering service

Each namespace has a service plan that defines both a storage tiering strategy and a data protection strategy for the objects in that namespace. At any given point in the lifecycle of an object, its storage tiering strategy specifies the types of storage on which copies of that object must be stored, and its data protection strategy specifies the number of object copies that must be stored on each type of storage.

The Storage Tiering service performs these functions according to rules specified in service plans:

- Moving copies of the objects in a given namespace among all of the storage tiers that are defined for that namespace by its service plan
- Creating and deleting copies of objects in a given namespace on each storage tier that is defined for that namespace to ensure that each tier always contains the correct number of copies of each object
- Changing objects stored on primary running storage to be metadata-only or restoring data to metadata-only objects

For the purpose of storage tiering, HCP treats these as individual objects:

- Parts of multipart objects. These parts are tiered based on the time of completion of the multipart upload that created the object.
- Chunks for erasure-coded objects. These chunks are tiered based on the object ingest time.
- Chunks for erasure-coded parts of multipart objects. These chunks are tiered based on the time of completion of the multipart upload that created the object.

The Storage Tiering service does not tier parts of in-progress multipart uploads.

The Storage Tiering service tiers full copies of the data for objects and parts that are subject to erasure coding if the target storage tier is primary running storage, HCP S Series storage, or primary spindown storage. The service does not tier full copies of the data for objects and parts that are subject to erasure coding if the target storage tier is extended storage.

The Storage Tiering service can move objects and parts that are subject to erasure coding to a metadata-only storage tier before they are due to be reduced to chunks, provided that a full copy of the object or part data exists on at least one other system. While on the metadata-only tier, the object or part has metadata but no data.

If an object or part on a metadata-only storage tier is due to be reduced to a chunk, the Geo-distributed Erasure-Coding service gets the applicable chunk from another system. That service then removes the object or part from the metadata-only tier and stores the chunk for the object or part on the previous tier, as specified by the applicable service plan.

The Storage Tiering service does not move chunks for erasure-coded objects and parts to metadata-only storage tiers.

The Storage Tiering service runs according to the active service schedule.

Important: HCP S Series Nodes run the risk of reaching maximum storage capacity. Objects do not tier to S Series Nodes that are full.

Moving copies of objects among storage tiers

One of the functions of the Storage Tiering service is to move copies of objects in a namespace among storage tiers that are defined for that namespace by its service plan. The tier on which HCP initially stores every object in the namespace is called the *ingest tier*. The ingest tier must be either primary running storage or HCP S Series storage.

For each storage tier, including the ingest tier, the service plan for a given namespace specifies:

- The storage pools that are used to store copies of each object on the tier. Each *storage pool* consists of one or more storage components. Each *storage component* represents a type of primary storage (running or spindown), HCP S Series storage, an extended storage device, or a cloud storage service endpoint.
- For each object that's stored on the tier, the number of copies of the object data that HCP must maintain on each storage pool and the number of copies of object metadata that HCP must maintain on the ingest tier.
- The transition criteria for each tier except for the ingest tier. The *transition criteria* for a storage tier are the rules that determine when one or more copies of each object in the namespace must be stored on the tier:
  - The object age (number of days since ingest) at which one or more copies of the object data must be moved from the previous tier onto this tier
  - For service plans that define exactly two tiers, including the ingest tier, whether a threshold will be applied to the second tier, and if so, the percentage of ingest tier storage capacity that must be used (the threshold) before object data can be moved to the second storage tier
  - For HCP systems with replication enabled, whether objects must be fully replicated before they can be transitioned from the previous tier onto this tier. If replication is disabled for the HCP system, this transition criterion does not appear in the HCP System Management Console.
- For a namespace that's currently being replicated to another system, whether the copies of the object that are stored on the tier are to be made metadata-only.

  Regardless of the transition criteria that are specified for a metadata-only tier, objects are moved to such a tier only after they are replicated. When a replicated object is moved to a metadata-only tier, all existing copies of the object data are deleted from the previous tier and from primary running storage, and the specified number of copies of the object metadata are stored on primary running storage.

- Whether the data for each object stored on the tier is *rehydrated* (that is, restored on the ingest tier) upon being read from the tier, and if so, the number of days HCP is required to keep a rehydrated copy of object data on the ingest tier.

If the service plan for a given namespace defines multiple storage tiers, then for each object in that namespace, the Storage Tiering service:

- Moves copies of the object data among the storage tiers that are defined for the namespace to satisfy the transition criteria that are defined for each storage tier.
- Upon moving all existing copies of the data for an object from one tier to another:
  - If the new tier has a different DPL from the previous tier, creates or deletes the number of copies of object data that's required to satisfy the DPL setting for the new tier
  - If the new tier has a different primary running storage metadata protection level (MPL) from the previous tier, creates or deletes the number of copies of object metadata that's required to satisfy the MPL setting for the new tier
- Upon moving a replicated object to a metadata-only tier, deletes all copies of the object data from the previous tier, and if the previous tier is not the ingest tier, deletes any copies of the object data that exist on primary running storage.
- Checks to see whether the object data has been read from a storage tier for which rehydration is enabled, and if so, creates an extra copy of the object data on the ingest tier.
- After moving a replicated object to a metadata-only tier for which rehydration is enabled and making that object metadata-only, checks to see whether that object has been read from a remote system, and if so, restores the data to each copy of the object that's stored on the ingest tier.

Maintaining the correct number of object copies on each tier

Another function of the Storage Tiering service is to maintain the correct number of copies of each object in a namespace on each storage tier that's defined for that namespace by its service plan.

If the number of object copies on a storage tier is less than the number of object copies specified for that tier in the applicable service plan, the Storage Tiering service creates the applicable number of new copies of that object on that tier. If the number of copies of an object on a storage tier is higher than the number of object copies specified for that tier in the applicable service plan, the Storage Tiering service deletes all unnecessary copies of that object from that tier.

Differences between the Storage Tiering service and the Protection service

The Protection service performs work that is nearly identical to the work performed by the Storage Tiering service to maintain the correct number of copies of object data and metadata on each service tier that's defined for a namespace. However, the two services perform the work that they do in slightly different ways.

The Storage Tiering service runs only when it's scheduled to run. When the Storage Tiering service processes an object in a given namespace, the Storage Tiering service first checks to see whether copies of the object data are stored on the correct storage tier and moves the object data among tiers if necessary. The Storage Tiering service then checks to see whether the correct number of object copies exists on each tier that's defined for the namespace and takes corrective action if necessary.

The Protection service runs when it's scheduled to run and in response to its triggers. When the Protection service processes an object in a given namespace, the service first checks to see whether the correct number of copies of the object exist on all storage tiers. If not, the Protection service first checks to see whether the correct number of object copies exist on the active storage tier (the one on which the object is currently supposed to be stored) and takes corrective action if necessary. The Protection service then checks to see if the correct number of object copies exists on the other storage tiers and takes corrective action if necessary.

The Storage Tiering service is designed to optimize storage utilization. The Storage Tiering service, therefore, first moves objects among storage tiers and then checks to make sure all copies of each object in a given namespace have been stored on the correct storage tiers.

The Protection service is designed to optimize data availability and maintain the correct level of data redundancy for each object in a given namespace. The Protection service, therefore, constantly checks to see whether the correct number of copies of the object data are available to clients, and takes corrective action as soon as a violation occurs. When

the Protection service runs on a schedule, it checks the availability of each object on the active storage tier first, and then checks whether the correct number of objects copies exists on the other tiers.

Making objects metadata-only

The third function of the Storage Tiering service is to delete all existing copies of the data for any object that's moved to a metadata-only storage tier and ensure that the correct number of copies of the metadata for that object are stored on primary running storage.

The Storage Tiering service also restores data for metadata-only objects to the ingest tier. Restoring the data for an object to the ingest tier is called *rehydrating* the object.

When the Storage Tiering service moves an object off the ingest tier and onto another storage tier, the service removes all copies of the object data from the ingest tier and stores the specified number of copies of the object data on the new storage tier. However, at least one copy of the object metadata must always remain on primary running storage. For each storage tier that's defined for a given namespace, the service plan specifies the number of copies of object data that must be stored on the tier and the number of copies of object metadata that must be stored on primary running storage.

If a given namespace is being replicated to another system, you can configure the service plan for that namespace to define a metadata-only storage tier. This type of tier specifies the number of copies of object metadata that must be stored on primary running storage, but it also specifies that no copies of the object data can be stored on any storage tier, including the ingest tier.

For a multipart object on a metadata-only storage tier, the applicable number of copies of the metadata for each part must be stored on primary running storage, and no copies of the part data can be stored on any storage tier.

The Storage Tiering service makes objects metadata-only only when all of these conditions are true:

- The service plan for the namespace that contains the object defines a metadata-only storage tier.
- The object is on the storage tier that immediately precedes the metadata-only tier defined in the namespace service plan, and the object meets the transition criteria specified for the metadata-only storage tier.
- A copy of the object data exists on at least one other HCP system in the replication topology in which the current system participates. (This is possible because service plans with the same name can have different definitions on different systems.)

When all of these conditions are true, the Storage Tiering service deletes all copies of the object data from the preceding storage tier. If the preceding storage tier is not primary running storage, the Storage Tiering service also deletes any copies of the object data that exist on primary running storage. After deleting all copies of the object data, the Storage Tiering service creates or deletes copies of the object metadata on primary running storage as necessary so that the number of copies of object metadata match the number of copies that the service plan requires for the metadata-only tier.

If rehydration is enabled for a metadata-only storage tier, when rehydrating a replicated object that's been read from primary running storage on a remote system, the Storage Tiering service rehydrates all copies of the object on the ingest tier on the local system

When replicating an object in a namespace to a system on which objects in that namespace can be made metadata-only, HCP replicates only the object metadata if the object is larger than one MB. If the object is smaller than one MB, HCP replicates both the data and metadata.

Here's a scenario that shows how allowing metadata-only objects can be used to advantage:

You have a many-to-one replication topology in which the HCP systems at the outlying sites are much smaller than the central HCP system to which they all replicate. To optimize the use of storage on the outlying systems, you allow the namespaces on those systems to have metadata-only objects while requiring the central system to have the object data. The outlying systems respond to client requests for object data by reading the data from the central system.

In this scenario, the replication topology should include a disaster recovery system (that is, a replica of the central system) to protect against data loss in case of a catastrophic failure of the central system.

Important: HCP does not prevent you from removing a namespace from a replication topology even if the namespace contains metadata-only objects on one or more systems in that topology. This can result in data for objects in that namespace being permanently inaccessible from those systems. In most cases, HCP warns you if the modification you're making to a replication link would cause this condition to occur.

Storage Tiering service processing

The Storage Tiering service processes one object at a time. For each object, the service checks the applicable service plan to determine the storage tiers on which copies of the object data should be stored, the number of copies of the object data that should be stored on each tier, and the number of copies of the object metadata that should be stored on primary running storage. The Storage Tiering service then checks to see whether the object data has been read from a storage tier for which rehydration is enabled. Finally, the Storage Tiering service checks to see whether the object data has been read from a remote system because that object is metadata-only on the local system, and if so, the service checks to see whether rehydration is enabled for the metadata-only tier on which the object resides.

For each object in a namespace, if all of these conditions are true, the storage plan takes no action on that object:

- The object is stored on the correct storage tier.
- The correct number of copies of the object data exist on the current storage tier.
- The correct number of copies of the object metadata exist on primary running storage.
- If the object is on a storage tier for which rehydration is enabled, the correct number of rehydrated copies of the object exist on the ingest tier.

If one or more of the above conditions is not true, the Storage Tiering service takes the applicable actions to bring the object into compliance with the namespace service plan.

Understanding storage tiering statistics

The Storage page in the HCP System Management Console displays graphs and statistics that provide information about the use of primary running storage, primary spindown storage, and each type of extended storage that's used to store objects in a repository. The Storage page also provides information about metadata-only objects.

Note: To view the Storage page, you need the monitor or administrator role. To modify the configuration of extended storage or to create, modify, or delete service plans, you need the administrator role.

To display the Storage page, in the System Management Console, click Storage.

System security

Through the HCP System Management Console, you can set various options that affect HCP system security.

In addition to creating and managing user and group accounts and login settings, you can:

- Specify whether HCP nodes should respond to ping requests
- Allow or disallow SSH access to HCP nodes

- View current Support access credentials
- Apply exclusive Hitachi Vantara Support access credentials
- Create domains and associate SSL server certificates with them
- Allow or deny access to the System Management Console from specific IP addresses
- Control the use of the HCP management API by users with system-level user accounts
- Allow or deny access to the Search Console for the default tenant from specific IP addresses
- Configure support for Windows Active Directory or Windows workgroups
- Clear the Active Directory cache
- Set up connections to RADIUS servers
- Set the system-wide permission mask for access to namespaces

Setting network security

The Network Security page in the HCP System Management Console lets you enable or disable the following services on HCP nodes:

Ping
: Checks network connectivity to HCP nodes.

SSH login by authorized service and Support representatives
: Facilitates troubleshooting when you request support.

Node Status
: Enables node status commands to check the health of your nodes.

3DES Ciphers
: Allows the system to use the Triple-DES cipher algorithm for data encryption. The more secure option is to disable this service. Changing this setting causes the HCP system to restart and requires your confirmation.

SSL renegotiation
: Allows SSL renegotiation. The more secure option is to disable this service.

Restrict anonymous access with CIFS
: Prevents anonymous users from using CIFS to access namespaces on the system. Tenant-level administrators can override this setting for individual namespaces.

Prevent data access with SMBv1
: Prevents users from using the SMBv1 protocol for data access with CIFS.

Minimum Security Protocol
: Allows you to set the minimum security protocol supported for front-end communications. The recommended minimum security protocol is TLS v1.3.
Note:

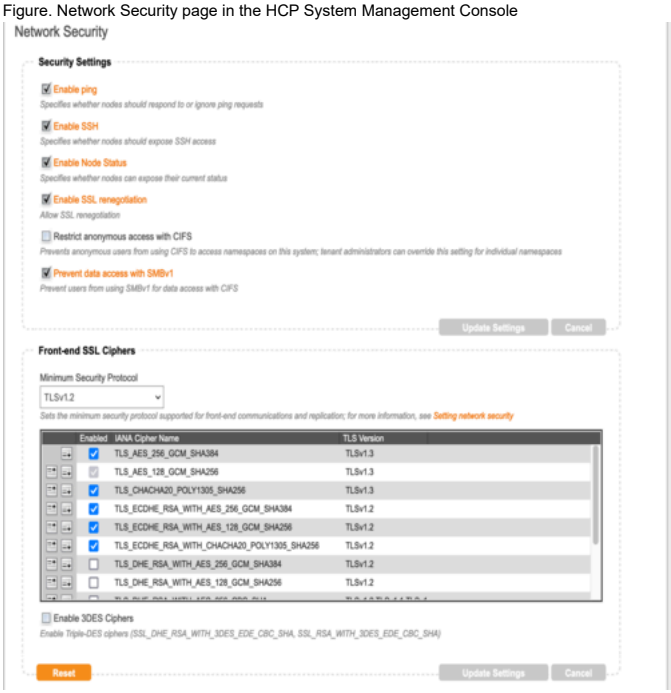
AWS Command Line Interface (AWS CLI) tool does not support TLS v1.3 in HCP. Though HCP Release 9.4 supports TLS v1.3, if you are using AWS CLI with HCP, we recommend using TLS v1.2 or an earlier version.

Enabling or disabling network security services on HCP nodes

To view the Network Security page, you need the monitor or administrator role. To change network security settings, you need the administrator role.

Use the Network Security page of the System Management Console to enable or disable network security services on HCP nodes.

Figure. Network Security page in the HCP System Management Console



1. In the top-level menu in the System Management Console, select Security > Network Security.
   The Network Security page opens.
2. For each security setting, select or clear the option to enable it.
   a. Click Minimum Security Protocol and select the minimum security protocol you want to use for front-end communications.
      You see a table that displays the list of available ciphers.
   b. Select or clear the option to enable each cipher.
   Note: Changing Minimum Security Protocol setting causes the HCP system to restart and requires your confirmation.
3. Click Update Settings.

4. Click Reset to restore all cipher settings to their default configuration.

   After upgrading to HCP v9.7, the table will display the previously used old ciphers. However, resetting will enable the default ciphers for HCP v9.7.

Setting exclusive Support access credentials

Exclusive Hitachi Vantara Support access credentials provide additional security compliance for an HCP system by enabling each system with a unique set of SSH keys. These keys, which are used for the sole purpose of system support and maintenance by authorized service and Support personnel, can be applied by an authorized service provider during final on-site setup or at a later time.

To apply exclusive Support access credentials on the HCP system after final on-site setup, the administrator obtains the exclusive credentials from an authorized service provider or Hitachi Vantara Support. The administrator can apply the credentials package using either the Upload Support Access Credentials wizard in the System Management Console, or the HCP management API `supportaccesscredentials` resource.

Applying the exclusive Support access credentials package

The administrator or service role is required to apply exclusive Hitachi Vantara Support access credentials.

1. Open the System Management Console.
2. From the Security menu, select Support Access Credentials.
   The Manage tab of the Support Access Credentials page is displayed. The Access Credentials Details section indicates whether the current Support access credentials are the default credentials or exclusive Hitachi Vantara Support access credentials.
3. Click Upload Support access credentials.
   The Upload tab of the Upload Support Access Credentials wizard is displayed.
4. Open your file system browser window, navigate to the location of the exclusive Hitachi Vantara Support access credentials package that you obtained from an authorized service provider or Support, and double-click the .plk file.
   The file system browser window closes and the Upload Support access credentials page is updated with the name of the .plk file.
5. Click Next.
   The package validation procedure runs.
   - If the package validation fails with an invalid package error, either return to step 4 to browse and select another exclusive Support access credentials package, or cancel the operation.
   - If the package validation succeeds, the Review tab of the Upload Support Access Credentials wizard is displayed.
6. Review the package validation details and any warning messages.
   - If the information is correct, click Finish.

     The Manage tab of the Support Access Credentials page is updated with details about the applied exclusive Support access credentials. Go to step 7.

   - If the information is incorrect, click Cancel.

     The wizard closes and the Manage tab of the Support Access Credentials page is displayed.
7. Review the HCP system log to ensure that it includes an informational event indicating that the exclusive Support access credentials have been applied to the system. If you see any error messages related to applying the exclusive credentials, notify your authorized service provider.

Managing domains and SSL server certificates

You can create multiple domains in HCP and associate one or more SSL server certificates with each domain. HCP uses these domains and certificates to facilitate and secure communications over its built-in and user-defined networks.

About domains

A *domain* is a group of computers or devices that are administered as a unit. In terms of HCP, a domain consists of nodes in a single HCP system.

Domains are associated with networks. Clients that communicate with HCP over a given network can use the name of the domain associated with that network to identify the system.

Each network specifies IP addresses for the system nodes. A single domain can be associated with multiple networks. Therefore, a single domain can correspond to multiple sets of IP addresses.

An HCP system can have at most 201 domains. You can create domains at any time. You can delete a domain only while it is not associated with any networks.

Domain names

Every domain has a name. A domain name can contain only letters, numbers, and hyphens (-). It must consist of at least three segments, separated by periods (.). Each segment must be one through 63 characters long. The entire domain name, including the periods between segments, must be less than 128 characters long.

When specifying a domain name, you can use both uppercase and lowercase letters. However, when you save the domain, HCP converts any uppercase letters to lowercase.

If the HCP system is configured to use DNS, the higher-level portion (minimally, the last two segments) of the name of each domain that you create must identify a DNS domain to which you have administrative access.

Domains cannot be subdomains of each other. For example, if a domain named hcp.example.com already exists, you cannot specify cust1.hcp.example.com as the name of another domain.

In the URL for access to a tenant, the tenant name is inserted before the name of the domain. For this reason, you should not specify the tenant name as part of the domain name.

For example, suppose you create a tenant named finance for Customer-1 and a domain named finance.cust1.com. If you select finance.cust1.com as the domain for the network you associate with the finance tenant for management purposes, the URL for access to the Tenant Management Console for the finance tenant is https://finance.finance.cust1.com.

During HCP installation, one domain is created automatically. The name of this domain is the name specified for the system during the installation procedure. This domain is created regardless of whether the system is configured to use DNS.

Domains and DNS

Typically, domains are defined in a DNS. For each domain, the DNS lists all node IP addresses assigned to each network with which the domain is associated.

With DNS, you can manage domains in a single set of corporate DNS servers. Alternatively, you can set up separate DNS servers for different networks that use the same domain. Or, you can use a combination of these two techniques. In any case, you need to ensure that your networking environment and DNS configuration allow client requests to be routed to the correct HCP network.

If DNS is in use at your site, you can take advantage of DNS configuration options to further enhance the security of the HCP networks. However, HCP does not require the use of DNS. Without DNS, you can still define multiple domains in HCP and associate them with networks. In this case, to enable client requests to be routed to an HCP network, users would use the hosts file on each client computer to map the node IP addresses assigned to the network to the fully qualified domain name (FQDN) of the domain associated with the network.

From the Networks page in the HCP System Management Console, you can display the stub zone definition that you need to include in the DNS for each combination of domain and network.

About SSL server certificates

Each domain in HCP must have at least one SSL server certificate or CSR. SSL server certificates are used to verify to clients that the HCP system is the system it claims to be and to set up secure communications between the system and those clients.

HCP uses SSL to provide security for:

- HCP System Management Console, Tenant Management Console, and Search Console
- HCP management API
- Replication
- HTTP, S3 compatible, and WebDAV namespace access protocols
- HCP metadata query API
- HCP Namespace Browser

HCP comes with one self-signed SSL server certificate, which is generated and installed automatically when the system is installed. This certificate is associated with the domain that's created during installation.

Self-signed SSL server certificates are not automatically trusted by web browsers and other HTTP client tools. However, clients can choose to trust them.

Certificates for domains

You add the first SSL server certificate to a domain as part of creating the domain. Once a domain exists, you can add certificates to it at any time. You can also delete certificates from a domain. However, if the domain is associated with any networks, you cannot delete the last certificate.

For example, you might choose to add a certificate from a trusted vendor and then delete any self-signed certificates associated with the domain. Or, you might choose to add a certificate before the last valid certificate for the domain expires.

You can add a certificate to a domain in these ways:

- By having HCP generate and install a new self-signed certificate. In this case, the new certificate has an expiration date that's five years later than the current date.
- By generating a CSR, sending it to a certificate authority (CA), and installing the returned certificate.

  A domain can have only one outstanding CSR at a time.

- By installing a certificate that's created outside of HCP.

At any given time, the combined number of certificates and outstanding CSRs for a domain cannot exceed ten.

CSR and returned certificates

SSL server certificates are available from several trusted sources. To obtain a certificate, you need to create a CSR and present it to a CA. The CA then generates the requested certificate and makes it available to you either as an email attachment, as text embedded in the body of an email, or as a download from a web page:

- If the certificate is an email attachment, save it to disk.

  Use .cer as the extension for the certificate file name.

- If the certificate is embedded in an email or downloadable from a web page, copy and paste it into a new text file. Then save the file to disk.
  Important: Use a simple text editor to do this. Do not use Microsoft® Word or any other word-processing program to create the text file.

You can create a CSR by using the HCP System Management Console or a third-party tool. When you use the System Management Console, however, HCP securely stores the private key needed for installing the returned certificate, so you don't need to save it yourself.

Certificates created outside HCP

You can create an SSL server certificate yourself by using a third-party tool such as OpenSSL, which is publicly available. Or, you can create a CSR yourself and use that to get a certificate from a CA.

Certificates created outside HCP have two passwords: one for the PKCS12 object containing the certificate and one for the private key for the certificate. To install the certificate in HCP, these passwords must be identical.

Common names

Every SSL server certificate has a common name. In HCP, the common name for a certificate must represent a subdomain of the domain with which the certificate is associated.

The first segment of the common name can be an asterisk (*) by itself, which represents any valid domain name segment. A common name can be at most 255 characters long.

Here are some examples of common names for certificates associated with the domain named hcp.example.com:

```
*.hcp.example.com

admin.hcp.example.com

ten1.hcp.example.com

*.ten1.hcp.example.com

ns1.ten1.hcp.example.com
```

The common name for the certificate generated during HCP installation is an asterisk followed by the name of the domain created during installation.

HCP supports subject alternative names for certificates created outside the system.

Certificate selection

At any given time, an SSL server certificate is in one of these three states: valid, expired, or future (that is, not yet valid). When choosing which certificate to present to a client for a given domain:

1. HCP first looks for a valid certificate for the domain and, if it finds any, uses the one with the earliest start date and time.
2. If the domain has no valid certificates, HCP looks for an expired certificate for the domain and, if it finds any, uses the one with the latest expiration date and time.
3. If the domain has no expired certificates, HCP uses the future certificate with the earliest start date and time.

HCP consistently chooses the same certificate. Any of these events, however, can cause HCP to start choosing a different certificate:

- The chosen certificate expires or is deleted.
- A future certificate for the domain becomes valid.
- A new certificate is added to the domain.

Note: After an event that causes HCP to choose a different certificate, the system may continue using the certificate initially chosen for a client session until the applicable cache is cleared.

HCP does not take the common name into consideration when choosing a certificate. This means that in response to a client request, HCP can use any certificate for the domain associated with the network over which the request arrives (subject to the selection process described above).

For example, suppose the domain named hcp.example.com has a certificate with the common name *.ten1.hcp.example.com. Suppose also that the management network for the tenant named ten2 uses the hcp.example.com domain. In response to a client request with a URL that specifies ten2.hcp.example.com, HCP could present the certificate with the common name *.ten1.hcp.example.com. The client is responsible for deciding how to handle certificates with common names that don't match the requested URL.

Managing domains and certificates

To view, create, and delete domains and the SSL server certificates associated with them, you use the Domains and Certificates page in the HCP System Management Console.

Note: To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

Creating a domain

You can create a domain by using the HCP System Management Console.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, click Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. Click Create Domain.
4. In the Domain Name field, type a unique name for the domain.
5. In the Certificates field, select one of these options:
   - Generate and install self-signed certificate
   - Generate CSR
   - Install PKCS12 certificate
6. Click Create Domain.

Adding a certificate to a domain

You can add an SSL server certificate to an existing domain by using the HCP System Management Console.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. In the list of domains, click the name of the domain that you want to add a certificate to.
4. In the panel that opens, click New Certificate.
5. Select one of these options:
   - Generate and install self-signed certificate
   - Generate CSR
   - Install PKCS12 certificate
6. Take one of these actions:
   - If you selected Generate and install self-signed certificate, click Generate Certificate.
   - If you selected Generate CSR, click Generate CSR.
   - If you selected Install PKCS12 certificate, click Install Certificate.

After you generate a CSR, you need to download it to a file that you can send to the CA. Later, when you receive the certificate from the CA, you need to upload it to HCP.

Creating a CSR

You can create a CSR when you create a new domain or add a new certificate to an existing domain.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. Select Generate CSR.

The Generate CSR section opens.

4. Fill in the field values that a CA needs to generate an SSL server certificate.

   Check with the CA that you plan to use to learn what information is needed.

   Common Name (CN) field
   : Required. Type the common name for the certificate. This value can range from 1-255 characters long and can contain any Latin-1 characters, including white space.

   Organizational Unit (OU) field
   : Type the name of the organizational unit that will use the certificate, for example, the name of a division or the name under which your company does business. This field accepts only alphanumeric characters. Do not include a comma (,), plus (+), or equals (=) sign.

   Organization (O) field
   : Type the full legal name of your company. This field accepts only alphanumeric characters. Do not include a comma (,), plus (+), or equals (=) sign.

   Location (L) field
   : Type the name of the city where your company headquarters are located.

   State/Province (ST) field
   : Type the full name of the state or province where your company headquarters are located.

Deleting a certificate or CSR

You can delete a SSL server certificate or CSR from a domain by using the HCP System Management Console.

Deleting a SSL server certificate or CSR from a domain is subject to several restrictions:

- If the domain is associated with any networks, it must have at least one SSL server certificate.
- If the domain is not associated with any networks, it must have at least one SSL server certificate or CSR.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. In the list of domains, click the name of the domain that has the certificate or CSR that you want to delete.
4. In the panel that opens, click the delete control ( ) in the Certificate Details or CSR Details section for the applicable certificate or CSR.
5. In response to the confirm message, click Delete.

Downloading a CSR

You can download a CSR by using the HCP System Management Console.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. In the list of domains, click the name of the domain for which you want to download a CSR.
4. In the panel that opens, in the CSR Details section for the applicable CSR, click Download CSR.
5. When prompted, save the file containing the CSR to a location of your choice.

   This is a plain text file. The default file name is certificate.txt.

Installing the certificate returned for an HCP generated CSR

You can install the SSL server certificate returned in response to an HCP generated CSR by using the HCP System Management Console.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Domains and Certificates.
   The Domains and Certificates page opens.
3. In the list of domains, click the name of the domain that has the HCP generated CSR for the SSL server certificate you want to install.
4. In the panel that opens, in the CSR Details section for the applicable CSR, click Browse and select the file containing the returned certificate.
5. Click Upload Certificate.

Installing a certificate created outside HCP

You can install a SSL server certificate that was created outside HCP when you create a domain or add a certificate to an existing domain.

To view existing domains and SSL server certificates, you need the monitor or administrator role. To create and delete domains and SSL server certificates, you need the administrator role.

1. Open the HCP System Management Console and follow the procedure for creating a domain or adding a certificate to a domain.
2. To install a certificate that was created outside HCP, in the New Certificate section of the Domains and Certificates page, select Install PKCS12 certificate.
   The Install PKCS12 certificate section opens.
3. Select the file containing the certificate that you want to install and enter the password for the certificate.
   a. In the PKCS12 Certificate field, click Browse and select the file containing the PKCS12 object.
   b. In the PKCS12 Password field, type the password for the PKCS12 object.

Controlling access to the System Management Console

The Console Security page in the HCP System Management Console lets you control access to the Console from specified IP addresses. To display this page, in the top-level menu of the Console, select Security > Console Security.

Note: To view and modify information on the Console Security page, you need the security role.

Valid IP address list entries

You can specify each IP address list entry in the Allow and Deny lists in one of the following formats:

- A single IP address
- A range of IPv4 addresses specified as *ip-address/subnet-mask* (for example, 192.168.100.197/255.255.255.0) or in CIDR format (for example, 192.168.100.0/24)
- A range of IPv6 addresses specified in CIDR format (for example, 2001:0db8::/32)

The CIDR entry that matches all IPv4 addresses is 0.0.0.0/0. The CIDR entry that matches all IPv6 addresses is 0::0/0.

IP address list handling

IP addresses can be included in one, both, or neither of the Allow and Deny lists. To specify how HCP should handle access requests from IP addresses that are either included in both lists or excluded from both lists, select or clear the Allow request when same IP address is used in both lists option. The following table describes the effects of selecting and clearing this option.

List entries	Allow requests when same IP address is used in both lists	
	Selected	Cleared
• Allow list: empty • Denylist: empty	All IP addresses have access.	No IP addresses have access.
• Allow list: at least one entry • Deny list: empty	All IP addresses have access.	Only IP addresses in the Allow list have access.
• Allowlist: empty • Deny list: at least one entry	All IP addresses not in the Deny list have access. IP addresses in the Deny do not.	No IP addresses have access.
• Allowlist: at least one entry • Deny list: at least one entry	IP addresses appearing in both or neither of the lists have access.	IP addresses appearing in both or neither of the lists do not have access.

Controlling access to HCP through the management API

You configure HCP to enable and disable the HCP management API and to control access to the API at both the system level and the tenant level.

To allow system-level users to access the management API for the HCP system to create, modify, and delete tenants and manage replication, the API must be enabled at the system level. To allow tenant-level and system-level users with administrative access to a specific HCP tenant to access the management API for that tenant, the API must be enabled at both the system and tenant levels.

You can access the HCP management API using a system-level URL (that is, a URL that starts https://admin...) only if at least one of your client IP addresses is allowed to access the management API for the HCP system. You can access the HCP management API using a tenant-level URL (that is, a URL that starts https://tenant-name...) only if at least one of your client IP addresses is allowed to access the management API for the HCP tenant specified in the URL.

You use the Management API page in the HCP System Management Console to enable the HCP management API at the system level and to configure HCP to control access to the management API for the HCP system. To display this page, in the top-level menu of the System Management Console, select Security > MAPI.

Note: To view and modify the HCP management API configuration, you need the security role.

Enabling the HCP management API

You can enable the HCP management API at the system level and configure HCP to control access to the management API for the HCP system, on the Management API page.

To view and modify the HCP management API configuration, you need the security role.

1. Go to the Management API Settings section.
2. Select Enable the management API.
3. Click Update Settings.

Specifying IP addresses to be allowed access to HCP

You can specify IP addresses to be allowed access to HCP through the management API.

To view and modify the HCP management API configuration, you need the security role.

1. Click the Allow tab.
2. Follow the instructions in Adding and removing entries in Allow and Deny lists.

Specifying IP addresses to be denied access to HCP

You can specify IP addresses to be denied access to HCP through the management API.

To view and modify the HCP management API configuration, you need the security role.

1. Click the Deny tab.
2. Follow the instructions in Adding and removing entries in Allow and Deny lists.

   To specify how HCP should handle access requests from IP addresses that appear in both or neither of the Allow and Deny lists, select or deselect Allow request when same IP is used in both lists. Changes to this option take effect immediately.

Controlling access to the Search Console for the default tenant

The Search Console for the default tenant enables users to search the default namespace and any namespaces owned by HCP tenants that allow system-level administrative access to themselves. You can choose to allow access to the Search Console for the default tenant only from specific IP addresses. Similarly, you can choose to deny access to the Search Console for the default tenant from specific IP addresses.

You use the Search Security page in the System Management Console to control access to the Search Console for the default tenant. To display this page, in the top-level menu of the System Management Console, select Security > Search Security.

Note: To view and modify information on the Search Security page, you need the security role.

To control access to the Search Console for the default tenant, on the Search Security page:

- Optionally, specify IP addresses to be allowed access to the Search Console. To do this:
    1. Click the Allow tab.
    2. Follow the instructions in Adding entries in Allow and Deny lists.
- Optionally, specify IP addresses to be denied access to the Search Console. To do this:
    1. Click the Deny tab.
    2. Follow the instructions in Removing entries in Allow and Deny lists.

Configuring Active Directory or Windows workgroup support

You can configure HCP to support Microsoft Active Directory (AD) or Windows workgroups. HCP cannot support AD and Windows workgroups at the same time.

You can configure HCP to support Active Directory authentication. An authenticated AD user can use any HCP interface that requires authentication, such as the System Management Console, Search Console, or namespace access protocols provided the user has the applicable HCP permissions.

A Windows workgroup is a named collection of computers on a LAN that share resources such as printers and file servers. User accounts are specific to each computer in a workgroup. No authentication is required for access to the shared resources.

When you configure HCP to support Windows workgroups, you provide the name of the workgroup in which you want CIFS-enabled namespaces to be shared resources. If HCP is on the same LAN as the computers in the workgroup, all CIFS-enabled namespaces are automatically exposed in the workgroup. HCP namespaces are displayed as a single shared resource with a name in this format:

tenant-name_namespace-name

For example, finance_accounts-receivable). The default namespace is displayed as two shared resources, fcfs_data and fcfs_metadata.

If the CIFS protocol is configured to require authentication for access to a given namespace, that namespace cannot be accessed through a workgroup.

About Active Directory

The following sections provide more information about using AD with HCP.

User authentication with Active Directory

When an AD user tries to access HCP using a client application that supports Integrated Windows authentication (such as Firefox, Internet Explorer, or Windows Explorer):

- If the user is logged into Windows with a recognized AD user account, HCP accepts the authenticated credentials from the client computer and lets the user access the requested interface by using single sign-on.
- If the user is requesting HCP access with a recognized AD user account that is not the account with which the user is currently logged in to Windows, HCP sends the specified user credentials to AD for authentication. If AD successfully authenticates the user, HCP lets the user access the requested interface.

A *recognized AD user account* is an AD account for a user who belongs to one or more AD groups with corresponding group accounts in HCP.

Note: Tenant administrators can configure individual namespaces not to support single sign-on with HTTP-based interfaces, for example, the HCP Namespace Browser.

HCP configuration for Active Directory support

For HCP to support AD, you need to configure HCP to identify the domain in the AD forest to be used for HCP user authentication and provide credentials for an existing AD account in that domain. This AD user account is used to configure HCP in the AD domain.

All AD domain controllers configured for the domain used for HCP user authentication must be able to communicate with HCP over the [hcp_system] network. Therefore, each AD domain controller must have at least one IPv4 or IPv6 address that is routable from the [hcp_system] network.

You also need to specify or accept the defaults for the existing organizational unit (OU) in which computer accounts will be created for the HCP nodes, along with the name of a computer account that HCP will use when querying AD for groups and other information. That computer account will be in the same AD groups as the user account you specify.

You can choose to enable secure communication between HCP and AD for the configuration of the computer account that HCP will use for querying AD. In this case, HCP needs a copy of the SSL certificate that allows clients to connect securely to the LDAP server used by AD. You need to export this certificate from AD as a base-64-encoded X509 certificate and then upload it to HCP on the Active Directory page.

For secure communication with AD when configuring computer accounts for HCP nodes, you can configure HCP to use NTLM or NTLMv2. The Use NTLMv2 authentication option appears only if you have selected Enable Authenticated CIFS Support. If you want HCP to use NTLM instead, deselect Use NTLMv2 authentication. In release 7.2.1 of HCP or later, new AD connections are created with the Use NTLMv2 authentication option enabled.

Additional considerations

- If you have more than one HCP system for which you are enabling support for AD, one or more of those systems may need to be reconfigured to prevent conflicts. Before enabling support for AD for any of the HCP systems, contact your authorized HCP service provider. Your provider can determine whether any reconfiguration is required and then make the necessary changes.
- For authenticated AD users to use a tenant- or namespace-level interface, such as the Tenant Management Console and the namespace access protocols, the tenant must also be configured to support AD authentication.
- If you disable support for AD after it has been enabled, tenants that support only AD authentication will not be able to access the Tenant Management Console. Therefore, before disabling AD support, you should ensure that all tenants support local authentication. Additionally, you should notify all tenant administrators that they need to create at least one locally authenticated user account with the security role.
- For HCP to use AD for user authentication:

  - HCP must be able to contact at least one DNS server that can resolve the AD domain name.
  - The AD time must be within five minutes of the HCP system time. A good practice is to configure HCP and AD to use the same time server.
  - All the domains in the AD forest HCP uses for user authentication must minimally be at the 2008 functional level.
- To ensure that AD users have continuous access to HCP, the AD infrastructure should have a robust and fault tolerant configuration.

Service principal name attributes for HCP

When you enable Active Directory (AD) support in HCP, HCP adds values to the service principal name (SPN) attribute of the HCP computer account in AD.

The initial values that HCP adds to the SPN attribute of the computer account in AD are:

- System Management Console
- Default tenant
- Search Console
- Each node in the HCP system

Subsequently, values are added for:

- Each tenant that supports AD authentication
- Each namespace that has both the HTTP protocol and AD single sign-on enabled
- Each node added to the HCP system

Each object for which an SPN value is created is referred to as a *single sign-on location*. If a single sign-on location for a tenant, namespace, or node is removed from the system, the value for that location is removed from the SPN attribute of the HCP computer account in AD.

AD has a size limit on values that applies to the SPN attribute. Any system-level operation in HCP that causes this limit to be exceeded fails with a message indicating that the failure is related to the number of single sign-on locations. Any tenant-level operation that causes this limit to be exceeded fails with a message indicating that single sign-on cannot be enabled.

Important: Active Directory imposes a practical limit of 1200 SPN values for a given AD object. When a tenant is created with AD enabled, HCP creates a SPN value corresponding to that tenant. Additionally, HCP creates a SPN value for each namespace created on the tenant. Because both the tenant and namespace SPN values are registered to the same AD object, the total number of AD enabled tenants plus their namespaces across the entire cluster must be less than 1200.

Configuring support for Active Directory

Before you configure support for AD in HCP, you need to prepare AD for access by HCP.

To enable and configure support for AD in HCP:

1. Log in to the HCP System Management Console with a user account that has the Security role.
2. Navigate to the Security > Active Directory page.
3. Select one of these options:

   Active Directory with SSL
   : Enables both support for AD and secure communication with the AD

   Active Directory without SSL
   : Enables support for AD without enabling secure communication with the AD

   With either of these options selected, the Active Directory page displays a Status section. This section contains alerts that report the status of various elements of HCP support for Active Directory.

4. If you selected Active Directory with SSL:
   a. In the Certificates panel, click Browse. Then select the file containing the AD SSL certificate.
   b. Click Upload Certificate.

      The Certificates section shows the uploaded certificate.

      You can download or delete the uploaded certificate if needed. To download the certificate, click the download control for it (). To delete the certificate, click the delete control () for it.

5. In the Configuration Settings section, select Enable Active Directory. Then:
   - In the Domain field, type the fully qualified name of the AD domain in the AD forest that is to be used for HCP user authentication. All letters in this domain name must be uppercase.
   - In the Domain User field, type the username of an existing AD user account in the applicable AD domain. Make sure the user account belongs to one or more groups that have the applicable permissions, as described earlier in this section.

     If the username that you specify is not all lowercase, HCP converts it to all lowercase before passing it to AD.

   - In the Password field, type the password that goes with the specified username. Passwords are case-sensitive.

     HCP uses the password that you type only to authenticate the username with the AD server. To help maintain AD security, HCP discards both the username and password after you submit the page. If you're modifying the AD configuration, you need to specify the password again.

6. Optionally, to specify an organization unit and computer account other than the defaults and to use NTLMv2 instead of NTLM, click Advanced Configuration. Then:
   - In the Organizational Unit field, type the distinguished name of the existing organizational unit in which you want the HCP computer accounts to be created. This is the distinguished name relative to the AD domain (for example, OU=HCP, OU=Storage). Do not include the domain name elements.
   - In the HCP Computer Account field, type the name of the computer account that HCP will use when querying AD for groups. This can be the name of an existing account in the specified organizational unit or the name of a new account to be created automatically in that organizational unit.

     For a new computer account, the name must be from one through 64 characters long, can contain only alphanumeric characters and hyphens (-), and cannot consist only of digits.

     If a computer account with the specified name already exists in a different organizational unit in the same Active Directory domain, the request to configure Active Directory support will fail.

   - Optionally, to specify how the HCP user account obtains permissions, do either of these:
     - If you created an AD group, select Add HCP Computer Account to groups of Domain User. This allows the HCP Computer account from inherit permissions associated with the specified domain user.

        - If you did not create an AD group, deselect Add HCP Computer Account to groups of Domain User. This prevents the HCP Computer account from inheriting the permissions associated with the specified domain user. If this checkbox is deselected, appropriate permissions need to be manually assigned to the HCP Computer account.
    - Optionally, select Non-Hierarchical Realm Configuration if you have multiple trees in your AD forest. This permits authentication from any domain in the forest, and is necessary if they have different domain names.
    - Optionally, select Enable Authenticated CIFS Support if you want to require authentication for data access via CIFS in your namespaces. Authenticated CIFS support is disabled by default for new AD joins.
    - If you selected Enable Authenticated CIFS Support, the Use NTLMv2 authentication option appears. Optionally, deselect Use NTLMv2 authentication to use NTLM for secure communication with AD when configuring the computer accounts for the HCP nodes. In release 7.2.1 of HCP or later, new AD connections are created with the Use NTLMv2 authentication option enabled.
    - Optionally, select Use reverse DNS if you want to join AD without requiring PTR records for domain controllers.
    - Select the Single Sign-On Support to determine how much control you want HCP to have over generating Service Principal Names (SPNs) for tenants and namespaces. The possible values are:

      None
      : HCP does not generate SPNs for new tenants namespaces and does not warn if SPNs are missing.

      Warning
      : HCP does not generate SPNs for new tenants and namespaces but does warn if SPNs are missing.

      Full
      : HCP generates SPNs for new tenants and namespaces and warns if SPNs are missing.

      SPNs are used for single sign-on. If you're not using single sign-on, you do not need to have HCP generate SPNs.

    - In the Trusted Forests field, type a comma-separated list of root domains of all trusted forests. This lets the HCP Computer Account authenticate with multiple forests.
7. Click Update Settings.

   This update may take a few minutes to finish.

   Tip: You can verify that AD support has been enabled by logging out of the System Management Console and checking that the Log In page now has a Domain field below the Password field.
8. Optionally, in the Domain Filtering panel, click Add New Domain. Then:
    - In the Domain Name field, type the name of the domain.
    - In the Domain Controllers field, type the name of the domain controller or controllers.
    - Click Add Domain.
    - Optionally, to associate another domain controller with a domain:
        a. Select an existing domain from the table in the Domain Filtering panel.
        b. In the Domain Controllers field, type the name of the domain controller or comma-separated list of controllers.
        c. Click Add New Domain Controllers.

           Domain controller filters are always added as a pairing of a domain and a domain controller or controllers. Each time you add one of these filters to the domain controller filter list, a one-time validation occurs. If a domain or domain controller fails the validation process, the filter is not added to the domain controller filter list. You can also manually invoke validation on the domain controller filter's entries by clicking the `Validate` button.
9. Click Update Settings.

   This update may take few minutes to finish.

Configuring support for Windows workgroups

You can enable and configure HCP support for Windows workgroups.

1. Log in to the HCP System Management Console with a user account that has the Security role.
2. Navigate to the Security > Active Directory page.
3. Select the Windows workgroup option.
4. In the Windows Workgroup field, type the name of the Windows workgroup in which you want HCP to automatically expose CIFS-enabled namespaces.

   The workgroup name can be up to 15 characters long.
5. Click Update Settings.

Refreshing the Active Directory status

Tenants and Namespaces can exist without Service Principal Names. HCP creates a table of unassigned Tenants and Namespaces under the Status panel of the Active Directory page under Security.

The Status panel automatically refreshes every twenty four hours, but it can also be manually refreshed. You can use the Active Directory page in the HCP System Management Console to refresh the status of the AD SPNs. The manual console refresh also attempts to automatically repair any SPNs that are missing. To display this page, in the top-level menu of the System Management Console, select Security > Active Directory.

Note: To view the Active Directory page and refresh the AD status, you need the security role.

To refresh the AD status, on the Active Directory page:

1. If support for AD is not currently enabled:
    a. Select Active Directory.
    b. Select Enable Active Directory.
2. Click Refresh Status.

Clearing the Active Directory cache

HCP caches information about authenticated AD users that access any of its interfaces. The cache also includes information about the AD groups to which those users belong. As long as the applicable information is in the cache, AD-authenticated users can perform any HCP activities for which they have permission without being reauthenticated.

HCP uses the same cache to store information about all the domains included in the AD forest that HCP uses for user authentication. HCP uses this information to supply the list of allowable domains in the Domain field on the login pages for its GUI interfaces.

You can clear the AD cache at any time. You might do this, for example, if the account for an authenticated AD user is deleted from AD. In this case, because the user information is already cached, the user can continue to access HCP even though the user account is no longer valid. Clearing the cache prevents the user from continuing to access HCP with the invalid account.

You also might clear the cache if a domain is added to or removed from the AD forest. This forces an immediate update to the list of allowable domains on the HCP login pages.

You use the Active Directory page in the HCP System Management Console to clear the AD cache. To display this page, in the top-level menu of the System Management Console, select Security > Authentication.

Note: To view the Active Directory page and clear the AD cache, you need the security role.

To clear the AD cache, on the Active Directory page:

1. If support for AD is not currently enabled:
   a. Select Active Directory.
   b. Select Enable Active Directory.
2. Click Clear Cache.

Configuring connections to RADIUS servers

For RADIUS authentication of an HCP user account, the HCP system must have network access to one or more RADIUS servers. To enable HCP to communicate with RADIUS, each RADIUS server must have at least one IPv4 or IPv6 address that is routable from the [hcp_system] network. To add and manage connections to one or more RADIUS servers, you use the RADIUS page in the HCP System Management Console. To display this page, in the top-level menu, select Security > RADIUS.

Note: To add, view, test, and manage connections to RADIUS servers, you need the security role.

Understanding the RADIUS server list

The RADIUS page lists the currently configured RADIUS servers. For each server, the page shows:

- The relative order in which HCP contacts the server.
- The hostname of the RADIUS server or the IPv4 or IPv6 address that HCP uses to communicate with the RADIUS server.
- The number of the UDP port on which the RADIUS server listens for authentication requests from HCP.
- The protocol the RADIUS server uses to authenticate users.

HCP does not limit the number of servers you can add to this list.

