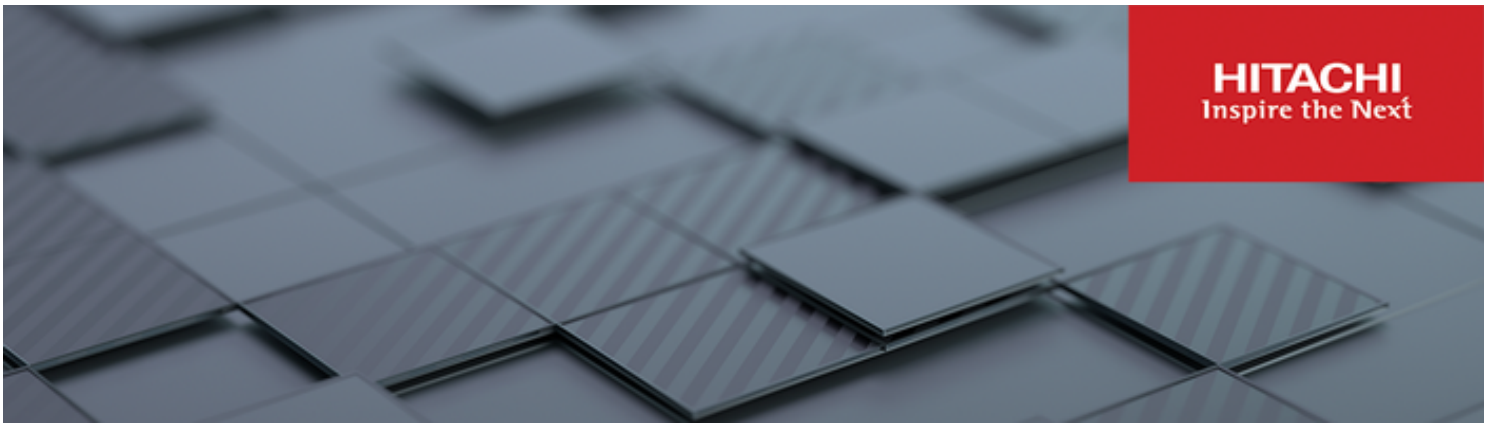


Content Platform System Management Help

9.7.x

Content Platform

MK-95HCPH001-20

Last updated: 2024-06-07

Generated from docs.hitachivantara.com

Hitachi Vantara

Managing a Tenant and Its Namespaces

Introduction to Hitachi Content Platform

Hitachi Content Platform (HCP) is a distributed storage system designed to support large, growing repositories of fixed-content data.

HCP stores objects that include both data and metadata that describes that data. HCP represents these 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 various HCP-specific interfaces.

About 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 internal processes 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.

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. Once 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 internal processes 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 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 own custom metadata and ACL.

HCP supports multipart uploads with 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 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.

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.

Each tenant can own multiple namespaces. An HCP system can have a maximum of 1,000 locally defined tenants and 10,000 locally defined namespaces. The system configuration can limit the number of namespaces an individual tenant can own.

Note: Replication can cause an HCP system to have more than 1,000 tenants and 10,000 namespaces.

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

System-level administrators are 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 are concerned with monitoring namespace usage at the tenant and namespace level, configuring individual namespaces, managing tenant-level users, and controlling access to namespaces.

System-level administrators create tenants. Tenant-level administrators create namespaces. System-level administrators can limit the number of namespaces an individual tenant can own.

Namespace access

HCP supports access to namespace content through several 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:

- 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*.
- 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 the SMTP protocol. This protocol is used only for storing email.

The namespace access protocols are configured separately for each namespace and are enabled or disabled independently of each other.

The REST, S3 compatible, and CIFS protocols can be configured to require authentication. To use a protocol that requires authentication, users and applications must present valid credentials for access to the namespace.

If the REST, S3 compatible or CIFS protocol is enabled but is not configured to require authentication or if the WebDAV or NFS protocol is enabled, users and applications can access the namespace anonymously. You can create a secure namespace by enabling only protocols that require authentication.