Adding a RADIUS server

To add a RADIUS server for remote authentication:

1. On the RADIUS page in the System Management Console, click Add RADIUS Server.
2. In the Add RADIUS Server panel:
   - In the RADIUS Host field, type the host name of the RADIUS server or the IP address that HCP uses to communicate with the RADIUS server.

     If you specify the RADIUS server host name, then at least one IPv4 or IPv6 address assigned to the RADIUS server must be routable from the [hcp_system] network.

     If you specify an IPv4 or IPv6 address assigned to the RADIUS server, then that IP address must be routable from the [hcp_system] network.

     Optionally, if a RADIUS server has multiple IP addresses that are routable from the [hcp_system] network, you can configure multiple RADIUS server list entries for that server — one list entry for each routable IP address.
   - In the Port field, type the number of the UDP port on which the RADIUS server listens for authentication requests from HCP. Typically, this is port number 1812.
   - In the Shared Secret field, type the text string that serves as a password for communications between HCP and the RADIUS server. The text string can contain any characters, including white space, and can be any length.
   - In the Retries field, type the number of times HCP should try again to contact the RADIUS server before giving up. Valid values are integers greater than or equal to zero.
   - In the Timeout field, type the number of seconds HCP should wait for a response from the RADIUS server before retrying the request. Valid values are integers greater than or equal to zero. A value of 0 tells HCP to wait indefinitely.
   - For Protocol, select the protocol the RADIUS server uses to authenticate users.
3. Click Add RADIUS Server.

Tip: After adding a RADIUS server, test the connection to it.

Testing the connection to a RADIUS server

You test the connection to a RADIUS server by sending the server a username and password it knows about. HCP indicates that the test was successful if all of these conditions apply:

- The connection information is correct.
- The RADIUS server is running.
- The specified user name and password are known to the RADIUS server.

If any of these conditions don't apply, HCP indicates that the test failed.

Note: A successful test does not log the user in.

Testing the connection to a RADIUS server

To add, view, test, and manage connections to RADIUS servers, you need the security role.

You can test the connection to a RADIUS server.

1. On the RADIUS page in the System Management Console, click the test control (☑) for the server you want to test.
2. In the Test RADIUS Server window, in the Username field, type the user name to use for the test.
3. In the Password field, type the password that goes with the specified user name.
4. Click Test RADIUS Server.
   If the test is successful, the panel displays this message:

```
Connected to RADIUS server and user was authenticated successfully.
```

5. When you're done testing the connection, click Cancel.

Modifying a RADIUS server

To add, view, test, and manage connections to RADIUS servers, you need the security role.

1. On the RADIUS page in the System Management Console, click the edit control ( ) for the server you want to modify.
2. In the Edit RADIUS Server window, make the changes you want.
   If you leave the Shared Secret field empty, the previously set shared secret remains in effect.
3. Click Update RADIUS Server.
4. Click Close.

Reordering RADIUS servers

When checking a login with remote authentication, HCP contacts the RADIUS servers in the order in which they're listed on the RADIUS page until one authenticates the user. If none of the servers authenticates the user, the user cannot log in.

You can change the order in which HCP contacts multiple RADIUS servers. If you configured separate RADIUS server list entries for multiple IP addresses assigned to the same server, you can change the order in which HCP uses those IP addresses to connect to the RADIUS server. You can use the RADIUS page in the System Management Console to:

- Move a RADIUS server host name or IP address up in the list, click the move up control ( ) for that entry in the RADIUS server list.
- Move a RADIUS server host name or IP address down in the list, click the move down control ( ) for that entry in the RADIUS server list.

Deleting a RADIUS server

To add, view, test, and manage connections to RADIUS servers, you need the security role.

1. On the RADIUS page in the System Management Console, click the delete control ( ) for the RADIUS server IP address or host name you want to delete.
2. In response to the confirm message, click Delete.

Configuring a key management server

Key management server

A key management server (KM server) is used to administer the full life cycle of HCP cryptographic keys. The KM server controls the generation, usage, storage, archival, and deletion of encryption keys. HCP authenticates with your KM server by using certificates that you install or generate to create a connection with KM server.

HCP supports using one or more KM servers to manage encryption keys. Best practices recommend that you use multiple KM servers for key management because it allows the servers to work together to provide failover and increased availability.

Observe the following guidelines when using KM servers:

- Make sure each namespace that uses encryption has access to the network where you configured the KM server.
- Make sure your network firewall settings allow the clusters to communicate through the port used for KMIP communications. The default is port number is 5696.
- You can host up to 8 KM servers on an HCP system.
- HCP system supports 8 active KM servers at any given time.

The security of encrypted data on an HCP system depends on keeping encryption keys secure. Encryption keys are encrypted using a Key Encryption Key (KEK). HCP delegates the storage and protection of KEKs to an external key manager.

Authenticating HCP and KM server using SSL

Mutual authentication allows HCP and KM server to authenticate each other prior to establishing a secure SSL or TLS connection. The connection begins with an SSL/TLS handshake between HCP and KM server to establish the connection details.

- The handshake starts when the KM server connects to HCP and requests a secure connection.
- KM server sends HCP a server certificate and then HCP uses the root certificate to authenticate the identity the certificate claims to represent.
- HCP sends KM server a client certificate and then the KM server uses the information on the server to authenticate the identity the certificate claims to represent.

You can use any of the following options to establish trust between HCP and the KM server:

- **Client certificate from KM server**: You can create a new certificate on the KM server. You can also register new client using a certificate signed by an external CA. For detailed instructions, see your KM server product documentation.
- **A certificate returned for an HCP-generated CSR**: For more information, see Creating a CSR
- **Domain certificate**: If you have an existing domain certificate, you can use it to register your HCP client.

CAUTION:
The client certificate on the KM server must remain current and not expired. If the client certificate expires or is not current, the HCP system will not be able to access the KM server.
Attention: To view or create certificates, you need the security role. Depending on the type of KM server (vendor, software version), you might need to perform additional configuration tasks. For more information about preparing the necessary services to accept connections from the storage system, see the documentation for your key management server.

Certificate types

Certificates are commonly used for both encryption and identification of the parties. The HCP system and KM server uses certificates for authentication. The exchange of certificates verifies access to the encryption keys that are stored on the KM server. The authentication of the HCP system ensures that the KM server provides access to keys only to a trusted source. The authentication of the KM server ensures that the HCP system can trust the server to access and store keys.

- **Root certificate** is a self-signed certificate defined by IETF RFC 5280 and issued by a root CA. The SSL ecosystem is based on a trust relationship called the *chain of trust*. When HCP validates a certificate, it compares the certificate issuer with the list of trusted CAs.
- **Client certificate** is a digital certificate used by client systems to prove their identity and make authenticated requests to a remote server. The KM server can validate the digital signature by using the client's public key (in the client certificate).

Creating a CSR

You can create a CSR for key management.

To view existing certificates, you need an administrator role. To create and delete certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Key Management.
   The Servers page opens.
3. On the left side of the Key Management page, click the CSRs tab.
4. Select Generate CSR.
   The Generate CSR section opens.
5. Fill in the field values that needs to generate a certificate.

   Common Name (CN) field
   : Required. Type the common name for the certificate. This value can range from 1-255 characters long and can contain any Latin-1 characters, including white space.

   Organizational Unit (OU) field
   : Type the name of the organizational unit that will use the certificate, for example, the name of a division or the name under which your company does business. This field accepts only alphanumeric characters. Do not include a comma (,), plus (+), or equals (=) sign.

   Organization (O) field
   : Type the full legal name of your company. This field accepts only alphanumeric characters. Do not include a comma (,), plus (+), or equals (=) sign.

   Location (L) field
   : Type the name of the city where your company headquarters are located.

   State/Province (ST) field
   : Type the full name of the state or province where your company headquarters are located.

   Country (C) field
   : Type the name of the country where your company is located.

6. Select Generate CSR.

Deleting a CSR

You can delete a CSR by using the HCP System Management Console.

To view, create and delete certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Key Management.
   The Servers page opens.
3. On the left side of the Key Management page, click the CSRs tab.
   The CSRs page opens.
4. In the list of CSRs, click the delete control ( ).

Downloading a CSR

You can download a CSR by using the HCP System Management Console.

To view, create and delete certificates, you need the administrator role.

1. Open the HCP System Management Console.
2. From the top-level menu, select Security > Key Management.
   The Servers page opens.
3. On the left side of the Key Management page, click the CSRs tab.
   The CSRs page opens.
4. In the list of CSRs, click the download control for it ( ).

Key management

Encryption

Storing and encrypting data with HCP requires using a central cryptographic key management service with multiple layers of keys for the encrypted data. An example of multiple layer of keys is envelope encryption, which is the process of encrypting a key with another key.

- **Data encryption keys**: The key used to encrypt data itself is called a data encryption key (DEK)

  HCP observes the following best practices for managing DEKs:

  - Generate DEKs locally.
  - When stored, make sure DEKs are encrypted at rest.
  - Generate a new DEK every time you write the data. This means you don't need to rotate the DEKs.
  - Do not use the same DEK to encrypt data from two different objects.
- **Key encryption keys**: The DEK is encrypted (or "wrapped") by a key encryption key (KEK). The process of encrypting a key with another key is referred to as envelope encryption.

  HCP observes the following best practices for managing KEKs:

  - Store KEKs centrally.
  - Set the granularity of the DEKs they encrypt based on their use case. For a workload that requires multiple DEKs to encrypt the workload's data chunks, for example, you can use a single KEK to wrap all DEKs that are responsible for that workload's encryption.
  - HCP rotates the keys automatically when the crypto period expires or when the maximum size of the data that you can encrypt with the encryption key is reached. However, if a key is compromised, you can force key rotation by using Replace All Keys option option on the KM Server management page on HCP.

Generating keys

HCP requests a KEK from the KM server during ingest. The KEKs are generated and maintained by the KM Server while HCP manages the life cycle. Each tenant that is part of a service plan that use the KM Server encryption, uses a unique KEK from the KM Server to encrypt all the unique DEKs associated with objects ingested to the tenant.

Rekeying, rotating and replacing keys

The crypto period and the amount of data that a key can protect are predetermined or system-defined. However, if a key is compromised, you can use Replace Keys option on the HCP to rotate all the encryption keys on the KM server.

Rekeying is one of the methods to preserve account permanence. HCP automatically rekeys the cryptographic keys before the crypto period expires. For example, if the system defined crypto period is 18 months and a key is no longer used for ingesting in the first 6 months, HCP generates a new key. After next 12 months, all the objects using this key are rekeyed with the currently active key. Rekeying requires an active key.

Key rotation happens automatically if one or more of the following conditions are true:

- The crypto period expires (for example, after a system-defined period of time has passed).
- Reached the maximum size of the data that you can encrypt with the encryption key (for example, a predetermined amount of data has been encrypted by a given key).

Important:

Compression/Encryption service handles key encryption life cycle. Disabling this service on HCP system will impact essential KM server functionalities or prevent features such as key rotation, key replacement from functioning correctly. Therefore the Compression/Encryption service should not be disabled.

Note: If you select Replace Keys, the Compression/Encryption service automatically re-encrypt DEK with a new KEK.

Destroying keys

If sensitive data is compromised in its encrypted state, you can change the key state to **compromised** on the KM server. Alternatively, you can choose Replace Keys on the KM server to replace the keys. When the objects requiring keys are re-keyed, HCP destroys the keys automatically.

Compromised or deactivated key alerts

HCP detects and deactivates keys on the KM Server when a key is either compromised or when its crypto period expires. When a key is either deactivated or compromised, the System Management Console displays an alert until the key is replaced. The Compression/Encryption service replaces the deactivated or compromised key and clears the alerts on the System Management Console. HCP automatically replaces the keys before the crypto period expires. To manually deactivate all the keys, use the Replace Keys option on the KM Server management page on HCP.

Note: If there is a performance problem with the Compression/Encryption service, HCP will be slow to replace keys. However, to temporarily improve the performance, you may clear all the three rewrite options on the Compression/Encryption Settings page.

Prioritizing and scheduling Compression/Encryption services

The priority of the Compression/Encryption service is set to low by default. However, the system administrator or the security administrator can increase the priority. Increasing the priority of the Compression/Encryption service improves the time taken to address the service requirements of the objects. A Compression/Encryption service runs as scheduled in the calendar. By default, the service runs only on Saturdays and Sundays. You can increase or decrease the frequency of running the Compression/Encryption service by creating a new schedule.

The system administrator or the security administrator can manually initiate the Compression/Encryption service from the Overview tab of the System Management Console. When a service is initiated from the System Management Console, that service will run at high priority.
Important: Manually initiating a service may stop other services and may degrade overall system performance.

Adding a key management server

- Obtain the root certificate of your KM server.
- Obtain the client certificate for your KM server using one of the following options:
  - Generate client certificate from your KM server.
  - Use the certificate returned for an HCP-generated CSR.
  - Use HCP's domain certificate.

1. In the top-level menu of the HCP System Management Console, select Security > Key Management.
2. On the left side of the Key Management page, click the Servers tab.
3. On the key management page in the System Management Console, click Add KM Server.
   An Add KM Server wizard opens.
4. In the Name page:
   a. In the Name field, type the name of the KM server.
   b. In the Description field, type the description for the KM server. Then click Next.
5. In the Configuration page:
   a. In the Hostname field, type the hostname.
   b. In the Port field, type the port number.
   c. In the Client Certificate section, click Browse and then select the client certificate.
   d. (Optional) Enter the password.
   e. In the Root Certificate section, click Browse and then select the root certificate.. Then click Next.
   f. Select a server from the Secondary KM Server dropdown menu.
   Note: If you are confguring a KM server first time, you will not see this option.
6. Review the information in the review page and then click Finish.

Modifying key manager settings

1. In the top-level menu of the HCP System Management Console, select Security > Key Management.
2. On the left side of the Key Management page, click the Servers tab.
3. In the key management servers list, double-click the name of the KM Server you want to modify.
4. In the Configuration page:
   a. In the Name field, type the name of the KM Server.
   b. In the Description field, type the description for the KM Server.
5. In the Certificates page:
   a. In the Client Certificates section, click Upload Certificate to upload a new client certificate.
   b. In the Root Certificates section, click Choose File to select a root certificate file, and then Upload Root Certificate to upload a new root certificate.
6. In the Retirement page:
   a. The Service Plans section lists the names of the available service plans and the names of tenants.

b. In the Optionally select a replacement server section, select a server from the Replacement server dropdown menu and then click Retire Server.
When you retire a KM Server, HCP removes it from all the service plans that it is using and then replaces it with the specified secondary KM Server. If you did not select a secondary KM Server, it will use local key management.

7. In the Manage page, in the Keys in use section, click Replace Keys.
Note: When you choose to replace the keys, the Compression/Encryption service automatically re-encrypts the DEK with a new KEK.

Viewing a key management server

The Servers tab in the Key Management page lists all the registered KM Servers.

1. In the top-level menu of the HCP System Management Console, select Security > Key Management.
2. On the left side of the Key Management page, click the Servers tab.
You see all the registered KM servers in the table. The page contains the following information about the KM server.
   - Name: Name of the KM server.
   - Hostname: The name of the KM server.
   - Secondary Server: The name or IP address of the secondary KM server.
   - Keys: Indicates whether any keys from the KM server are used to encrypt HCP objects.
   - Objects: Number of objects encrypted using the KM server.
   - Service Plans: Service plans associated with the KM server.

Deleting a key management server

1. In the top-level menu of the HCP System Management Console, select Security > Key Management.
2. On the left side of the Key Management page, click the Servers tab.
3. In the list of key management servers on the Servers page, click to select the KM server you want to delete and then click the delete control ( ).
The delete icon is enabled only if the KM Server is no longer associated with any keys and service plans. However, to delete a KM Server, the key count, object count, and service plan count must be zero.
CAUTION:
Delete operation is destructive and can't be undone. The KM Server will be permanently deleted.
4. In response to the confirming message, click Delete.

Encrypting storage pools

The Encryption License Key feature protects your sensitive data against breaches. Only authorized individuals with an encryption key will be able to decode the information. Encryption License Key includes an integrated key management functionality that can leverage third-party key management solutions.

1. In the top-level menu of the HCP System Management Console, select Security > Encryption.
2. On the Encryption page, select the Encrypt Storage Pools.
Note: This option encrypts all the HCP S Series Nodes and cloud pools in the HCP system.
3. Click Update Settings.
Note: You cannot unencrypt storage pools.

Setting the systemwide permission mask

A *data access permission mask* determines which of these operations are allowed in a namespace: read, write, delete, purge (delete all versions of an object), privileged delete (delete an object that's under retention), and search. Data access permission masks are set at the system, tenant, and namespace levels:

- The system-level mask applies across all namespaces (that is, systemwide).
- The tenant-level mask is set individually for each tenant. This mask applies only to the namespaces owned by that tenant.
- The namespace-level mask is set individually for each namespace and applies only to that namespace.

The effective permissions for a tenant are the operations allowed by both the system-level and tenant-level permission masks. That is, to be in effect for a tenant, a permission must be included in the system-level permission mask and in the tenant-level permission mask.

The effective permissions for a namespace are the operations that are allowed by the masks at all three levels. That is, to be in effect for a namespace, a permission must be included in the system-level permission mask, the tenant-level permission mask, and the namespace-level permission mask.

The following table shows an example of the effective permissions for a namespace given a set of data access permission masks.

Permission Mask	Permissions					
	Read	Write	Delete	Purge	Priv. delete	Search
Systemwide permission mask	✓	✓	✓	✓		✓
Tenant permission mask	✓	✓	✓	✓	✓	
Namespace permission mask	✓	✓	✓		✓	✓
Effective permission mask	✓	✓	✓			

What an individual user can do in a namespace is also limited by the permissions the user has from the applicable user or group accounts and, for HCP namespaces, the minimum data access permissions for the namespace.

The Permissions page in the HCP System Management Console lets you set the systemwide permission mask. You can change this mask at any time.

Tip: Before changing the systemwide permission mask, you should notify your tenant contacts.

To display the Permissions page, in the top-level menu of the System Management Console, select Security > Permissions.

To view the Permissions page, you need the monitor or administrator role. To set the systemwide permission mask, you need the administrator role.

Setting the systemwide permission mask for an HCP system

To view the Permissions page, you need the monitor or administrator role. To set the systemwide permission mask, you need the administrator role.

1. On the Permissions page, select the permissions you want to include in the systemwide permission mask:

Read

Lets users:

- Read and retrieve objects, including object metadata (system metadata, custom metadata, and ACLs)
- List directory contents
- View namespace information

Write

Lets users:

- Add objects to a namespace.
- Modify system metadata. For the default namespace, this includes holding and releasing objects. For HCP namespaces, these operations also require privileged permission.
- Add or replace custom metadata.
- Add or replace ACLs.
- Change object owners.
- View namespace information

Delete

Lets users:

- Delete objects, custom metadata, and ACLs from a namespace
- View namespace information

Purge

Lets users:

- Delete all versions of an object with a single operation. For users to perform purge operations, delete operations must also be allowed.
- View namespace information.

Selecting Purge automatically selects Delete.

Privileged

Lets users:

- Delete or purge objects that are under retention. For users to perform privileged delete operations, delete operations must also be allowed. For users to perform privileged purge operations, delete and purge operations must also be allowed.
- Hold and release objects in HCP namespaces. For users to perform hold and release operations in these namespaces, write operations must also be allowed.
- View namespace information.

Search

Lets users use the HCP metadata query API and the HCP System Management Console to query or search namespaces. For users to query or search a namespace, read operations must also be allowed.

Selecting Search automatically selects Read.

2. Click Update Settings.

System monitoring

HCP maintains a system log in which it records messages about events that happen within the system. You can view this log in the HCP System Management Console. You also have the option of sending system log messages to syslog servers, SNMP managers, and/or email addresses. Additionally, you can use SNMP to view and, when allowed, change HCP system settings.

The System Management Console lets you monitor CPU, memory, logical-volume, and network usage. You can use the information presented to analyze trends in the use of these resources and to decide when you need to take action to ensure that HCP uses its resources effectively.

To track system capacity and bandwidth usage at the tenant and namespace levels, you can generate chargeback reports. These reports can be used as input to billing applications.

You can configure HCP to push information to Hitachi Device Manager (HDvM) so you can monitor and manage HCP along with your other Hitachi storage systems from a single console.

The following sections:

- Describe the information available in the system log and explains how to view the log
- Explain how to send log messages to specified syslog servers, SNMP managers, and email addresses
- Explain how to configure SNMP for viewing and changing system settings
- Describe the information available about system resource usage
- Explain how to generate chargeback reports
- Explain how to configure the HDvM connection (HCP with SAN-attached storage systems only)

Understanding the HCP system log

While the Overview page in the System Management Console gives you a view of the system as a whole, the HCP system log lets you monitor system activity on a more detailed level. The log records system events such as:

- Nodes and services starting
- Changes to the system configuration
- Logical volume failures
- User logins to the HCP System Management Console

Each recorded entry about an event is called a *message*. The system log contains all the messages written to it since the HCP system was installed.

The System Management Console provides several views of the log:

- The All Events panel on the System Events page displays all the messages in the system log that your roles allow you to see.
- The Security panel on the System Events page displays only messages about attempts to log into the System Management Console with an invalid user name. Only users with the security role can see this panel.
- The Logs section on the Resources page displays all the messages in the system log that your roles allow you to see.
- The Major Events section on the Overview page displays only messages about major events (for example, the addition or failure of a node).
- The Events section on the Storage Node page displays only messages about events that relate to a particular node.
- The Service Events section on the Schedule page displays only messages related to HCP services that can be scheduled to run at specific times.

Viewing the complete event log

The All Events panel on the System Events page lists all event messages logged since the HCP system was installed. By default, the panel displays 20 messages at a time in reverse chronological order.

To view the All Events panel, you need the monitor, administrator, security, service, or compliance role. However, only users with the security role can see messages about attempts to log into the System Management Console with an invalid user name.

You can display the All Events panel.

Tip: Use the Search filter to monitor system events based on a user-specified date range, event ID, or node. For more information, see Managing the message list.

1. In the top-level menu of the System Management Console, select Monitoring > System Events.
2. On the left side of the System Events page, click All Events.

Viewing the system security log

The Security Events panel on the System Events page lists all messages about attempts to log into the System Management Console with an invalid username that have occurred since the HCP system was installed. By default, the panel displays 20 messages at a time in reverse chronological order.

Note: To view the Security Events panel, you need the security role.

To view the All Events panel, you need the monitor, administrator, security, service, or compliance role. However, only users with the security role can see messages about attempts to log into the System Management Console with an invalid user name.

You can display the All Events panel.

Tip: Use the Search filter to monitor security events based on a user-specified date range, event ID, or node. For more information, see Managing the message list.

1. In the top-level menu of the System Management Console, select Monitoring > System Events.
2. On the left side of the System Events page, click Security Events.

Understanding log messages

Each message displayed in the All Events and Security Events panel includes this information about an event:

- The user name of the event initiator:
  - For user-initiated events, this is the user name currently associated with the user account used by the user who initiated the event. These considerations apply:
    - For an HCP user account, if the account has been deleted, the user name is followed by the letter D in parentheses.
    - For an AD user account, if the account has been deleted or if HCP currently cannot contact AD, the user name for the message is blank.
  - For system-initiated events, the user name is [internal].
  - For events initiated through SNMP, the user name is [snmp].
  - For events initiated by HCP service or support personnel by means other than the System Management Console or SNMP, the user name is [service].
- The severity of the event. Possible values are:

  Notice
  : The event is normal and requires no special action. Events of this severity are informational only. Examples are:
    - Node started
    - Protection service finished: run complete
    - Syslog settings changed

  Warning
  : The event is out of the ordinary and may require manual intervention. Examples are:
    - Storage capacity warning
    - Protection service beginning repairs
    - Remote authentication server error

  Error
  : The event is serious and most likely requires manual intervention. Examples are:
    - Storage capacity critical
    - Volume failure
    - Network interface down
- The date and time at which the event occurred, shown for the time zone in which the HCP system is located.
- A short description of the event.

To view more details about an event, click anywhere in the row containing the event message. To hide the details, click again in the row.

The details displayed for an event are:

- The user ID of the event initiator
- For user-initiated events, the port through which HCP received the event request
- For user-initiated events, the IP address from which the event request was sent
- The message ID

- The number of the node on which the event occurred
- If the event applies to a specific logical volume, the volume ID
- The full text of the event message

Managing the message list

You can manage the message list using the All Events panel and the Search option.

Using the All Events Panel

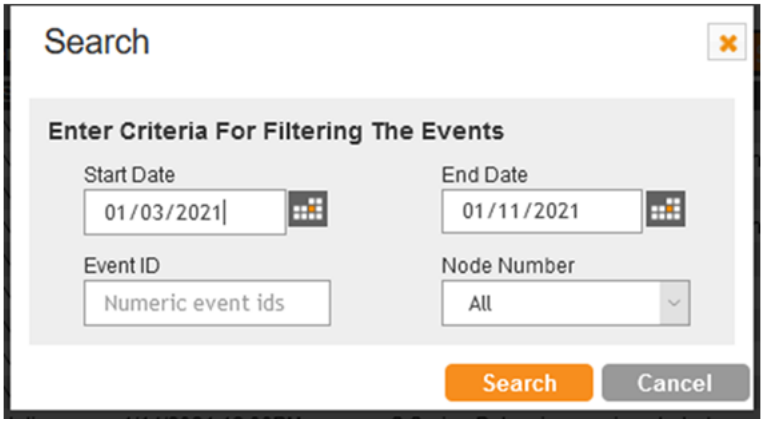
To view the All Events panel, you need the monitor, administrator, security, service, or compliance role. However, only users with the security role can see messages about attempts to log into the System Management Console with an invalid user name.

You can display the All Events panel.

1. To display details for all the listed events, click expand all. To hide all details, click collapse all.
2. To view a different number of messages per page, select the number you want in the Items field.
3. To page forward or backward through the messages, click the next (▶) or back (◀) control, respectively.

Using the Search Option

Another way to manage the message list is by using the Search option on the System Events and Tenant Events pages. This option allows you to view event log, security log, and compliance event records based on a user-specified date range, event ID, or node. When you click this option, the Search box appears.



For Node Number, you can specify one node or All. For Event ID, enter a single event ID or multiple IDs separated by a comma (for example, `3005,2606`). When finished, click Search. You can clear searched events when they are no longer needed.

Configuring syslog logging

You can have HCP send system log messages to one or more syslog servers. You can also have HCP send access log messages about HTTP data access events or log messages about management API access requests to the syslog servers. When you send log messages to syslog servers, you can use tools in your syslog environment to perform functions such as sorting the messages, querying for certain events, or forwarding error messages to a mobile device.

Tenant-level administrators can choose to include tenant log messages along with the system log messages sent to the syslog servers.

If you identify any syslog servers to HCP, HCP also sends the results of diagnostic commands to those servers.

System log messages sent to syslog servers

For each system log message about an event, HCP sends this information to the specified syslog servers:

- A unique identifier for the system log entry.
- A message segment number, if applicable. Messages that exceed 1,024 characters are split into two or more messages, all of which have the same log entry identifier. These message segments are numbered sequentially, starting with 0 (zero) for the first segment.

  HCP sends at most 100 segments for a log message, for a total of 102,400 characters. Any text beyond that is not sent.

- The message ID.
- The date and time the event occurred.
- The severity of the event.
- The front-end network IP addresses and node number assigned to the node on which the event occurred.
- If the event applies to a specific logical volume, the volume identifier.
- The user name and ID of the event initiator.
- The full message text.

You can choose the severity level of the log messages to be sent. You can also choose whether or not to send messages about security events (that is, attempts to log into the System Management Console with an invalid user name) and compliance events. Compliance events happen at the namespace level, so these messages are sent to the syslog servers only if syslog logging is enabled at the tenant level.

Note: System log messages are not guaranteed to arrive at the syslog servers to which they're sent. This is because the syslog protocol uses UDP for data transmission.

Enabling syslog logging

For HCP to send log messages through syslog, you need to specify the IP addresses of one or more syslog servers. Each syslog server IP address that you specify must be routable from the [hcp_system] network. For this reason, if you specify an IPv6 unique local address (ULA) for a syslog server, then the [hcp_system] network must be configured

with an IPv6 ULA that can be used to connect to that syslog server. When you specify multiple servers, HCP sends log messages to all of the specified servers.

You also need to select the syslog local facility to which to direct the log messages. This selection applies to all the syslog servers that you specify.

You use the Syslog page in the HCP System Management Console to set up logging through syslog. You also use this page to test the connections to the syslog servers you specify.

To display the Syslog page, in the top-level menu of the System Management Console, select Monitoring > Syslog.

To view the Syslog page, you need the monitor, administrator, security, or compliance role. To configure syslog logging and test the connections to syslog servers, you need the administrator or security role.

To configure HCP to send log messages to syslog servers, on the Syslog page:

- Specify syslog settings:
  - Select Enable syslog
  - To include log messages about compliance events, select Send compliance events.
  - To include log messages about security events, select Send security events.
  - In the Send log messages at this level or higher field, select the severity level of messages to be sent to the specified syslog servers:

    OFF
    : tells HCP not to send any log messages.

    NOTICE
    : sends messages with a severity level of Notice, Warning, or Error.

    WARNING
    : sends messages with a severity level of Warning or Error.

    ERROR
    : sends only messages with a severity level of Error.

  - In the HTTP access Facility field, select the syslog local facility to which to direct log messages. The options are local0 through local7.
  - To include log messages about HTTP-based data access events, select Send log messages for HTTP-based data access requests. When you enable this option, HCP sends information to the syslog regarding data access requests that use the HTTP namespace access protocol.
  - In the MAPI access Facility field, select the syslog local facility to which to direct log messages. The options are local0 through local7.
  - To include log messages about management API request events, select Send log messages for management API requests. When you enable this option, HCP sends information to the syslog regarding request events that use the HCP management API.

    Then click Update Settings.

    Tip: Before you submit your changes, you can test the connections to the specified syslog servers.
- Specify one or more syslog server IP addresses. For each syslog server that you want to use with HCP, specify the IPv4 or IPv6 address that you want HCP to use to connect to that server.

  You specify each syslog server IP address as a separate entry in the syslog server list.

Adding an IP address to the syslog server list

You can add an IP address to the syslog server list.

To view the Syslog page, you need the monitor, administrator, security, or compliance role. To configure syslog logging and test the connections to syslog servers, you need the administrator or security role.

1. In the Syslog Server IP Addresses field, type the IP address, optionally followed by a colon and a port number.

   If you omit the port number, HCP uses port number 514.

   Each entry in this list must be a single IP address. IP address ranges and comma-separated lists are not valid.

2. Click Add.
   The specified IP address moves into the list below the field.

To remove an IP address from the syslog server list, click the delete control ( ) for that IP address. To remove all the IP addresses from the list, click Delete All.

Testing syslog connections

At any time, you can test the connections to the syslog servers whose IP addresses appear on the Syslog page. Testing the connections causes HCP to send a message to the target IP addresses. To verify that the connections are working, you need to use your syslog tools to check that the message arrived.

The message HCP sends to the syslog servers has a severity level of Notice. Therefore, for the message to be sent successfully, the severity level of messages to be sent must be set to NOTICE.

To view the Syslog page, you need the monitor, administrator, security, or compliance role. To configure syslog logging and test the connections to syslog servers, you need the administrator or security role.

1. On the Syslog page, click Test.
   HCP sends this message to the syslog servers:

   ```
   User username sent system log test message.
   ```

2. Check each syslog server to ensure that the message arrived.

If a syslog server doesn't receive the message:

- Check that you've correctly specified the target IP address.
- Check that you can successfully ping the target IP address.
- If you're unable to determine the cause of the problem, contact your authorized HCP service provider for help.

HCP system log messages

HCP maintains a log that records messages about system events. The following table lists each possible event, provides an explanation of the event and a recommended action plan, and categorizes the event severity. The events are listed in ascending order by ID.

ID	Event	Explanation	Action	Severity
1000	HCP started	The HCP system started.	No action is required.	Notice
1001	HCP shutting down	The HCP system is shutting down.	If any nodes do not power off automatically, wait a few minutes and then power them off manually.	Notice
1002	Node started	A node started.	No action is required.	Notice
1003	Node shut down	A node shut down.	If this event is unexpected and the node does not restart automatically, contact your authorized service provider. Do not try to restart the node manually, as that may cause the loss of information needed to diagnose the problem.	Notice
1004	Volume started	A logical volume came online.	No action is required.	Notice
1005	Volume shut down	A logical volume went offline.	Contact your authorized service provider.	Notice
1006	Volume failure	A logical volume failed.	Contact your authorized service provider.	Error
1007	Node removed	A node has been permanently removed from the HCP system.	No action is required.	Notice
1008	Time sync problem	The internal clock on a node is out of sync with the clocks on the nodes in the rest of the HCP system.	If the problem persists, contact your authorized service provider.	Error
1009	Node added	A new node has been added to the HCP system.	No action is required.	Notice
1010	Previously removed node re-added	A node that was removed from the system has been powered on again.	Remove the node again.	Error
1012	Metadata DPL is 1	The system was configured with metadata DPL 1.	No action is required.	Warning
1013	Failover	A node in a cross-mapped pair failed. The other node has taken over management of the logical volumes previously managed by the failed node.	If the failed node does not restart automatically, contact your authorized service provider. Do not try to restart the node manually, as that may cause the loss of information needed to diagnose the problem.	Error
1014	HCP rebooting	The HCP system is restarting.	No action is required.	Notice
1015	Failover	A node in a cross-mapped pair failed. The other node will take over management of the logical volumes previously managed by the failed node.	If the failed node does not restart automatically, contact your authorized service provider. Do not try to restart the node manually, as that may cause the loss of information needed to diagnose the problem.	Error
1016	Volume recovered	A logical volume recovered.	No action is required.	Notice
1017	Node down for an extended amount of time	A node has been unavailable for an extended amount of time.	Contact your authorized service provider.	Error
1018	HCP is read-only	The HCP system has become read-only due to metadata unavailability. Configuration changes and changes to namespace content are not allowed. Services have been suspended.	Contact your authorized service provider.	Error
1019	HCP is no longer read-only	The previously unavailable metadata has become available, so the HCP system is no longer read-only due to metadata unavailability.	No action is required.	Notice
1020	Region-count setting is invalid	The region count was changed to a value that is either too large, too small, or not a number. The actual number of regions has not changed.	Contact your authorized service provider.	Error
1021	Region count is changing	The region count was set to a new value.	No action is required.	Notice
1022	Region count has changed	The region count has finished changing to a new value.	No action is required.	Notice
1023	Region-count change has been canceled	The region-count change was canceled.	No action is required.	Notice
1024	Support for DPL 1 changed	Support for DPL 1 was either enabled or disabled.	No action is required.	Warning
1025	External storage volume added	A user added an external storage volume.	No action is required.	Notice
1026	External storage volume updated	A user updated an external storage volume.	No action is required.	Notice
1027	External storage volume deleted	A user deleted an external storage volume.	No action is required.	Notice
1028	External storage volume missing necessary permissions	The share for a new or updated external storage volume was exported without permissions that HCP needs in order to mount the volume.	Ensure that the share is exported with the necessary permissions.	Warning
1029	Cannot mount external storage volume	HCP was unable to mount a new or updated external storage volume.	Ensure that the share is exported with the correct configuration on the external device. For more	Warning

ID	Event	Explanation	Action	Severity
			information about this event, see the mount command output displayed with the log message.	
1030	Cannot mount external storage volume	HCP was unable to mount a new or updated external storage volume.	Ensure that the share is exported with the correct configuration on the external device.	Warning
1031	External volume started	An external storage volume became available.	No action is required.	Notice
1032	External volume unavailable	An external storage volume is unavailable.	Ensure that the share is exported with the correct configuration on the external device and that the HCP node managing the volume is available.	Notice
1033	External volume failure	HCP was unable to connect to an external storage volume.	Ensure that the share is exported with the correct configuration on the external device and that all HCP nodes are allowed to mount the share.	Error
1034	External volume remounted	a user remounted an external volume.	No action is required.	Notice
1035	External storage volume missing necessary file naming support	The share for a new or updated external storage volume was exported without file naming support that HCP needs in order to mount the volume.	Ensure that the share is exported with the necessary file naming support.	Warning
1036	Node rebooting	A node is restarting.	No action is required.	Notice
1050	Storage pool created	A user created a storage pool.	No action is required.	Notice
1051	Storage pool updated	A user updated a storage pool.	No action is required.	Notice
1052	Storage pool deleted	A user deleted a storage pool.	No action is required.	Notice
1053	Storage component created	A user created a storage component.	No action is required.	Notice
1054	Storage component updated	A user updated a storage component.	No action is required.	Notice
1055	Storage component deleted	A user deleted a storage component.	No action is required.	Notice
1056	Storage component abandoned	A user abandoned a storage component.	No action is required.	Notice
1057	SSL certificate downloaded	A user downloaded an SSL server certificate for storage tiering.	No action is required.	Notice
1058	New SSL certificate added	A user added a new storage tiering client certificate.	No action is required.	Notice
1059	SSL certificate deleted	A user deleted a storage tiering client certificate.	No action is required.	Notice
1060	New storage license added	A user added a new storage license.	No action required.	Notice
1061	Storage license expired	A storage license expired.	Upload a new storage license.	Warning
1062	Storage license exceeded	Storage usage exceed licensed capacity.	Delete or relocate objects within the repository or add more licensed capacity.	Warning
1066	Storage license invalid	HCP serial number does not match storage license.	Upload a new storage license.	Warning
1067	Storage component status changed	Storage component status was changed.	No action is required.	Notice
1068	Storage component updated	A user updated a storage component.	No action is required.	Notice
1100	Storage capacity warning	The amount of free storage on the HCP storage nodes is low.	Consider adding storage capacity to the HCP system before the amount of free storage becomes critically low.	Warning
1101	Storage capacity critical	The amount of free storage on the HCP storage nodes may be insufficient to support the addition of new objects.	Increase the amount of free storage by adding more storage capacity or deleting objects from the repository.	Error
1104	Internal SLAB process down	The internal SLAB process is not running. The node will reboot automatically in order to restart the process.	No action is required. If this problem persists, contact your authorized service provider.	Error
1105	IPMI status became unavailable	A hardware condition has rendered IPMI status unavailable.	No action is required.	Warning
1106	Location metrics	Metrics have been logged according to schedule.	No action is required.	Notice
1107	Adding logical volumes	New logical volumes are being added to a node.	No action is required.	Notice
1108	Logical volumes added	New logical volumes were added to a node, thereby increasing the storage capacity of the node.	No action is required.	Notice
1109	Logical volumes added	New logical volumes were added to a node. These are standby volumes for zero-copy failover.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
1110	Failed to add logical volumes	The addition of new logical volumes to a node failed.	Contact your authorized service provider.	Error
1111	Front-end communication status became unavailable	A hardware condition has rendered front-end communication status unavailable.	No action is required.	Warning
1112	Storage status became unavailable	A hardware condition has rendered storage status unavailable.	No action is required.	Warning
1113	Spindown capacity warning	The amount of free spindown storage on the HCP storage nodes is low.	Consider adding spindown storage capacity to the HCP system before the amount of free spindown storage becomes critically low.	Warning
1114	Spindown capacity critical	The amount of free spindown storage on the HCP storage nodes may be insufficient to support the addition of new objects.	Increase the amount of free spindown storage by adding more storage capacity or deleting objects from the repository.	Error
1115	Moving database	The database is being moved to new logical volumes on a node.	No action is required.	Notice
1116	Database moved	The database has been moved to new logical volumes on a node.	No action is required.	Notice
1117	Failed to move database	The database move to new logical volumes on a node has failed.	Contact your authorized service provider.	Error
1118	Old database deleted	The old database has been deleted.	No action is required.	Notice
1119	Moving database	The database is being moved to the new dedicated logical volume on a node.	No action is required.	Notice
1120	Database moved	The database has been moved to the new dedicated logical volume on a node.	No action is required.	Notice
1200	Last update sent to Hitachi Device Manager was unsuccessful	HCP is unable to communicate with the HDvM server.	Ensure that you have correctly configured Hitachi Device Manager in the System Management Console and that the Hitachi Device Manager server is healthy.	Error
1201	Log handler test message	A user sent a test message to the syslog servers or SNMP managers.	No action is required.	Notice
1202	About to change syslog settings	A user changed the settings for syslog logging.	No action is required.	Notice
1203	Syslog settings changed	A user changed the settings for syslog logging.	No action is required.	Notice
1204	About to change SNMP settings	A user changed the settings for SNMP logging.	No action is required.	Notice
1205	SNMP settings changed	A user changed the settings for SNMP logging.	No action is required.	Notice
1206	Email notification failed	SMTP or email settings may be incorrect.	Check the SMTP and email settings. If the settings are correct, contact your SMTP administrator for help.	Warning
1220	Successfully downloaded logs	The HCP internal logs have been successfully downloaded.	No action is required.	Notice
1221	Started to download logs	A user has requested a download of the HCP internal logs.	No action is required.	Notice
1222	Failed to download logs	The requested download of the HCP internal logs has failed.	Try to download the logs again. If that fails, contact your authorized service provider.	Warning
1223	Started to download logs for node	HCP has started downloading the internal logs on a node.	No action is required.	Notice
1224	Successfully downloaded logs for node	HCP has finished downloading the internal logs on a node.	No action is required.	Notice
1225	Failed to download logs for node	HCP failed to download the internal logs from a node and is continuing with the next node.	No action is required.	Warning
1226	Logs marked	A user inserted a message into the HCP internal logs.	No action is required.	Notice
1227	Log encryption key uploaded	A user uploaded an encryption key for use when downloading the HCP internal logs.	No action is required.	Notice
1228	Log encryption key deleted	A user deleted an encryption key that was used when downloading the HCP internal logs.	No action is required.	Notice
1229	Log download preparation started	A user has requested a download of the HCP internal logs.	No action is required.	Notice
1230	Log download preparation complete	Log download preparation is complete, and the HCP internal logs are ready to be download.	No action is required.	Notice
1231	Log download started	The HCP internal logs have begun streaming to an HTTP client.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
1232	Log download complete	The HCP internal logs have been downloaded.	No action is required.	Notice
1233	Log download preparation complete with issues	Log download preparation finished with issues. The unaffected HCP internal logs are ready to be downloaded.	Download one or more of the available logs. Check the nodes identified in the error message.	Warning
1500	Successfully downloaded health check reports	The HCP health check reports have been successfully downloaded.	No action is required.	Notice
1501	Started to download health check reports	A user has requested a download of the HCP health check reports.	No action is required.	Notice
1502	Failed to download health check reports	The requested download of the HCP health check reports has failed.	Try to download the health check again. If that fails, contact your authorized service provider.	Warning
1503	Started to download health check for node	HCP has started downloading the internal health check on a node.	No action is required.	Notice
1504	Successfully downloaded health check for node	HCP has finished downloading the internal health check on a node.	No action is required.	Notice
1505	Failed to download health check for node	HCP failed to download the internal health check from a node and is continuing with the next node.	No action is required.	Warning
1506	Health check report download preparation started	The HCP system has started to prepare the HCP health check reports for downloading.	No action is required.	Notice
1507	Health check report download preparation complete	The HCP system has finished preparing the health check reports. The reports are now ready to be downloaded.	No action is required.	Notice
1508	Health check report streaming started	The HCP health check reports have begun streaming to an HTTP client.	No action is required.	Notice
1509	Health check report streaming complete	The HCP health check reports have been downloaded.	No action is required.	Notice
1510	Health check report download preparation complete with issues	Health check report download preparation finished with issues. The unaffected HCP health check reports are ready to be downloaded.	Download one or more of the available health check reports. Check the nodes identified in the error message.	Warning
1905	Service start skipped	A service was not started because the time remaining until a scheduled stop was less than the minimum runtime for the service.	No action is required.	Notice
1906	Scheduled service time period too short	A scheduled time period for a service is shorter than the minimum runtime for the service. The service will not run in that time period.	Increase the length of the applicable time period in the service schedule.	Warning
1980	Service schedule activated	A user activated a service schedule.	No action is required.	Notice
1981	Service schedule activation failed	A user tried to activate a service schedule, but the activation failed.	Check that the schedule has not been deleted. If the schedule has not been deleted, contact your authorized service provider.	Error
1982	Service schedule created	A user created a service schedule.	No action is required.	Notice
1983	Service schedule updated	A user updated a service schedule.	No action is required.	Notice
1984	Service schedule deleted	A user deleted a service schedule.	No action is required.	Notice
1900	Service worked on regions.	A service has finished processing some regions.	No action is required.	Notice
1901	Duplicate elimination service region information.	Duplicate elimination service has finished processing some regions.	No action is required.	Notice
2000	Protection service started	The Protection service has started.	No action is required.	Notice
2001	Protection service stopped: run complete	The Protection service finished successfully.	No action is required.	Notice
2002	Protection service stopped without finishing	The Protection service was interrupted without validating all objects or object parts.	No action is required.	Notice
2003	Protection service stopped without finishing	The Protection service was interrupted without validating all objects or object parts.	No action is required.	Warning
2004	Protection service changed protection sets	The Protection service changed protection sets.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2005	HCP found an unavailable object or object part	HCP could not repair an object or object part because the object or object part was unavailable.	Contact your HCP system administrator.	Warning
2006	HCP found an irreparable object or object part	HCP found a broken object or object part it could not repair.	Contact your HCP system administrator.	Error
2007	Protection service beginning repairs	Protection service is beginning object or object part repairs.	No action is required.	Warning
2008	Protection service: irreparable object or object part	The Protection service detected a violation it could not fix.	Contact your authorized service provider.	Error
2009	Protection service: unavailable object	The Protection service detected a violation it could not fix.	Contact your authorized service provider.	Warning
2010	Garbage Collection service started	The Garbage Collection service has started.	No action is required.	Notice
2011	Garbage Collection service finished: run complete	The Garbage Collection service finished successfully.	No action is required.	Notice
2012	Garbage Collection stopped without finishing	The Garbage Collection service stopped without completing its run. The service will resume automatically at a later time.	No action is required.	Notice
2013	Garbage Collection stopped without finishing	The Garbage Collection service stopped without completing its run. The service will resume automatically at a later time.	No action is required.	Warning
2017	Garbage Collection service beginning repairs	The Garbage Collection service has begun fixing violations.	No action is required.	Notice
2020	Scavenging service started	The Scavenging service has started.	No action is required.	Notice
2021	Scavenging service stopped: run complete	The Scavenging service finished successfully.	No action is required.	Notice
2022	Scavenging service stopped: run bypassed object(s) or object part(s)	The Scavenging service finished successfully. Some objects or object parts were not scavenged in this run.	No action is required.	Notice
2023	Scavenging service stopped without finishing	The Scavenging service stopped without completing its run. Scavenging will resume at a later time.	No action is required.	Warning
2024	Scavenging service stopped without finishing	The Scavenging service stopped without completing its run. The service will resume at a later time.	No action is required.	Notice
2027	Scavenging service beginning repairs	The Scavenging service has begun repairs.	No action is required.	Warning
2028	HCP found an irreparable object or object part	HCP was unable to repair the object. The repair may be retried at a later time.	Contact your HCP system administrator.	Error
2029	Scavenging service irreparable object	The Scavenging service was unable to repair the object. The repair may be retried at a later time.	Use the System Management Console to verify the health of the system. If the problem persists, contact your authorized service provider.	Error
2030	Capacity Balancing service started	The Capacity Balancing service has started.	No action is required.	Notice
2031	Capacity Balancing service stopped: run complete	The Capacity Balancing service finished successfully.	No action is required.	Notice
2032	Capacity Balancing service stopped: run bypassed object(s) or object part(s)	Some objects or object parts were bypassed during this run of the Capacity Balancing service. Those objects or object parts will be handled in a future run.	No action is required.	Notice
2033	Capacity Balancing service stopped without finishing	The Capacity Balancing service stopped without completing its run.	No action is required.	Warning
2034	Capacity Balancing service stopped without finishing	The Capacity Balancing service stopped without completing its run.	No action is required.	Notice
2037	Capacity Balancing service beginning repairs	Capacity Balancing service has begun repairs.	No action is required.	Warning