HCP Namespace Browser

The HCP Namespace Browser lets you manage content in and view information about 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

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 or 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 HCP metadata query engine:

The 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.
Note: When working with the metadata query engine, the Search Console is called the Metadata Query Engine Console.

The search facility is selected at the HCP system level. If you do not select the search facility, the HCP system does not support use of the Search Console to search namespaces.

The 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 facility automatically update their indexes to account for new and deleted objects and changes to object metadata.

Note: 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, objects with the S3 compatible API 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.

Tenant and namespace properties

Tenants and namespaces have certain properties that affect how they operate. Some of these properties are set when the tenant or namespace is created. Others are set after creation. Some can be modified after they are initially set; others cannot.

Namespace quota

The *namespace quota* for a tenant is the number of namespaces HCP reserves for the tenant out of the total number of namespaces the system can have. At any given time, the tenant can own only as many namespaces as specified by this quota.

The namespace quota is set when the tenant is created. HCP system-level administrators can change this quota at any time. However, the quota cannot be set lower than the number of namespaces the tenant currently owns.

Storage quotas

Both tenants and namespaces have hard and soft storage quotas:

hard quota
: An absolute number of bytes. For a tenant, it is the total amount of storage available to that tenant for allocation to its namespaces. For a namespace, it is the total amount of space available for storing objects in that namespace, including object data, metadata (except ACLs), and the redundant data required to satisfy the namespace DPL.
Note: 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 the tenant's namespaces can exceed the hard quota for the tenant.

soft quota
: The percentage point at which HCP notifies the tenant that allocated storage space is being used up. For a tenant, the soft quota measures the space used in all the namespaces the tenant owns relative to the hard quota for that tenant. For a namespace, the soft quota measures the space used in just that namespace relative to the hard quota for that namespace.

The storage quotas for a tenant are set when the tenant is created. HCP system-level administrators can change these quotas at any time. However, the hard quota for a tenant cannot be set lower than the amount of space the tenant has currently allocated to its namespaces.

The storage quotas for a namespace are set when the namespace is created. You can change these quotas at any time. However, the hard quota for a namespace cannot be set lower than the amount of space currently used in the namespace. And, the total of the hard quotas for all the namespaces owned by a tenant cannot exceed the hard quota for that tenant.

Data protection level

Each namespace has a *data protection level* (DPL) that specifies how many copies of each object HCP must maintain. HCP stores each copy of an object in a different location. All but one of these copies can become unavailable (for example, due to a hardware outage) without affecting access to the object.

The DPL for a namespace can be one (if allowed by the HCP system configuration), two, three, four, or dynamic. The highest allowed DPL is also determined by the HCP system configuration.

When the DPL is set to dynamic, the namespace uses the current HCP system-level DPL setting. Typically, this is the optimal DPL for the system configuration. If the system-level DPL setting changes, HCP adjusts the number of copies of objects in the namespace to match the new setting.

The DPL affects the amount of storage used when data is added to the namespace. With a DPL of one, HCP stores only one copy of the object. With a DPL of two, HCP stores two copies, thereby using twice as much storage.

The DPL for a namespace is set when the namespace service plan is created. You can change this setting at any time.

Cryptographic hash algorithm

At object creation, HCP uses a cryptographic hash algorithm to calculate a hash value for the object from the object data. HCP then uses this hash value to ensure the integrity of the object over time.

HCP supports these cryptographic hash algorithms:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- RIPEMD-160

The cryptographic hash algorithm HCP uses for a namespace is set when the namespace is created. Once set, it cannot be changed.

HCP Retention mode

Each object has a *retention setting* that specifies how long the object must remain in the namespace before it can be deleted; this duration is called the *retention period*. While an object cannot be deleted due to its retention setting, it is said to be *under retention*.

Retention mode is a property of a namespace that affects which operations are allowed on objects under retention. A namespace can be in either of two retention modes:

- In *compliance mode*, objects that are under retention cannot be deleted through any mechanism. Additionally, the duration of a retention class cannot be shortened, and retention classes cannot be deleted. Similarly, the Minimum Retention after Initial Unspecified value cannot be shortened and cannot be deleted.
- In enterprise mode, you can use the Tenant Management Console to delete objects under retention if you have the compliance role. This is called *privileged delete*.

  Also in enterprise mode, you can shorten the duration of a retention class, and you can delete retention classes.

  Note: Users can perform privileged deletes in a namespace that's in enterprise mode. To do this, however, they need the privileged data access permission.

The retention mode for a namespace is set when the namespace is created. You can change the retention mode of a namespace from enterprise to compliance mode but cannot do the reverse.

You can create namespaces in compliance mode only if allowed to do so by the tenant configuration. HCP system-level administrators can change this configuration from not allowing the creation of namespaces in compliance mode to allowing it. However, they cannot do the reverse.

Namespace owner

A namespace can optionally have an owner that corresponds to an HCP or Active Directory® (AD) user. Assuming that the user has the allow namespace management property, the owner of a namespace can use the S3 compatible and HCP management APIs to:

- View and change the versioning status of the namespace
- Delete the namespace
- See the namespace in a namespace listing

You can also use the Tenant Management Console and HCP management API to perform these activities if you have the administrator role, even if you're not the namespace owner.

You can specify the owner of a namespace when you create the namespace or at any time thereafter. You can also change namespace owners at any time.

When the S3 compatible API is used to create a namespace, the namespace creator automatically becomes the namespace owner.

When a user with an HCP user account becomes the owner of a namespace, that user account automatically gets the browse, read, write, read ACL, and write ACL data access permissions for that namespace. If the S3 compatible API was used to create the namespace, the owner user account also automatically gets the delete permission for the namespace.

You can limit the number of namespaces that can be owned by a single user. You can change this limit at any time.

Namespace tags

A tag is an arbitrary text string associated with a namespace. You can associate up to ten tags with any given namespace, and you can use the same tags for multiple namespaces.

You can use tags to group namespaces and filter namespace lists. For example, if you've created multiple namespaces for a company named ABC Corporation, you could associate the tag ABC with each of those namespaces. Then you could filter a list of namespaces to display only the namespaces with that tag.

You can associate tags with a namespace when you create the namespace or at any time thereafter. You can also remove tags from a namespace at any time.

Default retention setting

Each namespace has a default retention setting. This is the setting applied to an object when it is stored in the namespace unless the retention setting is explicitly specified in the request to store the object. After an object is stored, users can change its retention setting (subject to the rules for changing retention settings).

When you create a namespace, its default retention setting is Deletion Allowed. Objects with this retention setting can be deleted at any time except when they're on hold.

You can change the default retention setting for a namespace at any time. Changing this setting does not affect existing objects in the namespace.

Default shred setting

Shredding, also called *secure deletion*, is the process of overwriting the places where all the copies of an object were stored in such a way that none of the object data or metadata, including custom metadata, can be reconstructed. Each object has a shred setting that determines whether it is shredded when it's deleted from the namespace.

Each namespace has a default shred setting. This is the setting applied to an object when it is stored in the namespace unless the shred setting is explicitly specified in the request to store the object. After an object is stored, users can change its shred setting from don't shred to shred but not from shred to don't shred.

When you create a namespace, its default shred setting is not to shred. You can change this setting at any time. Changing this setting does not affect existing objects in the namespace.

Note: If HCP is allowed to use erasure coding to implement replication of a namespace, setting the default shred setting to shred for that namespace can significantly increase the load on all systems in the replication topology.

Default index setting

Each object in the repository has an index setting that is either true or false. This setting is present even if the namespace containing the object is not search-enabled or indexed.

The metadata query engine uses the index setting for an object to determine whether to index custom metadata for that object. The HCP search facility uses the index setting to determine whether to index the object at all. Metadata query API requests can use the index setting as a search criterion. Additionally, third-party applications can use this setting for their own purposes.

Note: If custom metadata indexing is disabled, the metadata query engine does not index custom metadata regardless of the index settings for individual objects.