ID	Event	Explanation	Action	Severity
2040	Content Verification service started	The authentication service has started.	No action is required.	Notice
2041	Content Verification service stopped: run complete	The authentication service finished successfully.	No action is required.	Notice
2042	Content Verification service stopped without finishing	The Content Verification service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2043	Content Verification service stopped without finishing	The Content Verification service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2044	HCP found an unavailable object or object part	HCP could not repair an object or object part because the object or object part was unavailable.	Contact your HCP system administrator.	Warning
2045	Content Verification service: unavailable object	The Content Verification service detected a violation it could not fix.	Contact your authorized service provider.	Warning
2046	HCP found an irreparable object or object part	HCP found a broken object or object part it could not repair.	Contact your HCP system administrator.	Error
2047	Content Verification service beginning repairs	The Content Verification service has begun repairs.	No action is required.	Warning
2048	Content Verification service: irreparable object or object part	The Content Verification service detected a violation it could not fix.	Contact your authorized service provider.	Error
2049	Annotation no longer present	One or more objects no longer have a previously added annotation.	If annotations were not intentionally deleted, contact your authorized service provider.	Warning
2050	Duplicate Elimination service started	The Duplicate Elimination service has started.	No action is required.	Notice
2051	Duplicate Elimination service stopped: run complete	The Duplicate Elimination service finished successfully.	No action is required.	Notice
2052	Duplicate Elimination service stopped: run bypassed object(s) or object part(s)	The Duplicate Elimination service finished successfully. Some objects or object parts were not checked during this run. They will be checked in a future run.	No action is required.	Notice
2053	Duplicate Elimination service stopped without finishing	The Duplicate Elimination service stopped during its merge phase without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2054	Duplicate Elimination service stopped without finishing	The Duplicate Elimination service stopped during its merge phase without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2057	Duplicate Elimination service beginning repairs	The Duplicate Elimination service has begun merging objects and object parts.	No action is required.	Notice
2058	Service beginning repairs from a remote system	A service has begun making repairs from a remote system.	No action is required.	Notice
2059	Fast Object Recovery service started	The Fast Object Recovery service has started.	No action is required.	Notice
2060	Fast Object Recovery service stopped: run complete	The Fast Object Recovery service finished successfully.	No action is required.	Notice
2061	Fast Object Recovery service stopped without finishing	The Fast Object Recovery service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2062	Fast Object Recovery service stopped without finishing	The Fast Object Recovery service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2064	Fast Object Recovery service beginning repairs	The Fast Object Recovery service has begun repairs.	No action is required.	Warning
2065	Fast Object Recovery service: irreparable object	The Fast Object Recovery service detected a violation it could not fix.	Contact your authorized service provider.	Error
2066	Fast Object Recovery service: failure limit	The Fast Object Recovery service experienced successive failures.	Contact your authorized service provider.	Error

ID	Event	Explanation	Action	Severity
	reached			
2070	Object or object part has been shredded	An object or object part was shredded.	No action is required.	Notice
2079	Compression/Encryption service stopped without finishing	The Compression/Encryption service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2080	Compression/Encryption service started	The Compression/Encryption service has started.	No action is required.	Notice
2081	Compression/Encryption service stopped: run complete	The Compression/Encryption service finished successfully.	No action is required.	Notice
2082	Compression/Encryption service stopped without finishing	The Compression/Encryption service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2083	Service could not start	A service was requested to run but could not start for some reason.	No action is required.	Warning
2084	Disposition service started	The Disposition service has started.	No action is required.	Notice
2085	Disposition service stopped: run complete	The Disposition service finished successfully.	No action is required.	Notice
2086	Disposition service stopped without finishing	The Disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2091	Disposition service stopped without finishing	The Disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2094	Compression service stopped without finishing	The Compression service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2095	Compression service started	Compression service started	No action is required.	Notice
2096	Compression service stopped: run complete	The Compression service completed successfully.	No action is required.	Notice
2097	Compression service stopped without finishing	The Compression service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2100	HCP search facility indexing.	HCP search facility has started indexing.	No action is required.	Notice
2102	HCP search facility indexing failure	HCP search facility could not index object(s). Displays specific details.	Contact your authorized service provider.	Error
2103	HCP search facility connection failure.	The search console failed to establish connection to the HCP search facility.	Ensure that the HCP search facility search configuration is correct. If the configuration is correct and the problem persists, contact your authorized service provider.	Error
2105	Replication link created	A user created a replication link.	No action is required.	Notice
2106	Replication link suspended	A replication link has been suspended.	No action is required.	Notice
2107	Replication link resumed	A suspended replication link has been resumed.	No action is required.	Notice
2108	Replication link failure	A replication link is not working.	Check network connectivity to the remote system.	Error
2109	Replication link deleted	A replication link was deleted.	If this event is unexpected, contact your authorized service provider.	Warning
2110	Replication link read-only	The tenants and directories included in a replication link are now read-only on this system.	No action is required.	Notice
2111	Replication link authorized	A replication link was authorized.	No action is required.	Notice
2112	Replication link updated	A user updated the configuration of a replication link.	No action is required.	Notice
2113	Replication link failed over	A user failed over a replication link. The replicated tenants and directories are now read-write on the replica and read-only on the primary system.	Redirect client requests to the replica.	Notice
2114	Replication link failed back	A user failed back a replication link.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2115	Replication data recovery started	Data recovery has started on a replication link. The replicated tenants and directories are read-write on the replica and read-only on the primary system.	Monitor the recovery progress in the System Management Console.	Warning
2116	Replication data recovery completed	Data recovery has completed on a replication link. The replicated tenants and directories are now read-write on the primary system and read-only on the replica.	Redirect client requests to the primary system.	Warning
2117	Replication link missing on remote system	A replication link configured on this system is missing on the remote system. The link has been suspended.	Restore the replication link to begin the recovery process.	Error
2118	Object replicated with collisions	An object being replicated conflicts with an existing object on the target system. The object has been stored in the .lost+found directory on the target system.	No action is required.	Warning
2119	Object did not replicate	An object was not replicated.	Contact your authorized service provider.	Error
2120	Object or object part did not replicate; will retry later	An object or object part was not replicated. Replication of the object or object part will be retried later.	Monitor the remote system to see whether this object or object part is eventually replicated. If the object or object part does not replicate within one week, contact your authorized service provider.	Warning
2121	Duplicate Elimination service sort started	The Duplicate Elimination service has started the sort phase of its run.	No action is required.	Notice
2122	Duplicate Elimination service sort finished	The Duplicate Elimination service successfully finished the sort phase of its run.	No action is required.	Notice
2123	Duplicate Elimination service sort stopped without finishing	The Duplicate Elimination service stopped during its sort phase without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2124	HCP search facility indexing failure.	The HCP search facility encountered an object it could not index but will try again at a later date.	Contact your authorized service provider.	Error
2125	HCP search facility indexing configuration problem.	During the initialization of the HCP search facility, an unexpected configuration problem occurred, resulting in the disabling of indexing.	Contact your authorized service provider.	Warning
2126	Replica capacity limit reached	HCP suspended a replication link due to insufficient capacity on the replica.	Add storage capacity to the replica and resume the replication link.	Warning
2127	Time sync problem	The time on this system is not in sync with the time on the other system in a replication link in which this system participates.	Ensure that time is synchronized on all the HCP systems in the replication topology.	Warning
2128	Collisions occurred on replication link	One or more collisions occurred on a replication link in the last 24 hours.	No action is required.	Warning
2129	Replication link failed over automatically	A replication link failed over automatically because communication was disrupted for an extended period of time. The replicated tenants and directories are now read-write on the replica and read-only on the primary system.	Redirect client requests to the replica.	Notice
2130	Replication link failed over automatically	A replication link failed over automatically because communication was disrupted for an extended period of time.	No action is required.	Notice
2131	Replication link final data recovery started automatically	Final data recovery has started automatically on a replication link. The replicated tenants and directories are now read-only on both the primary system and the replica.	No action is required.	Warning
2132	Replication link automatically failed back	A replication link failed back automatically.	No action is required.	Notice
2133	Objects in one or more namespaces could not be replicated; will retry later	One or more objects could not be replicated. Another attempt to replicate these objects will be made later.	Monitor the remote system to see whether these objects are eventually replicated. If the objects are not replicated within one week, contact your authorized service provider.	Warning
2134	Replication link is candidate for auto failover	Replication link is candidate for auto failover because communication is disrupted for an extended period of time.	No action is required.	Warning
2143	Replication link progress checkpoints reset	A user set the replication progress checkpoints to a specified time. Replication will begin from this new point in time.	No action is required.	Warning
2144	Replication link rejected	A replication link was rejected.	If this event is unexpected, contact your authorized service provider.	Warning
2145	Replication link final data recovery pass started	The final data recovery pass has started on a replication link. The replicated tenants and	No action is required.	Warning

ID	Event	Explanation	Action	Severity
		directories are now read-only on both the primary system and the replica.		
2146	Replication link suspended automatically	A replication link was suspended because of a problem.	Ensure that the primary system, the replica, and the network are healthy. Then resume the link.	Error
2147	Replication adversely affected due to failed network connections	A front-end network connection is unavailable.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2148	Replication automatically paused for a tenant due to error	Replication was automatically paused for a tenant due to a problem from which HCP could not recover by itself.	Ensure that the primary system, the replica, and the network are healthy and that no tenant collisions have occurred. Then resume replication for the paused tenant.	Error
2149	Replication paused for a tenant	A user paused replication of a tenant.	No action is required.	Notice
2150	Replication resumed for a tenant	A user resumed replication of a tenant.	No action is required.	Notice
2151	Replication link suspended according to schedule	A replication link was suspended according to schedule.	No action is required.	Notice
2152	Replication link performance level changed according to schedule	The performance level of a replication link changed according to schedule.	No action is required.	Notice
2153	Replication link schedule updated	The schedule for a replication link was updated.	No action is required.	Notice
2156	Replication has been stopped for this tenant	Replication of the tenant was stopped for the indicated reason.	If the cause is one or more namespace name collisions, rename each indicated namespace. If the cause is that the replica does not support the DPL of one or more namespaces, lower the DPL of each indicated namespace. Alternatively, in either case, you can deselect the namespace from being replicated. After you make the necessary changes, notify your HCP system administrator that the problem has been resolved.	Error
2157	Namespace replication collision detected	A namespace replication collision was detected, possibly requiring intervention from the tenant administrator.	If the cause is one or more namespace name collisions, rename each indicated namespace. If the cause is that the replica does not support the DPL of one or more namespaces, lower the DPL of each indicated namespace. Alternatively, in either case, you can deselect the namespace from being replicated. After you make the necessary changes, notify your HCP system administrator that the problem has been resolved.	Notice
2158	Additional top-level directories selected for replication	The indicated top-level directories were selected for replication.	No action is required.	Notice
2159	One or more top-level directories removed from replication	The indicated top-level directories were removed from replication.	No action is required.	Notice
2160	User account replicated with collisions	Either or both of two user accounts with the same user ID on a 4.x system were modified on that system, resulting in conflicting values for one or more properties. On replication to this system, the values for those properties were taken from the account with roles.	Ensure that the user account is configured correctly.	Warning
2161	All replication links shut down	A user shut down all replication links.	No action is required.	Notice
2162	All replication links reestablished	A user reestablished all replication links.	No action is required.	Notice
2163	Replication stalled	Replication stalled while replicating an object or object part.	If the problem persists, contact your authorized service provider.	Error
2164	Replication link failed over	A user failed over a replication link.	Redirect client requests to this system.	Notice
2165	Replication link failed over	A user failed over a replication link.	Redirect client requests to the remote system.	Notice
2166	Stalled replication link has recovered	Previous stalled replication has recovered.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2167	The broken replication link recovered	The broken replication link has been repaired.	No action is required.	Notice
2168	Replication automatically paused for tenant on link outside active erasure coding topology	A tenant in the active erasure coding topology is also on a replication link that is not part of the topology.	Either remove the tenant from the link, or remove the tenant from the active erasure coding topology.	Error
2200	Storage Tiering service started	The Storage Tiering service has started.	No action is required.	Notice
2201	Storage Tiering service stopped: run complete	The Storage Tiering service finished successfully.	No action is required.	Notice
2203	Storage Tiering service stopped without finishing	The Storage Tiering service was interrupted without examining all objects.	No action is required.	Warning
2204	Storage Tiering service stopped without finishing	The Storage Tiering service was interrupted without examining all objects.	No action is required.	Notice
2250	Geo-distributed Erasure Coding service started	The Geo-distributed Erasure Coding service has started.	No action is required.	Notice
2251	Geo-distributed Erasure Coding service stopped: run complete	The Geo-distributed Erasure Coding service finished successfully.	No action is required.	Notice
2253	Geo-distributed Erasure Coding service stopped without finishing	The Geo-distributed Erasure Coding service was interrupted without examining all objects.	No action is required.	Warning
2254	Geo-distributed Erasure Coding service stopped without finishing	The Geo-distributed Erasure Coding service was interrupted without examining all objects.	No action is required.	Notice
2280	S Series Balancing service started	The S Series Balancing service has started.	No action is required.	Notice
2281	S Series Balancing service stopped: run complete	The S Series Balancing service finished successfully.	No action is required.	Notice
2282	S Series Balancing service stopped without finishing	The S Series Balancing service was interrupted without examining all objects.	No action is required.	Warning
2283	S Series Balancing service stopped without finishing	The S Series Balancing service was interrupted without examining all objects.	No action is required.	Notice
2300	User account created	A user created a user account.	No action is required.	Notice
2301	User account updated	A user updated a user account.	No action is required.	Notice
2302	User account deleted	A user deleted a user account.	No action is required.	Notice
2303	User authenticated	A user login to the System Management Console was successfully authenticated.	No action is required.	Notice
2304	Authentication attempt by unknown user	A user tried to log in with an unknown username.	Have the user log in with a valid username and password.	Warning
2305	Account reenabled by timer	A disabled security user account has been automatically reenabled.	No action is required.	Notice
2306	Account is disabled	A user tried to log in with a disabled account.	Reenable the user account to allow the user to log in.	Warning
2307	Account has been inactive for too long	A user tried to log in with an account that was disabled due to inactivity.	Reenable the user account to allow the user to log in.	Warning
2308	Account does not include the required roles	A user tried to log in with an account that does not include a required role.	Update the account to include the required role to allow the user to log in.	Warning
2309	Password is invalid	A user tried to log in with an invalid password.	Have the user log in with a valid username and password.	Warning
2310	Remote authentication server error	The login for a remotely authenticated user failed due to an error communicating with a RADIUS server.	Check the health of the RADIUS servers and the connections to them. If you cannot detect any problems, contact your authorized service provider.	Warning
2311	Password changed	A user changed the password for a user account.	No action is required.	Notice
2312	Account enabled	A user account has been enabled.	No action is required.	Notice
2313	Account disabled	A user account has been disabled.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2314	Account disabled due to too many failed logins	A user account was automatically disabled due to too many failed login attempts.	Reenable the user account and have the user log in with a valid username and password.	Warning
2315	Account will be reenabled	A security user account will be reenabled automatically after a waiting period.	No action is required.	Notice
2316	All accounts reset	A user reset user accounts to their initial configuration. All accounts have been deleted and the initial accounts have been recreated.	No action is required.	Warning
2317	User authenticated	A user login to the Search Console was successfully authenticated.	No action is required.	Notice
2319	Active Directory server error	A user tried to log in with an invalid Active Directory username or password.	Have the user log in with a valid username and password.	Warning
2330	RADIUS server created	A user configured a new RADIUS server.	No action is required.	Notice
2331	RADIUS server updated	A user updated the configuration of a RADIUS server.	No action is required.	Notice
2332	RADIUS server deleted	A user deleted a RADIUS server.	No action is required.	Notice
2333	RADIUS server promoted	A user moved a RADIUS server up in the list.	No action is required.	Notice
2334	RADIUS server demoted	A user moved a RADIUS server down in the list.	No action is required.	Notice
2335	All RADIUS servers deleted	A user deleted all RADIUS servers. The list of RADIUS servers is now empty.	No action is required.	Warning
2340	An exception occurred while removing Service Principal Name from Active Directory	HCP failed to remove a Service Principal Name from Active Directory.	Verify that the Service Principal Name was removed from Active Directory.	Warning
2341	An exception occurred while removing Service Principal Name from Active Directory	HCP failed to remove a Service Principal Name from Active Directory.	Verify that the Service Principal Name was removed from Active Directory.	Warning
2342	Successfully added Service Principal Name to Active Directory	HCP successfully added a Service Principal Name to Active Directory.	No action is required.	Notice
2344	Failed to add Service Principal Name to Active Directory	HCP failed to add a Service Principal Name to Active Directory.	Verify that the Service Principal Name was added to Active Directory.	Warning
2346	An exception occurred while adding Service Principal Name to Active Directory	HCP failed to add a Service Principal Name to Active Directory.	Verify that the Service Principal Name was added to Active Directory.	Warning
2350	Group account created	A user created a group account.	No action is required.	Notice
2352	Group account updated	A user updated a group account.	No action is required.	Notice
2354	Group account deleted	A user deleted a group account.	No action is required.	Notice
2356	Active Directory SSL certificate downloaded	A user downloaded an SSL server certificate for Active Directory.	No action is required.	Notice
2357	Incompatible namespace setting for authenticated CIFS	One or more namespaces are configured for CIFS authenticated access only, but the system is not configured to support authenticated CIFS. As a result, CIFS cannot be used for access to those namespaces.	Either enable authenticated CIFS support for the system or have the tenant administrators reconfigure the affected namespaces to support both anonymous and authenticated access with CIFS.	Warning
2358	Incompatible namespace setting for authenticated CIFS	A namespace is configured for CIFS authenticated access only, but the system is not configured to support authenticated CIFS. As a result, CIFS cannot be used for access to that namespace.	Reconfigure the affected namespace to support both anonymous and authenticated access with CIFS.	Warning
2359	Active Directory authentication enabled	A user enabled Active Directory authentication for the HCP system.	No action is required.	Notice
2360	Active Directory authentication disabled	A user disabled Active Directory authentication for the HCP system.	No action is required.	Notice
2361	Active Directory cache cleared	A user cleared the Active Directory cache.	No action is required.	Notice
2362	Active Directory partially configured	CIFS configuration is not complete on the indicated node.	Reconfigure support for Active Directory in the System Management Console.	Warning
2363	Active Directory computer account is invalid	The Active Directory computer account is invalid.	Reconfigure support for Active Directory in the System Management Console.	Warning

ID	Event	Explanation	Action	Severity
2364	Active Directory communication disrupted	The CIFS services are no longer running on the indicated node.	Reconfigure support for Active Directory in the System Management Console to restart the CIFS service.	Warning
2365	Attempt to access the Active Directory server failed	A connection issue occurred while the indicated node was trying to access the Active Directory server.	No action is required.	Warning
2366	Active Directory configuration restored	A user updated the Active Directory configuration.	No action is required.	Notice
2367	Active Directory computer account restored	A user updated the Active Directory computer account.	No action is required.	Notice
2368	Active Directory communication restored	The indicated node can now communicate with the Active Directory server. HCP can again service CIFS requests.	No action is required.	Notice
2369	Communication restored when trying to access the Active Directory server	The indicated node can now communicate with the Active Directory server.	No action is required.	Notice
2370	Could not establish secure connection to the Active Directory server	The Active Directory computer account credentials are invalid, or there is no current Active Directory SSL server certificate.	Update the Active Directory credentials or SSL server certificate.	Notice
2371	Secure connection to Active Directory server restored	A user updated the Active Directory computer account credentials or SSL server certificate.	No action is required.	Notice
2372	Active Directory single sign-on misconfigured	The Active Directory SPN for a tenant and or namespace does not exist.	Update the Active Directory single sign-on setting for the tenant and or namespace. For information about which tenants are involved, see the Status section on the Active Directory page in the HCP System Management Console.	Warning
2373	Active Directory single sign-on restored	The Active Directory SPN was created for the misconfigured tenants and or namespaces.	No action is required.	Warning
2375	Active Directory service record lookup failed	The Active Directory service record lookup failed for the indicated domain.	Check the DNS configuration.	Warning
2376	Active Directory DNS reverse lookup succeeded	The Active Directory DNS reverse lookup succeeded for the indicated domain.	No action is required.	Notice
2377	Active Directory DNS reverse lookup failed	The Active Directory DNS reverse lookup failed for the indicated domain.	Check the DNS configuration.	Warning
2378	Active Directory service records were not found.	The Active Directory service records were not found during an Active Directory health check.	Check the DNS configuration.	Warning
2379	Winbind unavailable	Winbind was found to be unavailable during an Active Directory health check.	Update your Active Directory configuration.	Warning
2380	Failed to check Active Directory service account and connectivity	Exception occurred while validating service account and connectivity for Active Directory during health check.	Check the Active Directory connection and service account.	Warning
2381	Samba not running	HCP could not get the status of Samba during an Active Directory health check.	Update your Active Directory configuration.	Warning
2382	Missing SPN(s) on Active Directory Server	One or more tenant/namespace SPN/s are missing from the Active Directory database.	Update your Active Directory configuration.	Warning
2383	Active Directory LDAP service record lookup succeeded	HCP successfully looked up the LDAP service record for the indicated Active Directory domain.	No action is required.	Notice
2384	Active Directory LDAP service record lookup failed	Failed to look up the LDAP service record for Active Directory domain.	Check that the DNS server is configured to publish LDAP service records.	Warning
2385	Active Directory kerberos service record lookup succeeded	HCP successfully looked up the Kerberos service record for the indicated Active Directory domain.	No action is required.	Notice
2386	Active Directory Kerberos service record lookup failed	Failed to look up the Kerberos service record for Active Directory domain.	Check that the DNS server is configured to publish Kerberos service record and Kerberos server is running.	Warning
2387	Active Directory service account creation successful	HCP successfully created an Active Directory service account on the indicated Active Directory server.	No action is required.	Notice
2388	Failed to create Active Directory service	HCP failed to create the Active Directory service account for the domain.	Check that the Active Directory domain user's name and password are correct. Also make sure	Warning

ID	Event	Explanation	Action	Severity
	account		the domain user has sufficient permissions to create the service account.	
2389	Active Directory node account created	An Active Directory node account was successfully created for the indicated node.	No action is required.	Notice
2390	Active Directory has been disabled	HCP has disabled Active Directory because a change to the DNS settings affected Active Directory connectivity.	No action is required.	Notice
2391	Failed to disable Active Directory	A user attempt to disable Active Directory configuration failed.	Check that the Active Directory server was running and not already disabled.	Warning
2392	Active Directory node account deleted	Active Directory node account was successfully deleted.	No action is required.	Notice
2393	Active Directory service user password updated	Automatic password updated because password refresh period elapsed.	No action is required.	Warning
2394	Failed to update Active Directory service user password	HCP may not have sufficient permissions to update the service user password.	Update Active Directory configuration and provide a domain user with sufficient permissions for password update.	Warning
2395	Successfully removed Service Principal Name from Active Directory.	Successfully removed Service Principal Name from the Active Directory.	No action is required.	Notice
2397	Failed to remove Service Principal Name from the Active Directory	Failed to remove Service Principal Name from the Active Directory.	Verify that Active Directory Service Principal Name is cleaned up.	Warning
2400	New SSL server certificate uploaded	A user uploaded an SSL server certificate.	No action is required.	Notice
2401	New SSL server CSR generated	A user requested a new CSR.	No action is required.	Notice
2402	New SSL server certificate generated	A user requested the creation of a new SSL server certificate.	No action is required.	Notice
2403	SSL server certificate expires soon	The SSL server certificate for this system expires soon. If the certificate expires, HTTPS access to the system will fail, and replication will fail.	Install a new SSL server certificate with a later expiration date.	Warning
2404	SSL server certificate expired	The SSL server certificate for this system has expired. HTTPS access to the system is not allowed, and replication has stopped.	Install a new SSL server certificate with a later expiration date.	Error
2405	Trusted replication server certificate expires soon	The indicated trusted replication server certificate expires soon. If the certificate expires, replication with the system from which the certificate was obtained will fail.	When the other system in the replication pair installs a new SSL server certificate, obtain that certificate and upload it to this system as a trusted replication server certificate.	Warning
2406	Trusted replication server certificate expired	The indicated trusted replication server certificate has expired. Replication with the system from which the certificate was obtained has stopped.	When the other system in the replication pair installs a new SSL server certificate, obtain that certificate and upload it to this system as a trusted replication server certificate.	Error
2407	Active Directory server certificate expires soon	The Active Directory SSL server certificate expires soon. If the certificate expires, access to the Active Directory server may fail.	Install a new Active Directory SSL server certificate with a later expiration date.	Warning
2408	Active Directory server certificate expired	The Active Directory SSL server certificate has expired. Access to the Active Directory server may fail.	Install a new Active Directory SSL server certificate with a later expiration date.	Error
2409	SSL server certificate deleted	A user deleted an SSL server certificate.	No action is required.	Notice
2410	SSL server CSR downloaded	A user downloaded an SSL CSR.	No action is required.	Notice
2411	Active Directory service account deletion successful	HCP successfully deleted an Active Directory service account on the indicated Active Directory server.	No action is required.	Notice
2412	Failed to delete the Active Directory service account for the listed user and organization unit. Received response.	The Active Directory server is either unreachable or the service account does not exist.	Please manually delete the HCP computer service account from the Active Directory domain it belongs to, if it exists.	Warning
2413	Failed to join domain and create Active Directory node account	The Active Directory server is either unreachable or the node account does not exist.	Check that the user name and password are correct, and that the server is reachable.	Warning
2414	Failed to leave domain and delete the Active Directory node account	The Active Directory server is either unreachable or the node account does not exist.	Check that the user name and password are correct, and that the server is reachable.	Warning

ID	Event	Explanation	Action	Severity
	for the listed node. Received response.			
2415	Active Directory domain resolution successful	HCP successfully resolved an Active Directory domain.	No action is required.	Notice
2416	Active Directory domain resolution failed	The DNS server may not be configured to return Active Directory server IP addresses.	Check that the DNS server is configured to resolve domain name of the Active Directory server.	Warning
2417	Active Directory domain join failed	The Active Directory domain may be unreachable, or the user account may be invalid.	Check that the KDC, LDAP, and Global Catalog servers are running on the domain controller, and that the service account is valid.	Warning
2418	An error occurred while communicating with Active Directory	The Active Directory domain may be unreachable, or the service user account may be invalid.	Check that the service account is valid and the Active Directory server is reachable.	Warning
2419	Certificate signing request deleted	User deleted a certificate signing request.	No action is required.	Notice
2500	PGP private key uploaded	A user uploaded a PGP private key.	No action is required.	Notice
2501	PGP encryption key uploaded	A user uploaded a PGP encryption key.	No action is required.	Notice
2502	PGP key deleted	A user deleted a PGP private or encryption key.	No action is required.	Notice
2600	Node shutdown requested from System Management Console	A user shut down a node from the System Management Console.	No action is required.	Notice
2601	HCP shutdown requested from System Management Console	A user shut down HCP from the System Management Console.	No action is required.	Notice
2602	Service started	A user started a service from the System Management Console.	No action is required.	Notice
2603	Service stopped	A user stopped a service from the System Management Console.	No action is required.	Notice
2604	Service enabled	A user enabled a service from the System Management Console.	No action is required.	Notice
2605	Service disabled	A user disabled a service from the System Management Console.	No action is required.	Notice
2606	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Notice
2607	Version upgraded	A user completed a software upgrade by updating the internal messaging version.	No action is required.	Notice
2609	Irreparable object acknowledged	A user acknowledged an irreparable object.	No action is required.	Warning
2610	All irreparable objects acknowledged	A user acknowledged all irreparable objects.	No action is required.	Warning
2611	Eject CD requested from System Management Console	A user requested the ejection of the CD tray from a node.	No action is required.	Notice
2614	Unauthorized action	A user has requested an operation that is not authorized for the user account.	If the user should be allowed to perform this operation, add the required role to the user account.	Warning
2615	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Notice
2616	Upgrade started	A user has started an upgrade of the HCP software.	No action is required.	Notice
2617	Node restart requested from System Management Console	A user restarted a node from the System Management Console.	No action is required.	Notice
2618	HCP restart requested from System Management Console	A user restarted HCP from the System Management Console.	No action is required.	Notice
2619	Restart or shutdown command could not be executed	An attempt to restart or shut down a node was could not be executed. The node may already be down.	No action is required.	Notice
2620	Upgrade completed successfully	An upgrade of the HCP software completed successfully.	No action is required.	Notice
2626	Unavailable object detected	HCP detected unavailable objects.	This state is often caused by a temporary outage and should be resolved within 24 hours.	Warning

ID	Event	Explanation	Action	Severity
2630	Support access credentials installed	A request to install exclusive Hitachi Vantara Support access credentials succeeded.	No action is required.	Notice
2631	Failed to apply Support access credentials	Failed to apply exclusive Hitachi Vantara Support access credentials due to an internal software error.	Retry the operation. If the problem persists, contact your authorized service provider.	Error
2632	Support access credentials revoked	A request to revoke exclusive Hitachi Vantara Support access credentials succeeded.	No action is required.	Warning
2633	Failed to revoke exclusive Support access credentials	Failed to revoke exclusive Hitachi Vantara Support access credentials due to an internal software error.	Retry the operation. If the problem persists, contact your authorized service provider.	Error
2634	Invalid retention class	The namespace owned by a tenant has created an invalid retention class.	Delete the invalid retention class and then create a new valid retention class with the same name.	Error
2635	Syslog disabled.	Syslog has been disabled.	No action is required	Notice
2636	Syslog enabled.	Syslog has been enabled.	No action is required	Notice
2639	Minimum TLS version updated	The minimum TLS version has been updated from {0} to {1}	No action is required	Notice
2700	Simple search query performed	A user performed a simple search.	No action is required.	Notice
2701	Advanced search query performed	A user performed an advanced search.	No action is required.	Notice
2706	Search facility configuration changed	A user changed the search facility configuration.	No action is required.	Notice
2707	Search Console disabled	A user changed the search facility selection for the Search Console to none, thereby disabling the ability to perform searches in that Console.	No action is required.	Notice
2800	Network interface down	A network interface went down.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2801	Network interface up	A network interface came up.	No action is required.	Notice
2802	Temperature sensor alarm	A temperature sensor is reporting a temperature that is out of the recommended range.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2803	Temperature sensor alarm removed	A temperature sensor is reporting a return to an acceptable operating temperature.	No action is required.	Notice
2804	Fan sensor alarm	A fan sensor is reporting a fan speed that is out of the recommended range.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2805	Fan sensor alarm removed	A fan sensor is reporting a return to an acceptable fan speed.	No action is required.	Notice
2806	Voltage sensor alarm	A voltage sensor is reporting a voltage that is out of the recommended range.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2807	Voltage sensor alarm removed	A voltage sensor is reporting a return to an acceptable operating voltage.	No action is required.	Notice
2808	File system alarm	A file system has reached the capacity warning threshold.	Consider adding storage capacity to the HCP system before the amount of free storage becomes critically low.	Error
2809	File system alarm removed	A file system has fallen below the capacity warning threshold.	No action is required.	Notice
2810	Disk device alarm	A disk device is reporting that it is not in a fully functional state.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2811	Disk device alarm removed	A disk device is reporting that it has returned to a fully functional state.	No action is required.	Notice
2812	Power supply alarm	A power supply is indicating a problem.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2813	Power supply alarm removed	A power supply is reporting that it has returned to a fully functional state.	No action is required.	Notice
2814	Processor alarm	A processor is indicating a problem.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2815	Processor alarm removed	A processor is reporting that it has returned to a fully functional state.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2816	Multipath degraded	Redundant Fibre Channel connections to storage are not functioning correctly.	Check the connections to the storage. If a problem exists, contact your authorized service provider.	Error
2817	Multipath restored	Redundant access to the underlying storage has been restored.	No action is required.	Notice
2818	Failure trimming one or more volumes	Attempt to trim one or more volumes failed.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Warning
2819	SSD RAID is degraded	An SSD device went down	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider	Error
2820	IP configuration information changed	A user changed network configuration settings through the System Management Console.	No action is required.	Notice
2830	Time is unsynchronized	Neither the external nor internal time servers could be reached for synchronization.	Check that network and time settings are correct.	Warning
2831	Using internal time server	The external time server could not be reached for synchronization.	If your system is configured to use the internal time server, no action is required. Otherwise, check that network and time settings are correct.	Notice
2832	Using external time server	The external time server was successfully contacted for synchronization.	No action is required.	Notice
2833	Lost connection to external time server	The external time server could not be contacted for synchronization.	Check that network and time settings are correct.	Notice
2834	System time changed due to resynchronization with external time server	When HCP started, the system time was resynchronized to an external time server because the system time was off by more than 1000 seconds. This time change may affect object retention.	Check that network and time settings are correct.	Warning
2835	Battery backup unit failed	A battery backup unit sensor is reporting that a BBU has failed.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2836	Battery backup unit restored	A battery backup unit sensor is reporting that a BBU has returned to a fully functional state.	No action is required.	Notice
2837	Battery backup unit degraded	A battery backup unit sensor is reporting that the BBU is degraded.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2838	Battery backup unit diagnostic running.	A battery backup unit is running diagnostics.	No action is required.	Warning
2839	Battery backup unit diagnostic finished.	A battery backup unit has finished running diagnostics.	No action is required.	Notice
2840	Battery backup unit failed.	A battery backup unit sensor is reporting that a BBU has failed.	Check whether the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2841	Battery backup unit restored.	A battery backup unit sensor is reporting that a BBU has returned to a fully functional state.	No action is required.	Notice
2842	Battery backup unit degraded.	A battery backup unit sensor is reporting that the BBU is degraded.	Check whether the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2843	Front-end Ethernet communication error	A network switch may have become unavailable.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2844	Front-end Ethernet communication restored	The front-end Ethernet interface has returned to a normal state.	No action is required.	Notice
2845	Network interface degraded	Either the network interfaces in a bonded network interface are not operating at the same speed, or they are not operating at the requested speed.	Check that the hardware is functioning properly. If the problem persists, contact your authorized service provider.	Error
2846	Network interface recovered	A network interface is now operating correctly.	No action is required.	Notice
2847	Network interface not functioning properly	Either a network interface is missing, or a network interface exists on a node with no IP address assigned.	Check that the physical network is functioning properly. If it is, try resetting the network. If the problem persists, contact your authorized service provider.	Error
2848	Network interface recovered	A network interface is now operating correctly.	No action is required.	Notice
2849	Network interface degraded	A network interface is not operating at the requested MTU.	Check that the hardware is functioning properly. If it is, try resetting the network. If the problem persists, contact your authorized service provider.	Error

ID	Event	Explanation	Action	Severity
2850	Network interface recovered	A network interface is now operating correctly.	No action is required.	Notice
2851	Front-end IPv6 communication error	A network switch may have become unavailable, or IPv6 may not be functioning on the indicated interface.	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error
2852	Front-end IPv6 communication restored	IPv6 communication through the indicated front-end Ethernet interface has been restored.	No action is required.	Notice
2853	High load alarm	The node is experiencing a heavy load.	Please contact your authorized HCP service provider.	Notice
2854	High load alarm removed	The node is no longer experiencing a heavy load.	No action is required.	Notice
2855	Insufficient quantity of RAM installed	A node with an insufficient quantity of RAM for this software version may result in performance degradation and node failures.	Install the recommended amount of RAM on this node.	Warning
2856	Sufficient quantity of RAM installed	The node has the recommended amount of RAM installed.	No action is required.	Notice
2857	Disk swap alarm	The node is experiencing a high rate of page swapping.	Please contact your authorized HCP service provider.	Notice
2858	Disk swap alarm removed	The node is no longer experiencing a high rate of page swapping.	No action is required.	Notice
2860	SSD RAID rebuilding	SSD RAID is rebuilding.	No action is required	Warning
2861	SSD storage capacity warning	The amount of free SSD storage on the HCP storage nodes is low.	Please contact your authorized HCP service provider.	Warning
2862	SSD storage capacity critical	The amount of free SSD storage on the HCP storage nodes is critically low.	Please contact your authorized HCP service provider.	Error
2863	SSD RAID storage capacity expanded.	An SSD device has finished storage expansion.	No action is required.	Notice
2870	SSD near end-of-life warning.	An SSD is near the end of its expected life span.	Contact your authorized service provider.	Warning
2871	SSD at end of life.	An SSD is at the end of its expected life span.	Contact your authorized service provider.	Warning
2872	SSD no longer near end of life.	An SSD is no longer near the end of its expected life span.	No action is required.	Notice
2910	Retention class missing	HCP system detected a missing retention class.	Contact your authorized service provider.	Error
3000	System updated	HCP system properties have been updated.	No action is required.	Notice
3001	Tenant created	A user created a tenant.	No action is required.	Notice
3002	Tenant updated	A user updated a tenant.	No action is required.	Notice
3003	Tenant deleted	A user deleted a tenant.	No action is required.	Notice
3005	Namespace updated	The configuration value of the overwrite property for a namespace has been changed.	No action is required.	Notice
3007	Namespace purged	A user purged a namespace.	No action is required.	Notice
3026	Tenant over soft quota	The amount of storage used by all namespaces owned by a tenant exceeds the soft quota configured for the tenant.	Contact the tenant administrator about increasing the hard quota for the tenant.	Warning
3027	Tenant under soft quota	The amount of storage used by all namespaces owned by a tenant is under the soft quota configured for the tenant.	No action is required.	Warning
3029	Installed new HCP version	A new version of the HCP software was successfully installed.	No action is required.	Notice
3030	Tenant at namespace quota	The number of namespaces owned by the tenant is equal to the namespace quota for the tenant.	No action is required.	Warning
3031	Tenant over namespace quota	The number of namespaces owned by the tenant is greater than the namespace quota for the tenant.	Either increase the namespace quota for the tenant or have the tenant administrator delete one or more namespaces.	Warning
3034	Namespace maximum reached	The current number of namespaces is the maximum allowed for the HCP system.	No action is required.	Warning
3035	Namespace maximum exceeded	The current number of namespaces is greater than the maximum allowed for the HCP system.	Have the administrators for one or more tenants delete one or more namespaces to reduce the total number of namespaces to at or below the maximum allowed for the HCP system.	Warning
3036	Username conflict	The indicated tenant has multiple user accounts with the same name. For any given tenant, all user accounts must have a unique username.	Have the administrator for the tenant rename one account or merge duplicate accounts together.	Warning
3038	Minimum data access permissions updated	The minimum data access permissions for a namespace have been updated.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
3500	Running migration	The Migration service has begun migrating data.	No action is required.	Notice
3501	Migration complete	The Migration service has completed the data migration.	To remove the decommissioned hardware, contact your authorized service provider.	Notice
3502	Pausing migration	A user paused the data migration.	No action is required.	Notice
3503	Preparing migration	The Migration service has begun preparing to migrate data.	No action is required.	Notice
3504	Verifying migration	The Migration service has begun verifying the data migration.	No action is required.	Notice
3505	Migration service stopped	The Migration service is no longer running.	No action is required.	Notice
3506	Migration service performance level updated	A user changed the Migration service performance level.	No action is required.	Notice
3507	Migration description updated	A user changed the migration description.	No action is required.	Notice
3509	Migration service: irreparable object or object part	The Migration service was unable to migrate an object or object part and has marked it irreparable.	Contact your authorized service provider.	Error
3510	Pausing migration	The Migration service automatically paused the data migration because the HCP system does not have enough available space for the objects being migrated.	Contact your authorized service provider.	Error
3511	Error completing migration	The Migration service encountered an unrecoverable error while trying to complete the data migration.	Contact your authorized service provider.	Error
4103	Failure creating HCP search facility index for a namespace.	The HCP search facility could not create the index for a namespace.	No action is required.	Warning
4104	Failure deleting HCP search facility index for a namespace.	The HCP search facility could not delete the index for a namespace.	Contact your authorized service provider.	Warning
4105	Failure creating HCP search facility index for a namespace.	The HCP search facility could not create the index for a namespace but will try again later.	No action is required. If this situation persists, contact your authorized service provider.	Warning
4106	Ingest-time override setting has been changed	The ingest-time override setting was changed.	No action is required.	Warning
4107	Chassis communication error	HCP cannot communicate with the indicated chassis through SNMP.	Check network connectivity to the chassis. Also check that the chassis is configured to accept SNMP requests from the lowest-numbered available storage node in the HCP system.	Error
4108	Communication from unknown node	Nodes from another HCP system were detected on the network.	Check the back-end network. A back-end network can support only one HCP system.	Error
4109	Communication from node at previous version	Nodes from another HCP version were detected on the network, and no upgrade is in process.	Check the back-end network. A back-end network can support only one HCP system.	Error
4110	Metadata query engine indexing started	A user enabled metadata query engine indexing.	No action is required.	Notice
4111	Metadata query engine indexing stopped	A user disabled metadata query engine indexing.	No action is required.	Warning
4112	Metadata query engine is available	The metadata query engine is running on the indicated node.	No action is required.	Notice
4113	Metadata query engine is not available	The metadata query engine is not running on the indicated node. As a result, the query API is unavailable for object-based queries. If the Search Console is using the query engine, searching through the Console is also unavailable.	No action is required. If this situation persists, contact your authorized service provider.	Warning
4116	Metadata query engine index capacity warning	The size of the metadata query engine index has reached a warning threshold.	Increase the maximum size allowed for the metadata query engine index.	Warning
4117	Metadata query engine index capacity error	The size of the metadata query engine index has reached an error threshold.	Increase the maximum size allowed for the metadata query engine index.	Error
4118	Metadata query engine index capacity reached	The size of the metadata query engine index has reached the maximum threshold.	Increase the maximum size allowed for the metadata query engine index.	Error
4119	Metadata query engine index partially unavailable	Part of the metadata query engine index is unavailable due to one or more logical volumes being unavailable. Indexing is temporarily paused, and queries cannot be serviced.	Make the unavailable logical volumes available. Alternatively, rebuild the index by first deleting it and then reenabling indexing. Note that	Error

ID	Event	Explanation	Action	Severity
			rebuilding the index can take a significant amount of time.	
4120	Metadata query engine out of memory for indexing	No more memory is available for metadata query engine indexing. Indexing was automatically disabled.	Add memory to the system by adding nodes or upgrading existing nodes. Then reenable metadata query engine indexing.	Error
4121	Failure creating HCP search facility index for a namespace. Limit reached.	The HCP search facility was unable to create the index for a namespace due to reaching the system limit.	No action is required.	Warning
4129	Objects in namespace could not be replicated; will retry later	One or more objects could not be replicated. Another attempt to replicate these objects will be made later.	Monitor the remote system to see whether these objects are eventually replicated. If the objects are not replicated within one week, contact your authorized service provider.	Warning
4200	RAID group spun down	A RAID group was spun down.	No action is required.	Notice
4201	RAID group spun up	A RAID group was spun up.	No action is required.	Notice
4202	Error spinning down RAID group	An error occurred while spinning down a RAID group.	Contact your authorized service provider.	Error
4203	Error spinning up RAID group	An error occurred while spinning up a RAID group.	Contact your authorized service provider.	Error
4204	Back-end switch communication failure	A back-end switch is not communicating with HCP.	Check that the switch is functioning properly. If the problem persists, contact your authorized service provider.	Error
4205	Back-end switch failure	A back-end switch is reporting a problem.	Check that the switch is functioning properly. If the problem persists, contact your authorized service provider.	Error
4206	Back-end switch restored	A back-end switch is reporting a return to a functional state.	No action is required.	Notice
4207	Objects read from spindown storage	For the indicated tenant, one or more clients read objects from spindown storage.	Ensure that the service plan in use is appropriate for the data usage pattern.	Notice
4208	Objects read from spindown storage	For the indicated namespace, one or more clients read objects from spindown storage.	Ensure that the service plan in use is appropriate for the data usage pattern.	Notice
4209	Time server changed	A user changed the time server for the HCP system.	No action is required.	Notice
4210	Current time changed	A user changed the current time for the HCP system.	No action is required.	Notice
4211	Time zone changed	A user changed the time zone for the HCP system.	No action is required.	Notice
4212	Service plan created	A user created a service plan.	No action is required.	Notice
4213	Service plan updated	A user updated a service plan.	No action is required.	Notice
4214	Service plan deleted	A user deleted a service plan.	No action is required.	Notice
4215	Failover completed	A node in a cross-mapped pair became unavailable. The other node in the pair has finished taking over management of the logical volumes previously managed by the unavailable node.	No action is required.	Warning
4216	Failback started	A previously unavailable node in a cross-mapped pair has become available again and has begun the process of taking back management of its logical volumes from the other node in the pair.	No action is required.	Warning
4217	Failback completed	A node in a cross-mapped pair has finished taking back management of its logical volumes, which had previously failed over to the other node in the pair.	No action is required.	Notice
4218	Monitored component added	A user added a monitored component.	No action is required.	Notice
4219	Monitored component deleted	A user deleted a monitored component.	No action is required.	Notice
4221	Tenant tags updated	A user updated the tags for a tenant.	No action is required.	Notice
4222	Time settings compliance mode changed	A user changed the time settings compliance mode for the HCP system.	No action is required.	Notice
4223	Failover completed	A node in a cross-mapped pair became unavailable. The other node in the pair has finished taking over management of the logical volumes previously managed by the unavailable node.	No action is required.	Warning

ID	Event	Explanation	Action	Severity
4224	Failback started	A previously unavailable node in a cross-mapped pair has become available again and has begun the process of taking back management of its logical volumes from the other node in the pair.	No action is required.	Notice
4226	KM server created	A user created a KM server.	No action is required.	Notice
4227	KM server updated	A user updated a KM server.	No action is required.	Notice
4228	KM server deleted	A user deleted a KM server.	No action is required.	Notice
4229	KM server retired	A user retired a KM server.	No action is required.	Notice
4230	KM server keys replaced	A user replaced keys for a KM server.	No action is required.	Notice
5000	Time is unsynchronized between nodes	The HCP system detected an issue while checking the times on the nodes.	Contact your authorized service provider.	Warning
5100	Network created	A user created a network.	No action is required.	Notice
5101	Network updated	A user updated a network.	No action is required.	Notice
5102	Network deleted	A user deleted a network.	No action is required.	Notice
5103	Network alias created	A user created a network alias.	No action is required.	Notice
5104	Network alias updated	A user updated a network alias.	No action is required.	Notice
5105	Network alias deleted	A user deleted a network alias.	No action is required.	Notice
5106	Network IP address assigned to node	A user assigned a network IP address to a node.	No action is required.	Notice
5107	Node IP address changed	A user changed a network IP address for a node.	No action is required.	Notice
5108	Network IP address removed from node	A user removed a network IP address from a node.	No action is required.	Notice
5109	Network reset	A user reset a network.	No action is required.	Notice
5110	Domain created	A user created a domain.	No action is required.	Notice
5111	Domain deleted	A user deleted a domain.	No action is required.	Notice
5112	Network status changed	The status of a network changed due to one or more node IP addresses being added or removed.	No action is required.	Notice
5113	Replication network changed	A user chose a new replication network.	No action is required.	Notice
5114	Domain renamed	A user renamed a domain.	No action is required.	Notice
5115	Objects read from external storage	For the indicated tenant, one or more clients read objects from external storage.	Ensure that the service plan in use is appropriate for the data usage pattern.	Notice
5116	Objects read from external storage	For the indicated namespace, one or more clients read objects from external storage.	Ensure that the service plan in use is appropriate for the data usage pattern.	Notice
5117	System IP mode updated	A user updated advanced network settings.	No action is required.	Notice
5118	Virtual network management updated	A user updated advanced network settings.	No action is required.	Notice
5119	Failure accessing cloud storage	The HCP system encountered errors while accessing cloud storage.	Check network connectivity to the cloud storage. Also check account credentials and permissions.	Warning
5120	Service plans created during upgrade	New retired service plans were created during upgrade to satisfy namespace DPL requirements.	Review your service plans.	Notice
5121	Running retirement	The retirement service has begun storage volume retirement.	No action is required.	Notice
5122	Retirement service performance level updated	A user changed the retirement service performance level.	No action is required.	Notice
5123	Pausing retirement	A user paused the retirement service.	No action is required.	Notice
5124	Retirement service off	The retirement service is no longer running.	No action is required.	Notice
5125	HCP S Series Node warning message received	The component may not be functioning correctly.	Check that the HCP S Series Node is functioning properly. If a problem exists, contact your authorized service provider.	Warning
5126	HCP S Series Node error message received	The component may not be functioning correctly.	Check that the HCP S Series Node is functioning properly. If a problem exists, contact your authorized service provider.	Error
5127	Downstream DNS mode updated	A user updated downstream DNS mode.	No action is required.	Notice
5128	DNS server configuration reverted to	System detected invalid DNS server configuration at reboot and reverted to BASIC Downstream	Verify that Downstream DNS configuration for all front-end networks is correct.	Error

ID	Event	Explanation	Action	Severity
	BASIC Downstream DNS mode configuration.	DNS mode configuration.		
5129	Failure accessing cloud storage	The HCP system encountered errors while accessing cloud storage.	Check network connectivity to the cloud storage. Also check account credentials and permissions.	Warning
5130	Storage retirement canceled	A user canceled a storage retirement operation.	No action is required.	Notice
5131	Incomplete DNS forward_zone file	After adding a new node to the HCP system, the DNS forward_zone file remains incomplete.	Add the IP address of the new node to the forward_zone file.	Warning
5132	Certificate signing request downloaded	A user downloaded a certificate signing request.	No action is required.	Notice
5200	Default protocol optimization setting updated	A user updated the default protocol optimization setting.	No action is required.	Notice
5201	Namespaces optimized	A user optimized namespaces for cloud protocols.	No action is required.	Notice
5202	Default directory usage setting updated.	Default directory usage setting has been updated.	No action is required.	Notice
5301	Storage space reclamation failed	Error encountered during trimming operation	Check that the data LUNs support trimming and are configured properly.	Warning
5400	Erasure coding topology created	A user created an erasure coding topology.	No action is required.	Notice
5401	Erasure coding topology updated	A user updated an erasure coding topology.	No action is required.	Notice
5402	Erasure coding topology deleted	An erasure coding topology has been deleted.	If this event is unexpected, contact your authorized service provider.	Notice
5403	Erasure coding topology protection status changed	Some or all of the tenants in the erasure coding topology are not replicating to all systems in the topology.	Check the status of the replication links in the erasure coding topology.	Error
5404	Erasure coding topology protection status changed	An additional replication link failure could result in some or all tenants not replicating to all systems in the erasure coding topology.	Check the status of the replication links in the erasure coding topology.	Warning
5405	Erasure coding topology protection status changed	All tenants in the erasure coding topology are now replicating to all systems in the topology.	No action is required.	Notice
5406	Erasure coding topology read status changed	Erasure-coded objects in the erasure coding topology cannot be read.	Check the status of the replication links in the erasure coding topology.	Error
5407	Erasure coding topology read status changed	An additional replication link failure could result in the inability to read erasure-coded objects.	Check the status of the replication links in the erasure coding topology.	Warning
5408	Erasure coding topology read status changed	Erasure-coded objects in the erasure coding topology can now be read.	No action is required.	Notice
5409	Replication paused for tenant in erasure coding topology	The erasure coding topology includes a tenant for which replication was paused either automatically or by a user.	Resume replication of the tenant.	Warning
5410	Replication paused for tenants in erasure coding topology	The erasure coding topology includes tenants for which replication was paused either automatically or by a user.	Resume replication of the tenants.	Warning
5411	Replication no longer paused for tenants in erasure coding topology	All tenants in the erasure coding topology are now replicating.	No action is required.	Notice
5412	Erasure coding topology replication link not found	A replication link in the erasure coding topology could not be found.	Recover the missing replication link.	Error
5413	Erasure coding topology replication links not found	Replication links in the erasure coding topology could not be found.	Recover the missing replication links.	Error
5414	Erasure coding topology replication links no longer missing	All missing links in the erasure coding topology were recovered.	No action is required.	Notice
5415	Tenant in erasure coding topology not on replication link	A tenant was not automatically added to a replication link in the erasure coding topology.	Add the tenant to the replication link.	Error
5416	Tenants in erasure coding topology not on replication link	Tenants were not automatically added to a replication link in the erasure coding topology.	Add the tenants to the replication link.	Error
5417	Tenants added to erasure coding topology	All tenants in the erasure coding topology are on the replication link.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
	replication link			
6001	Replication verification setting changed	Replication verification setting was changed	No action is required.	Notice
6002	Replication verification run complete	Replication verification run completed successfully.	No action is required.	Notice
6003	Nonreplicating object	An object could not be replicated because it is open, irreparable, or unavailable.	Contact your authorized service provider.	Error
8000	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8001	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8002	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8003	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8004	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8005	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8006	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8007	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Notice
8008	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8009	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8010	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8011	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8012	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8013	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8014	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8015	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Warning
8016	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8017	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8018	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8019	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8020	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8021	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8022	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8023	Prometheus alert	Alertmanager sent one or more Prometheus alerts.	Contact your authorized service provider.	Error
8024	Prometheus alert	The Prometheus service started for one of the following reasons: • HCP was initiated. • Prometheus was enabled. • HCP detected a failure in Prometheus. • The storage capacity was no longer close to being full. • The Prometheus monitor determined that Prometheus should start.	Contact your authorized service provider.	Notice

ID	Event	Explanation	Action	Severity
8025	Prometheus alert	The Prometheus service stopped for one of the following reasons: • HCP was shutdown. • Prometheus was disabled. • The storage was nearing its capacity. • The service no longer ran on this node. • The node became unavailable.	Contact your authorized service provider.	Notice
8026	Prometheus alert	The Prometheus service stopped working, and attempts to restart it were unsuccessful.	Contact your authorized service provider.	Notice
8027	Prometheus alert	The Prometheus service stopped for one of the following reasons: • The storage used by Prometheus and Alertmanager service was almost full. • The SMC displayed a full file system error message when the Prometheus TSDB filesystem reached about 95% capacity.	Contact your authorized service provider.	Warning
8028	Prometheus alert	The Alertmanager service started for one of the following reasons: • HCP was initiated. • Prometheus was enabled with alert rules. • HCP detected an Alertmanager failure. • The Prometheus monitor determined that Alertmanager should start. • The configuration was modified.	Contact your authorized service provider.	Notice
8029	Prometheus alert	The Alertmanager service stopped for one of the following reasons: • HCP was shutdown. • Prometheus was disabled. • Alert rules were removed. • The configuration changed. • The storage was almost full. • The Prometheus no longer ran on this node. • The node became unavailable.	Contact your authorized service provider.	Notice
8030	Prometheus alert	The Alertmanager service experienced a failure and three attempts to restart it were unsuccessful.	Contact your authorized service provider.	Warning
8031	Prometheus alert	Alertmanager is not available on any node.	Contact your authorized service provider.	Error
8032	Prometheus alert	Prometheus is not available on any node.	Contact your authorized service provider.	Error
9000	A hardware failure occurred.	A hardware failure detected (RC={0}).	Check that the hardware is functioning properly. If a problem exists, contact your authorized service provider.	Error

Configuring SNMP

You can configure HCP to work with SNMP. With SNMP enabled, you can have HCP send system log messages to one or more specified SNMP managers. When you do this, you can use tools in your SNMP environment to perform functions such as sorting the messages, querying for certain events, or forwarding error messages to a mobile device.