Each namespace has a default index setting. This is the setting applied to an object when it is stored in that namespace unless the index setting is explicitly specified in the request to store the object. After an object is stored, users can change its index setting.

When you create a namespace, its default index setting is to index. You can change this setting at any time. Changing this setting does not affect existing objects in the namespace.

Default POSIX UID, GID, and permissions

To support the NFS protocol, HCP supports certain POSIX metadata for objects. This metadata includes the POSIX user ID (UID) of the object owner, the POSIX group ID (GID) of the owning group, and the POSIX permissions.

Note:

- POSIX object ownership is different from object ownership in HCP. The owner UID is not related to either HCP user accounts or Active Directory user accounts.
- POSIX permissions are different from HCP data access permissions and access control lists. They affect the operations that clients can perform only through the CIFS and NFS protocols.

POSIX UIDs and GIDs are visible through the HTTP, WebDAV, CIFS, and NFS protocols. POSIX permissions are visible through the WebDAV and NFS protocols. They map to CIFS permissions, which are visible through the CIFS protocol.

For objects stored through NFS, the POSIX UID and GID are determined by the current NFS user. Objects stored through other protocols do not have an explicit UID or GID. Instead, when you use NFS to view these properties for such an object, you see the default UID and GID currently specified in the NFS protocol configuration for the namespace that contains the object.

When you create a namespace, the default UID and GID in the NFS protocol configuration are both set to 0 (zero). You can change these settings at any time.

POSIX permissions for objects, directories, and symbolic links stored through NFS are determined by the client. POSIX permissions for objects stored through other protocols are always 555. POSIX permissions for directories and symbolic links stored through other protocols are always 777.

HCP Retention-related properties

Ownership and permission changes for objects under retention

Namespaces have two properties that affect objects under retention:

- Whether changes to POSIX UIDs and GIDs and to object owners are allowed
- Which custom metadata operations are allowed

Custom metadata operations for objects under retention

Custom metadata is user-supplied information that describes an object in a namespace. For objects that are not under retention, users can add, replace, and delete custom metadata annotations as needed. For objects that are under retention, the operations allowed for custom metadata annotations are determined by a namespace-level setting.

You can configure a namespace to:

- Allow annotations to be added, replaced, and deleted for objects under retention
- Allow annotations to be added for objects under retention but not replaced or deleted
- Disallow all annotations operations for objects under retention

When you create a namespace, only the addition of annotations is allowed for objects under retention. You can change this setting at any time.

Protocol optimization and directory usage

HCP namespace access protocols are categorized as either cloud protocols or noncloud protocols. The cloud protocols are the REST and S3 compatible APIs. The noncloud protocols are WebDAV, CIFS, NFS, and SMTP.

Protocol optimization

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 these features

- Multipart uploads
- Management of multipart objects
- Erasure coding as protection type
- Unbalanced directory usage

You can change the protocol optimization setting for a namespace from optimized only for cloud protocols to optimized for all protocols only if the namespace does not contain any objects. You can change the setting from optimized for all protocols to optimized only for cloud protocols only if no noncloud protocols are enabled for the namespace.

The default protocol optimization setting for new namespaces is set by the HCP system administrator.

Directory usage

Directory usage defines how the objects are stored within the HCP and it allows the user to choose an approach that best matches their data use patterns.

HCP namespaces can use either balanced or unbalanced directory usage. You can configure this setting at the time of creating a namespace and cannot modify later. Balanced directory usage is selected by default. This type of directory usage requires a well distributed directory structure to avoid hot spotting and to ensure maximized performance. This setting can be applied to namespaces optimized for cloud protocols as well as for those optimized for all protocols.

With unbalanced directory usage, you do not need to know how the applications ingest data or ensure that the objects are distributed across a diverse directory structure. Unbalanced directory usage setting can only be applied to namespaces that are optimized only for cloud protocols.

XML checking for custom metadata

By default, when a custom metadata annotation is added to or replaced in a namespace, HCP checks whether it contains well-formed XML. If the XML is not well-formed, HCP rejects the annotation.

For any given namespace, you can choose to allow users to provide annotations in non-XML formats (for example, as thumbnail images to accompany large objects with image content). In this case, you need to disable custom metadata XML checking for the namespace so that HCP accepts non-XML annotations.

XML checking applies only when annotations are added to or replaced in a namespace. It does not apply to annotations that already exist in the namespace.

You can enable or disable custom metadata XML checking for a namespace at any time.

Note: If the XML in an annotation for an object includes a very large number of different elements and attributes, HCP may determine that the XML is not well-formed, even if it is, and reject the annotation. If this happens, the user can try restructuring the XML so that it includes fewer different elements and attributes. Alternatively, you can temporarily disable custom metadata XML checking to allow that XML to be stored in the namespace.

Versioning

Versioning is the creation of multiple versions of objects. Versioning is supported only with the REST and S3 compatible APIs. Users cannot create new versions of objects or access old versions through any other protocol.

Any given namespace can be configured to support versioning or not to support it. However, you cannot enable versioning for a namespace while the WebDAV, CIFS, NFS, or SMTP protocol is enabled for that namespace. Conversely, you cannot enable the WebDAV, CIFS, NFS, or SMTP protocol for a namespace while versioning is enabled for that namespace. You can disable versioning at any time.

When versioning is enabled for a namespace, you can set a time for version pruning. *Version pruning* is the automatic deletion of previous versions of objects that are older than a specified amount of time.

If you disable versioning after it was enabled, old versions of objects remain in the namespace and continue to be pruned according to the pruning settings. If you change the pruning settings, the new settings apply to old versions regardless of whether versioning is enabled.

You can create namespaces with versioning enabled only if allowed to do so by the tenant configuration. system-level administrators can change this configuration from not allowing the creation of namespaces with versioning enabled to allowing it. However, they cannot do the reverse.

Compatibility property

To support compatibility with other storage products, POSIX atime values can be synchronized with HCP retention settings. For information about the effects of this option, see *Using a Namespace*.

When you create a namespace, both of this features is disabled. You can enable or disable it at any time.

Disposition

Disposition is the automatic deletion of objects. Disposition can be enabled for:

- Objects with expired retention periods. To be eligible for disposition, an object must have a retention setting that's either:

    - A date in the past
    - A retention class with automatic deletion enabled that results in a calculated expiration date in the past
- Objects flagged as replication collisions.

Disposition has the benefit of automatically freeing storage space for the creation of more objects. Without disposition, users need to explicitly delete qualified objects to free the occupied space.

Disposition deletes only the current version of a versioned object. It does not delete old versions.

Disposition is enabled on a per-namespace basis. When you create a namespace, this feature is disabled. You can change this setting at any time.

Automatic abort of multipart uploads

After initiating a multipart upload, the user who initiated it can upload parts at any time until the multipart upload is completed or aborted. Completing a multipart upload creates a multipart object from the uploaded parts. Aborting a multipart upload causes the uploaded parts to be deleted. After a multipart upload is aborted, no more parts can be uploaded for it, and it cannot be completed.

Note: When a multipart upload is aborted, its parts may not be deleted immediately. However, an aborted multipart upload cannot be completed even if its parts have not yet been deleted.

If a multipart upload is never completed or aborted, the disjointed parts can remain in HCP indefinitely. Even though the multipart upload is incomplete, these parts count toward the storage used by the bucket where they were uploaded.

To prevent parts of multipart uploads from remaining in HCP indefinitely, the tenant administrator can set the maximum amount of time for which a multipart upload can remain incomplete before the multipart upload is automatically aborted. This time is counted from the time the multipart upload was initiated.

Each bucket has its own automatic abort time for multipart uploads. This time is not visible through the S3 compatible API. By default, the automatic abort time for new buckets is 30 days.

You can change the automatic abort time for a namespace at any time. When you change the time, the new time applies to all subsequent multipart uploads as well as to multipart uploads that are already in progress.