To use HCP to send log messages to external SNMP managers, each SNMP manager must be configured to use at least one IPv4 or IPv6 address that is routable from the [hcp_system] network. For this reason, if you specify an IPv6 unique local address (ULA) for an external SNMP manager, then the [hcp_system] network must be configured with an IPv6 ULA that can be used to connect to that SNMP manager.

To send the log messages, HCP uses the arcAdminLogEvent trap in its own management information base (MIB), HCP-MIB. You can download this MIB from the SNMP page of the HCP System Management Console.

HCP can also send notification of certain types of events to the specified SNMP managers. These event types are determined by traps in several standard MIBs available to SNMP clients.

Tenant-level administrators can choose to include tenant log messages along with the system log messages sent to the SNMP managers.

Additionally, with SNMP enabled, you can use SNMP tools to view almost all the system settings available in the System Management Console, as well as other settings available only through standard MIBs. You can also allow or disallow the use of SNMP to change HCP settings such as the shredding rate or whether nodes should respond to ping requests. You can specify IP addresses from which viewing and changing these settings is allowed or denied.

To use SNMP for event notification, receiving log messages, and viewing and modifying system settings, you need to have an SNMP tool installed on your client. SNMP tools are available from multiple sources.

Note: When you change the SNMP configuration while SNMP is enabled, SNMP functions are briefly disrupted.

Log messages sent to SNMP managers

For each system log message about an event, HCP sends the information shown in the following table to the specified SNMP managers.

Information	Field in HCP-MIB	Data type
Severity of the event	hcpAdminLogEventSeverity	INTEGER. Possible values are: • 3 - Error • 4 - Warning • 5 - Notice
Date time the event occurred	hcpAdminLogEventTimestamp	DateAndTime
Message ID	hcpAdminLogEventType	Integer32
Full message text	hcpAdminLogEventMessage	LongDisplayString (up to 1,024 bytes)

You can choose the severity level of the log messages to be sent. You can also choose whether or not to send messages about security events (that is, attempts to log into the System Management Console with an invalid user name) and compliance events. Compliance events happen at the namespace level, so these messages are sent to the SNMP managers only if SNMP logging is enabled at the tenant level.

Note: System log messages are not guaranteed to arrive at the SNMP managers to which they're sent. This is because the SNMP protocol uses UDP for data transmission.

Some HCP startup events occur before the internal SNMP server starts. Therefore, messages about these startup events are not sent to SNMP managers.

Enabling and configuring SNMP

You use the SNMP page in the HCP System Management Console to enable and configure SNMP for HCP. You also use this page to test the connections to the SNMP managers that you specify.

To display the SNMP page, in the top-level menu of the System Management Console, select Monitoring > SNMP.

Note: To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

Enabling SNMP for HCP

You can enable SNMP for HCP by going to the SNMP page.

To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. Specify SNMP settings.
   a. To enable all uses of SNMP with HCP, select Enable SNMP at snmp.*hcp-domain-name*.
   b. Optionally, select Allow writes/updates of HCP settings through SNMP to allow users to change the HCP system configuration through SNMP.

      This option applies only when SNMP is enabled.

   c. To indicate the version of SNMP you want to use, select either Use version 1 or 2c or Use version 3.

      SNMP version 1 does not support fields with the Counter64 data type. In the HCP MIB, several fields have that data type. When you use SNMP version 1 to retrieve system information, it will not return values for those fields.

   d. To secure access to HCP through SNMP, for SNMP version 1 or 2c, type the name of a community in the Community field.

      Community names can contain can be from 1 through 63 characters long and are case-sensitive.

   e. To secure access to HCP through SNMP for SNMP version 3, in the New Password field, type a password to go with the system-supplied name in the Username field.

      Passwords must be at least eight characters long and can contain any valid UTF-8 characters, including white space; however, the recommended usage is to limit the password to only ASCII characters. Passwords are-case sensitive.

      If you're modifying the SNMP settings and you leave the New Password field empty, the previously set password remains in effect.

      In the Confirm Password field, type the password again.

      In the Community field, type a community access string. Community access strings can contain only alphanumeric characters and hyphens (-) and can be from 1 through 63 characters long. These strings are case-sensitive.

   f. To include log messages about compliance events with the messages sent to the specified SNMP managers, select Send compliance events.
   g. To include log messages about security events with the messages sent to the specified SNMP managers, select Send security events.
   h. In the Send log messages at this level or higher field, select the severity level of log messages to be sent to the specified SNMP managers:

      OFF
      : tells HCP not to send any log messages.
      NOTICE
      : sends messages with a severity level of Notice, Warning, or Error.
      WARNING
      : sends messages with a severity level of Warning or Error.
      ERROR
      : sends only messages with a severity level of Error.

2. Click Update Settings.
   Tip: Before you submit your changes, you can test the connections to the specified SNMP managers

Specifying IP addresses to be allowed access to HCP through SNMP

Optionally, you can specify IP addresses to be allowed access to HCP through SNMP.

To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. On the SNMP page, click the Allow tab.
2. To add an entry to an Allow or Deny list, in the field above the list, type the entry you want and click Add.
3. To remove a single entry from an Allow or Deny list, click the delete control ( ) for that entry.
4. To remove all entries, click Delete All.

Changes you make to either list of IP addresses take effect immediately.

Specifying IP addresses to be denied access to HCP through SNMP

Optionally, you can specify IP addresses to be denied access to HCP through SNMP.

To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. On the SNMP page, click the Deny tab.
2. To add an entry to an Allow or Deny list, in the field above the list, type the entry you want and click Add.
3. To remove a single entry from an Allow or Deny list, click the delete control ( ) for that entry.
4. To remove all entries, click Delete All.

Changes you make to either list of IP addresses take effect immediately.

Specifying how HCP should handle IP addresses that appear in both or neither of the Allow and Deny lists

To specify how HCP should handle IP addresses that appear in both or neither of the Allow and Deny lists, select or deselect Allow request when same IP is used in both lists on the SNMP page. Changes to this option take effect immediately.

Specifying one or more external SNMP manager IP addresses

Optionally, you can specify one or more external SNMP manager IP addresses. For each external SNMP manager that you want to use with HCP, specify the IPv4 or IPv6 address that you want HCP to use to connect to that SNMP manager.

You specify each external SNMP manager IP address as a separate entry in the SNMP trap addresses list. You can add an IP address to the SNMP trap addresses list.

To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. On the SNMP page, in the Trap Addresses field, type the IP address.

   Each entry in this list must be a single IP address. IP address ranges and comma-separated lists are not valid.

2. Click Add.
   The IP address moves into the list below the field.
3. To remove an external SNMP manager IP address from the list, click the delete control ( ) for that IP address.
4. To remove all the IP addresses from the list, click Delete All.

IP addresses that appear in both the Trap Addresses list and the Deny list do not receive trap notifications.

Testing SNMP connections

At any time, you can test the connections to the external SNMP managers whose IP addresses appear on the SNMP page. Testing the connections causes HCP to send a message to the target IP addresses. To verify that the connections are working, you need to use your SNMP tools to check that the message arrived.

The message HCP sends to the SNMP managers has a severity level of Notice. Therefore, for the message to be sent successfully, the severity level of messages to be sent must be set to NOTICE.

To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. On the SNMP page, click Test.
   HCP sends this message to the specified SNMP managers:

   ```
   User username sent system log test message.
   ```

2. Check each SNMP manager to ensure that the message arrived.

If an SNMP manager doesn't receive the message:

- Check that you've correctly specified the target IP address.
- Check that you can successfully ping the target IP address.
- If you're unable to determine the cause of the problem, please contact your authorized HCP service provider.

Viewing and downloading the HCP-MIB.txt file

The SNMP MIB for HCP is described in the HCP-MIB.txt file. To use this MIB, you need to download the file to your SNMP tool.

Tip: You can download the HCP-MIB.txt file even if your user account includes only the monitor role.
To view the SNMP page, you need the monitor, administrator, security, or compliance role. To configure SNMP for HCP and test connections to SNMP managers, you need the administrator or security role.

1. To view the HCP-MIB.txt file, click HCP-MIB.txt on the SNMP page.
2. To download the HCP-MIB.txt file, right-click HCP-MIB.txt on the SNMP page and select the browser-specific option for downloading the file.
3. Save the file as HCP-MIB.txt in the applicable directory for your SNMP tool.

Using SNMP to view or change HCP settings

You can use the fields HCP-MIB and other MIBs to view and, when allowed, change HCP settings. The interface you use for these activities depends on your SNMP tool. Here are examples of viewing and changing HCP settings with the command-line tool net-snmp:

- To view the total storage capacity of the HCP system:

Command:

```
snmpget -v 2c -c public -m +/usr/share/snmp/mibs/HCP-MIB.txt
snmp.hcp-ma.example.com HCP-MIB::totalCapacity.0
```

Response:

```
HCP-MIB::totalCapacity.0 = Counter64: 562110914560
```

- To set the shredding rate to low:

  Command

```
snmpset -v 2c -c public -m +/usr/share/snmp/mibs/HCP-MIB.txt
snmp.hcp-ma.example.com HCP-MIB::shreddingRate.0 i 5000
```

  Response:

```
HCP-MIB::shreddingRate.0 = INTEGER: low(5000)
```

net-snmp is a publicly available tool.

Monitoring HCP performance using Prometheus

HCP supports Prometheus, an open-source monitoring and alerting framework that collects, organizes, and stores performance metrics. When Prometheus is used with a visualization tool like Grafana, data collected by Prometheus provides operational visibility into the performance of your HCP instance.

The Prometheus server runs on two storage nodes in the cluster: the node with highest IP address and the node with the second lowest IP address. By default, Prometheus retains all the collected metrics in a time series database for 15 days.

For a list of the HCP metrics collected by Prometheus, see HCP performance metrics collected by Prometheus

Enabling and configuring Prometheus

Enabling Prometheus allows you to collect various HCP performance metrics. HCP exposes Prometheus metrics on TCP port 9094. Use this unauthenticated port to monitor system performance without exposing sensitive data. To prevent user access, block the port on user data networks. HCP system blocks all POST requests to the unauthenticated port. You can only send GET requests.

To enable Prometheus on HCP nodes, you need an administrator or security role.

1. From the System Management Console main menu, select Monitoring > Prometheus > Configuration .
2. To enable Prometheus, select the Enable Prometheus option.
3. In the Prometheus Settings pane, enter the configuration information. The following table describes the values that you can specify.

Field	Description	Values
Scrape interval	The frequency at which Prometheus retrieves metrics from endpoints on each HCP node.	Default value: 60 seconds. Valid value: 10 seconds or greater.
Scrape timeout	Duration of time Prometheus will wait for a response from an endpoint before it determines that the target is down.	Default value: 60 seconds. Valid value: 1 second or greater.
Evaluation interval	The frequency at which Prometheus evaluates alert rules to see if a rule has been triggered.	Default value: 60 seconds. Valid value: 10 seconds or greater.
TSDB retention time	Duration of time Prometheus keeps the data in the time-series database. When the specified retention time limit is reached, Prometheus begins discarding data starting with the oldest first.	Default value: 15 days. Valid value: Greater than or equal to 1 day; and lesser than or equal to 365 days.
TSDB retention size	Specifies the maximum number of storage blocks (in GB) to retain on disk. When the specified retention size limit is reached, Prometheus begins discarding data starting with the oldest first. Important: If you specify both TSDB retention time and TSDB retention size, whichever limit is reached first will take effect.	Default value: 100 GB. Valid value: Greater than or equal to 1 GB; and lesser than or equal to 1000 GB. Important: Prometheus accepts the data setting in gigabytes (GB), but reports it back in gibibytes (GiB). GB is a metric measurement, while GiB is a binary measurement. One GB equals 0.93 GiB.

4. In the Prometheus Metrics pane, select the performance metrics you want to monitor. The following table describes the various metric categories.

Performance metrics category	Description
Gateway metrics	Provides information about gateway operations. These metrics can be used to monitor system performance.
Storage metrics	Provides information about the storage usage of a system. These metrics can be used to monitor disk space usage, disk I/O, and disk latency etc.
Node metrics	Provides information about hardware and OS-level system metrics. These metrics can be used to monitor node (or server) performance.
Replication metrics	Provides information about the replication process of the system. These metrics can be used to monitor replication status.
Event metrics	Provides information about system events. These metrics can be used to monitor system status.

Note: If you are performing a new installation of HCP v9.6 or upgrading from an older version, all performance metrics collectors will be automatically enabled when Prometheus is enabled.

For a list of the HCP metrics collected by Prometheus, see HCP performance metrics collected by Prometheus.

5. Click Update Settings.

Configuring Alert rules

Alert rules allow you to define alert conditions in order to trigger alerts and send notifications to HCP. Prometheus processes the alerts before forwarding them to an internal Alertmanager server, which handles sending them to HCP. Alertmanager operates on two storage nodes within the cluster: the node with the highest IP address and the node with the second-lowest IP address. The alert functionality remains operational even if one of these nodes fails. If one of the nodes running Alertmanager is permanently removed, Alertmanager will initiate on another node.

You can configure HCP to use syslog messages, SNMP traps, and email notifications to notify you when important or critical events are detected. Notifications are triggered immediately after an event occurs. The events are displayed in the Major Events pane on the HCP Overview page.

- To configure syslog messages, see Configuring syslog logging
- To configure SNMP traps, see Configuring SNMP
- To configure email notifications, see Configuring email notification

To configure Alert rules, you need an administrator, or security role.

1. From the System Management Console main menu, select Monitoring > Prometheus > Alert Rules .
2. Edit Alert Rules text box to create a new rule or edit an existing rule.

   The example alert rule configuration is commented out by default. For more information about defining alert rules, see Alerting Rules in the Prometheus documentation at: https://prometheus.io/docs/prometheus/latest/configuration/alerting_rules/.

   To create alert rules, you may specify these custom labels. Labels are optional. If you do not specify a label, a default value is used.

```
severity:   notice   | warning | error (default: warning)
security:   false    | true (default: false)
compliance: false    | true (default: false)
importance: major    | minor (default: minor)
```

   The following example creates a new alert rule if one of the instances in the cluster is not reachable for more than five minutes.

```
# Alert rules for HCP metrics
# Please see HCP documentation for the list of HCP metrics
# HCP will convert the alerts into HCP events. Please use the following four labels to categorize the alerts:
#  - severity: notice | warning | error
#  - security: true | false
#  - compliance: true | false
#  - importance: major | minor
#  Example alert for any instance that is unreachable for >5 minutes.
#  Remove the following comment markers (#) to enable this example alert.
groups:
name: example
   rules:
   - alert: InstanceDown
    expr: up == 0
     for: 5m
     labels:
      severity: warning
          security: false
      compliance: false
      importance: major
      annotations:
      summary: "Instance {{ $labels.instance }} down"
      description: "{{ $labels.instance }} of job {{ $labels.job }} has been down for more than 5 minutes."
```

3. Click Update Settings.

Viewing HCP metrics in Grafana

Grafana is an open-source tool for metrics visualization. You can use it with Prometheus as the data source to visualize HCP metrics for operational visibility into the performance of your HCP instance.

The following are some of the Grafana dashboard and panel templates that you can use to visualize HCP performance metrics collected by Prometheus to perform deeper analysis. You can download these templates from the Product Downloads page of the Hitachi Support Connect portal.

- **Application Load**: Displays metrics related to HCP gateway operations and HTTP connections.
- **HCP Overview**: Displays a selected collection of panels from other HCP dashboards to provide an overview of system behavior.
- **Replication**: Displays metrics related to replication operations such as pending operations, replicated objects, and replication errors.
- **Resources**: Displays metrics related to node hardware status, such as CPU utilization, disk I/O, and network I/O.
- **Storage and Objects**: Displays metrics related to object storage and system capacity.

- Enable Prometheus and configure its settings in HCP.
- Install and configure Grafana in your environment.

  For more information about installing Grafana, see "Install Grafana" in the Grafana documentation at https://grafana.com/docs/grafana/latest/setup-grafana/installation/

1. From the System Management Console main menu, select Monitoring > Prometheus.
2. To access the Prometheus dashboard, click the Prometheus URL: `https://<prometheus.example.com>:<port>`)
   - `<prometheus.example.com>`: FQDN that refer to the complete domain name of your Prometheus server.
   - `<port>`: HCP access port number. The reserved port number for Prometheus is 9094.

3. To view HCP metrics in Grafana, copy the Prometheus URL to add it as a data source in Grafana.

   For more information about adding a data source in Grafana, see "Add a data source" in the Grafana documentation at: https://grafana.com/docs/grafana/latest/datasources/add-a-data-source/

   Note: Grafana may display empty graphs if there is no data or if the datasource is not correctly configured.
4. Import the template, that you downloaded, into Grafana.

   For more information about importing dashboard templates in Grafana, see "Import dashboard" in the Grafana documentation at: https://grafana.com/docs/grafana/latest/setup-grafana/installation/

5. Configure Grafana dashboard.

   For more information about configuring Grafana dashboards, see "Configuring Dashboards" in the Grafana documentation at: https://grafana.com/docs/grafana/latest/dashboards/use-dashboards/.

6. Visualize Prometheus data in Grafana.

   For more information about visualizing data using Prometheus, see "Grafana support" in the Prometheus documentation at: https://prometheus.io/docs/visualization/grafana.

Resetting alert rule settings

When you reset alert rule settings, HCP removes all alert rules and resets the configuration to default settings.

To reset alert rule settings, you need an administrator or security role.

1. From the System Management Console main menu, select Monitoring > Prometheus > Alert Rules .
2. Click Reset .
3. Select the I Understand check box, and then click Reset Settings.

Controlling access to the Prometheus by IP address

You can use the IP Filter page to allow or deny access to Prometheus from specific IP addresses.

1. From the System Management Console main menu, select Monitoring > Prometheus > IP Filter.
2. (Optional) Specify IP addresses to be allowed access to the Prometheus. To do this:
   a. Click the Allow tab.
   b. Follow the instructions in Adding an entry to an Allow or Deny list.
3. (Optional) Specify IP addresses to be denied access to the Prometheus. To do this:
   a. Click the Deny tab.
   b. Follow the instructions in Removing entries from an Allow or Deny list.
4. To specify how HCP should handle IP addresses that appear in both or neither of the Allow and Deny lists, select or deselect the Allow request when same IP is used in both lists option.
   Changes to this option take effect immediately.

Adding an entry to an Allow or Deny list

Changes you make to either list of IP addresses take effect immediately.

1. In the field above the list, type the entry you want. Each entry in an Allow or Deny list can be one of:
   - An IP address
   - A comma-separated list of IP addresses
   - A range of IP addresses specified as ip-address/subnet-mask (for example, 192.168.100.197/255.255.255.0) or in CIDR format (for example, 192.168.100.0/24)

     The CIDR entry that matches all IP addresses is 0.0.0.0/0.

2. Click Add.

Removing entries from an Allow or Deny list

Changes you make to either list of IP addresses take effect immediately.

1. To remove a single entry, click the delete control ( ) for that entry.
2. To remove all entries, click Delete All.

Disabling Prometheus

Disabling Prometheus removes the current configuration settings, disables Alertmanager, and halts collection of HCP performance metrics.

To disable Prometheus on HCP nodes, you need an administrator or security role.
CAUTION:
Disabling **Prometheus** deletes all monitoring data that has been collected.

1. From the System Management Console main menu, select Monitoring > Prometheus.
2. To disable Prometheus, clear the Enable Prometheus option.
3. Click Update Settings.
4. Select the I Understand check box, and then click Update Settings.

HCP performance metrics collected by Prometheus

Performance metrics provide information about the different operations of an HCP component.

Prometheus server and Alertmanager provides high availability by running on two storage nodes in the cluster: the node with the highest IP address and the node with the second highest IP address. If one of these nodes become unavailable, Prometheus server switches to the other node. If both the nodes become unavailable, you cannot collect or view metrics until one of the nodes become available again.

If you permanently remove a node running a Prometheus server from the system, HCP starts a replacement Prometheus server on another node. Prometheus metrics collection continues even if one node running the Prometheus server goes down. In this situation, HCP automatically connects to the second node to retrieve metrics. Both the nodes remain active at all times. The replacement server synchronizes its historical metrics data with the other active node running the Prometheus server. If HCP can’t start one or both of the

Prometheus or Alertmanager servers, it creates a system event to indicate that the server is unavailable. This situation could occur if the volume storing the metrics runs out of space, forcing the Prometheus server to shutdown.

Prometheus collects performance metrics in the following categories:

- Gateway metrics
- Storage metrics
- Node metrics
- Replication metrics
- Event metrics
- Services metrics

After you upgrade to HCP v9.6 or later versions and enable Prometheus, all the collectors are enabled by default and HCP begins collecting performance metrics. However, if the filesystem storing the Prometheus TSDB reaches or exceeds 95% of its total capacity, the filesystem will become read-only and Prometheus will stop collecting metrics until there is sufficient disk space.

The following table describes the performance metrics collected by Prometheus.
Note: In the following table, the instance label refers to the node from where the HCP performance metrics is collected.

Metric	Description	Label
disk_transfers_per_second	The speed at which data can be transferred between the node and the disk drives.	instance, disk_name, job
gateway_operation_latency_milliseconds_count	Count of gateway operations.	instance, tenant, request_code, response_code, interface, namespace
gateway_operation_latency_milliseconds_bucket	Count of gateway operations by bucket based on the latency in milliseconds. Valid values must be less than or equal to the one of the following values: • 10 milliseconds • 1000 milliseconds • 1 second • 10 seconds • infinity	instance, tenant, request_code, response_code, interface, namespace
gateway_operation_latency_milliseconds_sum	Sum of the latency of gateway operations in milliseconds.	instance, tenant, request_code, response_code, interface, namespace
gateway_operation_size_bytes_sum	Sum of the size of the gateway operations in bytes.	instance, tenant, request_code, response_code, interface, namespace
gateway_operation_size_bytes_bucket	Count of gateway operations by bucket based on size in bytes. Valid values must be less than or equal to one of the following values: • 1000 (1K) • 100000 (100K) • 10000000 (10M) • 1000000000 (1G) • infinity	instance, tenant, request_code, response_code, interface, namespace
gateway_operation_size_bytes_count	Count of gateway operations.	instance, tenant, request_code, response_code, interface, namespace
http_connections	Count of HTTP connections.	instance
https_connections	Count of HTTPS connections.	instance
http_connections_limit	Maximum number of supported HTTP connections on an HCP node. Note: The `http_connections_limit` setting specifies the maximum number of concurrent connections that can be made to a server. The number of connections can exceed the HTTP connections limit. The queue size may not be limited, but it can grow.	instance
https_connections_limit	Maximum number of supported HTTPS connections on an HCP node. Note: The `https_connections_limit` setting specifies the maximum number of concurrent connections that can be made to a server. The number of connections can exceed the HTTPS connections limit. The queue size may not be limited, but it can grow.	instance

Metric	Description	Label
replication_objects_pending	Count of objects pending for replication.	instance, link_name
replication_bytes_pending	Count of bytes pending for replication.	instance, link_name
replication_operations_per_second	Count of replication operations per second.	instance, link_name
replication_errors_per_second	Count of errors per second during replication.	instance, link_name
replication_bytes_per_second	Count of bytes per second during replication.	instance, link_name
cpu_utilization	Percentage of time that a process on an HCP node is using the CPU.	instance, space (user, system)
cpu_io_wait_percentage	Percentage of time that the CPU was idle with an outstanding I/O request.	instance
disk_io_kilobytes_per_second	Count of disk I/O per second in kilobytes.	instance, io_type (read, write), disk_name
disk_utilization	Percentage of time that the disk was utilized on an HCP node.	instance
network_io_bytes_per_second	Network I/O rate in bytes per second.	instance, io_type (read, write), interface (back-end, front-end, management)
network_io_bytes_per_second_limit	Limit of the network I/O rate in bytes per second.	instance, interface (back-end, front-end, management)
primary_storage_bytes	Size of primary storage in bytes.	instance, capacity used (physical) total
s_series_storage_bytes	Size of an HCP S Series storage in bytes.	instance, capacity (physical_used, logical_used (from this HCP), total)
s_series_network_bandwidth_bytes	Size of S Series Node network bandwidth in bytes.	name, capacity (used, total)
s_series_cpu_utilization	Amount of time that the process is using the CPU of S Series Node.	name
configured_storage_bytes	Storage configured per tenant in bytes. Note: This value is calculated for each tenant.	capacity (used, total), tenant
volume_storage_bytes	Size of storage volume in bytes.	name, capacity (used, total)
stored_objects	Count of objects stored.	instance, tenant
tsdb_storage_bytes	The disk usage capacity of Prometheus TSDB	instance, capacity, job Note: In this scenario, the instance label appears only on nodes with the highest and second-lowest IP addresses.
replication_up_to_date_as_millis	The date and time that a task was added to the backlog.	instance, link_name, job
scrape_duration_seconds	The time took to collect the metrics from the system.	instance, job
system_events_total	The count of system events by severity level. It is a measure of the number of system events that have occurred, grouped by severity level.	instance, severity, job
system_events_created	The timestamp when a unique combination of this metric's labels was first scraped. It is the date and time that the metric was first collected with the specified labels.	instance, severity, job
scrape_samples_post_metric_relabeling	The number of samples remaining after metric relabeling was applied.	instance, job
scrape_samples_scraped	Number of samples exposed to target.	instance, job
scrape_series_added	The approximate number of new series in this scrape.	instance, job
network_io_kilobytes_per_second	The amount of data that is transferred over the network in one second.	instance, io_type, interface, job

Metric	Description	Label
network_io_kilobytes_per_second_limit	The maximum amount of data that is allowed to be transferred over the network in one second.	instance, interface, job
replication_bytes_pending_remote	Replication remote byte pending. The number of bytes that are waiting to be replicated to a remote system.	instance, link_name, job
replication_objects_pending_remote	The number of objects that are waiting to be replicated.	instance, link_name, job
replication_objects_verified	The number of replicated objects that have been successfully verified.	instance, link_name, job
service_events_total	Count of service events per object.	action, instance, job, service

Services metrics

Starting with HCP v9.7, HCP enhances Prometheus metrics collection to include support for the metrics of the following services. Executing any of these services will increment the metrics based on the action performed.

All the following services tracks the count of these three common metrics: `objectsExamined`, `objectsServiced`, and `objectsUnableToService`. The following list summarizes each service, its description, and any additional service-specific metrics it collects.

- **Capacity balancing:** Assesses the storage level for each node. If there's a significant disparity in storage levels across nodes, the service redistributes objects to achieve a more balanced state. It measures the number of objects moved across nodes for balancing. In addition to the three common metrics, it also tracks the count of `bytesMoved` during these balancing operations. You must manually start this service.
- **Compression:** Compresses object data to optimize HCP storage space utilization. It adheres to the active service schedule and tracks metrics such as total bytes saved by compression, percentage of storage saved, and the number of objects or object parts compressed. In addition to the three common metrics, it also tracks the count of `objectsCompressed`, `objectsDecompressed` and `objectEncryptionStateChanged`.
- **Content verification:** Detects and rectifies corrupted data and metadata discrepancies. It follows the active service schedule and measures the number of objects serviced, including those repaired or deemed irreparable. In addition to the three common metrics, it also tracks the count of `ObjectWithDeletedCustomMetadata`.
- **Disposition:** Hides expired object data and its metadata and marks them for deletion. By default, it's disabled at the system level and operates based on the active service schedule. Metrics include the number of expired objects marked for deletion.
- **Duplicate elimination:** Increases available storage space by merging data associated with identical objects. It runs according to the active service schedule and quantifies the number of duplicate objects or parts merged. In addition to the three common metrics, it also tracks the count of `bytesDupEliminated` and `duplicateFiles`.
- **Garbage collection:** Identifies and deletes hidden objects or parts marked for deletion by deleting objects and cleaning up transaction logs. It measures the number of objects deleted.
- **Protection:** Ensures repository stability by maintaining a specified data redundancy level (DPL) for each object. It operates based on the active service schedule and specific events, tracking the number of objects serviced.
- **Scavenging:** Ensures metadata integrity by verifying and repairing metadata. It operates per the active service schedule, measuring the number of objects serviced, including those with repaired or unrepaired metadata.
- **Storage tiering:** Moves copies of objects among defined storage tiers and manages object copies within each tier. It operates based on the active service schedule and tracks metrics related to object movement and storage tier adjustments. In addition to the three common metrics, it also tracks the count of `objectsMovedToCloud`, `objectsMovedToMO`, `objectsMovedToTOU`, `objectsMovedToRU`, `objectsMovedToSDU`, `objectsEncryptionCompressionStateFixed`, `legacyObjectCompressionEncryptionStateFixedInRemoteCloud`, and `legacyObjectCompressionEncryptionStateFixedInSnode`.
- **HCP S Series balancing:** Redistributes objects to achieve a balanced state by evaluating storage levels across nodes within a pool. It adheres to the active service schedule and measures the number of objects moved across S nodes for balancing. In addition to the three common metrics, it also tracks the count of `bytesExamined`, and `bytesServed`.

Configuring email notification

You can configure each email recipient to receive notification of only selected messages based on the message importance, severity, and type. Message severity levels are notice, warning, and error. Message types are general, security, and compliance. In all cases, HCP makes a best effort to send the applicable email in a timely manner.

Recipients are added to the blind carbon copy (bcc) list for each email, so the recipients of an email are not visible to one another. The To list remains empty.

You can configure the content of the email that HCP sends. For example, you could choose to have HCP send the full text, severity, and date and time, and node number for each log message. Or, if you're concerned about exposing system tenant and namespace information in what is by nature an insecure medium, you could format the email to say only that a log message was recorded.

HCP writes messages to the log about email that the email server fails to accept. The messages about failed email are not sent to email recipients.

You use the Email page in the System Management Console to enable and configure email notification.

To display the Email page, in the top-level menu of the System Management Console, select Monitoring > Email.

Note: To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

Enabling email notification

You can configure HCP to send email about log messages.

To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

1. On the Email page, select Enable email notification.
2. Specify the email server through which you want HCP to send email.
3. Optionally, test the email server settings.
4. Optionally, change the format of the email to be sent.

5. Specify one or more recipients to receive email about log messages.

Specifying the email server

You can specify the email server through which you want HCP to send email about log messages.

To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

1. On the Email page, click SMTP Settings.
2. In the SMTP Settings panel:
   a. In the Host field, type the host name or IP address that you want HCP to use to connect to the email server.
   b. In the Port field, type the port on which the email server listens for email messages.
   c. In the Security field, select the security protocol used by the email server (SSL or STARTTLS) or None if the email server doesn't use a security protocol.
   d. If the email server is configured to require authentication, select Authenticated.
      - Then, in the Username field, type the user name for an email account that's authorized to establish the connection between HCP and the email server.
      - In the Password field, type the password for the email account. If you have previously set a password and you leave the password field empty, the previously set password is replaced by no password.
3. Optionally, test the email server settings.
4. In the SMTP Settings panel, click Update Settings.

Testing the connection to the email server

Testing causes HCP to send an email to an address that you specify. This email comes from the email address specified in the From field in the Message Settings section on the Email page. The email subject is "`Test email from HCP.`"

To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

1. On the Email page, in the Test Email Notification window, type the email address to which you want HCP to send the test email.
2. Click Send.

Constructing the email message template

The content of the email messages HCP sends is determined by the message template specified in the Message Settings section on the Email page. You can modify this template at any time. The Message Preview section shows a sample email that uses the current template.

The email template has three fields, each of which can be filled in with any combination of plain text and email template variables:

- The From field specifies the content of the email From line. This field must have a value. That value must have the form of a valid email address.

  Some email servers require that the value in the From line be an email address that is already known to the server.

- The Subject field specifies the content of the email Subject line. This field must have a value.

  For the email template subject, plain text can include spaces but not line breaks or tabs.

- The Body field specifies the body of the email. This field is optional.

  For the email template body, plain text can include spaces and line breaks but not tabs. The character sequence consisting of a backslash (\) followed by a lowercase n creates a line break.

Modifying the template HCP uses for email notification about log messages

To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

1. On the Email page, in the From, Subject, and Body fields in the Message Settings section, specify the values that you want to use.
2. Optionally, click Preview to preview the sample email with the specified format in the Message Preview field.
3. Click Update Settings at the bottom of the page.

Email template variables

The values you specify in the From, Subject, and Body fields in the email template can include variables that correspond to the information available for each log message (for example, the severity of the event that triggered the message or the short description of the event). When sending email, HCP replaces the variables in the email message with the applicable information.

To include a variable in the email template, you specify the variable name preceded by the dollar sign ($). A dollar sign followed by anything other than a variable name is displayed as a dollar sign in the email HCP sends.

The following table lists the variables you can use in the email template:

Variable	Description
$action	The action to take in response to the message
$date	The date and time at which the event occurred (for example, Wed Feb 8 2012 3:15:57 PM EST)
$fullText	The full text of the message
$id	The message ID
$location	The fully qualified name of the HCP system on which the event occurred (for example, hcp-ma.example.com)
$origin	For user-initiated events, the IP address from which the event request was sent and the port through which HCP received the event request, separated by a colon (for example, 192.168.152.181:8000)
$reason	The reason why HCP issued the message
$scope	
$severity	The severity of the event that triggered the message

Variable	Description
$shortText	A brief description of the event that triggered the message
$type	The type of message (General, Security, or Compliance), preceded by Important and a comma if the message is important (for example, Important, Security)
$user	The user ID and username of the event initiator (for example, 105ff38f-4770-4f98-b5b3-8371ab0af359 lgreen)

Restoring the default template

The following table shows the format of the default email template.

Field	Default value
From	log@$location
Subject	[$severity] $shortText
Body	The following event occurred on $date: $fullText Reason: $reason Action: $action Details: User: $user Origin: $origin

Changing the email template back to the default

To view the Email page, you need the monitor, administrator, security, or compliance role. To configure email notification and test the connection to the email server, you need the administrator or security role.

1. On the Email page, click Reset.
2. Optionally, click Preview to preview the sample email with the default format in the Message Preview field.
3. Click Update Settings at the bottom of the page.

Specifying email recipients

You use the Recipients section on the Email page to specify the email addresses to which HCP sends email about log messages. HCP sends email as blind carbon copies, so email recipients are not visible to one another.

Each row in the Recipients section contains one or more email addresses and indicates which messages are sent to those addresses. The section can have at most 25 rows.

Because each row in the Recipients section can contain multiple email addresses, you can specify a total of more than 25 addresses in this section. However, HCP sends each email only to an arbitrary 25 of the addresses that are supposed to receive the email. For example, if 34 email addresses are supposed to receive email about log messages that are important and have a severity level of error and a type of general, HCP sends such email only to 25 of those addresses.

You can add, modify, and delete rows in the Recipients section at any time.

Understanding the recipients list

Each row in the Recipients section specifies:

- One or more email addresses.
- Whether to send email only about important log messages (Major) to the specified email addresses or to send email about all log messages (All).
- The severity of the log messages about which to send email:

  Notice
  : tells HCP to send email about log messages with a severity level of notice, warning, or error.

  Warning
  : tells HCP to send email about log messages with a severity level of warning or error.

  Error
  : tells HCP to send email only about log messages with a severity level of error.

- Whether to send email about general log messages ( ). General log messages are all messages that do not have a type of security or compliance.
- Whether to send email about log messages with a type of security ( ).
- Whether to send email about log messages with a type of compliance ( ).

Email recipients receive email only about log messages that have all the selected properties.

Adding, modifying, and deleting rows in the recipients list

To add, modify, and/or delete rows in the recipients list, on the Email page:

1. Take one or more of these actions:
   - To add a row:
     a. Optionally, in the Recipients field, type a comma-separated list of one or more well-formed email addresses.
     b. Click Add.

        A new row appears in the recipients list with importance set to Major, severity set to Error, and only general selected as the type. The row is highlighted in green.

        To remove the new row, click the delete control ( ) for the row.

- To modify a row:
  - Optionally, in the Address field, type additional well-formed email addresses and/or modify or delete existing addresses. This field must contain at least one well-formed email address and no incorrectly formed addresses.
  - Optionally, change the properties based on which HCP sends email to the specified addresses.

    If you deselect all the types, no email is sent to the specified addresses.
- To delete a row, click the delete control ( ) for the row.

  The row turns red. To undo the deletion, click again on the delete control.

2. Click Update Settings at the bottom of the page.

Monitoring resources

You use the Resources page in the HCP System Management Console to monitor the use of system resources. The information on this page can help you determine the causes of system issues such as slowed responses to client read and write requests or abnormal conditions reported in the system log.

The Resources page uses graphs to show statistics about the use of these resources over time:

- CPU
- Local logical volumes
- Memory
- Front-end, back-end, and, if it is enabled, management networks

The graphs let you analyze trends across individual storage nodes and compare node performance to the performance of the system as a whole. The graphs are coordinated with each other, allowing you to easily view the use of multiple resources during the same time period. Additionally, the Resources page can display the HCP system log, so you can correlate resource usage with system events.

The graphs let you analyze trends across individual storage nodes and compare node performance to the performance of the system as a whole. The graphs are coordinated with each other, allowing you to easily view the use of multiple resources during the same time period. Additionally, the Resources page can display the HCP system log, so you can correlate resource usage with system events.

To display the Resources page, in the top-level menu of the System Management Console, select Monitoring > Resources.

Note: To view the Resources page, you need the monitor or administrator role.

About the resource usage graphs

HCP uses System Activity Reporter (SAR) data as the basis for resource usage reporting. SAR is a utility that runs on each node in the HCP system. Every ten minutes, SAR records statistics representing the average use of various resources in the node during the past ten-minute interval. The graphs on the Resources page in the System Management Console show these statistics for a subset of those resources.

For the CPU, memory, and network resources, the graphs can show either the average of the SAR statistics across all storage nodes or this average along with the SAR statistics for an individual storage node. For the logical volume resource, the graphs can show can show the SAR statistics only for an individual logical volume.

CPU

CPU statistics provide information about the processing load on the HCP system. HCP reports CPU statistics in these graphs:

CPU Usage
: This graph shows both the percent of CPU capacity used by the operating system kernel (OS in the graph legend) and the percent of CPU capacity used by HCP processes (HCP in the graph legend).

CPU IO Wait
: This graph shows the percent of CPU capacity spent waiting to access logical volumes that are in use by other processes.

These two statistics together equal the total processing load on the system.

If CPU usage is consistently high across all nodes and system performance is degraded, the namespace application workload may be too heavy for the system to handle efficiently. In this case, you may need to add nodes to the system or upgrade the existing nodes to nodes with greater CPU capacity.

If CPU usage is high on a recurring basis, check the system log to see whether the high CPU usage correlates with recurring events such as services running. If the high usage correlates with services running, you may want to change the service schedule.

High CPU usage on only a small number of nodes may mean that applications are repeatedly using the same IP addresses to access the system. In this case, you may want to suggest to tenant administrators that their applications use DNS or some other mechanism to help balance the workload across all the nodes in the system.

Consistently high CPU IO wait with low CPU usage may mean that HCP cannot access the system storage fast enough to keep up with application demand. In this case, you may need to add storage to the system so that attempts to access storage are spread across a larger number of logical volumes.

In an HCP with SAN-attached storage system with spindown storage, high IO wait on nodes with logical volumes that can be spun down may indicate that these volumes are being spun up frequently. Check the LUN Utilization graph for the load on spindown volumes. If the load is high, you may want to redefine service plans to have a longer wait time before objects are moved to spindown storage. To see which logical volumes are spindown volumes, check the Hardware page in the System Management Console.

A brief period of high CPU IO wait that corresponds to increased workload does not necessarily indicate a problem.

Logical volumes

Logical volume usage statistics provide information about the load on storage managed by HCP. These statistics are available only for individual logical volumes. HCP reports logical volume usage statistics in these graphs:

LUN Read/Write
: This graph shows the number of blocks read from the logical volume per second and the number of blocks written to the logical volume per second.

LUN Utilization
: This graph shows the usage of the communication channel between the operating system and the logical volume as a percent of the channel bandwidth.

The way logical volumes are used depends on the HCP system configuration. Some logical volumes can store only objects, some can store only the metadata query engine index, and some can store both. Additionally, in an HCP with SAN-attached storage system, some logical volumes may used for spindown storage. How you interpret the statistics in the logical volume usage graphs is partly dependent on the these factors.

High read, write, and access values for all logical volumes along with low CPU usage may mean that the HCP system storage has insufficient bandwidth to support its workload. In this case, you may need to add storage to the system to spread read and write operations across more logical volumes.

High read and write rates for some but not all logical volumes may mean that the distribution of objects across the nodes in the system is uneven. To verify that this is the case, check the logical volume usage statistics on the Hardware page in the System Management Console. To resolve the issue, submit a request to your authorized HCP service provider to run the Capacity Balancing service to bring the object distribution to a more balanced state.

Memory

HCP reports on memory usage in the Memory Swap graph. This graph shows the number of pages swapped out of memory per second.

Typically, the page-swap rate for an HCP system is less than one page per second. A consistently high page-swap rate may indicate that the system has insufficient memory to handle its workload. In this case, you may need to add nodes to the system, add memory to the existing nodes, or upgrade existing nodes to nodes with more memory to resolve the issue.

Networks

Network statistics provide information about bandwidth usage on the front-end, back-end, and, if it is enabled, management networks used by the HCP system. HCP reports network statistics in these graphs:

Front-end Network
: This graph shows the number of bytes read from the node per second and the number of bytes written to the node per second over the front-end network. These are the total numbers of bytes across the [hcp_system] network and all user-defined networks.

Back-end Network
: This graph shows the number of bytes read from the node per second and the number of bytes written to the node per second over the back-end network.

Management Network
: This graph shows the number of bytes read from the node per second and the number of bytes written to the node per second over the management network. These are the total numbers of bytes across the [hcp_management] network. The management network graph is only shown if the network is enabled.
Note: The amount of back-end network traffic generated by any given namespace is directly related to the ingest tier DPL defined for the namespace by its service plan. The higher the ingest tier DPL, the more back-end network traffic the namespace creates.

Heavy traffic (greater than 120 MB per second) on both the front-end and back-end networks may mean that the HCP system has insufficient bandwidth to accommodate its workload. In this case, you may need to add nodes to the HCP system to increase the available bandwidth.

Heavy front-end traffic on some nodes, but not all of them, may indicate one of the following problems:

- The HCP subdomain is not correctly configured in your DNS.
- Applications are repeatedly using the same IP addresses to access the system. In this case, you may want to suggest to tenant administrators that their applications use DNS or some other mechanism to help balance the workload across all the nodes in the system.

Heavy back-end traffic on some but not all nodes may mean that the distribution of objects across the nodes in the system is uneven. To verify that this is the case, check the logical volume usage statistics on the Hardware page in the System Management Console. To resolve the issue, submit a request to your authorized HCP service provider to run the Capacity Balancing service to bring the object distribution to a more balanced state.

Managing the resource usage graphs

To manage the resource usage graphs on the Resources page, you can:

- Choose which graphs to display
- Choose whether the graphs show information about an individual node or all nodes
- Zoom in to more easily see the individual data points in the graphs
- Select a time for which you want to know the resource usage details
- Specify the time period you want to see in the graph windows
- Scroll left and right to change the time period shown in the graph windows

Switching graphs

The Resources page shows four graphs at a time. By default, the page shows these graphs: CPU Usage, CPU IO Wait, Back-end Network, and Front-end Network. At any time, you can change which graphs are shown.

To switch one graph for another, in the title bar of the graph you want to switch, click the icon for the graph you want. The graph icons are:

- (%) - CPU Usage
- (IO) - CPU IO Wait
- (r/w) - LUN Read/Write
- (%) - LUN Utilization
- (M) - Memory Swap
- (F) - Front-end Network
- (B) - Back-end Network
- (M) - Management Network

Setting the scope

The CPU, memory, and network graphs can show statistics for all nodes or for an individual node along with the statistics for all nodes. The logical volume graphs can show statistics only for an individual volume and only while a node is selected for display in the other graphs.

To set the scope of the information shown in the graphs, select either All Nodes or the node you want in the field above the top right graph. The selection applies to all the graphs.

To set the logical volume for a logical volume graph, while an individual node is selected for display, select the volume you want in the field in the graph title bar. The selection applies only to that graph.

Zooming

The graphs on the Resources page can show resource usage statistics for at most 30 days (or fewer if the system was installed less than 30 days ago). However, the longer the time period shown, the harder it is to see short-term changes in resource usage.

You can zoom in on the graphs to more easily see the individual data points in them. Zooming in changes the time period visible in each graph but does not change the height of the graphs. You can zoom in until the visible time period is one day. You can zoom out until the visible time period is 30 days.

Zooming affects all the graphs equally.

To zoom in, click the plus control ( ) above the top left graph.

To zoom out, click the minus control ( ) above the top left graph.

After each zoom action, the zoom controls are momentarily grayed.

Setting the amount by which zooming increases or decreases

You can set the amount by which zooming increases or decreases the visible time period each time you zoom.

To view the Resources page, you need the monitor or administrator role.

1. On the Resources page, click the edit control ( ) above the top left graph.
2. In the Modify Zoom and Scroll Settings window, select one of these in the Zoom Settings section:

   Incremental zoom
   : to increase or decrease the visible time period by a factor of two each time you zoom in or out

   Maximum zoom
   : to decrease the visible time period to one day when you zoom in or to increase the visible time period to 30 days (or fewer if the system was installed less than 30 days ago) when you zoom out

3. Click Update Settings.

Viewing details for a point in time

In each resource usage graph, a vertical line serves as a time marker. The marked time is displayed in the middle above the graphs. The graph legends show the detailed resource usage statistics for the marked time.

To show detailed statistics for a different time, you reposition the time marker. The time marker is always in the same location in all the graphs, so when you reposition it in one graph, it changes in all.

To reposition the time marker, click in the graph at the point in time to which you want the marker to move.

Specifying a time period

Above the resource usage graphs, the Resources page displays the start time of the currently visible time period on the left and the end time on the right. By default, when you open the page, the graphs show statistics for 30 days (or fewer if the system was installed less than 30 days ago), ending with the day of the most recently recorded SAR data.

You can change the time period shown in the graphs by selecting new start and end dates. The time period you specify can be at most 30 days. This time period applies to all the graphs.

HCP keeps SAR data for 180 days. As a result, the start date you specify cannot be more than 180 days in the past.

You can change the time period shown in the resource usage graphs.

To view the Resources page, you need the monitor or administrator role.

1. On the Resources page, click the calendar control ( ) above the top left graph.
2. In the Modify Date Range window, in the From field, specify the start date for the time period you want the graphs to cover. If you leave this field blank, the graphs use a start date of 30 days before the date specified in the To field (or fewer if the system was installed less than 30 days ago).
3. In the To field, specify the end date for the time period you want the graphs to cover. If you leave this field blank, the graphs use an end date of 30 days after the date specified in the From field (or fewer if the From date is less than 30 days ago).

   In both fields, you can specify the date in either of these ways:

   - Click the calendar control ( ) next to the applicable field and select the date you want.
   - Type the date you want, in this format: m/d/y

     In this format, m is the one- or two digit month, d is the one- or two-digit day, and y is the two- or four-digit year.

     You can specify values in either or both of the From and To fields. You cannot leave both fields empty.

4. Click Update Settings.

Scrolling

You can scroll left and right in the resource usage graphs to shift the time period that's visible in the graphs. Scrolling affects all graphs equally.

To scroll left to see an earlier time period, click the left arrow ( ) above the top left graph.

To scroll right to see a later time period, click the right arrow ( ) above the top left graph.

To scroll right or left to see the time period with the currently marked time in the middle, click the vertical line ( ) above the top left graph.

After each scroll action, the scroll controls are momentarily grayed.

Setting the percent by which scrolling shifts the visible time period

You can set the percent by which scrolling shifts the visible time period each time you scroll left or right.

To view the Resources page, you need the monitor or administrator role.

1. On the Resources page, click the edit control ( ) above the top left graph.
2. In the Modify Zoom and Scroll Settings window, select one of these in the Scroll Settings section:

   Move left/right by 25%

to shift the visible time period by 25% each time you scroll left or right.

Move left/right by 50%

to shift the visible time period by 50% each time you scroll left or right.

Move left/right by 100%

to shift the visible time period by 100% each time you scroll left or right.

3. Click Update Settings.

Viewing system log messages on the Resources page

To display the HCP system log on the Resources page, click Logs at the bottom of the page.

When the Logs section opens, the message at the top of the list is the most recently recorded message before the end of the time period shown in the graphs.

Generating chargeback reports

You can generate chargeback reports from the HCP System Management Console. A *chargeback report* contains current and historical usage statistics for HCP tenants and their namespaces. For each chargeback report, you specify the start and end dates of the *report period*, which is the time period that's covered by the report, and select the *reporting interval*, which determines whether HCP generates hourly, daily, or total statistics for the specified report period.

Chargeback reports are a good source of information for system analysis, enabling you to adjust storage and bandwidth allocations based on usage patterns. These reports can also serve as input to billing systems that need to determine charges for capacity and bandwidth usage at the tenant or namespace level.

Chargeback reports cover only HCP tenants and their namespaces. They do not include the default tenant or its namespace.

About chargeback reports

A chargeback report contains aggregated namespace statistics for each HCP tenant that's defined on the HCP system. For any given tenant, the total number of reads shown for a specific reporting interval is the total number of read operations that occurred during that interval in all the namespaces owned by that tenant.

Chargeback reports also contain aggregated HCP-tenant statistics for the HCP system as a whole. For example, the total number of reads for an HCP system shown for a specific reporting interval is the total number of successful read operations that occurred during that interval in each namespace that's owned by each HCP tenant that's defined on the HCP system. System statistics shown in chargeback reports do not include usage data for the default tenant and namespace.

For any HCP tenant that has granted system-level administrative access to itself, chargeback reports also contain statistics for the individual namespaces owned by that tenant.

When generated from the System Management Console, chargeback reports are in CSV format. Each line in a report contains the values for one namespace, for one tenant, or for the entire HCP system during a specific reporting interval (that is, during a specific hour, during a specific day, or during the entire report period).

If a chargeback report includes the namespaces that are owned by a tenant, the lines for those namespaces are ordered alphabetically below the lines for that tenant. The lines for the HCP system are at the end of the report. Multiple lines for a tenant, a namespace, or the HCP system are ordered in ascending chronological order.

Generating a chargeback report

When generating a chargeback report, you need to specify the report period and the reporting interval.

To specify the *report* period, you select start and end dates. The report period starts at 12:00:00 a.m. on the start date (shown as 00:00:00) and ends at 11:59:59 p.m. on the end date.

The earliest start date you can specify is either 30 days earlier than the current date or the date when the HCP system was installed (if the system was installed less than 30 days ago). The latest end date you can specify is the current date.

You can use the same date as the start date and the end date for a report period. In this case, the report period starts at 12:00:00 a.m. on the specified date and ends at 11:59:59 p.m. on that date.

The *reporting interval* you select determines whether the report contains hourly, daily, or total statistics:

- An *hourly report* contains one set of statistics for each hour in the report period for which statistics are available.

  If the report period starts on the day when the HCP system was installed, the first set of statistics in the report covers the time the system first came online through the end of the last minute in that hour. For example, if the system came online at 2:30:20 p.m. on July 25th and the report period starts on July 25th, the first set of statistics in the report covers 2:30:20 p.m. through 2:59:59 p.m. on July 25th.

  If the report period ends on the current day, the last set of statistics in the report covers the time from the start of the current hour to the time when you requested the report. For example, if you request an hourly report at 2:30:15 p.m., the last set of statistics in the report covers 2:00:00 p.m. through 2:30:15 p.m. on the current day.

- A *daily report* contains one set of statistics for each day in the report period, where a day is defined as the period from 12:00:00 a.m. through 11:59:59 p.m. on any given date.

  If the report period starts on the day when the HCP system was installed, the first set of statistics in the report covers the time the system first came online through the end of the last minute on that day. For example, if the system came online at 2:30:20 p.m. on July 25th and the report period starts on July 25th, the first set of statistics in the report covers 2:30:20 p.m. through 11:59:59 p.m. on July 25th.

  If the report period ends on the current day, the last set of statistics in the report covers 12:00:00 a.m. on the current day to the time when you requested the report. For example, if you request a daily report at 2:30:15 p.m., the last set of statistics in the report covers 12:00:00 a.m. through 2:30:15 p.m. on the current day.

- A *total report* contains one set of statistics for the entire report period.

  If the report period starts on the day when the HCP system was installed, the statistics in the report cover the time the system first came online either through 11:59:59 p.m. on the last day of the report period or through the time when you requested the report on the currrent day.

  For example, if the system came online at 2:30:20 p.m. on July 25th and, on August 7th, you request a total report with a start date of July 25th and an end date of August 7th, the statistics in the report cover 2:30:20 p.m. on July 25th through 2:50:25 p.m. on August 7th.

  Statistics collected for the current hour may not include some reads and writes that have already occurred during the hour. After the hour is over, however, the statistics collected for it are complete.

  Tip: You can use the HCP management API to generate chargeback reports that cover time periods that are longer than one month and are in XML, JSON, or CSV format. You can use this feature to create applications that generate chargeback reports at regular intervals and feed those reports to a billing system.

Generating a chargeback report

To generate a chargeback report, you need the monitor or administrator role.

1. In the top-level menu of the System Management Console, select Monitoring > Chargeback.
2. On the Chargeback page select the reporting interval for the type of storage usage report that you want to generate, and specify the start and end dates for the report period, in the Reporting Interval field, select Hour, Day, or Total to generate an hourly, daily, or total storage usage report, respectively.
3. Use the Start Date field to specify the start date of the report period.
   - Enter the start date in the text field in mm/dd/yyyy format.
   - Click the calendar icon to display a monthly calendar. Then use the arrows at the top of the calendar to navigate to the month containing the start date that you want to define for the report period, and click that date to select it.
4. Use the End Date field to specify the end date of the report period.
   - Enter the end date in the text field in mm/dd/yyyy format.
   - Click the calendar icon to display a monthly calendar. Then use the arrows at the top of the calendar to navigate to the month containing the end date that you want to define for the report period, and click that date to select it.
5. To generate and download a complete, detailed chargeback report, click Download Report.

   By default, the name of the downloaded report file is Hourly-Chargeback-Report.csv, Daily-Chargeback-Report.csv, or Monthly-Chargeback-Report.csv, as applicable.

Chargeback statistics collection

Chargeback statistics either reflect a specific point in time or are dynamic. Point-in-time statistics are measurements taken at the end of a reporting interval, such as the used storage capacity for a namespace at the end of an hour. Dynamic statistics are measurements, such as the number of reads or writes to a namespace, that are accumulated over time.

HCP accumulates dynamic statistics on an hourly basis, starting at the beginning of each hour. So, for example, one statistic might represent the number of successful writes to a namespace that occurred between 11:00:00 and 11:59:59. Another might represent the number of successful writes to the same namespace that occurred between 12:00:00 and 12:59:59.

Chargeback report content

The first line of a chargeback report contains identifiers for the values in the subsequent lines. The following table describes each of these values and indicates whether it is point in time (P) or dynamic (D).

Identifier	Type	Value
bytesIn	D	The total number of bytes successfully written to the given namespace, to any of the namespaces owned by the given tenant, or to any of the HCP namespaces in the HCP system during the reporting interval. The total number of bytes written includes all parts uploaded for multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload. If data was compressed before being transmitted, this is the number of bytes before compression.
bytesOut	D	The total number of bytes read from the given namespace, from any of the namespaces owned by the given tenant, or from any of the HCP namespaces in the HCP system during the reporting interval. If data (including XML for directory listings) was compressed before being transmitted, this is the number of bytes before compression.
deleted	N/A	One of: true The namespace or tenant was deleted after the statistics in the set were collected. false The namespace or tenant currently exists. included For a tenant or the HCP system, the statistics in the set include values for one or more namespaces that were subsequently deleted.
deletes	D	The total number of delete and purge operations successfully performed in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system during the reporting interval. A delete of a multipart object counts as a single delete operation. The count of delete and purge operations does not include automatic deletions of replaced parts, parts of aborted multipart uploads, or unused parts of completed multipart uploads.
endTime	N/A	The end time of the reporting interval for the set of statistics in the line, in the same format as is used for the startTime value.
erasureCoded Objects	P	The total number of erasure-coded objects and erasure-coded parts of multipart objects currently stored in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
ingestedVolume	P	The total size of the stored data and custom metadata, in bytes, before the data and custom metadata were added to the given namespace, to any of the namespaces owned by the given tenant, or to any of the HCP namespaces in the HCP system.
metadataOnly Bytes	P	The total number of bytes of object data currently not stored for metadata-only objects in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
metadataOnly Objects	P	The total number of objects that are currently metadata-only in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system. A multipart object that is metadata-only counts as a single object.

Identifier	Type	Value
multipartObject Bytes	P	The total number of bytes of object data in all the parts of multipart objects currently stored in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
multipartObject Parts	P	The total number of parts of multipart objects currently stored in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
multipartObjects	P	The total number of multipart objects currently stored in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
multipartUpload Bytes	P	The total number of bytes of object data in all the successfully uploaded parts of multipart uploads that are currently in progress in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system. This number does not include bytes of data in replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.
multipartUpload Parts	P	The total number of successfully uploaded parts of multipart uploads that are currently in progress in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system. This number does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.
multipartUploads	P	The total number of multipart uploads that are currently in progress in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system.
namespaceName	N/A	The name of the namespace to which the set of statistics in the line applies. In lines that contain tenant or systemwide statistics, this field has no value.
objectCount	P	The number of objects in the given namespace in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system. Each version of an object counts as a separate object. The object count does not include object versions that are *delete markers* or *delete records*. A delete marker is a special version of an object that indicates that a version of the object has been deleted. A delete marker has a version ID but does not have any data or metadata. For more information on delete markers and delete records please see *Enabling delete markers* section in Versioning. Each multipart object counts as a single object. Objects that are in the process of being created by multipart uploads are not included in the object count.
reads	D	The total number of read operations performed in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system during the reporting interval. A read of a multipart object counts as a single read operation.
startTime	N/A	The start time of the reporting interval for the set of statistics in the line, in this format: yyyy-MM-ddhh:mm:ss hh is hours on a 24-hour clock. For example: 2017-10-07 14:32:47
storageCapacity Used	P	The total number of bytes of primary running storage occupied by stored data for the given namespace, for all the namespaces owned by the given tenant, or for all the HCP namespaces in the HCP system. This includes object data, system and custom metadata, and any redundant data required to satisfy the applicable service plan. Used storage capacity also includes storage occupied by the parts of in-progress multipart uploads that have already been written to HCP. Used storage capacity does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.
systemName	N/A	One of: • The name of the domain associated with the data access network for the tenant that owns the namespace to which the set of statistics in the line applies • The name of the domain associated with the data access network for the tenant to which the set of aggregated statistics in the line applies • The name of the domain associated with the [hcp_system] network for the HCP system to which the set of aggregated statistics in the line applies
tenantName	N/A	Either: • The name of the tenant that owns the namespace to which the set of statistics in the line applies • The name of the tenant to which the set of statistics in the line applies In lines that contain systemwide statistics, this field has no value.
tieredBytes	P	Total number of bytes of object data currently stored on primary spindown storage (if the system includes spin down storage), on HCP S Series, or on extended storage for the given namespace, for all the namespaces owned by the given tenant, or for all the HCP namespaces in the HCP system. On HCP S Series only, the total number of bytes includes parts of in-progress multipart uploads regardless of whether the upload of the part has finished. This number does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed

Identifier	Type	Value
		multipart uploads.
tieredObjects	P	The total number of objects with data currently stored on primary spindown storage (if the system includes spindown storage), on HCP S Series, or on extended storage for the given namespace, for all the namespaces owned by the given tenant, or for all the HCP namespaces in the HCP system. Each part of a multipart object counts as a separate object and, on HCP S Series only, each part of an in-progress multipart upload counts as a separate object.
valid	N/A	The status of the set of statistics in the line. Possible values are: true HCP successfully collected all statistics in the set. false The statistics in the set do not reflect all the activity that occurred during the reporting interval. This may be due, for example, to one or more nodes being unavailable during that time, to a network failure, or to other hardware issues.
writes	D	The total number of write operations successfully performed in the given namespace, in all the namespaces owned by the given tenant, or in all the HCP namespaces in the HCP system during the reporting interval. Each upload of a part for a multipart upload counts as a separate write operation. This applies even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Sample chargeback report

Here's an example of a daily chargeback report, where the report was requested for February 17, 2017, through February 18, 2017. The report shows statistics for the canada and europe tenants. Because system-level users have administrative access to the europe tenant, the report also shows statistics for the individual namespaces owned by the europe tenant. The report is shown as it would appear in a spreadsheet.

systemName	tenantName	namespaceName	startTime	endTime	objectCount	IngestedVolume	storageCapacityUsed	bytesIn	bytesOut	reads	writes	deletes	tieredObjects
hcp.example.com	canada		2/17/2017 0:00:00	2/17/2017 23:59:59	15	276947364	276947364	206315331	247634	6	15	0	0
hcp.example.com	canada		2/18/2017 0:00:00	2/18/2017 23:59:59	27	297791424	318572455	91476093	64387	2	27	0	0
hcp.example.com	europe	finance	2/17/2017 0:00:00	2/17/2017 23:59:59	6	134243721	134270976	123986263	87561	1	10	0	0
hcp.example.com	europe	finance	2/18/2017 0:00:00	2/18/2017 23:59:59	15	186496747	186548224	52253026	0	0	12	0	0
hcp.example.com	europe	hr	2/17/2017 0:00:00	2/17/2017 23:59:59	7	9609368	9621504	9609368	0	0	7	0	0
hcp.example.com	europe	hr	2/18/2017 0:00:00	2/18/2017 23:59:59	15	19707387	19730432	10098019	0	0	8	0	0
hcp.example.com	europe		2/17/2017 0:00:00	2/17/2017 23:59:59	13	143853089	143892480	133595631	0	0	17	0	0
hcp.example.com	europe		2/18/2017 0:00:00	2/18/2017 23:59:59	30	206204134	206278656	62351045	0	0	20	0	0
hcp.example.com			2/17/2017 0:00:00	2/17/2017 23:59:59	28	420800453	420839844	339910962	335195	7	32	0	0
hcp.example.com			2/18/2017 0:00:00	2/18/2017 23:59:59	57	503995558	524851111	153827138	64387	2	47	0	0

Chargeback page graphs

The Chargeback page contains four graphs. These graphs how information about the usage of the HCP system during the past 30 days (or since HCP was installed if that was less than 30 days ago).

The graphs are:

Writes (bytes)
: Shows the number of bytes of data written to the HCP system.

The number of bytes written includes all parts written for multipart uploads regardless of whether the upload of the part has finished, the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Writes (operations)
: Shows the number of successful write operations that targeted the HCP system.

Each upload of a part for a multipart upload counts as a separate write operation. This applies even if the part was subsequently replaced, the multipart upload was aborted, or the part was not used in the completed multipart upload.

Reads (bytes)
: Shows the number of bytes of data read from the HCP system.

Reads (operations)
: Shows the number of read operations that targeted the HCP system.

A read of a multipart object counts as a single read operation.

Checking the status of your nodes

You can use the node status command to check the status of a target node in your HCP system. Any user can perform the node status command. System-level users with the administrator role can enable and disable the node status API.

The request to check the status of a node requires a URL specifying the front-end IP address of the target node. You enter the command in the following format:

```
http://node-front-end-ip-address/node_status
```

You can also request node metrics to be returned with the node HTTP status return code. To request node metrics, you additionally need to:

- Specify a *type* URL query parameter with a value of metrics.
- Specify the *format* URL query parameter with a value of xml or json.

If you omit the format parameter, you are only returned a response status code.

Request-specific return codes (node status)

The following table describes the HTTP return status codes that can be returned from a node status request.

Code	HTTP status	Description
204	OK	Node is configured to return node status
403	Forbidden	The HCP node status check returns a 403 forbidden message for the following reasons: • The system administrator has not enabled node status through the System Management Console. • The HCP system does not have a load balancer or the system administrator has not added the load balancer IP address to the Security Console Allow list.
540		System is in Read Only mode
541		Node is not available

Response body (node status)

The following table describes the properties included in the node status metrics.

Property name	Data type	Description
httpConnections	integer	The number of HTTP connections.
cpuUser	float	The percentage of CPU capacity used by HCP processes.
cpuSystem	float	The percentage of CPU capacity used by the operating system kernel.
iowait	float	The percentage of CPU capacity spent waiting to access logical volumes that are in use by other processes.
swapout	float	The average number of pages swapped out of memory per second.
id	float	The volume name.
blocksRead	float	The average number of blocks read from the logical volume per second.
blocksWrite	float	The average number of blocks written to the logical volume per second.
diskUtilization	float	The usage of the communication channel between the operating system and the logical volume as a percent of the channel bandwidth.
frontendBytesRead	float	The average number of bytes read from the node per second over the front-end network.
frontendBytesWrite	float	The average number of bytes written to the node per second over the front-end network.
backendBytesRead	float	The average number of bytes read from the node per second over the back-end network.
backendBytesWrite	float	The average number of bytes written to the node per second over the back-end network.
requestTimestamp	integer	The exact time that the timestamp request was issued in milliseconds.
metricsTimestamp	integer	The exact time that the metrics were collected in milliseconds.

Example: Retrieving node status

Here's a sample request that retrieves a return status code and node metrics for a node in the system. In this example, the target node IP address is 192.168.210.16 and the requested output format is JSON.

Request with cURL command line

curl -i http://192.168.210.16/node_status?type=metrics&format=json

Response headers

HTTP/1.1 200 OK

Response body in JSON

```
curl -i http://<node-ip>/node_status?type=metrics&format=json
curl -i -H "Accept: application/json" http://<node-ip>/node_status?type=metrics

    Response status code: 200
    Response body:
{
  "httpConnections" : "1",
```

```
  "cpuUser" : "0.47",
  "cpuSystem" : "0.58",
  "iowait" : "0.04",
  "swapout" : "0.00",
  "volume" : [ {
    "id" : "archive033",
    "blocksRead" : "0.00",
    "blocksWrite" : "0.27",
    "diskUtilization" : "0.00"
  }, {
    "id" : "archive034",
    "blocksRead" : "0.00",
    "blocksWrite" : "0.20",
    "diskUtilization" : "0.00"
  } ],
  "frontendBytesRead" : "0.08",
  "frontendBytesWrite" : "1.36",
  "backendBytesRead" : "0.75",
  "backendBytesWrite" : "0.71",
  "requestTimestamp" : "1510870948196",
  "metricsTimestamp" : "1510870801000"
}
```


Configuring the Hitachi Device Manager connection

With HCP with SAN-attached storage systems only, HCP can push information to Hitachi Device Manager (HDvM), so you can monitor and manage HCP along with your other Hitachi storage systems from a single console. You use the HDvM page in the HCP System Management Console to configure and test the connection between HCP and HDvM.

HCP supports IPv4 and IPv6 network connections to HDvM servers. However, HDvM support for IPv6 network connections varies based on the HDvM server operating system. For information about requirements for HDvM servers that support IPv6 networks, see the applicable Hitachi Command Suite documentation.

You can configure HCP to automatically push the information. You can also manually request a push at any time.

To display the HDvM page, in the top-level menu of the System Management Console, select Monitoring > HDvM.

To view the HDvM page, you need the monitor or administrator role. To configure the HDvM connection, you need the administrator role.

The HDvM page shows the date and time HCP last pushed information to HDvM and the HDvM response to that action. If the last attempt to push information was unsuccessful, the panel also shows the time of and response to the last successful push.

Note: A response message of "`Partial update`" may be the result of a transient error (for example, a LUN scan that hasn't finished yet). If you see this message, wait a few minutes. Then request the information push again. If you see this message repeatedly, contact your authorized HCP service provider for help.

For information about using HDvM, see the applicable HDvM documentation.

Configuring HCP to work with HDvM

To view the HDvM page, you need the monitor or administrator role. To configure the HDvM connection, you need the administrator role.

1. On the HDvM page of the System Management Console, to have HCP automatically push information to HDvM, select Enable scheduled updates to HDvM.
2. In the Device Manager Server field, type the host name or IP address that you want HCP to use to connect to HDvM.
3. In the Username field, type your username for logging in to HDvM.
4. In the Password field, type your password.

   If you're modifying the HDvM settings and you leave the Password field empty, the previously set password remains in effect.

5. In the Frequency field, select the frequency with which you want HCP to automatically update HDvM with new information.

   You can use the Send Now button on this page to force an update at any time.

6. Optionally, click Test to verify that HCP can contact HDvM with the settings you've specified.
   HCP displays a message at the top of the page indicating whether the test was successful. If it wasn't, correct the settings.

   You can use the Test button to test the HDvM connection at any time.

7. Click Update HDvM Settings.

Preparing and downloading health check reports

Health check reports provide information about the health status of the available nodes in your HCP cluster.

You can prepare and download health check reports using either the HCP System Management Console or the HCP management API.

Using the System Management Console to prepare and download health check reports

You can create health check reports on HCP nodes in a cluster that are running and available.

1. In the top-level menu of the System Management Console, select Monitoring > Health Check Reports.
   The Health Check Reports page is displayed.
2. (Conditional) If you recently prepared health check reports for download and the Download Health Check Reports button is enabled, you can download the reports if desired. Then click Cancel to reinitialize the Prepare Reports for Download pane.
3. In the Prepare Reports for Download pane:
   a. In the Start Date and End Date fields, enter or select a date range for the reports.
      The default values for these fields is the current day.
   b. (Optional) Enter a comment to include in the manifest.csv file that is included in the reports download archive.
4. Click Prepare Health Check Reports.

The HCP system runs a health diagnostic tool on the available system nodes. The tool runs various signatures to collect system health information. You do not need to remain on the Health Check Reports page while the report preparation is in progress.

After the health diagnostic tool finishes and the reports are prepared, status messages are displayed in the General Node Preparation Status pane in the Status column associated with each node, the checkboxes associated with each node for which the reports were successfully prepared are selected, and the Download Health Check Reports button is enabled.

5. Complete one of these actions:
   a. To download an archive that contains health check reports for all selected nodes, click Download Health Check Reports.
   b. To download an archive that contains a subset of the prepared reports, select only the checkboxes associated with the nodes for which you want to download reports. Then click Download Health Check Reports.

   The collected data is saved in a .zip archive. A system dialog box opens prompting you to save the file to a designated location.
6. Save the file.

Extract the contents of the .zip archive and the node-specific .tar archives to view the health check reports and manifest.csv file contents.

Health check reports archive contents

The HCP health check reports .zip archive contains the following contents:

- A manifest.csv file, which contains the optional comment that you might have added when you prepared the health check reports
- A separate .tar archive for each available node in the cluster

  Within each node-specific .tar archive:

  - In the /var/ris/retired folder, the health check reports .tar files corresponding to the date range you specified when you prepared the health check reports
  - In the /var/ris/logs/HealthCheckReport folder, the latest run of the health check report at the time you prepared the reports for the specified date range

Health check report signatures

When you prepare health check reports, the HCP system runs a health diagnostic tool on the available nodes in the cluster. This tool runs various signatures to collect information about the health of the HCP nodes.

Signatures are JSON files containing different shell commands that gather configuration information and collect data on potential issues related to the health of a node. Signatures are classified into *components* and *types* (*info* and *issue*).

Components include items such as replication, admin, or JVM. Info signatures collect node configuration information such as memory configuration, HCP version, hot fixes, and other HCP configurations. Issue signatures report if a node either is experiencing a certain issue or is at risk of experiencing an issue, such as server issues, object issues, repeated node restarts, or other general issues.

Example: Signature that provides information about disk errors

The following sample health check report signature provides information about specific disk errors on an HCP system. The output format is a JSON file.


```
{
    "name": "DiskErrors",
    "description": "Get the disk errors",
    "issueId": "N/A",
    "component": "Operating System",
    "executionTime": 15,
    "modifiedDate": "July 28, 2020 5:57:26 PM",
    "product": "Hitachi Content Platform",
    "signatureType": "GeneralIssue",
    "hcpVersion": "9.2.0",
    "signatureStatus": "NotMatched",
    "runMode": "online",
    "steps": [
      {
        "stepId": "1",
        "command": "cat /var/log/messages | grep -iE \u0027(error|scsi|unexpected|failure|conflict)\u0027 ",
        "expectedOutputCommand": "if [[ $(grep -i [A-Z] \"%s\" | wc -l) -gt 0 ]]; then  echo true; fi",
        "logTrace": "",
        "signatureMatched": false,
        "executionTime": 15,
        "timedOut": false,
        "stepExecutionFailure": "No Error",
        "timeOutMillis": 10000
      }
    ]
}
```


Licensing

A license specifies the amount of storage and the HCP features that you can use. The storage can either be on HCP and S Series Nodes or on an extended storage tier. Licenses are available for all system configurations (HCP with internal storage, HCP with SAN-attached storage, and HCP Virtual Machine).

All HCP systems are required to have a basic license or a premium license. A newly installed system comes with a default basic license and a default extended license. The default basic license lets you use two terabytes of HCP system and S Series Node storage. The default extended storage license lets you tier two terabytes of data to extended storage. You can request to have other licenses added when your configuration is installed.

If a basic, premium, or extended storage license is exceeded or expires, a warning message is displayed on the System Management Console Overview page under System Status. Monitoring mechanisms such as syslog, system log messages, and SNMP send reminders every twenty-four hours asking the system administrator to upload a new storage license. You must get a new basic license or premium license to increase your storage capacity. You must get a new extended license to increase your tiering capacity.

In HCP with internal storage systems with a data protection level (DPL) of two, object copies do not take up storage license space. For example, if you have two terabytes of DPL 2 objects, you have used only one terabyte of your storage license.

If the HCP system serial number changes, you must upload a new license with an updated serial number.

Viewing a License

To view your licenses, go to Storage > Licenses page of the System Management Console. From there, you can monitor your current license and the license history.

Note: You need the administrator or monitor role to access Storage > Licenses.

The page contains the following information about your current license:

- Type: the type of license that is used. The possible types are:
  - Basic
  - Premium
  - Extended
- HCP system serial number: Is the serial number for the HCP system.
- Capacity: the amount of storage capacity that the license provides.
- Remaining: the amount of storage capacity on the license that is unused.
- Expiration date: the date that the license expires. There may not be an expiration date.
- Status: describes the current state of the storage license. The possible values are:
  - OK: The storage license has not been exceeded or expired.
  - Storage license has expired: The storage license is out of date. Even if the storage license capacity hasn't been exceeded, a new license needs to be uploaded if the current one expires.
  - Storage license is not a valid license for this system: The storage license serial number does not match the HCP system serial number. This only occurs if the HCP system serial number changes during an upgrade, but, if it happens, a new license with an updated system serial number must be uploaded.
  - Usage has exceeded license capacity: The storage capacity of the basic, premium, or extended license has been exceeded. If the storage space of a license has been exceeded, a new license with a larger amount of storage capacity must be uploaded to replace the current one.

The License History panel keeps a record of all licenses uploaded to the system. If a license is uploaded, expires, is in danger of being exceeded, or is exceeded, the event is visible in the License History panel. Click any event in the panel to see more information about it.

Uploading a license

To upload a storage license, you need the administrator role.

To upload a new storage license:

1. On the Storage > Licenses page, click Add License.
2. In the Add license wizard window, in the Enter license key below field, type your license key string.
3. Click Next.
4. Review your license information.
5. Click Finish.

Licenses and Features

The following table show the features that can be used under the basic and premium licenses. The extended license does not provide extra functionality.

Feature	License	
	Basic	Premium
Data-at-rest encryption	✓	✓
Using cloud protocols (REST, S3 compatible)	✓	✓
Content authenticity	✓	✓
Creating custom metadata	✓	✓
The ability to have 10,000 namespaces	✓	✓
Storage management	✓	✓
Content repair service	✓	✓
Content verification service	✓	✓
Scavenging service	✓	✓
Local data protection	✓	✓
Global replication	✓	✓
Object versioning	✓	✓
Storage quotas	✓	✓
Object compression	✓	✓
Object migration (automated technology refresh)	✓	✓
Access control lists	✓	✓
IPv6 VLAN	✓	✓
Using the management API	✓	✓
Duplicate elimination service	✓	✓
Metadata query engine		✓
Creating more than one tenant		✓
Generating chargeback reports		✓

Feature	License	
	Basic	Premium
Creating virtual networks		✓
Configure tenant logging and alerting through Syslog, snmp, SMTP		✓
System and tenant level branding		✓
Using WebDAV		✓
Using CIFS		✓
Using NFS		✓
Using SMTP		✓
Using the namespace compliance log		✓
Tenant privileged delete log		✓
Holding objects		✓
Object retention		✓
Disposition service		✓
Shredding service		✓
Metadata only replication plan		✓
SAN storage zero copy failover		✓

Troubleshooting

From the system console for any HCP node, you can run selected diagnostics that can help with analyzing and resolving issues with interactions between the node and other components in the HCP environment.

Additionally, HCP maintains internal logs that can help support personnel resolve problems. Using the System Management Console, you can insert messages into these internal logs. For example, you can insert messages that describe conditions that could indicate a problem with the HCP system. If problems occur with the HCP system, you can download the internal logs into a single file, which you can then send to your HCP support center.

This chapter:

- Describes the available diagnostics and explains how to run them
- Contains instructions for marking and downloading the HCP internal logs

Running diagnostics

You can run selected diagnostics on the nodes in an HCP system to help analyze and resolve issues related to interactions between the nodes and other components in the HCP environment. The available diagnostics let you:

- Ping a specified device (ping)
- Display the network path being used for communications between the node and a specified device (traceroute)
- Query the DNS for the records that match a specified IP address or domain name (dig)
- Display the routing table for the node (route)
- Display the NFS exports table for a specified device (showmount)
- On HCP with SAN-attached storage systems, display information about the logical volumes that are mapped to the node on the Fibre Channel SAN arrays (fchbainfo)
- Display the ethtool command output command for both front-end interfaces (ethtool)

You run diagnostics from the system console for a node. To use the system console, you need a keyboard and monitor.

To run diagnostics, you use the Appliance Diagnostics menu. To display this menu in the system console, press Alt+F8.

```
Appliance Diagnostics
=====================================
  [1] ping       - Check Network Connectivity
  [2] traceroute – Check Routing
  [3] dig        - Check DNS Resolution
  [4] route      - List the Kernel Routing Table
  [5] showmount  - Show Exports from NFS Servers
  [6] fchbainfo  - List Fibre Channel HBA and LUN Mapping Information

  [c] clear      - Clear the Screen and Redisplay the Menu

Enter a selection:
```

To run diagnostics from the Appliance Diagnostics menu:

- To execute a diagnostic command, enter the option number for that command. If the command requires an argument, HCP prompts you to enter a valid value for that argument. HCP then executes the command and displays the results on the screen.
- To cancel a command before it finishes, press Ctrl+C.
- If the information displayed in response to a command is longer than the space available on the screen, use Shift+PgUp and Shift+PgDn to scroll the display up or down, respectively.
- To return to the Appliance Diagnostics menu after viewing the information displayed by a command, press Enter.
- To clear the screen and redisplay the Appliance Diagnostics menu at the top, use option c from the menu.
- To return to the console login prompt from the Appliance Diagnostics menu, press Alt+F1.

In addition to being displayed on screen, the results of each diagnostic command that you execute are sent to the syslog servers that you specify on the Syslog page in the HCP System Management Console.

For more information about the diagnostic commands that you can execute from the Appliance Diagnostics menu, see the man pages for the commands on a Linux system.

ping

The ping command pings a device that you identify by IP address or fully qualified domain name (FQDN). You might run this diagnostic, for example, to determine whether the node you're on can communicate with a specific DNS server, external time server, or external storage device.

The ping command pings the specified device 10 times, displaying the result of the ping each time. However, if the device is unreachable, the command displays only the summary of the ping attempts after the 10 tries.

To execute the ping command:

1. From the Appliance Diagnostics menu, enter 1.
   A prompt for an IP address or FQDN appears.

   ```
   This command tries to ping (count=10) an address or FQDN.
   Please enter the address or FQDN:
   ```

2. Enter the target device IP address or FQDN.
   The results of the ping command are displayed on the screen.
3. After viewing the display, press Enter to return to the Appliance Diagnostics menu.
   The following is a sample response to the ping command:

   ```
   Pinging 172.20.33.40...

   PING 172.20.33.40 (172.20.33.40) 56(84) bytes of data.
   64 bytes from 172.20.33.40: icmp_req=1 ttl=63 time=0.331 ms
   64 bytes from 172.20.33.40: icmp_req=2 ttl=63 time=0.443 ms
   64 bytes from 172.20.33.40: icmp_req=3 ttl=63 time=1.93 ms
   64 bytes from 172.20.33.40: icmp_req=4 ttl=63 time=2.20 ms
   64 bytes from 172.20.33.40: icmp_req=5 ttl=63 time=3.23 ms
   64 bytes from 172.20.33.40: icmp_req=6 ttl=63 time=5.28 ms
   64 bytes from 172.20.33.40: icmp_req=7 ttl=63 time=0.247 ms
   64 bytes from 172.20.33.40: icmp_req=8 ttl=63 time=0.254 ms
   64 bytes from 172.20.33.40: icmp_req=9 ttl=63 time=2.87 ms
   64 bytes from 172.20.33.40: icmp_req=10 ttl=63 time=4.38 ms

   --- 172.20.33.40 ping statistics ---
   10 packets transmitted, 10 received, 0% packet loss, time 9008ms
   Rtt min/avg/max/mdev = 0.247/2.120/5.287/1.732 ms
   ```

traceroute

The traceroute command displays the network path through which the node you're on communicates with a device that you identify by IP address or FQDN. You might run this diagnostic, for example, if communication between the node and another device, such as a DNS server, is taking longer than expected.

For each pair of points in the network path, the traceroute command displays the round-trip time between the two points for each of three probes. You can use this information, for example, to determine whether the network topology is configured correctly.

To execute the traceroute command:

1. From the Appliance Diagnostics menu, enter 2. A prompt for an IP address or FQDN appears.

   ```
   This command tries to trace routing to an address or FQDN.
   Please enter the address or FQDN:
   ```

2. Enter the target device IP address or FQDN. The results of the traceroute command are displayed on the screen.
3. After viewing the display, press Enter to return to the Appliance Diagnostics menu.
   The following is a sample response to the traceroute command:

   ```
   Traceroute to 192.168.100.45 (192.168.100.45), 30 hops max, 60 byte packets
    1  172.20.43.253 (172.20.43.253)  0.286 ms  0.368 ms  0.425 ms
    2  2001:0db8::101 (2001:0db8::101) 0.531 ms 0.604 ms 0.669 ms
    3  192.168.100.45 (192.168.100.45)  0.339 ms  0.343 ms  0.330 ms
   ```

dig

The dig command queries the DNS for records that match an IP address or FQDN that you specify. You might run this diagnostic with an HCP domain name, for example, if you have user-defined networks that are not working as expected.

When you execute the dig command, you are prompted for arguments. Although you can specify any dig command arguments, this document describes only IP addresses and FQDNs.

To execute the dig command:

1. From the Appliance Diagnostics menu, enter 3. A prompt for dig command arguments appears.

   ```
   This command runs dig with he arguments you provide.

   Enter dig arguments:
   ```

2. Enter one of these arguments:
   - *-x* followed by an IP address (for example, *-x 172.20.33.40*)
   - An FQDN
3. In response to the confirming prompt, enter y to confirm your entry or n to try again. When you enter y, the results of the dig command are displayed on the screen.
4. After viewing the display, press Enter to return to the Appliance Diagnostics menu.
   The following is a sample response to the dig command with the argument hcp.example.com:

```
;<<>> DiG 9.7.4-P1-RedHat-9.7.4-2.P1.fc14 <<>> hcp.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49028
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
; hcp.example.com IN        A

;; AUTHORITY SECTION
hcp.example.com. 825 IN     NS      hcp.example.com
hcp.example.com. 825 IN     NS      hcp.example.com
hcp.example.com. 825 IN     NS      hcp.example.com
hcp.example.com. 825 IN     NS      hcp.example.com

;; ADDITIONAL SECTION:
d9-014.hcp.example.com. 825 IN A    172.20.37.14
d9-015.hcp.example.com. 825 IN A    172.20.37.15
d9-016.hcp.example.com. 825 IN A    172.20.37.16
d9-017.hcp.example.com. 825 IN A    172.20.37.17
```

Route

The route command displays the routing table for the node you're on. This table shows the subnets that the node belongs to. The information for each subnet includes the subnet mask and the network interface. For the [hcp_system] network (shown as default) and the network used for replication, the subnet information also includes the network gateway IP address.

This diagnostic is useful, for example, for exposing network connectivity problems such as missing interfaces. If you've created multiple networks in HCP, the display from the route command should show the subnet and interface for each network for which the node has an IP address.

To execute the route command:

1. From the Appliance Diagnostics menu, enter 4.
   The results of the route command are displayed on the screen.
2. After viewing the display, press Enter to return to the Appliance Diagnostics menu.
   The following is a sample response to the route command:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.20.43.254   0.0.0.0         UG    0      0        0 eth0
132.17.10.0     *               255.255.255.0   U     0      0        0 eth0.0010
Link-local      *               255.255.0.0     U     1002   0        0 eth0
Link-local      *               255.255.0.0     U     1003   0        0 eth1
172.20.42.0     *               255.255.254.0   U     0      0        0 eth0
172.21.52.0     *               255.255.255.0   U     0      0        0 eth1
```

showmount

The showmount command displays the NFS exports table for a device that you identify by IP address or FQDN or for the node you're on. You might run this diagnostic, for example, to check whether shares associated with external storage volumes are properly exported on the external storage device.

Each line in the exports table shows a path that can be mounted by other devices. For an HCP node, the exports table includes the paths to namespaces for which the NFS protocol is enabled.

To execute the showmount command:

1. From the Appliance Diagnostics menu, enter 5.
   A prompt for an IP address or FQDN appears.

   ```
   This command runs 'showmount -e' for the node you specify by address or FQDN.
   Please enter the address or FQDN:
   ```

2. Enter the target device IP address or FQDN. For the FQDN of the node you're on, use localhost.

   The results of the showmount command are displayed on the screen.

3. After viewing the display, press Enter to return to the Appliance Diagnostics menu.

   The following is a sample response to the showmount command:

   ```
   Export list for 172.20.43.150:
   /hcp_shares/share2 172.20.43.151
   /hcp_shares/share1 172.20.43.151
   ```

fchbainfo

For HCP with SAN-attached storage systems only, the fchbainfo command displays information about the logical volumes that are mapped the node you're on for all the Fibre Channel SAN arrays to which the node is connected. You might run this command, for example, to diagnose issues with zero-copy failover.

The information displayed by the fchbainfo command is broken out by HBA port. For each logical volume that maps to the port, the display includes the volume number and size.

To execute the fchbainfo command:

1. From the Appliance Diagnostics menu, enter 6.
   The results of the fchbainfo command are displayed on the screen.
2. After viewing the display, press Enter to return to the Appliance Diagnostics menu.

   The following is a sample response to the fchbainfo command:

```
General Fibre Channel Host Adapter Information:
04:00.0 Fibre Channel: Emulex Corporation Zephyr-X LightPulse Fibre Channel Host
 Adapter (rev 02)
04:00.1 Fibre Channel: Emulex Corporation Zephyr-X LightPulse Fibre Channel Host
 Adapter (rev 02)

Host Adapter Information for ID: 0
Adapter Type: Emulex LPe11002-M4-H FV2.82A4 DV8.3.25
HBA Port WWN: 0x10000000c973d7a2
        Maps to Remote Port: 0x200b00051e7f1649
        Maps to Remote Port: 0x21fc00051e7f1649
        Maps to Remote Port: 0x50060e8010252593
              SCSI Device:0:0:0:0   Block Device:sda
              Vendor:HITACHI   Model:DF600F   Size:31GB
                        Partition: sda2   Size: 1MB
                        Partition: sda3   Size: 3GB
                        Partition: sda4   Size: 1KB
                        Partition: sda5   Size: 2GB
                        Partition: sda6   Size: 2GB
                        Partition: sda7   Size: 11GB
                        Partition: sda8   Size: 11GB
              SCSI Device:0:0:0:1   Block Device:sdb
              Vendor:HITACHI   Model:DF600F   Size:104GB
              SCSI Device:0:0:0:129   Block Device:sdh
              Vendor:HITACHI   Model:DF600F   Size:104GB
              SCSI Device:0:0:0:130   Block Device:sdi
              Vendor:HITACHI   Model:DF600F   Size:104GB
              SCSI Device:0:0:0:192   Block Device:sdj
              Vendor:HITACHI   Model:DF600F   Size:52GB
              SCSI Device:0:0:0:193 Block Device:sdk
              Vendor:HITACHI   Model:DF600F   Size:52GB
              SCSI Device:0:0:0:2   Block Device:sdc
              Vendor:HITACHI   Model:DF600F   Size:104GB
              SCSI Device:0:0:0:64   Block Device:sdd
              Vendor:HITACHI   Model:DF600F   Size:52GB
              SCSI Device:0:0:0:65   Block Device:sde
              Vendor:HITACHI   Model:DF600F   Size:52GB

Host Adapter Information for ID: 3
Adapter Type: Emulex LPe11002-M4-H FV2.82A4 DV8.3.25
HBA Port WWN: 0x10000000c973d7a3
        Maps to Remote Port: 0x200b00051e80a7ff
        .
        .
        .
```

ethtool

The ethtool command displays information about the NIC parameters and device drivers for both front-end interfaces. You might run this command, for example, to diagnose issues with 10 gigabyte Ethernet network configurations.

To execute the ethtool command:

1. From the Appliance Diagnostics menu, enter 6.
   The results of the ethtool command are displayed on the screen.
2. After viewing the display, press Enter to return to the Appliance Diagnostics menu.

Working with HCP internal logs

In addition to the HCP system log, which is displayed in the System Management Console, HCP maintains internal logs. These logs record the processing activity of various components of the HCP system. If a problem with the system occurs, the internal logs can help HCP support personnel diagnose and resolve it.

Internal logs can be generated for both HCP General Nodes and HCP HCP S Series Nodes. The logs can be created separately for the two types of nodes or together.

There are four different types of logs. Each is responsible for capturing information about a different component of the HCP system. If you request logs for S Series Nodes, you get all of the S Series Node logs regardless of whether you selected specific log types for the HCP system.

At any time, you can insert a comment into the internal logs. You can use this capability, for example, to note unusual events that occur in the HCP system. This can later help support personnel understand the symptoms that indicate a possible problem. It can also help them determine when a problem started.

To help with troubleshooting, you can download the internal logs and send them to your HCP support center. For ease of handling, HCP downloads the logs into a single file.

HCP keeps internal logs for at most 90 days. You can download the logs for any length of time within that period. When taking this action, be sure to include all the days on which you observed problems with the system.

When downloading the logs, you can provide a message for the support center. This message should include a description of the problem, your contact information, the applicable case number (if one has been assigned), and any other information that can help support personnel resolve the problem.

Encryption for logs is disabled by default. In order to enable encryption contact your HCP support provider. If encryption is enabled, only HCP support personnel have the key required to decrypt the logs.

Important: Downloading the internal logs puts a heavy load on the HCP system. Do not take this action unless explicitly told to do so by HCP support personnel.

You use the Internal Logs page in the HCP System Management Console to insert comments into and download the HCP internal logs. To display this page, in the top-level menu of the System Management Console, select Monitoring > Internal Logs.

Adding a comment to the internal logs

To insert comments into the internal logs, you need the monitor, administrator, or security role. To download the HCP internal logs, you need the administrator role.

To insert a comment into the HCP internal logs:

1. On the Internal Logs page, click Mark Internal Logs.
2. In the Insert this message into the internal logs field in the Mark Internal Logs panel, type the comment text. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
3. Click Mark Internal Logs.

Downloading internal logs for one or more storage nodes

You can download the internal logs for both HCP General and S Series Nodes. For HCP S Series Node logs, you cannot choose what type of log to download; they are all downloaded at once. S Series Node logs appear in their own separate Storage Preparation Status panel. If the HCP system doesn't use S Series Nodes, this panel is not visible.

To prepare and download the HCP Software logs:

1. On the Internal Logs page, click Download Internal Logs to expand that section on the page.
2. In the Download Internal Logs section:
   a. Use the Start Date and End Date fields to specify the start and end dates for the time period for which you want to generate the internal logs. For the date format, use `mm/dd/yyyy`.
   Note: The time period for which HCP generates the internal logs includes the specified start and end dates.
   b. Optional) in the Insert this message into the internal logs field, type a message to be inserted into the logs before they're downloaded and to be included in the manifest that accompanies the downloaded logs. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
3. Click Prepare Internal Logs.
   HCP prepares the logs for downloading. During this process, in the Download Internal Logs panel, the active Prepare Internal Logs button changes to a grayed-out Download Internal Logs button, and the panel displays the Preparation Status table, which lists the nodes in the HCP system in numeric order (by node number), and reports on the status of the log preparation process on each node. You do not need to remain on the Internal Logs page during the log preparation process.
   Note: HCP can perform only one log preparation operation at a time.
   When HCP finishes preparing the logs, the node and S Series Node Preparation Status tables show the status of each node in the HCP system, and the checkboxes at the end of each row become selectable.
   Tip: If you want to prepare the logs again before you download them (for example, to prepare the logs for a different time period), click Cancel to reactivate the Prepare Internal Logs button.
4. In the Choose type of log for download panel, select the type or types of logs you want to download. The possible log types are:
   - Access: These logs capture all user requests related to the HTTP-based APIs (REST, S3 compatible, MAPI), such as object GET, PUT, and DELETE requests.
   - System State: These logs capture the current state of the HCP operating system and application states and provide useful information for diagnosing issues related to node restarts and unexpected service behaviors.
   - Service Procedure: These logs capture information about service procedures performed on HCP such as the add node procedure, upgrade procedure, or add LUN procedure.
   - HCP Software: These logs collect information about HCP software not listed in the other log types.
5. In the General Node Preparation Status panel, select the General Nodes you want to download logs for.
6. (Optional) if you have HCP S Series Nodes in your system, in the S Series Node Preparation Status panel, select the S Series Nodes you want to download logs for.
7. (Optional) Insert a message into the logs before downloading them:
   a. Click Mark Internal Logs to expand that section on the page.
   b. In the Insert this message into the internal logs field, type a message to be inserted into the logs before they're downloaded and to be included in the manifest that accompanies the downloaded logs. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
8. In the Download Internal Logs section, use the checkboxes in the last column in the Preparation Status table to select the nodes for which you want to download the internal logs:
   Note: By default, all nodes for which the logs were successfully prepared are automatically selected.
9. When you finish selecting the nodes for which you want to download the internal logs, click Download Internal Logs.
   HCP downloads the logs from the selected nodes and creates a .zip file that contains all of the internal logs for those nodes. For each selected node, HCP reports the progress of the log download in the Download Internal Logs panel.
   You do not need to remain on the Internal Logs page during this process
10. When prompted, save the .zip file containing the downloaded logs in the location of your choice.
    Note: If the System Management Console session times out due to inactivity before the prompt to save the file appears, the download fails. If this happens, increase the inactivity timeout interval; then try the download again..
11. Take one of these actions:
    - To create another .zip file that contains the internal logs you just generated for any or all of the HCP storage nodes, repeat Step 4 through Step 7 above.
      Note: You can perform any number of log download procedures for the time frame that you selected in Step 2, and you can download these logs for each node any number of times.
    - If you're finished downloading all of the internal logs you need, or if you need to prepare the logs again before downloading any additional logs, click Cancel.

      The Internal Logs page displays a success message and collapses the Mark Internal Logs and Download Internal Logs panels on the page.

System Management Console Alerts

The HCP System Management Console uses icons with hover text, called alerts, to provide high-level health status reports for specific elements of the HCP system and to identify problems that need your attention.

System Management Console alerts are displayed on the Overview, Hardware, Storage Node, Storage, Networks, Tenants, Domains and Certificates, and Authentication pages.

The Console uses two types of alert icons:

- System health icons: Indicate the current health of one or more elements of the HCP system, such as the metadata query engine or the power supplies for a storage node. These icons appear on the Overview, Hardware, Storage Node, Tenants, Domains and Certificates, and Active Directory pages. System health icons on the Overview, Storage Node, and Active Directory pages are also accompanied by text.
- Error and warning icons: Indicate error and warning conditions related to one or more elements of the HCP system. This type of icon appears only when an error or warning condition exists. These icons appear on the Storage and Networks pages.

This help section describes the alerts that can display on the Console pages and provides guidance on how to respond to alerts that indicate problems.

Overview page alerts

The System Management Console uses system health icons for alerts that appear on the Overview page. These alerts are described in the following table. The alerts are listed alphabetically by their hover text.

Abnormal temperature

IPMI sensors are detecting one or more nodes with temperature readings outside the recommended range.

Abnormal voltage

IPMI sensors are detecting one or more nodes with voltage readings outside the recommended range.

Active Directory certificates expire soon

One or more AD SSL certificates will expire within 90 days. If a certificate expires, communication with AD may fail.
To ensure that communication with AD is not disrupted, export a new SSL certificate from AD and upload it to HCP.

Active Directory certificates expire soon

One or more AD SSL certificates will expire within 30 days. If a certificate expires, communication with AD may fail.
To ensure that communication with AD is not disrupted, export a new SSL certificate from AD and upload it to HCP.

Active Directory secure connection issue

HCP could not communicate with AD due to a problem with the AD SSL server certificate uploaded to HCP.
Make sure that you have the correct certificate. Then upload the certificate again on the Active Directory page in the HCP System Management Console.
If the problem persists, contact your authorized HCP service provider.

AD credentials invalid

The credentials for the HCP computer account used to query AD for groups are invalid. Reconfigure support for AD on the Active Directory page in the HCP System Management Console.
The recommended procedure is to specify an HCP computer account that does not already exist in AD, thereby allowing the account to be created automatically.

AD partially configured

AD authentication is enabled only for the default namespace and is not currently supported for HCP namespaces. This can happen after an upgrade, where the CIFS protocol was enabled for the default namespace with AD authentication before the upgrade occurred.
To enable support for AD for HCP namespaces, enable HCP support for AD on the Active Directory page in the HCP System Management Console.

All metadata is intact

HCP policies have found no problems with object metadata.

All objects are intact

HCP services have found no problems with object data.

All *operation-types* operations are disabled

The indicated types of operations are currently not allowed. This alert appears when any permissions are disabled in the systemwide permission mask.

An unrecoverable error has occurred

HCP is experiencing a problem it cannot fix by itself.
Contact your authorized HCP service provider.

Back-end switch error

One or more back-end switches are not operating normally. contact your authorized HCP service provider.

BBU charging

For HCP with internal storage systems only, the battery backup unit in one or more nodes is charging.

BBU degraded; charging

For HCP with internal storage systems only, the battery backup unit in one or more nodes is charging.
The write-cache is disabled on those nodes.

BBU degraded; discharging

For HCP with internal storage systems only, the battery backup unit in one or more nodes is discharging.
The write-cache is disabled on those nodes.

BBU discharging

For HCP with internal storage systems only, the battery backup unit in one or more nodes is discharging.

BBU failed

For HCP with internal storage systems only, the battery backup unit in one or more nodes has failed.
The write-cache is disabled on those nodes.
If this alert appears for more than a few hours, contact your authorized HCP service provider.

BBU in learn cycle

For HCP with internal storage systems only, the battery backup unit in one or more nodes is in a learn cycle.
System performance may be temporarily degraded.

Below metadata protection level. Repairing...

Primary running storage contains too few copies of metadata for one or more objects.
The ingest tier metadata DPL defined for the namespace that contains each object is higher than the number of copies of metadata for that object currently found in primary running storage.
The Protection service is in the process of repairing this problem.

Broken fan

IPMI sensors are detecting one or more nodes or CB 320 server chassis with fan speeds outside the recommended range.

Cannot access Key Distribution Center

HCP cannot access the Key Distribution Center in the AD domain specified in the HCP AD configuration.
Check that both the AD domain controller and the network connection between HCP and that server are healthy.
If they both appear to be working properly, contact your authorized HCP service provider.

Cannot access LDAP server

HCP cannot access the LDAP server for the AD domain specified in the HCP AD configuration.
Check that both the LDAP server and the network connection between HCP and that server are healthy.
If they both appear to be working properly, contact your authorized HCP service provider.

Cannot communicate with chassis

The storage node specified in the CB 320 server chassis configuration cannot communicate with one or more chassis. Ensure that the chassis configuration is correct.
If it is, contact your authorized HCP service provider.

Cannot connect to AD server

HCP cannot connect to the server for the AD domain specified in the HCP AD configuration.
Make sure both the AD domain controller and the network connection between HCP and that server are healthy. Also make sure that AD is correctly configured in your DNS.
If the problem persists, contact your authorized HCP service provider.

CIFS AD access disabled

One of these conditions is true:

- The SPN attribute for one or more HCP nodes is missing from the AD domain.
- An internal error with the CIFS protocol occurred on one or more HCP nodes. In either case, reconfigure HCP support for AD on the Active Directory page in the HCP System Management Console.
-

If the problem persists, contact your authorized HCP service provider.

CIFS/NFS limit exceeded

The number of namespaces with the CIFS or NFS protocol enabled is above the maximum supported by HCP. System performance may be slower as a result.
If this is an issue, ask one or more tenant administrators to disable CIFS and NFS for one or more of their namespaces.

CIFS/NFS limit reached

The number of namespaces with the CIFS or NFS protocol enabled is at the maximum supported by HCP.
Enabling CIFS or NFS for additional namespaces may slow system performance.

Conflicting CIFS settings detected

One or more namespaces are configured for CIFS authenticated access only, but the system is not configured to support authenticated CIFS. As a result, CIFS cannot be used for access to those namespaces.

Either enable authenticated CIFS support for the system or have the tenant administrators reconfigure the affected namespaces to support both anonymous and authenticated access with CIFS.

Content verification repair disabled

The Content Verification service is currently not checking for or repairing objects with corrupted data.

This alert appears when Do not check and repair objects is selected on the Content Verification page.

Data access failover

For HCP with SAN-attached storage systems with zero-copy failover enabled, a node has taken over management of storage normally managed by another node. contact your authorized HCP service provider.

Degraded network assigned

One or more tenants are associated with a degraded network for management or data access purposes. A degraded network presents a single point of failure for clients accessing HCP over that network.

Check the Networks page for degraded networks that are associated with tenants. Then reconfigure each network to assign IP addresses to one or more additional nodes.

Empty network assigned

One or more tenants are associated with an empty network for management or data access purposes.

A tenant with an empty management network cannot be accessed through the Tenant Management Console or HCP management API.

Namespaces belonging to a tenant with an empty data access network are inaccessible.

Check the Networks page for empty networks that are associated with tenants. Then reconfigure each network to assign IP addresses to one or more nodes.

Erasure coding error

One or more of these conditions exist:

- The protection status of the active erasure coding topology is broken.
- The read status of an erasure coding topology is broken.
- One or more tenants added to an erasure coding topology have not been added to one or more replication links in the topology. HCP does not report this condition for a tenant until ten minutes after the tenant was added to the topology.
- HCP cannot find one or more replication links that are included in an erasure coding topology.

Erasure coding warning

One or more of these conditions exist:

- The protection status of the active erasure coding topology is vulnerable.
- The read status of an erasure coding topology is vulnerable.
- Replication is paused for one or more tenants on one or more replication links in the active erasure coding topology.
- The Geo-distributed Erasure Coding service is not in the active service schedule. New erasure coding activity is limited.
- The Geo-distributed Erasure Coding service is disabled. New erasure coding activity is limited.

Error spinning down volume

An error occurred while a logical volume was in the process of spinning down. contact your authorized HCP service provider.

Error spinning up volume

An error occurred while a logical volume was in the process of spinning up. contact your authorized HCP service provider.

Expired Active Directory certificates

One or more AD SSL certificates have expired. Communication with AD may fail.

To make sure communication with AD is not disrupted, export a new SSL certificate from AD and upload it to HCP.

Expired replication certificates

One or more trusted replication server certificates have expired. Replication with the systems from which the applicable certificates were obtained has stopped.

When the other system in any of the applicable replication pairs installs a new SSL server certificate, download that certificate and upload it to this system as a trusted replication server certificate.

For ease of maintenance, delete expired certificates from the list of trusted replication server certificates.

Expired SSL server certificate

One or more SSL server certificates for one or more HCP domains have expired.

If a domain has no valid certificates, clients must accept the invalid certificate presented by HCP for access to namespaces in that domain.

If the domain associated with the replication network has no valid certificates, replication fails.

Check the Domains and Certificates page to see which certificates have expired. Then make sure each affected domain has at least one valid certificate.

External storage volumes unavailable

One or more external storage volumes have a status of unavailable, broken, or initializing. Check the Storage page to see which volumes are having problems. Then make sure the devices hosting those volumes and the network connections to those devices are functioning properly.

Also make sure the exported shares are configured correctly, that any NFS servers being used are running on each device, and that any NFS security software on the device is not blocking access by any of the HCP nodes.

If the problem persists for a volume, remount the volume in HCP. If that doesn't resolve the problem, contact your authorized HCP service provider for help.

Front-end connection error

All front-end connections to one or more storage nodes are unavailable.

If this system is currently a source for replication, some objects will not be replicated.

If the system is a replication target, replication performance is degraded.

Full file system

One or more file systems have no more available space or no more available inodes. contact your authorized HCP service provider.

Hardware functioning properly

All of the HCP hardware is functioning normally.

HCP computer account missing

The HCP computer account is missing from the AD domain.

Reconfigure HCP support for AD on the Active Directory page in the HCP System Management Console.

HCP upgrade is in progress

The HCP software is being upgraded to a new release with the HCP system online (that is, without shutting down the system).

High load or swap

One or more nodes are experiencing a heavy load or a high rate of page swapping. contact your authorized HCP service provider.

IP mode mismatch

The system-level front-end network IP mode is Dual, but the [hcp_system] network is configured to use only IPv4 addresses or only IPv6 addresses.

Submit a request to your authorized service provider to set the system-level IP mode and set the [hcp_system] network IP mode, to provide support only for the type(s) of IP address you want to configure for user-defined networks.

Last HDvM update failed

The most recent attempt to push information to Hitachi Device Manager was unsuccessful. For details, check the HDvM page.

KM Server certificate expired

Certificate expired for the following KM Servers: <KM Server names>

KM Server unavailable

The following KM Servers are unavailable: <KM Server names>

KM Server has deactivated or compromised keys

Keys of the following KM Servers are compromised: <KM Server names>

Maximum namespaces exceeded

The number of namespaces defined in the HCP system is greater than the maximum number allowed.

This situation can happen if one or more HCP tenants being replicated to a given HCP system have namespace quotas on their source systems that cause the total number of allocated namespaces on the target system to exceed the number allowed for an HCP system.

While these tenants are included in their respective replication links, neither the actual number of namespaces they own nor their quotas count on the target system. However, if one or more of the tenants are removed from their links, the namespaces and quotas for those tenants then count on the target system. This can result in the total number of namespaces defined on the target system exceeding the total allowed for the system.

To ensure proper system operation, if the maximum number of namespaces allowed for the system is exceeded, you should lower the number of namespaces as soon as possible. To do this, one or more tenant administrators must delete one or more of their namespaces.

Maximum namespaces reached

The number of namespaces defined in the HCP system is the maximum number allowed.

Metadata balancing...

HCP is in the process of moving object metadata between nodes to achieve a more even distribution of the metadata.

Migration completing - balancing metadata

The Migration service has completed the process of copying objects during a data migration and is now in the process of moving metadata between the remaining nodes to achieve a more even distribution of the metadata.

Migration in progress

A data migration is in progress.

MQE index at 50%

The size of the metadata query engine index is 50 to less than 80 percent of either the maximum size allowed for the index or the actual space available for the index, whichever is less. HCP can no longer optimize the space used by the index.

As the index grows, responses to metadata query engine API requests will become slower, as will responses to searches in the Search Console when that Console is using the metadata query engine. Consider adding more storage capacity for the metadata query engine index.

If the index includes custom metadata, you can create more space for the index by deleting and then rebuilding the index with custom metadata indexing disabled.

MQE index at 80%; indexing disabled

The size of the metadata query engine index is 80 percent or more of either the maximum size allowed for the index or the actual space available for the index, whichever is less.

Metadata query engine indexing has stopped.

To enable indexing to continue, add more storage capacity for the metadata query engine index.

If the index includes custom metadata, you can create more space for the index by deleting and then rebuilding the index with custom metadata indexing disabled.

MQE index partially unavailable

At least one part of the metadata query engine index is unavailable.

As a result, indexing has stopped, the metadata query API does not support object-based queries, and, if the metadata query engine is selected for use with the Search Console, searches in that Console return an error.

This status can appear, for example, while an index-enabled logical volume is unavailable. When the situation is resolved, indexing resumes automatically.

MQE indexing unavailable

Metadata query engine indexing is disabled due to insufficient memory.

Increase the system memory either by adding storage nodes or by adding memory to existing storage nodes.

Multipath degraded to one

For HCP with SAN-attached storage systems configured with multipathing, the physical connection between a node and the SAN storage has failed

Contact your authorized HCP service provider.

Network error

One or more nodes are experiencing problems with one or more of their networks. Possible causes for this alert include:

- One or more physical network connections to one or more nodes are not working. Check the Storage Node page for each indicated node to see which network interfaces show errors. Then correct any problems with the applicable physical networks. If the networks appear to be working properly, contact your authorized HCP service provider.
- One or more network interfaces are missing in one or more nodes. Check the Networks page to see which networks have this problem. Then restart those networks. If the problem persists, contact your authorized HCP service provider.
- One or more nodes have one or more network interfaces for networks in which the nodes do not have IP addresses. Check the Networks page to see which networks have this problem. Then restart those networks. If the problem persists, contact your authorized HCP service provider.

Network warning

One or more nodes are experiencing problems with one or more of their networks. Possible causes for this alert include:

- The current MTU for one or more networks on one or more nodes does not match the configured MTU. If the problem is with a user-defined network, restart the network. If that doesn't resolve the problem, reboot the applicable nodes. If the problem persists, contact your authorized HCP service provider.
- The current speed of the [hcp_system] network on one or more nodes does not match the configured speed. contact your authorized HCP service provider. (This alert does not apply if the [hcp_system] network speed is set to auto.)
- The current speed of the [hcp_backend] network on one or more nodes is not the maximum speed possible for that network. contact your authorized HCP service provider.

No external time server configured

HCP is configured to use itself as a time server. For HCP to work with AD, HCP time must be within five minutes of AD time.

The recommended configuration is for HCP and AD to use the same external time server.

No Key Distribution Center found

HCP cannot find a Key Distribution Center for the AD domain specified in the HCP AD configuration. Ensure that AD is correctly configured in your DNS.
If the problem persists, contact your authorized HCP service provider.

No LDAP server found

HCP cannot find an LDAP server for the AD domain specified in the HCP AD configuration. Ensure that AD is correctly configured in your DNS.
If the problem persists, contact your authorized HCP service provider.

Nonreplicating object detected

One or more nonreplicating objects have been detected. The objects have either remained in the open state for too long or are irreparable.
If this occurs, contact your authorized HCP service provider.

Partial network assigned

One or more tenants are associated with a partial network for management or data access purposes. The load from client requests for access to those tenants or their namespaces is not being fully distributed across the nodes in the HCP system.
Check the Tenants page to see which tenants have partial networks. Then either reconfigure each network to assign IP addresses to all nodes in the HCP system, or select different networks for the affected tenants.

Partial network assigned to replication

The network selected for replication is a partial network. The load from replication activity is not being fully distributed across the nodes in the system.
Check the replication Settings page to see which network is selected for replication. Then either reconfigure that network to assign IP addresses to all nodes in the HCP system, or select a different network for replication.

Power supply failure

One or more power supplies are not working on one or more nodes or CB 320 server chassis.
Contact your authorized HCP service provider.

Processor failure

IPMI sensors are detecting one or more nodes with processors that are not working.
Contact your authorized HCP service provider.

Regions per node is low

HCP storage management is currently not configured for optimal performance.
To resolve this issue, contact your authorized HCP service provider.

Remote storage almost full

Primary running storage space on the remote system for a replication link is at least 90% used.
Consider adding more primary running storage capacity to the remote system or changing storage tiering strategies on that system to create more space in the existing primary running storage.
For an active/active link, this alert appears only in the System Management Console for the local system.
For an active/passive link, this alert appears only in the System Management Console for the primary system.

Remote storage full (link suspended)

Primary running storage space on the remote system for a replication link is 94% used. The remote system cannot act on any more replication data transmissions from the local system.
HCP has automatically suspended activity on the link
Either add more primary running storage capacity to the remote system, or change storage tiering strategies on that system to create more space in the existing primary running storage. Then resume activity on the link.
For an active/active link, this alert appears only in the System Management Console for the local system. For an active/passive link, this alert appears only in the System Management Console for the primary system.

Replication certificates expire soon

One or more trusted replication server certificates will expire within 90 days. If a certificate expires, replication with the system from which the certificate was obtained will fail.
To ensure that replication is not disrupted, when the other system in the replication pair installs a new SSL server certificate for the domain that's associated with the replication network, download that certificate and upload it to this system as a trusted replication server certificate.

Replication certificates expire soon

One or more trusted replication server certificates will expire within 30 days. If a certificate expires, replication with the system from which the certificate was obtained will fail.
To ensure that replication is not disrupted, when the other system in the replication pair installs a new SSL server certificate for the domain that's associated with the replication network, download that certificate and upload it to this system as a trusted replication server certificate.

Replication link failure

An active/active or outbound active/passive replication link is not working as expected.
Check the network connection between the two systems involved in the link. If the connection appears to be working properly, contact your authorized HCP service provider for help.

Replication link has autopaused tenants

HCP has automatically paused replication of one or more HCP tenants.
For each tenant, correct the situation that caused replication to be paused. Then resume replication of the tenant.

Replication link pending

Either the system has sent a request for a replication link to another system and is waiting for a response, or the system has received a request for a replication link and has not yet responded.

Replication link stalled

Replication has unexpectedly stopped on a replication link. Check the network connection between the two systems involved in the link.
If the connection appears to be working properly, contact your authorized HCP service provider for help.

Replication links shut down

All replication links in which this system is involved are shut down.
No replication or recovery activity is occurring on these links, and the links cannot be used for read-from-remote or object-repair purposes.

Reverse IP lookup failed for Key Distribution Center

HCP was able to do a reverse IP lookup of an IP address used for communication with the primary AD domain controller for the Key Distribution Center.
However, HCP was unable to do a reverse IP lookup of an IP address used for communication with another AD domain controller in the same domain or in another domain.
For more information about the problem, go to the Active Directory page in the HCP System Management Console.

Reverse IP lookup failed for Key Distribution Center

HCP was unable to do a reverse IP lookup of an IP address used to communicate with the primary AD domain controller for the Key Distribution Center.
For more information about the problem, go to the Active Directory page in the HCP System Management Console.

Reverse IP lookup failed for LDAP server

HCP was able to do a reverse IP lookup of an IP address used to communicate with the primary AD domain controller for the LDAP server.
However, HCP was unable to do a reverse IP lookup of an IP address used to communicate with another domain controller in the same domain or in another domain.
For more information about the problem, go to the Active Directory page in the HCP System Management Console.

Reverse IP lookup failed for LDAP server

HCP was unable to do a reverse IP lookup of an IP address used to communicate with the primary AD domain controller for the LDAP server.
For more information about the problem, go to the Active Directory page in the HCP System Management Console.

S Series Balancing service is missing from current schedule

The S Series Balancing service is not included in the current schedule.

SSD RAID degraded

An SSD is experiencing errors or has failed completely.
Contact your authorized HCP service provider for help.

SSD RAID rebuilding

The SSD RAID volume is rebuilding. It cannot be accessed until the rebuild process is complete.

Single sign-on issue

The SPN attribute for one or more tenants or namespaces is missing from the AD domain.
If the HCP system is involved in replication, these tenants and namespaces could be defined in any system in the replication topology.
For information about which tenants are involved, see the Status section on the Active Directory page in the HCP System Management Console.
If the missing SPN attribute is for a namespace, have the administrator for the tenant that owns the namespace disable and reenable AD single sign-on for the namespace.
If the missing SPN attribute is for a tenant, disable and reenable AD authentication for the tenant. If the issue is still not resolved, reconfigure HCP support for AD on the Active Directory page in the HCP System Management Console.
If the problem persists, contact your authorized HCP service provider.

Some nodes not using the correct time source

One or more nodes are using a time source other than what is configured for the system. That is, they are using internal time when external time is configured, or they are using external time when internal time is configured.

Spindown storage usage is *percent used*

For HCP with SAN-attached storage systems with spindown storage, spindown storage is less than 75 percent full.

Spindown storage usage is *percent used*

For HCP with SAN-attached storage systems with spindown storage, spindown storage is 75 to less than 90 percent full. Consider adding more spindown storage capacity to the HCP system.

Spindown storage usage is *percent used*

For HCP with SAN-attached storage systems with spindown storage, spindown storage is 90 or more percent full.
HCP will not move any more objects to spindown storage until either objects are removed from spindown storage or spindown storage capacity is increased.

Storage Tiering service is missing from the current schedule

The HCP system includes the Storage Tiering service which should be, but is not scheduled. No objects will be moved to spindown or external storage.

SSL server certificate expires soon

One or more SSL server certificates for one or more HCP domains will expire within 90 days
If a domain has no valid certificates, clients must accept the invalid certificate presented by HCP for access to namespaces in that domain.
If the domain associated with the replication network has no valid certificates, replication fails.
Check the Domains and Certificates page to see which certificates are expiring. Then make sure each affected domain has at least one certificate that will be valid when the expiring certificates expire.

SSL server certificate expires soon

One or more SSL server certificates for one or more HCP domains will expire within 30 days.
If a domain has no valid certificates, HTTPS access to namespaces in that domain is not allowed. If the domain associated with the replication network has no valid certificates, replication fails.
Check the Domains and Certificates page to see which certificates are expiring. Then make sure each affected domain has at least one certificate that will be valid when the expiring certificates expire.

Storage device reporting errors

One or more physical drives are experiencing problems.
Contact your authorized HCP service provider.

Storage license has expired

The storage license is past its expiration date and no longer valid.
Contact HCP support to procure a new license.

Storage license is not a valid license for this system

The HCP system serial number does not match the serial number on the storage license. A new storage license must be uploaded with a matching serial number.
Contact HCP support to procure a new license.

Storage usage is *percent used*

The storage managed by the storage nodes is less than 75 percent full.
In a HCP with SAN-attached storage system with spindown storage, this value applies only to running storage.

Storage usage is *percent used*

The storage managed by the storage nodes is 75 to less than 90 percent full. Consider adding more storage capacity to the HCP system.
In a HCP with SAN-attached storage system with spindown storage, this value applies only to running storage.

Storage usage is *percent used*

The storage managed by the storage nodes is 90 or more percent full.
When storage usage is 95 or more percent full, HCP will not store any new objects or any new or replacement custom metadata. It will, however, continue to allow metadata changes.
In a HCP with SAN-attached storage system with spindown storage, this value applies only to running storage.

Default service plan DPL setting is 1

For HCP with internal storage systems only, the ingest tier DPL defined for namespaces by the default service plan is 1 (one). To ensure that stored data is protected, all HCP namespaces that use the default service plan should be replicated.
Additionally, if the default namespace uses the default service plan, all directories in that namespace should be replicated.

System is starting

The HCP system is in the process of starting up.

Tenants inaccessible due to network configuration

One or more tenants are associated with a network other than [hcp_system], but virtual network management is disabled. A tenant with a management network other than [hcp_system] cannot be accessed through the Tenant Management Console or HCP management API.

Namespaces belonging to a tenant with a data access network other than [hcp_system] are inaccessible.

This error can occur when tenants on an HCP system that has virtual network management enabled are replicated to a system that does not.

To have virtual network management enabled, contact your authorized HCP service provider.

Tenants inaccessible due to network configuration

One or more networks specified as the management or data access network for one or more tenants do not exist. A tenant with a nonexistent management network cannot be accessed through the Tenant Management Console or HCP management API.

Namespaces belonging to a tenant with a nonexistent data access network are inaccessible.

This error can occur on an HCP system that's a replication target when a network defined on a source system is not defined on the target system.

Check the Networks page for the list of nonexistent networks that are associated with tenants. For each listed network, create a network with the same name.

Time out of sync between replicating systems

The system time on this system is more than one minute out of sync with the system time on one or more other systems with which this system participates in a replication link.

The recommended practice is to have all HCP systems in a replication topology use the same external time server.

Unavailable nodes

One or more nodes are unavailable.

If the status of a node changes spontaneously from available to unavailable and the node does not restart automatically, contact your authorized HCP service provider.

Do not try to restart the node manually, as that may cause the loss of information needed to diagnose the problem.

Unavailable objects

One or more unavailable objects have been detected. These objects cannot be replicated until they are repaired.

If the objects cannot be recovered, they become irreparable.

If this occurs, contact your authorized service provider.

Usage has exceeded license capacity for the storage

The storage capacity of the storage license has been exceeded.

Contact HCP support to procure a new license.

Username mapping invalid

In the username mapping file used by the CIFS protocol for the default namespace, one or more usernames map to the same UID.

Only one username can map to any given UID.

Hardware page alerts

The System Management Console uses system health icons for alerts that appear on the Hardware page. These alerts are described in the table below. The alerts are listed alphabetically by their hover text. Alerts with text beginning with a number are listed first, in alphabetical order by the variable that represents the number.

HCP

bad-fan-count of *fan-count* chassis fans indicating problems

One or more fans in one or more CB 320 server chassis are not functioning properly. Contact your authorized HCP service provider.

bad-power-supply-count of *power-supply-count* chassis power supplies indicating problems

One or more power supplies in one or more CB 320 server chassis are not functioning properly. Contact your authorized HCP service provider.

fan-count of *fan-count* chassis fans operating normally

All fans on all CB 320 server chassis are functioning properly.

power-supply-count of *power-supply-count* chassis power supplies operating normally

All power supplies on all CB 320 server chassis are functioning properly.

BBU charging

For HCP with internal storage systems only, the battery backup unit in the node is charging.

BBU degraded; charging

For HCP with internal storage systems only, the battery backup unit in the node is charging.
The write-cache is disabled on the node.

BBU degraded; discharging

For HCP with internal storage systems only, the battery backup unit in the node is discharging.
The write-cache is disabled on the node.

BBU discharging

For HCP with internal storage systems only, the battery backup unit in the node is discharging.

BBU failed

For HCP with internal storage systems only, the battery backup unit in the node has failed. The write-cache is disabled on the node. If this alert appears for more than a few hours, contact your authorized HCP service provider.

Fan speed critical

IPMI sensors are detecting one or more fans with critically high or low speeds. Shut down the node and contact your authorized HCP service provider.

Fan speed out of normal range

IPMI sensors are detecting one or more fans with speeds above or below the recommended range, but not critically so.
Monitor the fan speeds on the Storage Node page.
If they do not return to normal, contact your authorized HCP service provider.

File system failure

One or more file systems have no more available space or no more available inodes.
Contact your authorized HCP service provider.

Metadata query engine failure

The metadata query engine is not running on the node, most likely because the node is unavailable.
When the node becomes available again, the engine should automatically restart on it.
If it doesn't, disable and then reenable metadata query engine indexing.
If the problem persists, contact your authorized HCP service provider.

Multipath degraded

For HCP with SAN-attached storage systems configured with multipathing, the physical connection between the node and the SAN storage has failed. Contact your authorized HCP service provider.

NIC failure

The node is experiencing problems with one or more of its networks. Possible causes for this alert include:

- One or more physical network connections to the node are not working. Check the Storage Node page for the node to see which network interfaces show errors. Then correct any problems with the applicable physical networks. If the networks appear to be working properly, Contact your authorized HCP service provider.
- The node is missing one or more network interfaces. Check the Networks page to see which networks have this problem. Then restart those networks. If the problem persists, contact your authorized HCP service provider.
- The node has one or more network interfaces for networks in which it does not have IP addresses. Check the Networks page to see which networks have this problem. Then restart those networks. If the problem persists, contact your authorized HCP service provider.

No IPMI status available for chassis fans

The storage node specified in the CB 320 server chassis configuration cannot communicate with one or more chassis.
Make sure the chassis configuration is correct. If it is, contact your authorized HCP service provider.

No IPMI status available for chassis power supplies

The storage node specified in the CB 320 server chassis configuration cannot communicate with one or more chassis.
Make sure the chassis configuration is correct. If it is, contact your authorized HCP service provider.

Node has been removed

The node has been permanently removed from the HCP system.
You cannot reuse its back-end IP address for any nodes you subsequently add to the system.

Node problem

The node is experiencing a heavy load or a high rate of page swapping.
Contact your authorized HCP service provider.

Power supply error

The node has only one power supply working normally.
Contact your authorized HCP service provider.

SSD RAID degraded

An SSD is experiencing errors or has failed completely.
Contact your authorized HCP service provider for help.

SSD RAID rebuilding

An SSD device is rebuilding. It cannot be accessed until the rebuild process is complete.

Storage failure

One or more physical storage devices managed by the node are not functioning properly.
If this alert is raised by a removed or a failed drive, it can take up to an hour before it appears on the Hardware page of the System Management Console.
Contact your authorized HCP service provider for assistance.

Temperature critical

IPMI sensors are detecting one or more components with critically high or low temperature readings.
Shut down the node and contact your authorized HCP service provider.

Temperature out of normal range

IPMI sensors are detecting one or more components with high or low, but not critical, temperature readings.
Monitor the temperature readings on the Storage Node page. If they do not return to normal, contact your authorized HCP service provider.

Temperature within normal range

IPMI sensors are not detecting any components with temperature readings outside the normal range.

Voltage critical

IPMI sensors are detecting one or more components with critically high or low voltage readings.
Shut down the node and contact your authorized HCP service provider.

Voltage out of normal range

IPMI sensors are detecting one or more components with high or low, but not critical, voltage readings.
Monitor the voltage readings on the Storage Node page. If they do not return to normal, contact your authorized HCP service provider.

Voltage within normal range

IPMI sensors are not detecting any components with voltage readings outside the normal range.

Storage node page alerts

The System Management Console uses system health icons for alerts that appear on the Storage Node page. These alerts are described in the table below. The alerts are listed alphabetically by their hover text. Alerts with text beginning with a number are listed first, in alphabetical order by the variable that represents the number.

bad-interface-count of *interface-count* network interfaces are not functioning properly

One or more NICs in the node are not functioning properly. Contact your authorized HCP service provider.

bad-storage-device-count of *storage-device-count* storage devices are not functioning correctly

One or more physical storage devices managed by the node are not functioning properly. Contact your authorized HCP service provider.

file-system-count file systems on storage-device-count devices

The node has the indicated number of file systems, which map to the indicated number of physical storage devices.

sensor-count IPMI sensors are indicating problems

The indicated number of IPMI sensors are detecting one or more problems in the node. For more information, review the IPMI details.

All *file-system-count* file systems have sufficient space and inodes

All the file systems on the node have space and inodes available for storing additional objects.

All IPMI sensors report normal operation

All components monitored by IPMI are functioning normally.

All network interfaces are functioning properly

All NICs in the node are functioning properly.

Core hardware is functioning normally

The load and rate of page swapping on the node are within the acceptable range.

Core hardware may need attention

The node is experiencing a heavy load or a high rate of page swapping. Contact your authorized HCP service provider.

File system is running out of space or inodes

One or more file systems have no more available space or no more available inodes. Contact your authorized HCP service provider.

Logical volume usage

The logical volumes managed by the node have the status, capacity, and used space shown when you expand the alert.

Multipath degraded

For HCP with SAN-attached storage systems configured with multipathing, a physical connection between the node and the SAN storage has failed. Contact your authorized HCP service provider.

No IPMI status is available

The node does not contain IPMI sensors.

Node has been removed

The node has been removed from the HCP system permanently. You cannot reuse its back-end IP address for any nodes you subsequently add to the system.

Node is not available

The node is unavailable for one of these reasons:

- It is starting up but not yet able to perform HCP functions.
- It is shutting down and no longer able to perform HCP functions.
- It is not running or is unable to communicate with the rest of the HCP system.

Storage page alerts

The System Management Console uses warning and error icons for alerts that appear on the Storage page.

The icon used to indicate a warning condition is a white circle containing an orange exclamation point. When this icon appears in a table row, that row is highlighted in orange.

The icon used to indicate an error condition is a white triangle containing a red exclamation point. When this icon appears in a table row, that row is highlighted in red.

The warning and error alerts that appear on the Storage page are described in separate sections below.

Storage page warning alerts

Warning alerts that appear on the Storage page are listed alphabetically by their hover text.

Storage components list

One or more volumes in this storage pool have problems

One or more of the external storage volumes in the external storage pool have a status other than available. To see which volumes have problems, open the panel for the storage pool. For more information about problem volumes, check the HCP system log.

Storage pools list

External volume *volume-id* on node *node-number* - *volume-status*

The external storage volume has a status other than available. For information about the cause, check the HCP system log.
If the status is broken, check the export configuration and verify that the NFS server is running. If the configuration is correct and the NFS server is running, ensure that the device is functioning properly and that the network connecting HCP to the device is healthy.
If the status is unavailable and does not change to available or broken within a short amount of time, try remounting the volume.
If this alert persists, contact your authorized HCP service provider for help.

Storage page error alerts

Error alerts that appear on the Storage page are listed alphabetically by their hover text.

Storage components list

One or more volumes in this storage pool have problems

One or more of the external storage volumes in the external storage pool have a status other than available. To see which volumes have problems, open the panel for the storage pool. For more information about problem volumes, check the HCP system log.

Storage pools list

External volume *volume-id* on node *node-number* - *volume-status*

The external storage volume has a status other than available. For information about the cause, check the HCP system log.
If the status is broken, check the export configuration and verify that the NFS server is running. If the configuration is correct and the NFS server is running, ensure that the device is functioning properly and that the network connecting HCP to the device is healthy.
If the status is unavailable and does not change to available or broken within a short amount of time, try remounting the volume.
If this alert persists, contact your authorized HCP service provider for help.

Networks page alerts

The System Management Console uses warning and error icons for alerts that appear on the Networks page.

The icon used to indicate a error condition is a white triangle containing an red exclamation point. When this icon appears in a table row, that row is highlighted in red.

The icon used to indicate an warning condition is a white triangle containing a orange exclamation point. When this icon appears in a table row, that row is highlighted in orange.

The warning and error alerts that appear on the Networks page are described in separate sections below.

Networks page error condition alerts

Error condition alerts that appear on the Networks page are listed alphabetically by their hover text.

Network has no node IP addresses
The network is empty; that is, no nodes have any IP addresses defined for the network. Clients cannot access the HCP system over an empty network.
Configure the network to assign IP addresses to one or more nodes. Each node must have a separate IP address on each subnet defined for the network.

Network not functioning properly
The network is experiencing problems on one or more nodes. Possible causes for this error condition alert include:

- One or more physical network connections to one or more nodes are not working. Check the Storage Node page for each node to see which network interfaces show errors. Then correct any problems with the applicable physical networks. If the networks appear to be working properly, contact your authorized HCP service provider.
- The network interface for the network is missing in one or more nodes. Restart the network. If the problem persists, contact your authorized HCP service provider.
- One or more nodes have network interfaces for the network but do not have IP addresses in the network. Restart the network. If the problem persists, contact your authorized HCP service provider.

Networks page warning alerts

Warning condition alerts that appear on the Networks page are listed alphabetically by their hover text.

Network disabled
The network has been manually disabled by a system administrator. Clients cannot access the HCP system over a disabled network and tenants and namespaces cannot be replicated over a disabled network.
Check the Tenants page to determine whether the disabled network is assigned to any tenants. Also check the replication Settings page to determine whether the disabled network is selected as the replication network.
If the network is assigned to one or more tenants, take one of these actions:

- On the Tenants page, reconfigure the affected tenants to use only enabled networks for data and management access.
- On the Networks page, click the gear icon next to the disabled network to display the network Settings panel. Then select the option to enable the network and click Update Settings.

If the network is selected as the replication network, take one of these actions:

- On the replication Settings page, select a different network for replication.
- On the Networks page, click the gear icon next to the disabled network to display the network Settings panel. Then select the option to enable the network and click Update Settings.

If the network is not assigned to any tenants, and is not used for replication, no action is required. You can use the Networks page to reconfigure, reenable, or delete the network at any time without affecting access to the HCP system.

IP mode mismatch
The system-level front-end network IP mode is Dual, but the [hcp_system] network is configured to use only IPv4 addresses or only IPv6 addresses.
Submit a request to your authorized service provider to set the system-level IP mode and set the [hcp_system] network IP mode, to provide support only for the type(s) of IP address you want to configure for user-defined networks.

Network has only one node IP address
The network is degraded; that is, only one node has IP addresses defined for the network. A degraded network presents a single point of failure for clients accessing HCP over that network.
Reconfigure the network to assign IP addresses to one or more additional nodes.

Network is missing node IP addresses
The network is a partial network; that is, at least two nodes have IP addresses defined for the network and at least one node does not. The load from client requests over a partial network is not fully distributed across the nodes in the HCP system.
Reconfigure the network to assign IP addresses to all the nodes in the HCP system. Each node must have an IP address on each subnet defined for the network.

Network not functioning properly
The network is experiencing problems on one or more nodes. Possible causes for this warning condition alert include:

- The current MTU for the network on one or more nodes does not match the configured MTU. If the problem is with a user-defined network, restart the network. If that doesn't resolve the problem, reboot the applicable nodes. If the problem persists, Contact your authorized HCP service provider.
- For the [hcp_system] network, the current speed of the network on one or more nodes does not match the configured speed. Contact your authorized HCP service provider. (This does not apply if the speed is set to auto.)
- For the [hcp_backend] network, the current speed of the network on one or more nodes is not the maximum speed possible for that network. Contact your authorized HCP service provider.

Tenants page alerts

Tenant page alerts are listed alphabetically by their hover text.

Degraded network assigned

The tenant is associated with a degraded network for management or data access purposes. A degraded network presents a single point of failure for clients accessing the tenant or its namespaces over that network.
Take one of these actions:

- On the Tenants page, reconfigure the affected tenant to use only networks that have IP addresses defined for at least two nodes in the HCP system.
- On the Networks page, reconfigure each degraded network to assign IP addresses to one or more additional nodes.

Empty network assigned

The tenant is associated with an empty network for management or data access purposes. If the management network is empty, the tenant cannot be accessed through the Tenant Management Console or HCP management API. If the data access network is empty, namespaces belonging to a tenant are inaccessible.
Take one of these actions:

- On the Tenants page, reconfigure the affected tenant to use only networks that have IP addresses defined for at least two nodes in the HCP system.
- On the Networks page, configure each empty network to assign IP addresses to one or more nodes. Each node must have a separate IP address on each subnet defined for the network.

Inaccessible due to network configuration

The management and/or data access network specified for the tenant does not exist. If the management network does not exist, the tenant cannot be accessed through the Tenant Management Console or HCP management API. If the data access network does not exist, namespaces belonging to a tenant are inaccessible.
This error can occur on an HCP system that's a replication target when a network defined on a source system is not defined on the target system.
For each undefined network, create a network with the name of the undefined network.

Namespace quota exceeded

The number of namespaces owned by the tenant is greater than the namespace quota for the tenant.
This situation can happen if the tenant is included in an active/active replication link. With this type of link, namespaces can be created for the tenant independently on each system involved in the link. Namespaces from both systems can then be added to the link such that the total number of namespaces replicated on the link exceeds the namespace quota for the tenant. As a result, the total number of namespaces for the tenant on each system exceeds the namespace quota for the tenant.

Namespace quota reached

The number of namespaces owned by the tenant equals the namespace quota for the tenant.

Nonreplicating objects

The tenant contains objects that are not replicating. Contact your HCP system administrator.

Partial network assigned

The tenant is associated with a partial network for management or data access purposes. The load from client requests for access to the tenant or its namespaces is not being fully distributed across the nodes in the HCP system.
Take one of these actions:

- On the Tenants page, reconfigure the affected tenant to use only networks that have IP addresses defined for all nodes in the HCP system.
- On the Networks page, reconfigure each partial network to assign IP addresses to all nodes in the HCP system. Each node must have a separate IP address on each subnet defined for the network.

Read-only, set by replication

For HCP tenants only, the tenant is read-only because it's included in an active/passive link and one of the following is true:

- The current system is the replica for the link, and normal replication is occurring on the link.
- The current system is the primary system for the link, and the initial stage of data recovery is occurring on the link.
- The current system is either the primary system or the replica for the link, and the final stage of data recovery is occurring on the link.

Soft quota exceeded

For HCP tenants only, the amount of storage used by all namespaces owned by a tenant exceeds the soft quota configured for the tenant. Contact the tenant administrator about increasing the hard quota for the tenant.

Tenant has *namespace-count* namespace(s) configured for CIFS with authenticated access only, but CIFS authenticated access is not currently supported

One or more of the tenant's namespaces are configured for CIFS authenticated access only, but the system is not configured to support the use of authenticated CIFS. As a result, CIFS cannot be used for access to those namespaces. Reconfigure the affected namespace(s) to support both anonymous and authenticated access with CIFS.

Tenant *tenant-name* has *irreparable-object-count* irreparable objects

One or more of the tenant's namespaces contain the indicated total number of irreparable objects. Contact your authorized HCP service provider.

Tenant *tenant-name* has *irreparable-object-count* irreparable objects and *unavailable-object-count* unavailable objects

One or more of the tenant's namespaces contain the indicated total number of irreparable objects, and one or more of the tenant's namespaces contain the indicated total number of unavailable objects. Contact your authorized HCP service provider.

Tenant *tenant-name* has *unavailable-object-count* unavailable objects

One or more of the tenant's namespaces contain the indicated total number of unavailable objects. This is most likely due to one or more nodes being unavailable, If the situation persists, please contact your authorized HCP service provider.

Tenant may have directories that are not being replicated

For the default tenant in HCP with internal storage systems only, the default namespace has a DPL of one and at least one of the directories in it is being replicated. When the default namespace has a DPL of one, all directories in it should be replicated to ensure that the stored data is protected.

Tenant with DPL 1 namespaces that are not replicating

In HCP with internal storage systems only:

- For HCP tenants, the tenant owns one or more namespaces that have a DPL of one and are not being replicated. All HCP namespaces with a DPL of one should be replicated to ensure that the stored data is protected.
- For the default tenant, the default namespace has a DPL of one and none of the directories in it are being replicated. When the default namespace has a DPL of one, all directories in it should be replicated to ensure that the stored data is protected.

Domains and certificates page alerts

Domains and certificates page alerts are listed alphabetically by their hover text.

Domain list

All certificates for domain are invalid

All the certificates associated with the domain have either an expiration date in the past or a start date in the future. Add a valid certificate to the domain.

All valid certificates for the domain are expiring

All the valid certificates associated with the domain will expire within 30 days. Ensure that the domain has at least one certificate that will be valid when the expiring certificate expires.

Certificate list

Certificate has a start date in the future

The start date for the certificate is in the future, so the certificate is currently invalid.
Make sure the domain has at least on valid certificate.

Certificate is expired

The certificate has expired and is no longer valid. Delete the certificate.

Certificate is expiring

The certificate will expire within 90 days.
Make sure the domain has at least one certificate that will be valid when this certificate expires.

Common name for certificate does not match domain name

The common name of the certificate does not represent a subdomain of the domain with which the certificate is associated. The certificate is invalid.
If a domain has no valid certificates, clients must accept the invalid certificate presented by HCP for access to namespaces in that domain. If the domain associated with the replication network has no valid certificates, replication fails.
Make sure that domain has at least one valid certificate. Then delete the certificate with the common name mismatch.

Active directory page alerts

Active Directory page alerts are listed alphabetically by their hover text.

Active Directory enabled for default namespace only

Either:

- AD authentication is enabled only for the default namespace and is not currently supported for HCP namespaces. This can happen after an upgrade, where the CIFS protocol was enabled for the default namespace with AD authentication before the upgrade occurred.

  To enable support for AD for HCP namespaces, enable HCP support for AD on the Active Directory page in the HCP System Management Console.

- In the username mapping file used by the CIFS protocol for the default namespace, one or more usernames map to the same UID. Only one username can map to any given UID.

Active Directory secure connection issue

HCP could not communicate with AD due to a problem with the AD SSL server certificate uploaded to HCP.
Make sure you have the correct certificate, then upload the certificate again on the Active Directory page in the HCP System Management Console.
If the problem persists, contact your authorized HCP service provider.

Cannot access Key Distribution Center

HCP cannot access the Key Distribution Center in the AD domain specified in the HCP AD configuration.
Check that both the AD domain controller and the network connection between HCP and that AD domain controller are healthy.
If they both appear to be working properly, contact your authorized HCP service provider.

Cannot access LDAP server

HCP cannot access the LDAP server for the AD domain specified in the HCP AD configuration.
Check that both the LDAP server and the network connection between HCP and that server are healthy.
If they both appear to be working properly, contact your authorized HCP service provider.

Could not establish connection with Active Directory - add certificate again

HCP could not communicate with AD due to a problem with the AD SSL server certificate uploaded to HCP.
Make sure you have the correct certificate, then upload the certificate again on the Active Directory page in the HCP System Management Console.
If the problem persists, contact your authorized HCP service provider.

DNS correctly configured

HCP is configured to use DNS.

DNS is not enabled. Active Directory requires DNS be enabled.

HCP is not configured to use DNS. For HCP to work with AD, HCP must be configured as a subdomain in your DNS.

HCP computer account missing

The HCP computer account is missing from the AD domain.
Reconfigure HCP support for AD on the Active Directory page in the HCP System Management Console.

IP lookup failed for Active Directory server *server-name*

HCP was unable to do an IP lookup of an IP address used to communicate with the AD domain controller for either the Key Distribution Center or the LDAP server.
Make sure the DNS configuration includes all A and AAAA records needed to resolve the IP addresses that HCP uses to communicate with the indicated domain controller.

No external time server configured. Active Directory recommends an external time server.

HCP is configured to use itself as a time server. For HCP to work with AD, HCP time must be within five minutes of AD time.
The recommended configuration is HCP HCP and AD to use the same external time server.

No Key Distribution Center found

HCP cannot find a Key Distribution Center in the AD domain specified in the HCP AD configuration.
Make sure AD is configured correctly in your DNS.
If the problem persists, contact your authorized HCP service provider.

No LDAP server found

HCP cannot find an LDAP server in the AD domain specified in the HCP AD configuration.
Make sure AD is configured correctly in your DNS.
If the problem persists, contact your authorized HCP service provider.

Nodes correctly configured

All of these conditions are true:

- The computer accounts for all nodes are present in the AD domain. These accounts are created automatically when you configure HCP to support AD.
- All nodes have valid credentials for the HCP computer account used to query AD for groups.
- All nodes can connect to AD.

Nodes misconfigured

At least one of these conditions is true:

- The computer account for one or more nodes is missing from the AD domain. These accounts are created automatically when you configure HCP to support AD.
- The credentials for the HCP computer account used to query AD for groups and other information are invalid on one or more nodes.
- One or more nodes cannot connect to AD. To resolve these issues, reconfigure support for AD on the Active Directory page in the HCP System Management Console.

  If the problem persists, contact your authorized HCP service provider.

Reverse IP lookup failed for Active Directory server *server-name*. Record for *server-ip-address* not found.

Given the indicated IP address, HCP was unable to do a reverse IP lookup of the hostname of the AD domain controller.
Make sure your DNS includes a PTR record for that IP address that specifies the correct domain controller hostname.

Reverse IP lookup mismatch for Active Directory server *server-name*. Record for *server-ip-address* points to *server other-server-name*.

HCP was able to do a reverse IP lookup of an IP address used to communicate with the AD domain controller, but the PTR record identifies a different domain controller.
Make sure your DNS configuration includes a PTR record for the indicated IP address that specifies the correct domain controller hostname.

Service principal names are missing

The SPN attribute for one or more tenants or namespaces is missing from the AD domain. If the HCP system is involved in replication, these tenants and namespaces could be defined in any system in the replication topology.
If the missing SPN attribute is for a namespace, have the administrator for the tenant that owns the namespace disable and reenable AD single sign-on for the namespace. If the missing SPN attribute is for a tenant, disable and reenable AD authentication for the tenant. If the issue is still not resolved, reconfigure HCP support for AD on the Active Directory page in the HCP System Management Console.
If the problem persists, contact your authorized HCP service provider.

System correctly configured

All of the following are true:

- No HCP components are missing from the AD domain.
- The HCP configuration of AD support is complete (that is, it's not configured only for the CIFS protocol for the default namespace).
- The username mapping file used by the CIFS protocol does not contain any invalid mappings.

Time server correctly configured

HCP is configured to use an external time server.

Zero-copy failover behavior

In a HCP with SAN-attached storage system, zero-copy failover is the process of one node automatically taking over management of storage previously managed by another node that has failed. Support for zero-copy failover is configured at the storage tier and enabled in the HCP system configuration.

Zero-copy failover is supported for storage nodes only.

This chapter describes the storage setup required to support zero-copy failover and explains how zero-copy failover works.

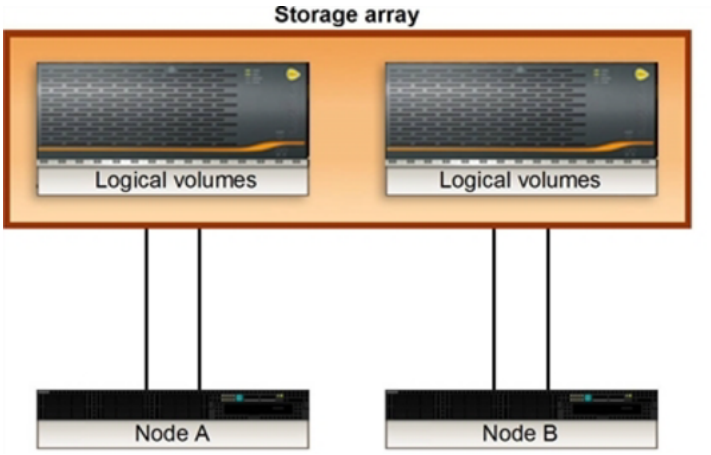
Storage setup for zero-copy failover

In a HCP with SAN-attached storage system, nodes have both physical and logical connections to the SAN storage. The physical connections are through paths established by Fibre Channel cables and, in some systems, Fibre Channel switches. The logical connections are through mappings of the logical volumes in the storage array to the nodes.

Physical paths

In an HCP with SAN-attached storage system, each node has two physical paths to the storage array. This is called multipathing.

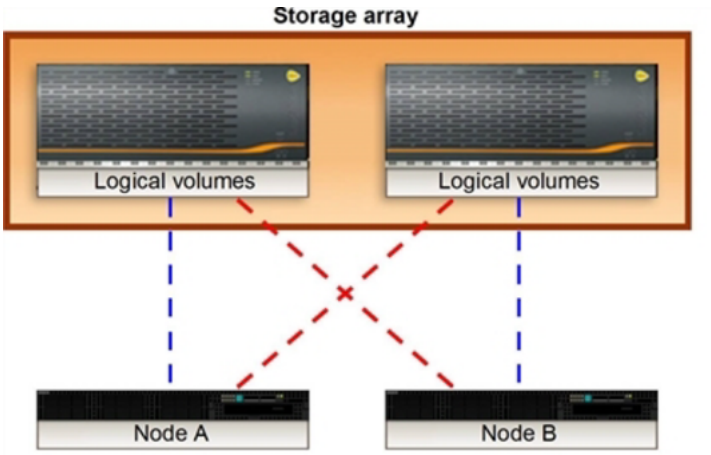
The following figure shows two nodes, A and B, at the bottom, each with a multipath connection to the storage array at the top.



Logical mappings

To support zero-copy failover, the logical volumes in the storage array must be cross-mapped to the nodes. Cross-mapping means that each logical volume that maps to one node (A) must also map to the same second node (B), called the peer node. The mappings to node A are the primary mappings for those logical volumes, and the mappings to node B are the standby mappings. Similarly, each logical volume with a primary mapping to node B must have a standby mapping to node A.

The following figure shows two sets of logical volumes in a storage array that map to two nodes, A and B. The primary mappings for each node are shown in blue. The secondary mappings are shown in red.



Failing over and failing back

Under normal circumstances, each node in a cross-mapped pair manages the logical volumes with primary mappings to it. However, if one node becomes unavailable and zero-copy failover is enabled, its peer can take over management of those volumes. The process of one node taking over storage management from another is called failover.

When an unavailable node rejoins the HCP system, it normally takes back management of its own logical volumes. This process is called failback.

Note:

- During failover, all spindown volumes on the node taking over are spun up. During failback, all spindown volumes on both nodes are spun up.
- Zero-copy failover does not apply to external storage volumes. If a node becomes unavailable, the external storage volumes it manages also become unavailable.

System Management Console information on failover

During failover, the logical volumes associated with the node that became unavailable first appear as initialized

on the Hardware page in the HCP System Management Console. After the peer takes over a logical volume, the icon moves from the row for the unavailable node to the row for the peer, where it once again shows as available.

While any logical volumes are in a failed-over state, this daily access failover alert appears in the alerts section on the Overview page.

Data outages during failover

While a logical volume is failing over, the data stored on it is temporarily unavailable. If the node that managed the volume became unavailable because you shut it down from the System Management Console, the data outage lasts less than 5 minutes.

If the node became unavailable for some other reason (for example, all physical paths between the node and the storage array broke, or the node itself failed), the data outage can last significantly longer. Factors that affect how long it lasts include:

- The number of logical volumes involved
- The size of the logical volumes
- The number of objects stored on the logical volumes
- The amount of data storage activity occurring when the node became unavailable

Data outages during node restart

When you restart a node from the System Management Console, its storage fails over to its peer during the shutdown part of the restart. The failover process finishes before the node completes its shutdown processing. The data outage caused by the failover lasts less than 5 minutes.

When the node comes back up, the failback process extends the startup processing by about 15 to 30 seconds. The data outage caused by the failback also lasts less than 5 minutes.

Data protection mechanism

Zero-copy failover uses a data protection mechanism that prevents the two nodes in a peer group from accidentally overwriting each other’s storage. This mechanism needs to be accessible on all storage paths. It is used any time a node in the pair needs to mount or unmount a storage volume. This occurs when:

- A node starts
- A node stops
- A node takes over storage management from its peer (failover)
- A node releases control of storage it’s managing (failback)

To ensure access to the data protection mechanism, both paths between the node and the storage array must be available during these transitions. If either path is not available, the node makes itself unavailable to guarantee the safety of the data.

If a path outage occurs, you should find and repair the cause of the outage before trying to start or stop any affected node.

Failover and physical path outages

When one physical path between a node and the storage array breaks, processing continues normally. If the second path for that node breaks while the first one is still broken, the node becomes unavailable, and failover occurs.

To return the node to service and fail back the logical volumes, you need to fix both paths before you reboot the node. The node will not return to service while either path is broken.

If a node managing failed-over storage has a path outage while its peer is still unavailable, processing continues normally. However, if the peer returns to service and takes back its storage, the node with the path outage then becomes unavailable, and failover occurs in the other direction. That is:

1. Node A fails.
2. Node A storage fails over to node B.
3. Node B has a path outage.
4. Node A returns to service.
5. Node A storage fails back to node A.
6. Node B becomes unavailable.
7. Node B storage fails over to node A.

SNMP MIB support

You can use SNMP with HCP to view and modify system settings and receive notifications of certain types of events. HCP comes with a MIB, defined in the HCP-MIB.txt file, that includes fields and traps specific to the system. HCP also supports many of the standard Linux-based MIBs available with SNMP.

HCP-MIB exposes information about the HCP system as a whole, so you get the same information regardless of which storage node you access.

The standard MIBs, on the other hand, expose information about individual nodes, so the information you get applies only to the specific storage node that you access. You can use many of the fields in HCP-MIB to both view and modify system values.

With the fields in the standard MIBs, you can view only system values. This chapter lists the supported standard MIBs and explains how to find out which fields are exposed through them. (HCP exposes all the fields in HCP-MIB.)

Supported standard MIB files

The standard MIBs that HCP supports contain fields in subtrees under the mib-2 and ucdavis roots. The fields HCP exposes are in the following MIBs, with exclusions as noted:

- With fields under mib-2:
  - DISMAN-EVENT-MIB
  - HOST-RESOURCES-MIB
  - IF-MIB
  - IP-FORWARD-MIB
  - IP-MIB (excluding these groups: ipAddrTable, ipRouteTable, and ipNetToMediaEntry)
  - IPV6-MIB
  - MTA-MIB
  - NOTIFICATION-LOG-MIB
  - RFC1213-MIB (excluding this group: atTable)
  - SNMPv2-MIB
  - TCP-MIB (excluding this group: tcpConnTable)
  - UDP-MIB (excluding this group: udpTable)
- With fields under ucdavis:
  - LM-SENSORS-MIB
  - UCD-DISKIO-MIB
  - UCD-DLMOD-MIB
  - UCD-SNMP-MIB

You can download:

- Files for all these MIBs, except MTA-MIB and RFC1213-MIB, from http://www.net-snmp.org/docs/mibs
- The file for MTA-MIB from http://www.oidview.com/mibs/0/MTA-MIB.html
- The file for RFC1213-MIB from http://www.oidview.com/mibs/0/RFC1213-MIB.html.

Walking the MIB

To find out exactly which fields HCP exposes under mib-2 and ucdavis, you can have the SNMP client query HCP for the exposed fields. This is called walking the MIB.

How you walk the MIB depends on your SNMP tool. The following instruction uses the command-line tool from the publicly available net-snmp package, which you can download from http://www.net-snmp.org. To walk the MIB with net-snmp, you use the `snmpwalk` command with this format:

```
snmpwalk-v snmp-version -csnmp-community-name
node-ip-address-or-hostnamemib-root
```

The string *`node-ip-address-or-hostname`* is a valid front-end IP address or hostname of a storage node in the HCP system. The node that you specify must be running and healthy (that is, it must be available to the system).

his sample snmpwalk command queries the node with the IP address 192.168.210.16 for the fields that HCP exposes in subtrees branching from mib-2:

```
snmpwalk -v 2c -c public 192.168.210.16 mib-2
```

Configuring DNS for HCP

Domain name system (DNS) is a network service that translates, or resolves, domain names (for example, example.com) into IP addresses for client access. The service is provided by one or more servers, called name servers, that share responsibility for resolving client requests.

An HCP system can exist as multiple domains in the DNS: one for each front-end network defined in the system. Each domain must be a subdomain of a DNS domain to which you have administrative access, such as your corporate domain. All nodes that have IP addresses defined for a given front-end network belong to the HCP domain defined for that network.

Note: If you enable the management network, you cannot access your front-end network through DNS unless you create secondary zones for the management network.

To enable access to HCP by domain name on any given network, you need to configure the HCP domain for that network in your DNS. To do this, you can use either secondary zones or stub zones.

This chapter contains:

- A discussion of the advantages of using DNS
- A description of zones, secondary zones, and stub zones
- Windows and Unix instructions for configuring HCP domains in the DNS
- Instructions for verifying the HCP domain definitions
- DNS considerations for implementing HCP service by remote systems

Note:

- HCP does not require DNS.
- When communicating with a DNS server, HCP may send packets that are larger than 512 bytes. You must make sure these packets can pass through your corporate firewall.

DNS advantages

Using DNS provides several advantages over using IP addresses for access to the HCP system. For example:

- When you use a domain name for namespace access, the HCP DNS manager, which runs on all storage nodes, is responsible for distributing client requests among those nodes. If you use IP addresses, you are responsible for ensuring that the processing load is balanced across the HCP nodes.
- If an application uses a domain name for access to the HCP system and you change the IP addresses of the HCP nodes, you don't need to change the application. If the application uses IP addresses and you change the node IP addresses, you must update the application to specify the new IP addresses.
- If both IPv4 and IPv6 addresses are defined for a front-end network, applications can use the domain name associated with that network to access the HCP system from client computers that have IPv4 addresses and from client computers that have IPv6 addresses. If an application uses IP addresses to access the HCP system over a front-end network with multiple IP addresses defined for each node, you need to configure the application to access the HCP system using only the IP addresses that are routable from the client computer on which the application is running.
- If you use a domain name to identify the other system when you create a replication link and the IP addresses for that domain are changed on that system, replication continues without interruption. If you use IP addresses to identify the system and the IP addresses for the system change, replication stops until you change the IP addresses in the definition of the replication link.
- If you use domain names to identify the systems in a replication topology and you enable DNS failover on those systems, client requests can be automatically redirected to other systems in the topology if the target system fails. If you use IP addresses to identify a system in a replication topology and that system fails, client requests that target that system cannot be automatically redirected to other systems.

Zones

The domain names resolved by DNS are divided into zones, where each zone is defined by a set of related hostnames. A corporate domain, for example, is associated with a zone.

Each domain you define in HCP is a subdomain of a higher-level domain. In the DNS, you need an HCP domain definition for each combination of network and domain you define in HCP. The IP addresses for each HCP domain in the DNS make up a zone within the zone for the applicable higher-level domain.

For example, suppose that you configure HCP to define two domains, *hcpma.example.com* and *hcp-ca.example.com.* Suppose also that you configure HCP to define three user-defined networks, net1, net2, and net3,and you configure these three networks to associate net1 and net2 with domain hcp-ma.example.com and associate net3 with domain hcpca.example.com. In this case, you need to add three zones to the DNS, one for each of these domain and network combinations:

```
Domain name: hcp-ma.example.com
         Node IP addresses defined for network net1
         Domain name: hcp-ma.example.com
         Node IP addresses defined for network net2
         Domain name: hcp-ca.example.com
         Node IP addresses defined for nodes in network net3
```

Secondary zones and stub zones

In the DNS, you configure each HCP domain as a secondary zone or as a stub zone. A DNS server in which a given HCP domain is configured as a secondary zone maintains a full copy of the HCP DNS information for that domain and can, therefore, satisfy requests for resolution of the HCP domain name by itself. You might use secondary zones, for example, if the firewall that HCP sits behind is configured to allow client requests for DNS name resolution to go only to a corporate DNS server.

A DNS server in which a given HCP domain is configured as a stub zone gets only partial DNS information for that domain from HCP. Stub zones minimize zone replication and are less resource intensive for the DNS server.

If you enable hidden primary or notify for a network, the HCP domain for that network must be configured as a secondary zone, not a stub zone, on each DNS server specified in the network configuration.

Secondary zone and stub zone definitions are basically the same. Each definition lists the IP addresses of primary name servers for a domain but does not include individual records for those servers. Those records are stored on the primary name servers themselves. The DNS servers get the individual name server records from the primary name servers listed in the zone definition.

For each network defined in HCP, HCP automatically generates name server records for all storage nodes that have IP addresses in that network. Each of those storage nodes stores a copy of these records, thereby making each storage node eligible to be a primary name server for the applicable domain.

Before HCP can accept client requests that identify the system by a domain name, you need to register some or all of the eligible nodes as primary name servers for the applicable HCP secondary zone or stub zone. You register a node by listing its IP addresses in the secondary zone or stub zone definition.

For any given HCP domain, all storage nodes with IP addresses defined for the applicable network can act as name servers for the HCP DNS manager, regardless of whether they're registered as primary name servers. However, for HCP to be accessible over that network, at least one registered node must be running. Therefore, you need to register a sufficient number of nodes for each network to minimize the risk that all registered nodes for a given network will fail at the same time.

Tip: If HCP has a small number of storage nodes, consider registering them all as primary name servers. The more nodes you register, the more distributed the DNS queries will be.

When defining a secondary zone or stub zone for an HCP domain, you specify a fully qualified domain name for the HCP system. This is the name of the domain associated with the network that is defined in HCP.

Configuring an HCP secondary zone or stub zone in Windows

You can use either the GUI or a command line to configure a secondary zone or stub zone in Windows. The following sections present the GUI configuration procedure for Windows. For information about which Windows servers are supported, check the HCP release notes for the version of HCP that you have installed.

Configuring an HCP secondary zone in Windows

1. Open the DNS Manager
   a. In the Windows Control Panel, double-click Administrative Tools.
   b. In the Administrative Tools window, double-click DNS.
   The DNS Manager window shows the hierarchy of zones currently defined in the DNS.
2. In the DNS Manager window, right-click Forward Lookup Zones under higher-level zone within which you want to configure the HCP secondary zone. On the dropdown menu, select New Zone.
   The New Zone Wizard window opens.
3. In the New Zone Wizard window, click Next.
4. On the Zone Type page, select Secondary zone. Then click Next.
5. In the Zone name field on the Zone Name page, type the applicable fully qualified domain name for the HCP system. Then click Next.
6. On the Primary DNS Servers page, for each HCP storage node you want to register as a primary name server, in the list box, type the IPv4 and IPv6 addresses assigned to the node for the applicable network. Then press Enter.

When you’re finished adding all the node IP addresses, click Next.

7. Click Finish.
   The new HCP secondary zone appears in the zone hierarchy in the DNS manager window .

Configuring an HCP stub zone in Windows

How to configure an HCP domain as a stub zone in Windows:

1. Open the DNS Manager:
   a. In the Windows Control Panel, double-click Administrative Tools.
   b. In the Administrative Tools window, double-click DNS.
   The DNS Manager window shows the hierarchy of zones currently defined in the DNS.
2. In the DNS Manager window, right-click Forward Lookup Zones under higher-level zone within which you want to configure the HCP stub zone. On the dropdown menu, select New Zone.
   The New Zone Wizard window opens.
3. In the New Zone Wizard window, click Next.
4. On the Zone Type page, select Stub zone.
5. To configure the stub zone with Windows Active Directory integration, take one of these following actions:
   a. Select Store the zone in Active Directory.
   b. On the Active Directory Zone Replication Scope page, select the option for the way in which you want DNS data to be replicated throughout your network.
   c. Then click Next.
      Note: You need to configure the stub zone with Windows Active Directory integration if you plan to enable HCP support for AD. For information about doing that, see *Configuring Active Directory or Windows workgroup support*.
   d. To configure the stub zone without Windows Active Directory integration, click Next.
6. In the Zone name field on the Zone Name page, type the applicable fully qualified domain name for the HCP system. Then click Next.
7. On the Zone File page, select Create a new file with this file name and leave the default file name in the accompanying field. Then click Next.
8. On the Primary DNS Servers page, for each HCP storage node you want to register as a primary name server, in the list box, type the IPv4 and IPv6 addresses assigned to the node for the applicable network. Then press Enter.
   When you’re adding all the node IP addresses, click Next.
9. Click Finish.
   The HCP new stub zone appears in the zone hierarchy in the DNS manager window.

Verifying the configuration

You can verify that an HCP secondary zone or stub zone is working properly from either a Windows command-prompt window or a Unix shell. In both cases, you use either the dig or nslookup command, depending on which is available. The syntax for this is:

```
dig|nslookup (admin|nfs|cifs|www).hcp-domain-name
```

The response to this command should be a list of the IP addresses of all the HCP storage nodes that have IP addresses defined for the network for which the secondary zone or stub zone is defined.

Here’s an example of the output from the nslookup command when six out of the ten nodes in the network are registered as primary name servers for the secondary zone or stub zone:

```
  #nslookup www.hcp-ma.example.com
  Server: adc1850.example.com
  Addresses: 192.168.80.45
  2001:0db8::201
Name: www.hcp-ma.example.com
Addresses: 192.168.210.11, 2001:0db8::101, 1192.168.210.12, 2001:0db8::102,
192.168.210.13, 2001:0db8::103, 192.168.210.14, 2001:0db8::104, 192.168.210.15,
2001:0db8::105, 192.168.210.16, 2001:0db8::106, 192.168.210.17, 2001:0db8::107,
192.168.210.18, 2001:0db8::108, 192.168.210.19, 2001:0db8::109, 192.168.210.20,
2001:0db8::10a
```

If you don’t see the expected node list, the secondary zone or stub zone is not defined correctly.

DNS considerations for service by remote systems

When you configure a secondary zone or stub zone for an HCP system, you specify a domain name and the IP addresses of the primary name servers for the applicable HCP domain. This causes client requests that identify the system by that domain name to be forwarded to those primary name servers.

Namespaces can be configured to accept client requests on HCP systems other than the system targeted by the request when that system is unavailable. To enable this redirection to occur automatically for a namespace:

- DNS failover must have been enabled on the target system.
- The applicable replication link must be failed over. The applicable replication link is the link between the target system and the system to which requests must be redirected. Attention: DNS failover affects all the tenants on an HCP cluster. For DNS failover to succeed, all Active-Active and Active-Passive links must fail over to the target system. If the HCP cluster has tenants that are not part of a replication link, or if the tenant is on a replication link that has not failed over, write requests to the tenant and read requests from the tenant fail if the domain name is used in the request. Requests will succeed if the request includes the IP address of the primary cluster instead of the domain name.
- The applicable secondary zone or stub zone for the target system must include the IP addresses of the applicable primary name servers for the system to which requests must be redirected, where:
  - The applicable secondary zone or stub zone on the target system is the one defined for the data network for the tenant that owns the namespace
  - The applicable primary name servers for the system to which requests should be redirected are the ones included in the secondary zone or stub zone for the network with the same name as the tenant data network on the target system

  For examples, you may suppose:

- The data network for a tenant is the network named net1.
- The system targeted by a client request has primary name servers with IPv4 addresses 192.168.210.15, 16, 17, and 18 and with IPv6 addresses 2001:0db8::101, 102, 103, and 104 for net1. The system to which requests must be redirected has primary name servers with IPv4 addresses 192.168.24.72, 73, 74, and 75 and with IPv6 addresses 2001:0db8::201, 202, 203, and 204 for net1.

- The system targeted by a client request has primary name servers with IPv4 addresses 192.168.210.15, 16, 17, and 18 and with IPv6 addresses 2001:0db8::101, 102, 103, and 104 for net1. The system to which requests must be redirected has primary name servers with IPv4 addresses 192.168.24.72, 73, 74, and 75 and with IPv6 addresses 2001:0db8::201, 202, 203, and 204 for net1.

In this case, the secondary zone or stub zone for net1 on the target system have these IP addresses:

```
192.168.210.15
          2001:0db8::101
          192.168.210.16
          2001:0db8::102
          192.168.210.17
          2001:0db8::103
          192.168.210.18
          2001:0db8::104
          192.168.24.72
          2001:0db8::201
          192.168.24.73
          2001:0db8::202
          192.168.24.74
          2001:0db8::203
          192.168.24.75
          2001:0db8::204
```

Configuring Active Directory to support HCP

An HCP system can be configured to support Active Directory. With the system configured this way, you can create HCP group accounts that correspond to AD groups at both the system and tenant levels. AD users in those AD groups then have access to HCP through the various HCP interfaces, subject to the roles and permissions associated with the HCP group accounts.

For HCP to work with AD, you first need to prepare AD for access by HCP. Then you need to configure HCP to support AD. The table below outlines the major steps in this procedure.

This appendix describes the prerequisites for configuring AD to support HCP and contains instructions for the first six steps outlined above. These instructions are for Windows Server 2008 R2, but the concepts are the same for all versions of Windows Server.

Prerequisites for configuring support for HCP in AD

This chapter assumes the following:

- You have a basic understanding of AD concepts.
- You have an AD user account with the administrator role in the AD domain you plan to use when configuring support for AD in HCP.
- If you plan to secure communication between HCP and AD:
  - The applicable AD domain is configured with a CA.
  - You have access to a Windows server running the AD CA.
  - You have access to the Windows client from which you plan to access the HCP System Management Console for the purpose of configuring support for AD.
- For creating the AD group and user account, you have access to a Windows or Unix server from which you can access AD.
- The OU or CN in which you want to create the AD group already exists in the applicable domain.
- The OU or CN in which you want to create the AD user account already exists in the applicable domain. This can be, but does not have to be, the same OU or CN as the one in which you create the AD group.
- The OU or CN in which computer accounts will be created for the HCP nodes already exists in the applicable domain. This is the OU or CN you specify as the organizational unit in the HCP configuration of support for AD. The default for this in HCP is the CN Computers.
- Your DNS is configured on a Windows server.
- Your DNS contains a stub zone for HCP that’s configured for AD integration.
- Your DNS contains a forward lookup zone definition for the applicable AD domain.
- You have access to a Windows server from which you can configure your DNS.
- Optionally, you have prepopulated the domain controller filter list even if HCP was not joined to Active Directory at the time.

Considerations for the information you need to supply

These considerations apply to the information you need to supply when configuring HCP support for AD:

- Before configuring AD support in HCP:
  - Create an AD group in the target domain. Give the group permission to add members to itself. Then give the group these permissions in the specified OU:
    - Read all properties on descendant computer objects
    - Write all properties on descendant computer objects
    - Change password on descendant computer objects
    - Reset password on descendant computer objects
    - Delete on descendant computer objects
    - Create computer objects in this object and all descendant objects
    - Delete computer objects in this object and all descendant objects
  - Create an AD user account and add it to only that group. This is the user to specify as the domain user in the AD configuration in HCP.
  - If HCP is not joined to AD, you can still prepopulate the domain controller filter list.
- Allow a new computer account for use in querying AD for groups to be created automatically. Do not create this account ahead of time.
- If you have more than one HCP system for which you are enabling support for AD, specify a computer account name that’s unique among those systems.
- By default, for the OU in which computer accounts will be created, HCP uses CN=Computers. For the computer account, HCP uses HCPSrv-*hcp-name* (for example, HCPSrv-hcp), where *hcp-name* is the first segment of the domain name associated with the [hcp_system] network.

Required permissions for Active Directory Domain

When HCP joins a domain, it creates an HCP Computer account by authenticating with the user account created by the Active Directory domain admin. The HCP Computer Account is used in all Active Directory operations unless the HCP needs to rejoin the domain. Using the HCP Computer Account for authentication, HCP then joins each of the HCP nodes to the domain through Samba which is required for CIFS authentication of legacy applications.

Once HCP has successfully joined the domain, the HCP Computer Account will update SPNs and add new nodes to the domain if physical nodes are added to the HCP system. HCP will automatically change the password of the HCP Computer Account every 30 days.

The following permissions are required by HCP to join the Active Directory Domain:

- For the HCP Admins SELF group you need read and write permissions. They are required to add the computer object to the group OU permissions.
- Create Computer objects and Delete Computer objects permissions are required to create the HCP Computer Account.
- Change Password and Reset Password permissions are required to reset the password of the HCP Computer Account.
- Read All Properties, Write All Properties, and Delete permissions are required to create and update SPNs.

Configuring Active Directory to support HCP

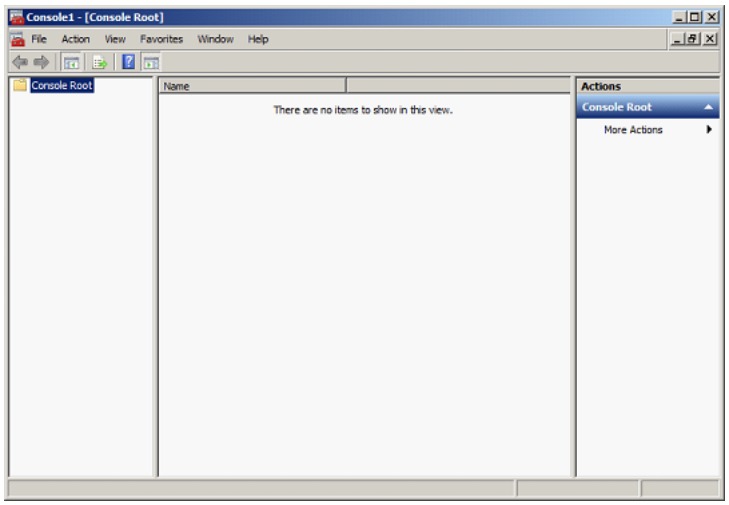
To enable SSL secured LDAP communication between HCP and AD, you need to create an SSL certificate on each domain controller in AD used by HCP. Installing a valid certificate on a domain controller automatically enables SSL connections for both LDAP and global catalog traffic.

If you don't want to secure communication, skip Step 1.

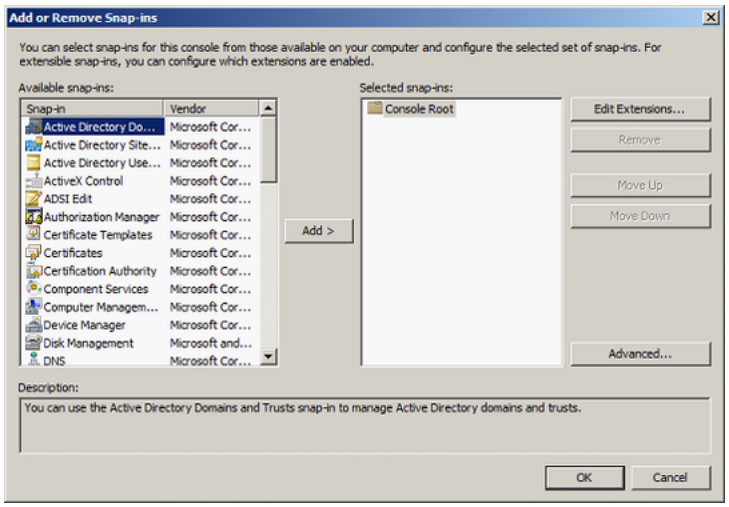
To create SSL certificates for communication between HCP and AD, you need to create a certificate on every domain controller that communicates with HCP.

To create the SSL certificate, do the following:

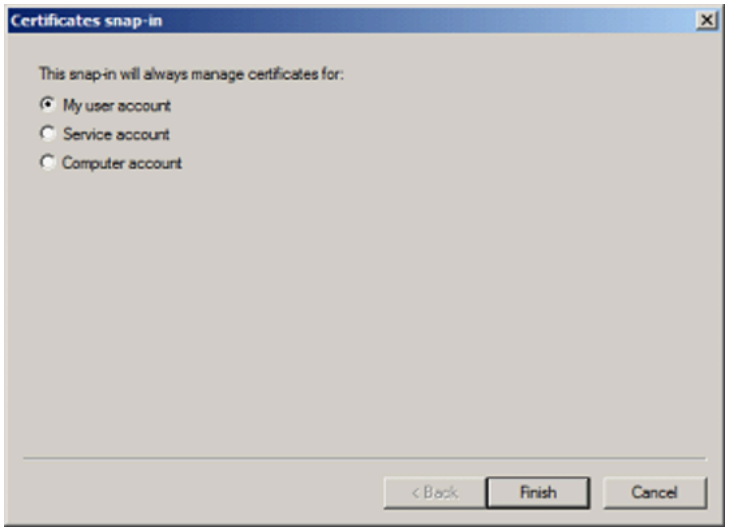
1. (Optional) Create the SSL certificate.
   a. On the Windows server, click Start.
   b. In the Search programs and files field, enter: `mmc`
   The Console1 - [Console Root] window opens.



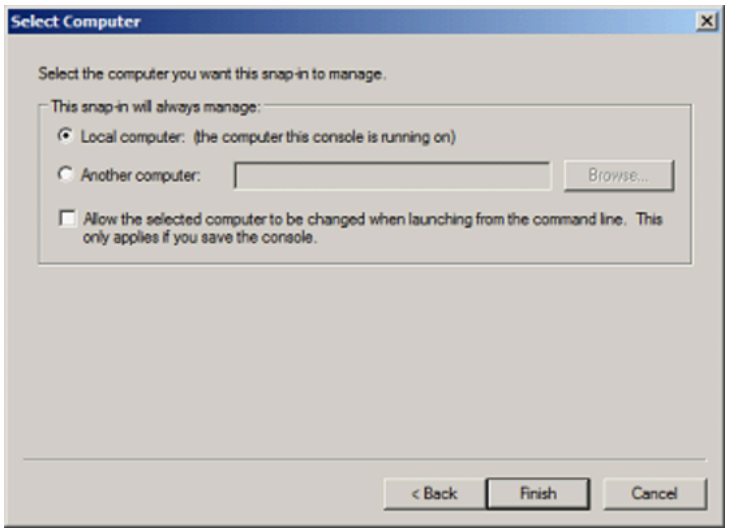
   c. On the File menu, select Add/Remove Snap-in.
   The Add or Remove Snap-ins window opens.



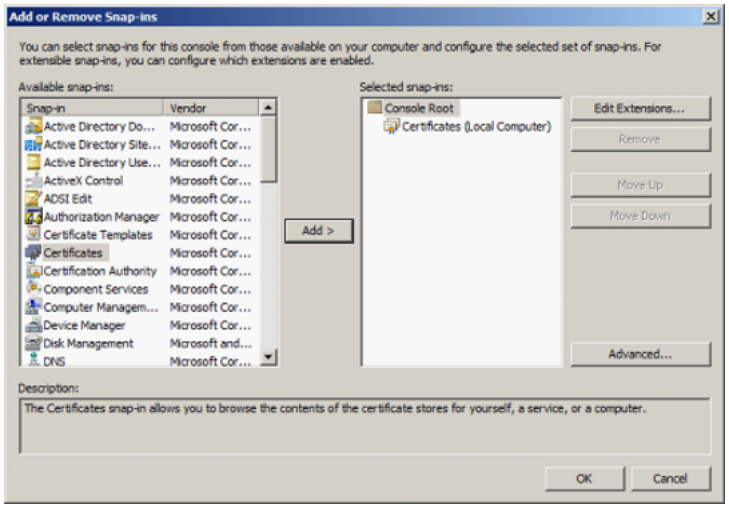
   d. In the Available snap-ins list, select Certificates, then click Add.
   The Certificates snap-in window opens.



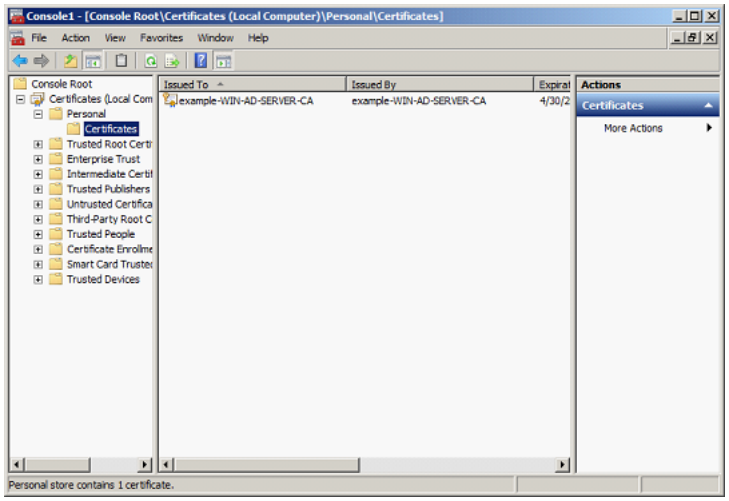
e. Select Computer account, then click Next.
The Select Computer window opens.



f. Click Finish.
Certificates (Local Computer) appears in the Selected snap-ins list in the Add or Remove Snap-ins window.



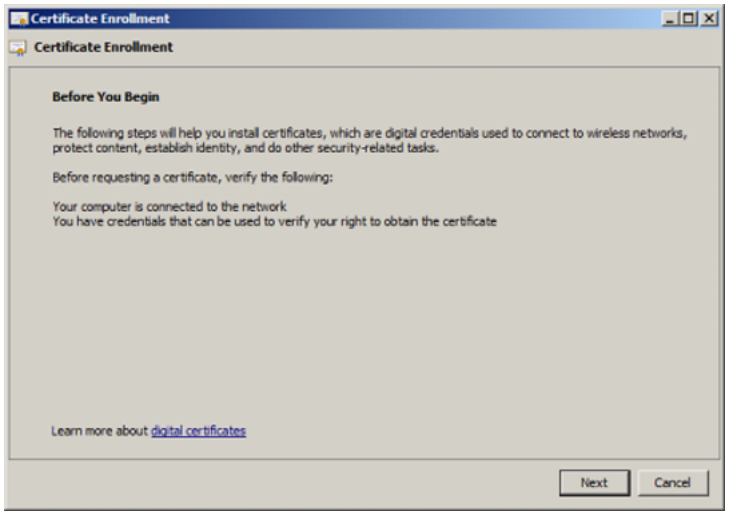
g. Click OK.
h. In the tree view in the left panel of the Console1 - [Console Root] window, expand Certificates (Local Computer) > Personal, then select Certificates.
The middle panel in the window lists information about the CA root certificate.



Note: The CA root certificate is only shown on the Domain Controller where the CA service is installed.

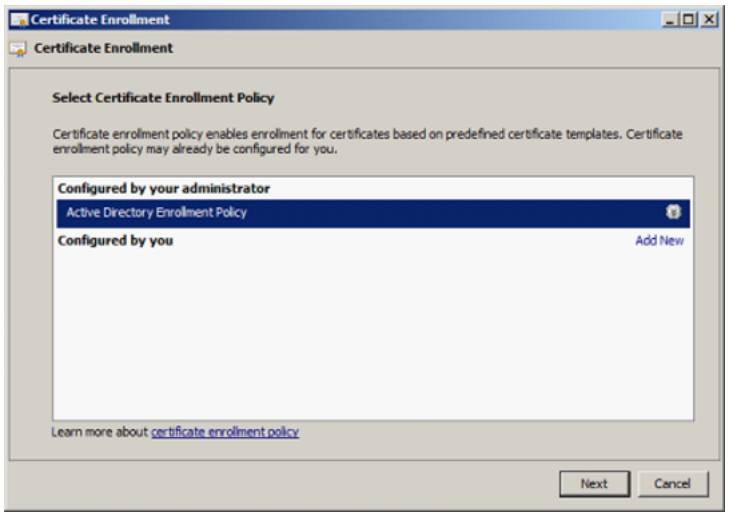
i. On the Action menu, select All Tasks > Request New Certificate.

The Certificate Enrollment window opens.



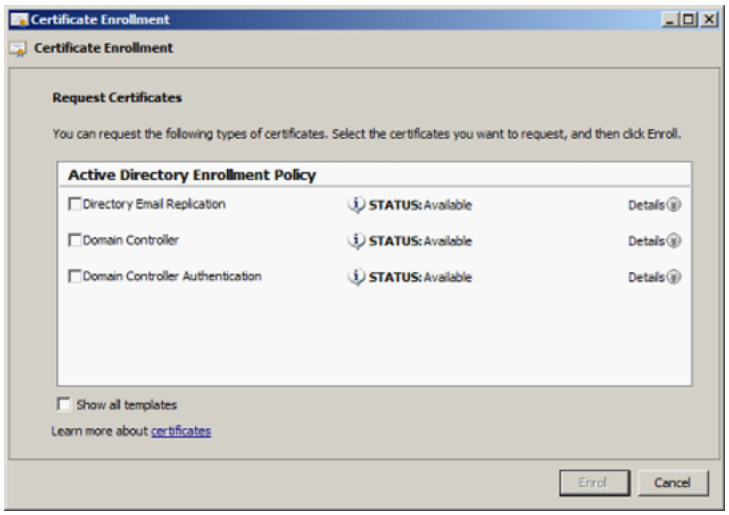
j. Click Next.

The Select Certificate Enrollment Policy page appears.

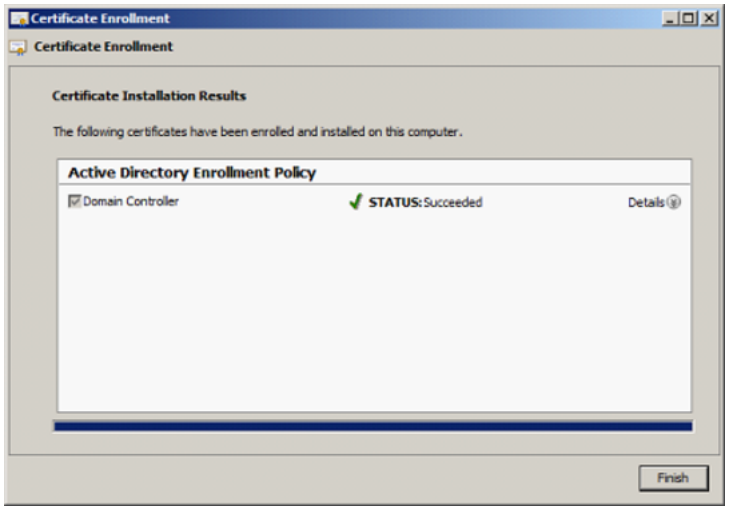


k. Click Next.

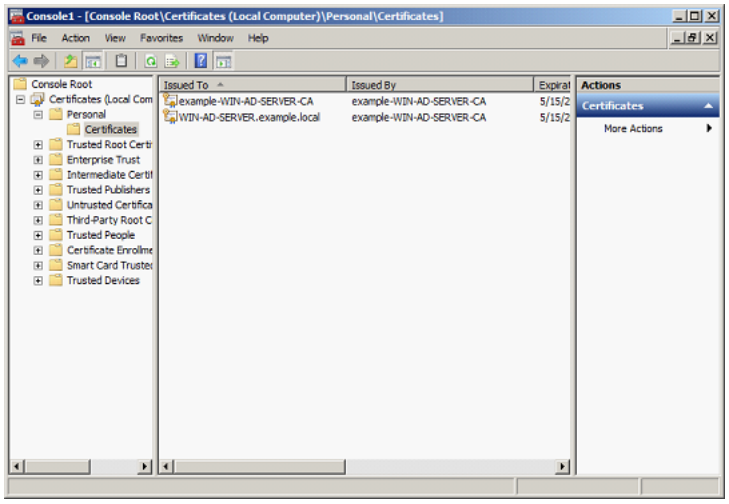
The Request Certificates page appears.



l. Select Domain Controller. Then click Enroll.
The Certificates Installation Results page appears.



m. Click Finish.
The Certificates list now includes the SSL certificate for LDAP communication.



The value in the Issued To column for this certificate is the concatenation of the computer name and the FQDN of the AD domain (for example, WIN-AD-SERVER.example.local).

2. (Optional) Export the SSL certificate.
If you are securing communication between HCP and AD, you must export the SSL root certificate of the CA that you created in Create the SSL certificate so that you can upload it to HCP. If you did not create an SSL certificate, skip this step.
   a. 1.On the Windows server running the AD CA, click Start.
   b. In the Search programs and files field, enter: `cmd`
   A Windows command prompt window opens.
   c. Change to the directory to which you want to write the file containing the exported certificate.
   d. Enter the following command to export the certificate:
   `certutil -ca.cert` *`cert-name`*`.cer`

In this command, *cert-name* is the name (minus the `.cer` extension) of the file that will contain the exported certificate.

If the export is successful, the window displays the contents of the certificate followed by this message:

```
CertUtil: -ca.cert command complete successfully.
```

If you don't see this message, make sure the applicable AD domain has a domain controller that is configured with the CA role and that you ran this command on the domain controller that has the CA role installed.

After verifying, try the procedure again, starting from Step 9 in Create the SSL certificate.

e. Copy the file containing the exported certificate to the Windows client from which you plan to access the HCP System Management Console.

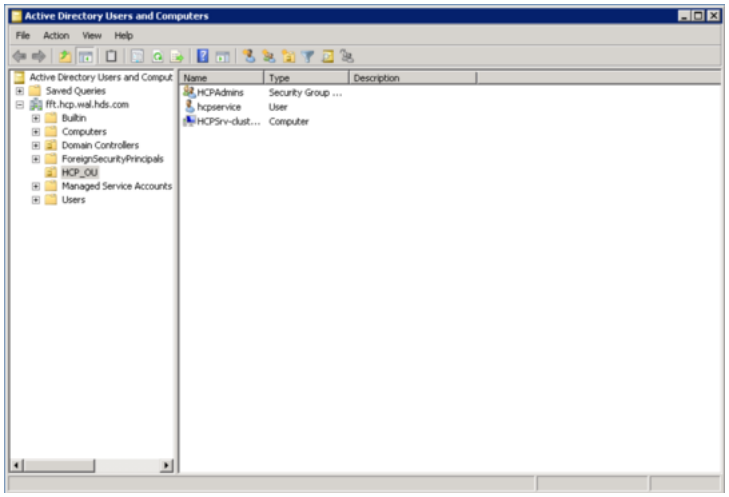
3. (Optional) Create an AD group.

For Active Directory to work with HCP, the HCP computer account must have certain permissions. The HCP computer account may either inherit its HCP management permissions from an AD group created specifically for this purpose or from the Domain Computers group.

If you are creating a new AD group to configure HCP management permissions:

a. On the Windows server from which you can access AD, click the Start button and select Administrative Tools > Active Director Users and Computers.

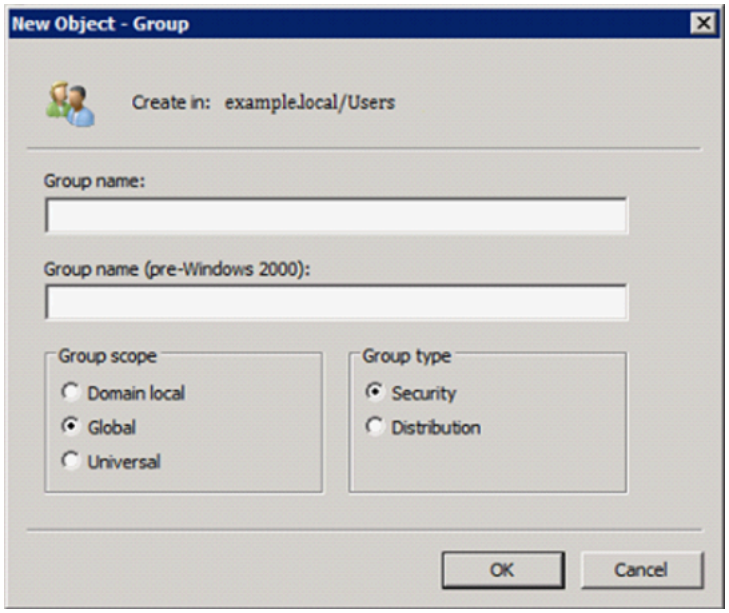
The Active Directory Users and Computers window opens.



b. On the View menu, select Advanced Features.

c. Under ad-domain-name, right-click the OU or CN in which you want to create the AD group and select New > Group from the drop-down menu.

The New Object - Group window opens.



d. In the Group name field, type a name for the new group (for example, "HCP Admins").

Then click the OK button.

e. In the left panel of the Active Director Users and Computers window, double-click the OU or CN in which you created the new group.

The middle panel of the Active Director Users and Computers window lists the items in the OU or CN, including the group you just created.

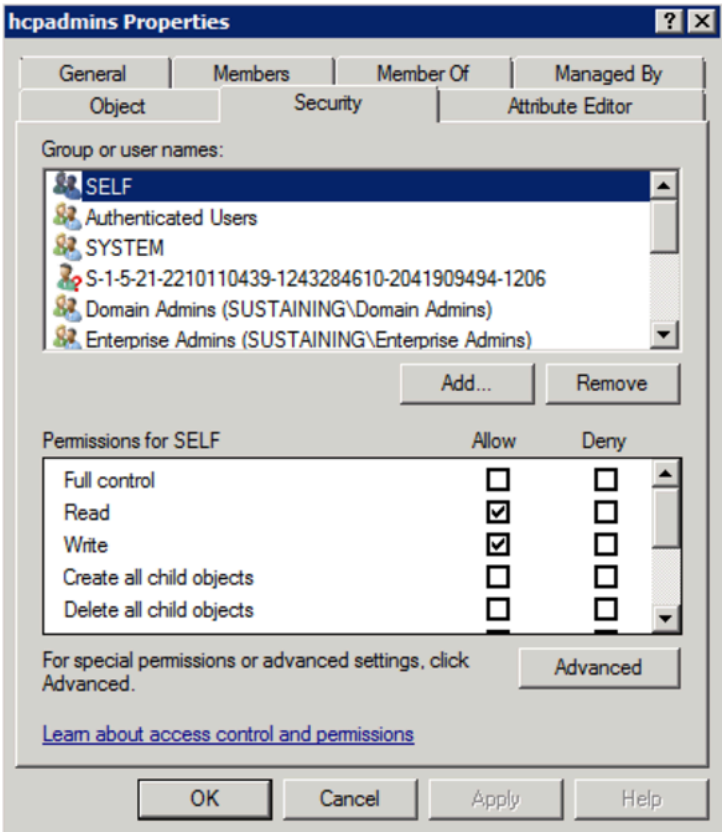
f. Right-click the new group and select Properties from the drop-down menu.

The Properties window opens.

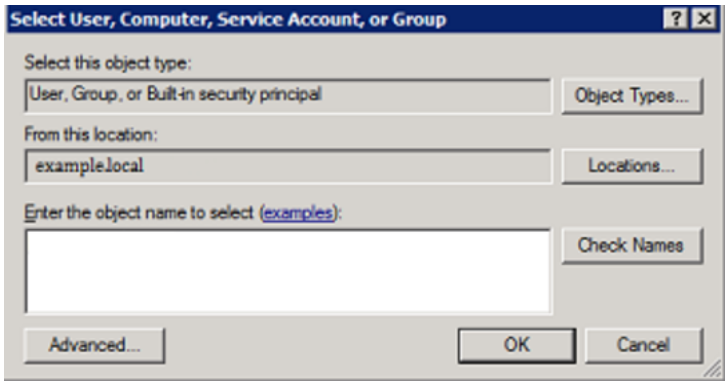
g. Click the Security tab.

h. With SELF selected in the Group or user names list, select the box for Write in the Allow column under Permissions for SELF.

Then click the OK button.



4. Give permissions to the new AD group or to the Domain Computers group.
   To grant the HCP computer account HCP management permissions, you need to assign the necessary permissions either to the AD group you created or to the Domain Computers group.
   HCP management permissions allow the HCP computer account to create computer accounts and manage computer account properties for each node in the system.
   To assign permissions to the AD group or to the Domain Computers group:
   a. In the left panel of the Active Director Users and Computers window, right-click the OU or CN in which you want HCP computer accounts to be created and select Properties from the dropdown menu.
      The Properties window opens.
   b. Click the Security tab.
   c. On the Security tab, click the Advanced button.
      The Advanced Security Settings window opens.
   d. Click the Add button.
      The Permission Entry for HCP window opens.
   e. Click the Select a Principle link.
      The Select User, Computer, Service Account, or Group window opens.



   f. In the Enter object name to select field, type the name of the AD group you created in the previous step, or type `Domain Computers` if you decided not to create an AD group for HCP management in the previous step.
      Then click the OK button.
      The Permission Entry window opens.
   g. In the Permission Entry window:
      i. In the Apply to field, select Descendant Computer objects.
      ii. Under Permissions, select the boxes in the Allow column for:
         - Read all properties
         - Write all properties
         - Delete
         - Change password
         - Reset password

      Then click the OK button.

Depending on the version of Active Directory that you are using, the Permission Entry page will appear as one of the two following images.

Figure. New version of AD

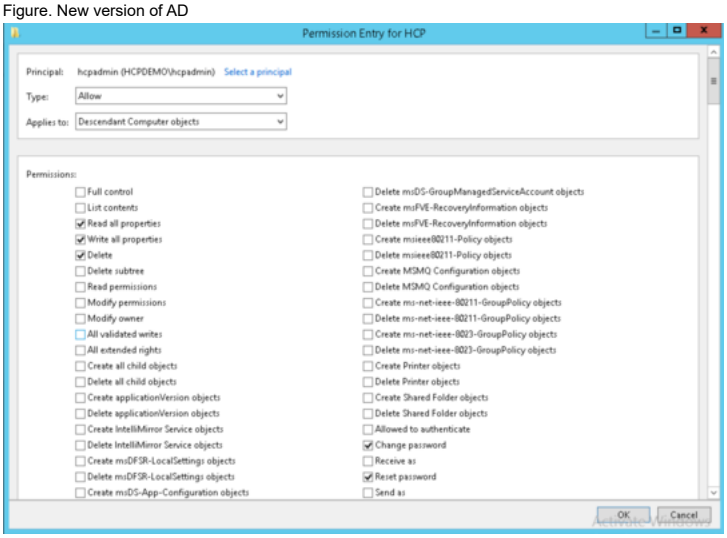
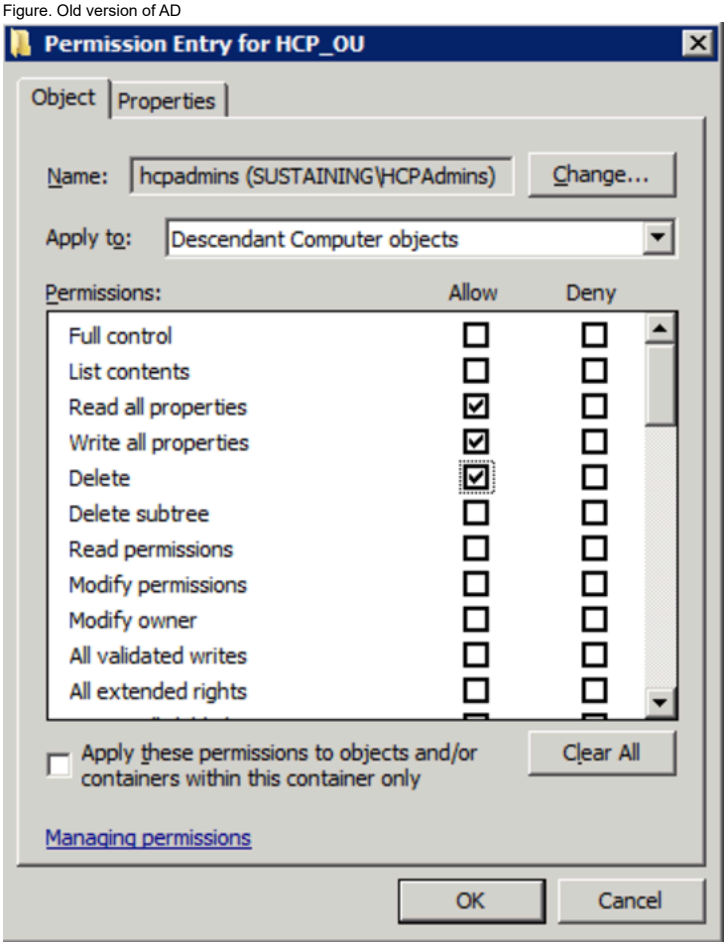
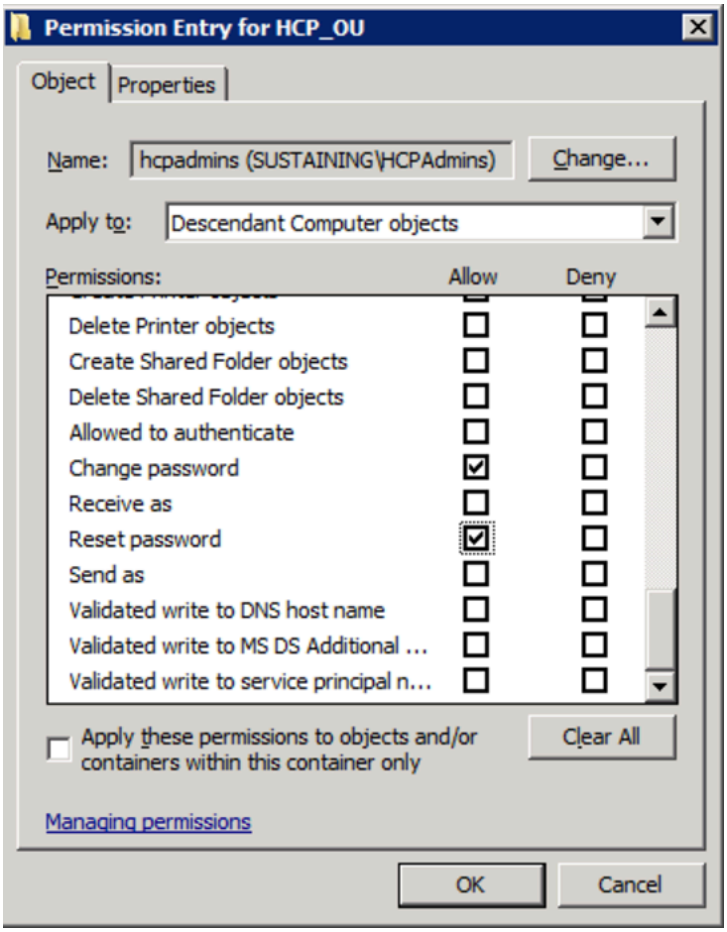


Figure. Old version of AD





h. In the Advanced Settings window, click the Add button again.
   The Select User, Computer, Service Account, or Group window opens.
i. In the Enter object name to select field, type the name of your AD group, or type `Domain Computers` if you decided not to create an AD group for HCP management in the previous step.
   Then click the OK button.
   The Permission Entry window opens.
j. In the Permission Entry window:
   i. In the Apply to field, select This object and all descendant objects.
   ii. Under Permissions, select the boxes in the Allow column for:
      - Create Computer objects
      - Delete Computer objects

   Then click the OK button.

   Depending on the version of Active Directory that you are using, the Permission Entry page will appear as one of the two following images.

Figure. New version of AD

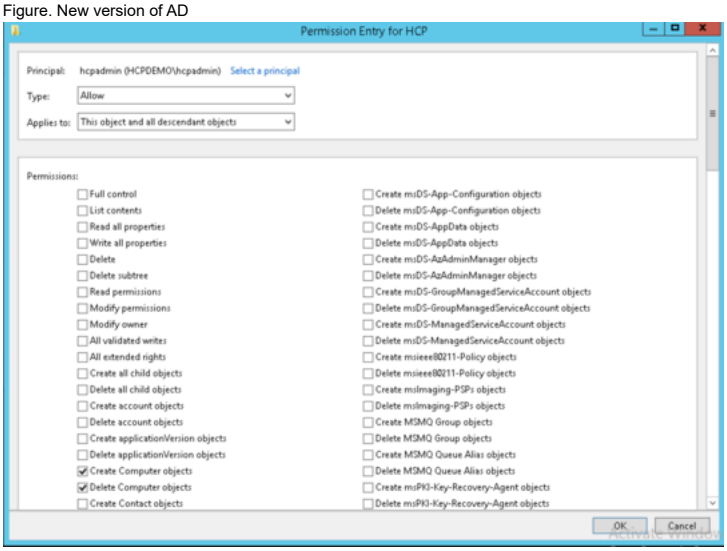
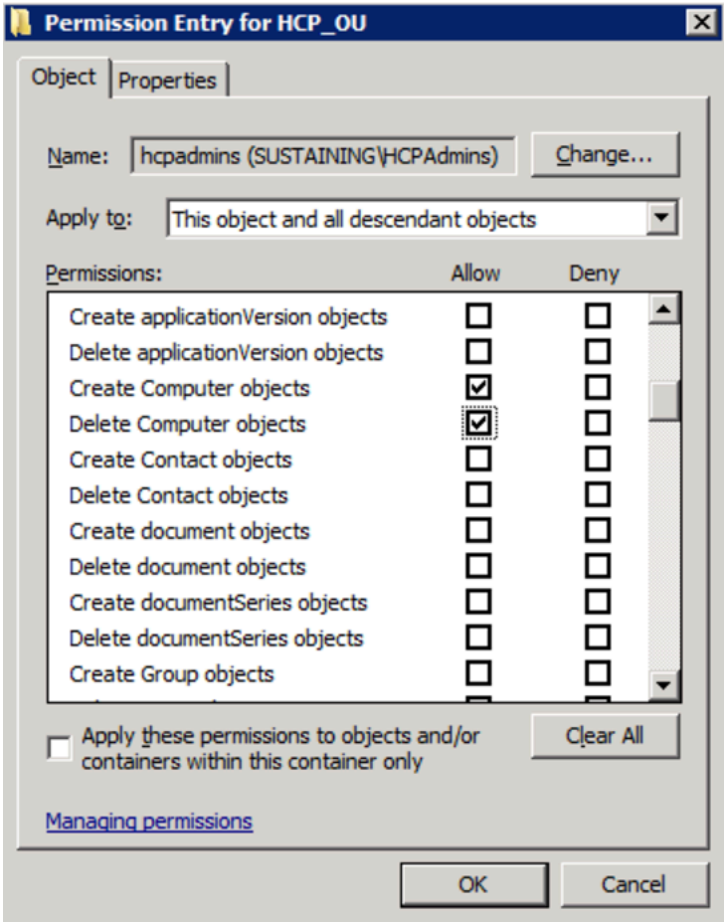


Figure. Old version of AD



k. In the Advanced Security Settings window, click the OK button to close the window.

l. In the Properties window, click the OK button to close the window.

5. Grant permissions to an AD user account.

To join HCP with your AD domain, you can either create a new AD user account that inherits permissions from the AD group you created in Create an AD group, or you can use an existing AD user account and assign it permissions in the OU or CN in which you want HCP computer accounts to be created. HCP uses this AD user account only once during the AD join process and then never uses the AD user account again. HCP does not store AD user account credentials.

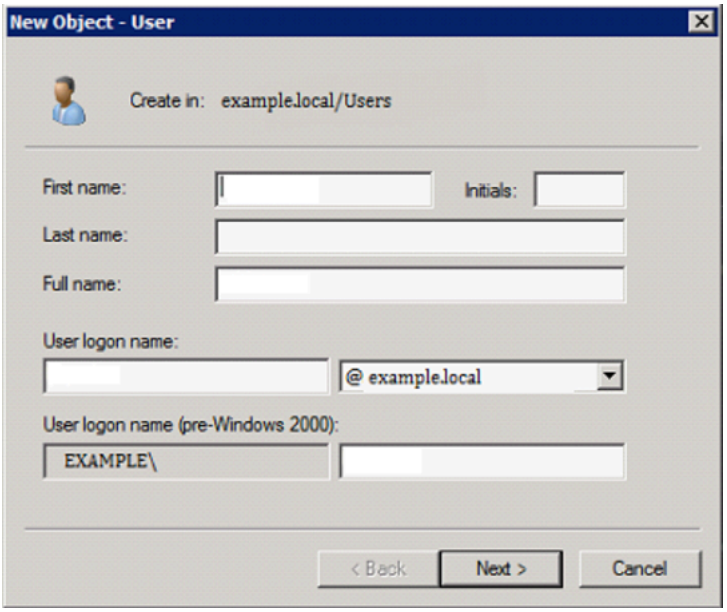
If you are creating a new AD user, follow the Creating a new AD user account and assigning it to your AD group procedure.

If you have disabled the Add HCP Computer Account to groups of Domain User check box on the HCP Active Directory page, you must use an existing AD user account. To grant permissions for an existing AD user account, follow the Configuring an existing AD user account for HCP management procedure.

To create a new AD user account and assign it to the AD group you created:

a. In the tree view in the left panel of the Active Director Users and Computers window, right-click the OU or CN in which you want to create the AD user account and select New > User from the dropdown menu. The New Object - User window opens.

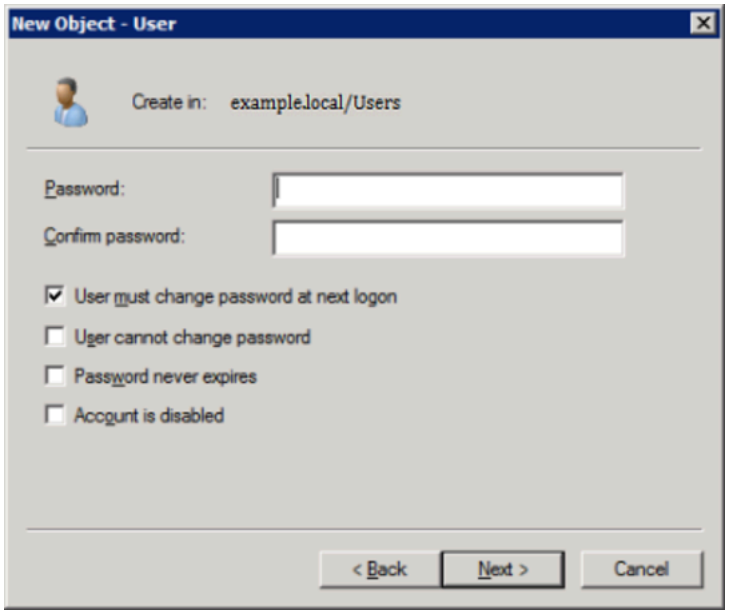
b. In the New Object - User window:



- In the First name field type a name for the user account (for example, HCP Admin).
- In the User logon name field, type a username for the user account (for example, hcpadmin).

Then click the Next button.
The display in the New Object - User window changes.

c. In the New Object - User window:



i. In the Password field, type a password for the user account.
ii. In the Confirm password field, type the password again.
iii. Deselect the User must change password at next logon option.

Then click the Next button.
The display in the New Object - User window changes.

d. Click the Finish button.
The list in the middle panel of the Server Manager window now includes the user account you just created.

e. Right-click the new user account and select Properties from the drop-down menu.
The Properties window opens.

f. Click the Member Of tab.

g. On the Member Of tab, click the Add button. The Select Groups window opens.

h. In the Enter the object names to select field, type the name of the group you created in Create an AD group, then click the OK button.
The AD user account inherits the permissions granted to the AD group you specify.

i. In the Properties window, click the OK button to close the window.

Note: You should perform the following step only if you already have an existing AD user account.

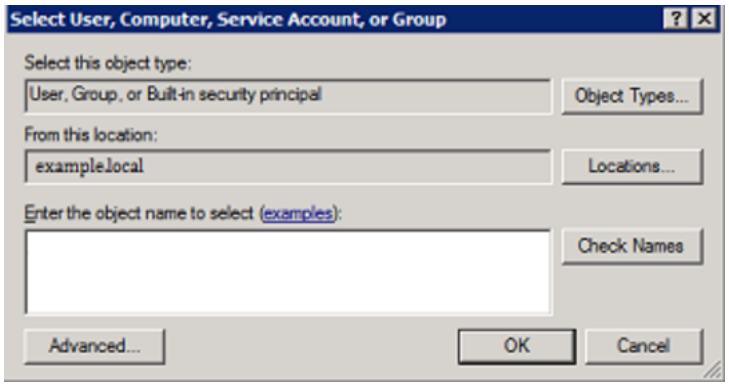
To grant HCP management permissions to an existing AD user account:

a. In the left panel of the Active Directory Users and Computers window, right-click the OU or CN in which you want computer accounts for the HCP nodes to be created and select Properties from the dropdown menu.
The Properties window opens.

b. Click the Security tab.

c. On the Security tab, click the Advanced button.
The Advanced Security Settings window opens.

d. Click the Add button.
The Select User, Computer, Service Account, or Group window opens.



e. In the Enter object name to select field, type the name of the AD user that is joining HCP to the AD domain.
Then click the OK button.
The Permission Entry window opens.

f. In the Permission Entry window:

i. In the Apply to field, select Descendant Computer objects.
ii. Under Permissions, select the boxes in the Allow column for:

- Read all properties
- Write all properties
- Delete
- Change password
- Reset password

Figure. New version of AD

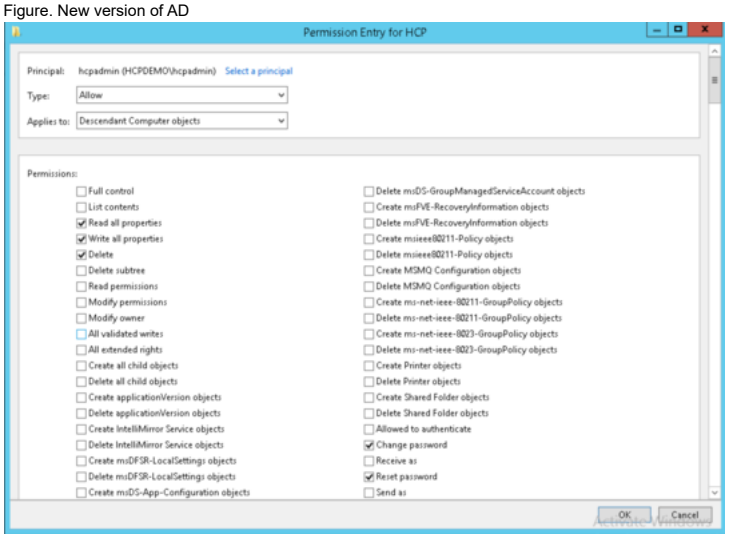
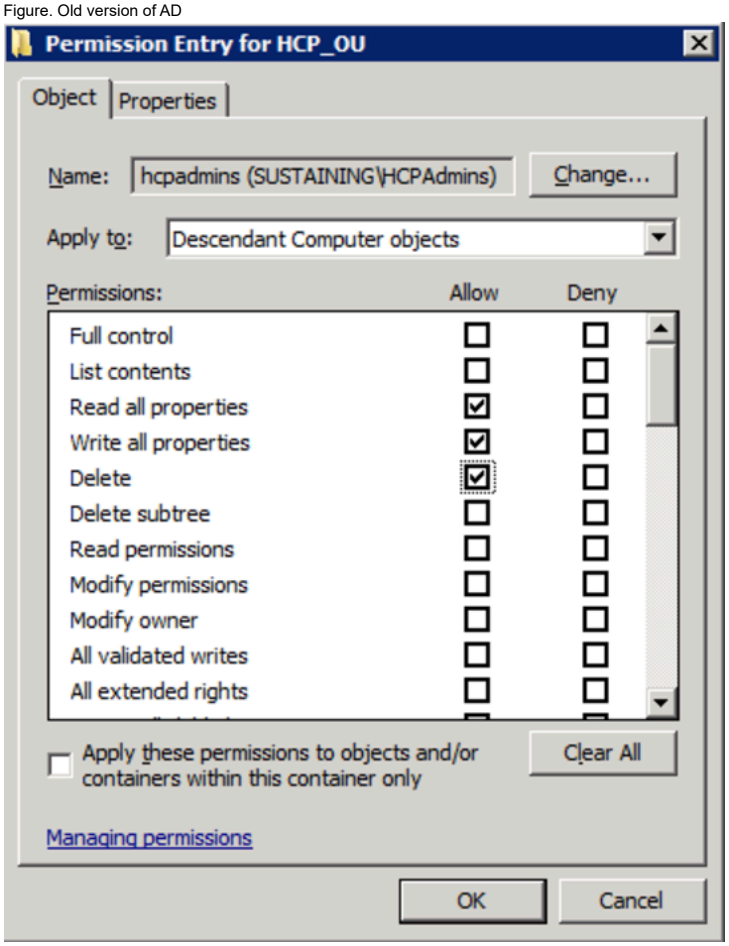
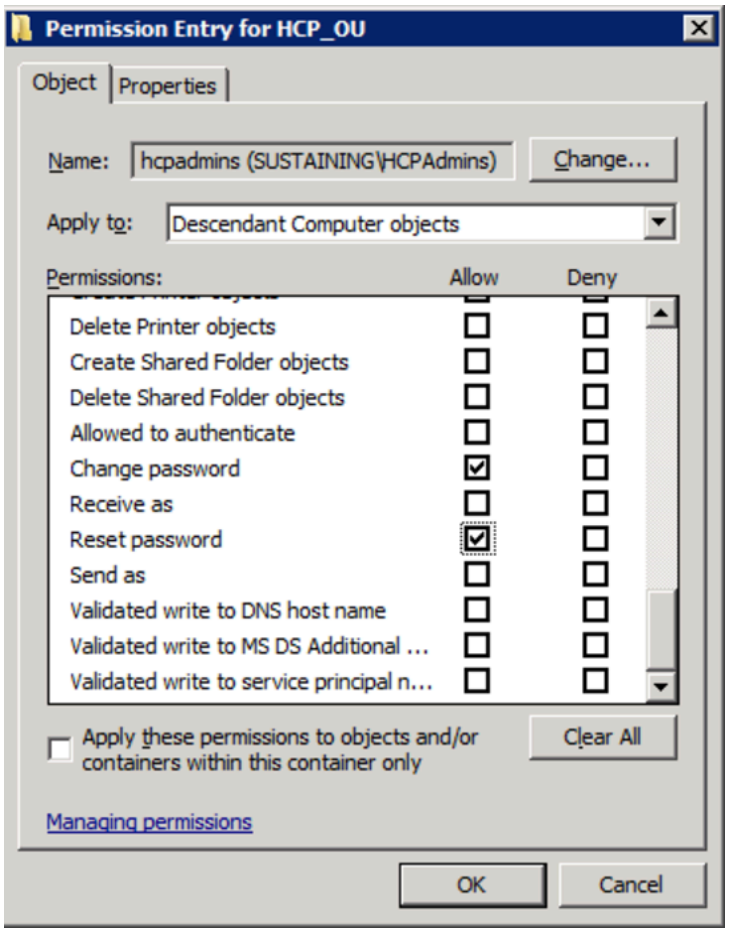


Figure. Old version of AD





Then click the OK button.

Depending on the version of Active Directory that you are using, the Permission Entry page will appear as one of the two following images.

g. In the Advanced Settings window, click the Add button again.

The Select User, Computer, Service Account, or Group window opens.

h. In the Enter object name to select field, type the name of the AD user that is joining HCP to the AD domain.

Then click the OK button.

The Permission Entry window opens.

Figure. New version of Permission Entry window

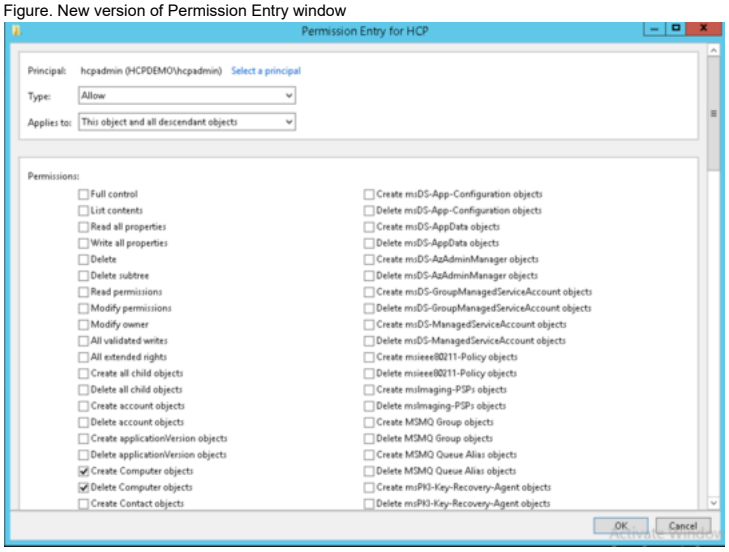
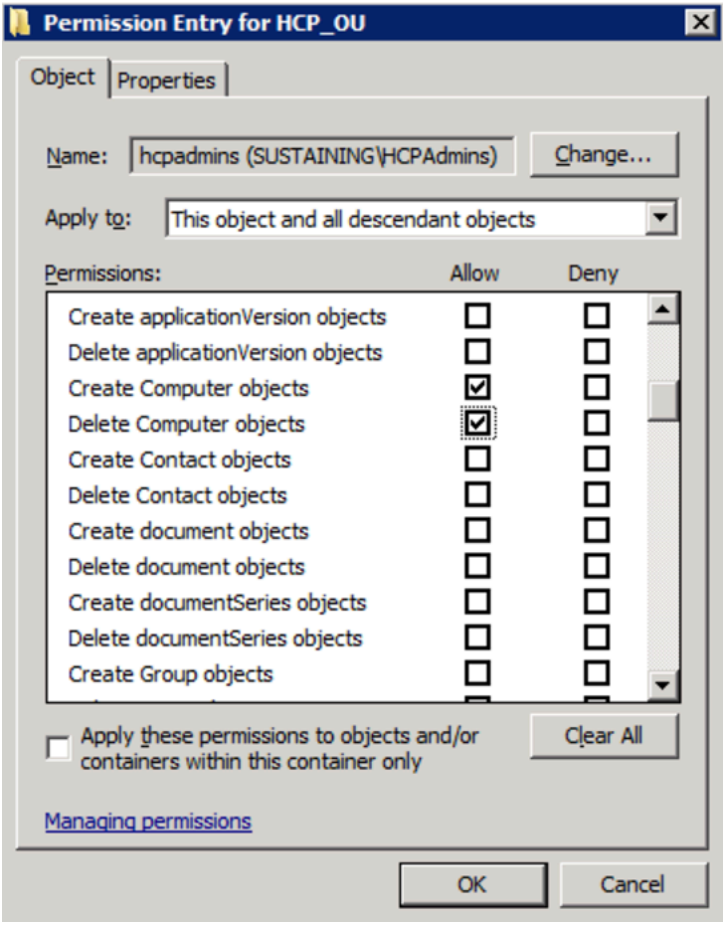


Figure. Old version of Permission Entry window



i. In the Permission Entry window:

   i. In the Apply to field, select This object and all descendant objects.

   ii. Under Permissions, select the boxes in the Allow column for:

      - Create Computer objects
      - Delete Computer objects

   Then click the OK button.

   Depending on the version of Active Directory that you are using, the Permission Entry page will appear as one of the two following images.

   Figure. New version of AD

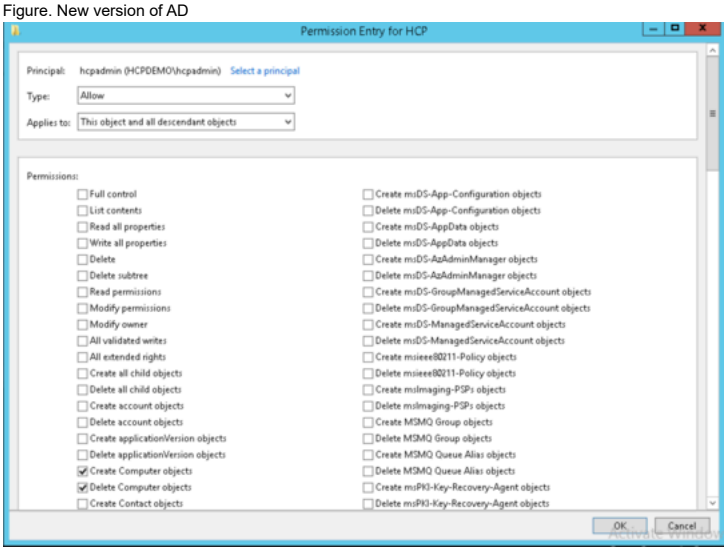
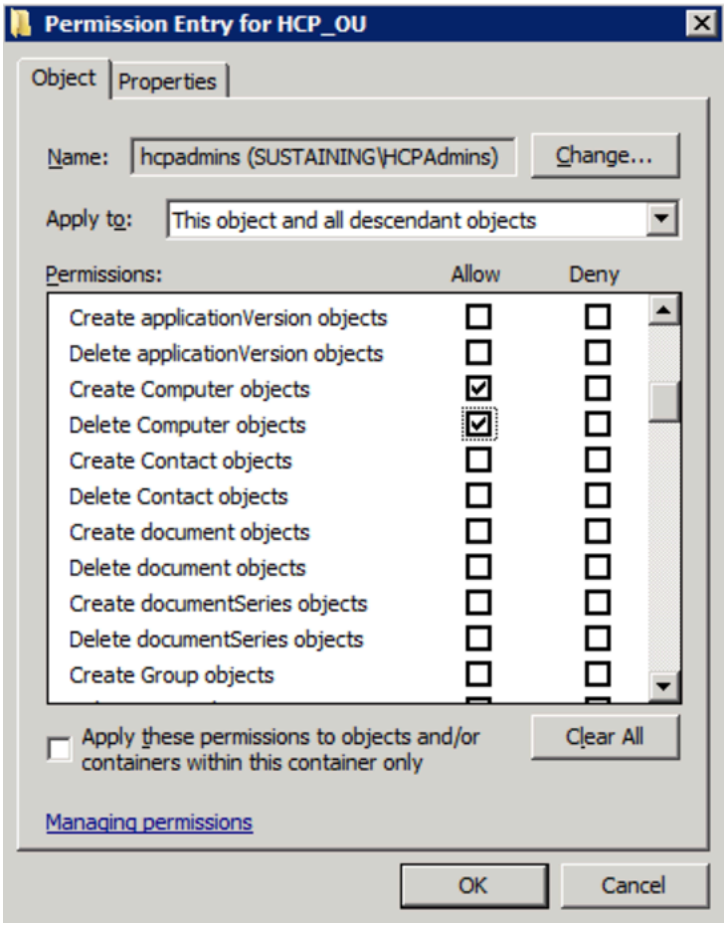


Figure. Old version of AD



j. In the Advanced Security Settings window, click the OK button to close the window.

k. In the Properties window, click the OK button to close the window.

6. (Optional) Create the reverse lookup zone for the AD domain.

If your AD domain does not already have a reverse lookup zone, you can create one for the applicable AD domain in your DNS.

a. On a Windows server from which you can configure your DNS, click the Start button and select Administrative Tools > Active Director Users and Computers.

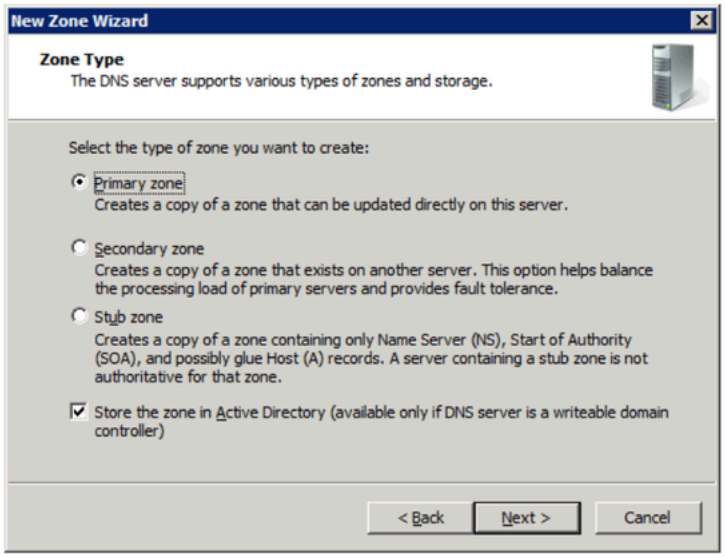
b. Under Roles in the tree view in the left panel of the Active Director Users and Computers window, expand DNS Server > DNS > ad-domain-name > Reverse Lookup Zones.

c. Right-click Reverse Lookup Zones and select New Zone from the drop-down menu.

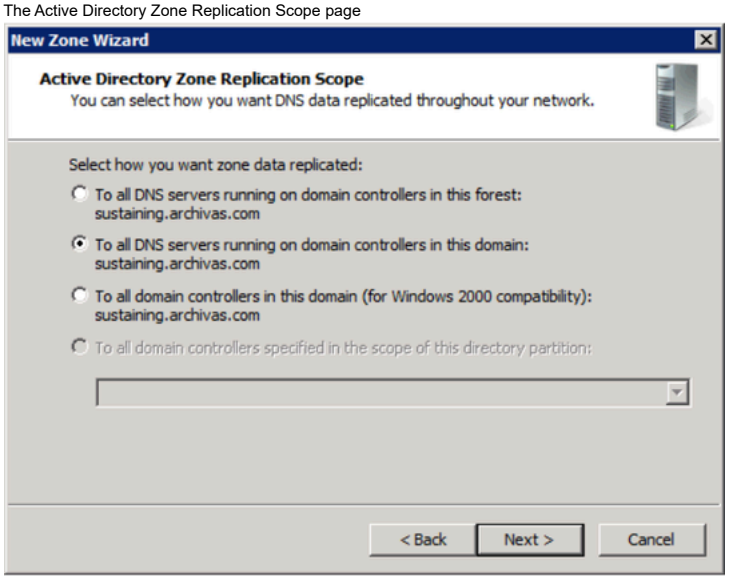
The New Zone Wizard window opens.

d. In the New Zone Wizard window, click the Next button.

The Zone Type page appears.

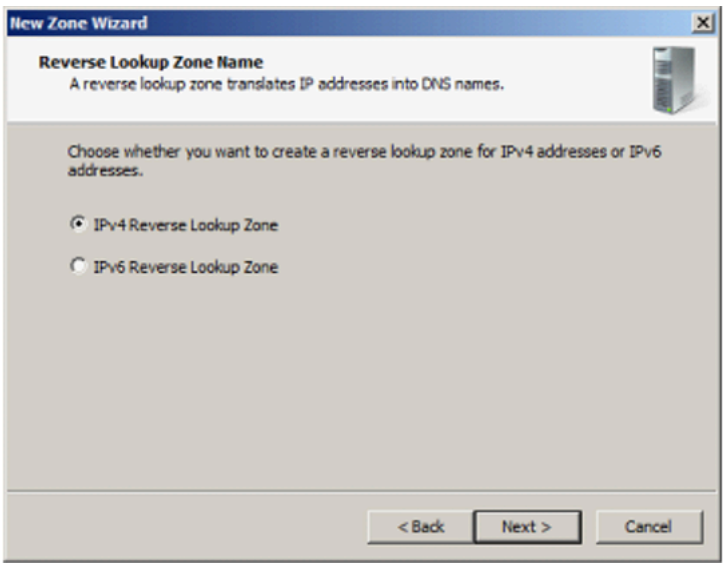


e. Select the Primary zone option. Then click the Next button.
The Active Directory Zone Replication Scope page

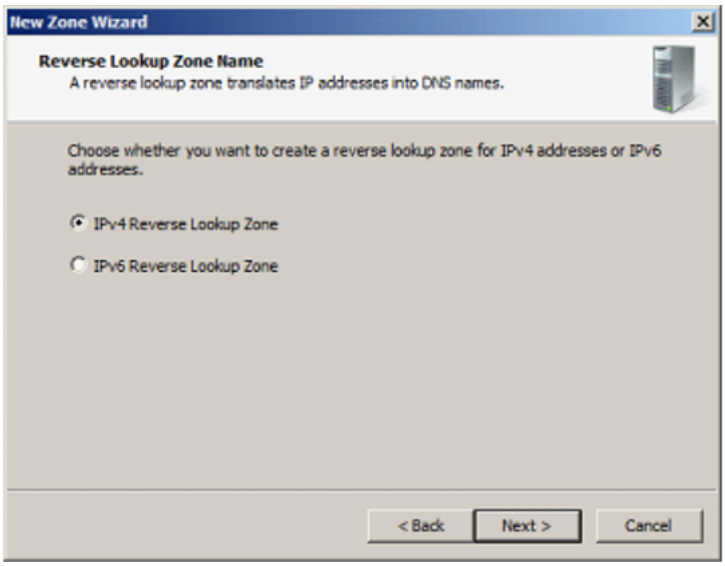


appears.

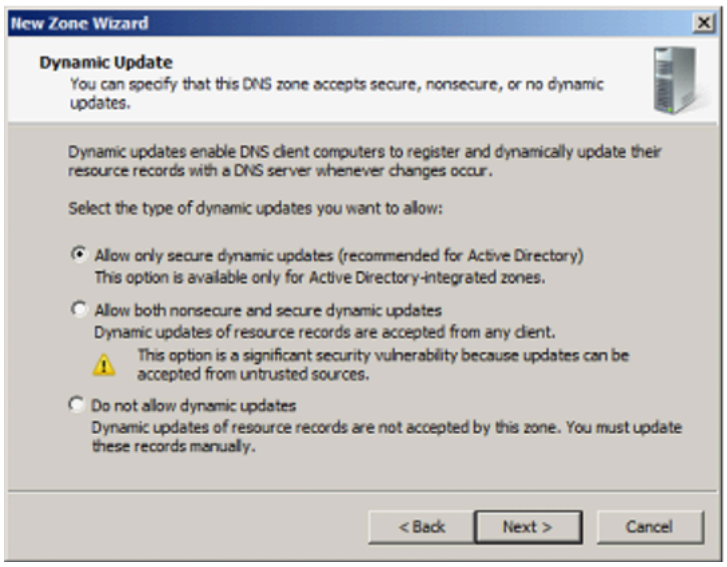
f. Click the Next button.
The Reverse Lookup Zone Name page appears.



g. Click the Next button.
The Reverse Lookup Zone Name page display changes.

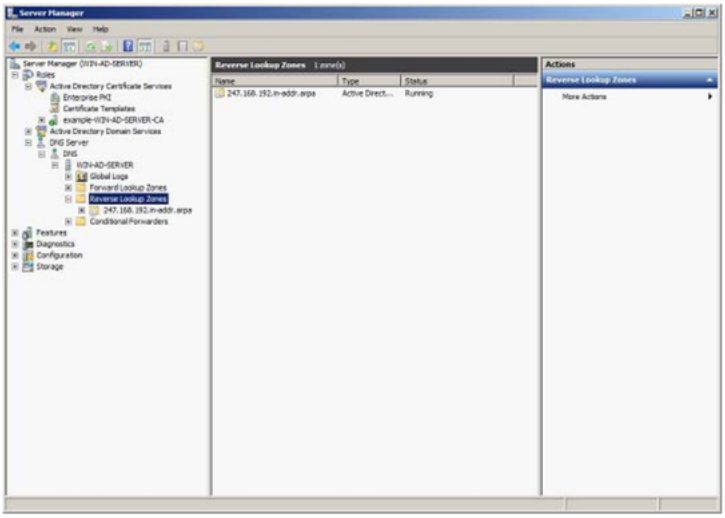


h. In the Network ID field, type the first three octets of the subnet for the applicable AD domain.
Then click the Next button.
The Dynamic Update page appears.



i. Click the Next button.
The Completing New Zone Wizard page appears.

j. Click the Finish button.
To see the reverse lookup you just created, expand Reverse Lookup Zones in the tree view in the left panel of the Active Director Users and Computers window. The name of the reverse lookup zone, which appears under Reverse Lookup Zones, consists of the first three octets that you specified in Step 8 above in reverse order, followed by `in-addr.arpa.`, as in this sample Active Director Users and Computers window.



7. Configure support for AD in HCP

Now that you've completed the steps for preparing AD for communication with HCP, you need to use the HCP System Management Console to configure support for AD in HCP.

Browser configuration for single sign-on with Active Directory

Configuring Windows Internet Explorer for single sign-on

Before you set up single sign-on, you need to configure Windows Internet Explorer. The following instructions apply with Windows Internet Explorer 11.

1. Open Internet Explorer.
2. On the Tools menu, click Internet Options.
3. In the Internet Options window, click the Security tab.
4. On the Security page, select Local intranet.
5. Click Sites.
6. In the Local intranet window, ensure that all the options are selected.
7. Click Advanced.
8. In the Add this website to the zone field, take either of these actions:
   - To enable single sign-on with HTTP, type:

     `http://*.hcp-name.domain-name`

     For example:

     `http://*.hcp.example.com`

   - To enable single sign-on with HTTPS, type:

     `https://*.hcp-name.domain-name`

     For example:

     `https://*.hcp.example.com`
9. Click Add.
10. Click Close.
11. In the Local intranet window, click OK.
12. In the Internet Options window, click the Advanced tab.
13. In the Settings list, under Security, select Enable Integrated Windows Authentication.
14. Click OK.
15. Close Internet Explorer.

Configuring Mozilla Firefox for single sign-on

1. Open Firefox.
2. In the address field in the Firefox window, enter:

   `about:config`
3. In response to the warning message, click I'll be careful, I promise!.
4. In the Preference Name list, double-click network.negotiate-auth.delegation-uris.
5. In the Enter string value window, type:

   `http://*.hcp-name.domain-name,https://*.hcp-name.domain-name`

   For example:

   `http://*.hcp.example.com,https://*.hcp.example.com`
6. Click OK.
7. In the Preference Name list, double-click network.negotiate-auth.trusted-uris.
8. In the Enter string value window, type:

   `http://*.hcp-name.domain-name,https://*.hcp-name.domain-name`
9. Click OK.
10. Close Firefox.

SSL server certificate providers

An SSL server certificate provides security for:

- HCP System Management Console
- HCP Tenant Management Console
- HCP management API
- Replication
- HTTP and WebDAV protocols
- HCP metadata query API
- HCP Search Console

HCP is installed with its own SSL server certificate. If you want, you can replace this with a different certificate.

SSL server certificates are available from several sources. The following table lists some vendors with products that are suitable for use with HCP.

Vendor	Suitable SSL Products	Website
thawte, Inc.	• SGC SuperCert • SSL Web Server Certificate	http://www.thawte.com

Vendor	Suitable SSL Products	Website
	• SSL123	
VeriSign, Inc.	• Secure Site Pro • Secure Site	http://www.verisign.com
Entrust, Inc.	• Entrust Certificate • Management Service	http://www.entrust.com
IPS Certification Authority, S.L.	• Certificado Digital de • Servidor SSL Tipo A1	http://www.ipsca.com/en
Comodo Group	• PremiumSSL • PremiumSSL Wildcard • InstantSSL Pro • InstantSSL	http://www.instantssl.com
GeoTrust, Inc.	• Enterprise SSL • True BusinessID • Power Server ID	http://www.geotrust.com