For example, if a user initiates a multipart upload on September 9th while the automatic abort time is set to 30 days, that multipart upload will be automatically aborted on October 9th. If, before October 9th, you change the automatic abort time to 35 days, the date on which the multipart upload will be automatically aborted changes to October 14th. If you change the automatic abort time to an amount of time that has already elapsed since the multipart upload was initiated, the multipart upload is immediately aborted.

Note: The value of the `x-amz-abort-date` header returned in response to an S3 compatible request to list the parts of a multipart upload is the date on which the multipart upload will be automatically aborted, as determined by the current automatic abort time setting.

Data access permission masks

A *data access permission mask* determines which of these operations are allowed in a namespace:

Read
: Lets users:

    - View and retrieve objects, including object metadata (system metadata, custom metadata, and ACLs)
    - View and retrieve previous versions of objects
    - List annotations for objects
    - List directory contents

Write
: Lets users:

    - Add objects to the namespace.
    - Modify system metadata. For users to modify the hold status of objects, privileged operations must also be allowed.
    - Add and replace custom metadata.
    - Add, replace, and delete ACLs.
    - Change object owners.

Delete
: Lets users delete objects and custom metadata from the namespace.

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.

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. For users to perform hold and release operations, write operations must also be allowed.

Search
: Lets users use the HCP metadata query API and the HCP Search Console to query or search the namespace. For users to query or search a namespace, read operations must also be allowed.

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 table below 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	✓	✓	✓			

A tenant initially has all permissions in its data access permission mask. When you create a namespace, it also has all permissions in its data access permission mask.

HCP system-level administrators can change the systemwide permission mask at any time. You can change the tenant and namespace permission masks at any time.

You can make a namespace effectively read-only be removing all operations except read from its data access permission mask.

Minimum data access permissions

The configuration of a namespace can include minimum data access permissions for all users (that is, authenticated users and users that access the namespace anonymously) and for authenticated users only. When accessing the namespace:

- Authenticated users have all the data access permissions associated with the applicable user account or group accounts and all the minimum data access permissions for authenticated users. Additionally:
  - When using a protocol that requires authentication, authenticated users may or may not also have the minimum data access permissions for all users. This is determined by a namespace option that's intended to support the following scenario:
    - Data can be written to the namespace only from within a secured environment and only from a limited number of client computers through a protocol such as NFS that does not support authentication. This requires write permission for all users.
    - Objects can be accessed from outside the secured environment but only through a protocol that requires authentication. This requires read permission but not write permission for authenticated users.
  - When using a protocol that does not require authentication, authenticated users also have the all minimum data access permissions for all users.

  Authenticated users also have any object-specific permissions granted to them by object ACLs.

- Unauthenticated users (that is, users who access the namespace anonymously) have the minimum data access permissions for all users and any object-specific permissions granted to all users by object ACLs.

  If you don't set any minimum data access permissions for all users, the only operations unauthenticated users can perform in the namespace are those for which they are granted permission by ACLs.

Tip: If you enable only namespace access protocols that don't support authentication, consider setting at least one minimum data access permission for all users.

For both all users and authenticated users, the set of minimum data access permissions can include only these permissions:

Browse
: Lets users list directory contents.

Read
: Lets users:

  - View and retrieve objects, including system metadata and custom metadata for objects
  - View and retrieve previous versions of objects
  - Check the existence of objects
  - List annotations for objects

  For this permission to be granted, users must also have browse permission.

Read ACL
: Lets users view and retrieve object ACLs.

Write
: Lets users:

  - Add objects to the namespace
  - Modify system metadata (except retention hold)
  - Add or replace custom metadata

Write ACL
: Lets users add, replace, and delete object ACLs.

Delete
: Lets users delete objects, and custom metadata, and ACLs from the namespace.

Purge
: Lets users delete all versions of an object with a single operation. For this permission to be granted, users must also have delete permission.

Users with any data access permissions for a namespace can view information about that namespace.

Note: To store an object with CIFS on a Windows client, a user must have both read and write permissions.

When you create a namespace, the set of minimum data access permissions is empty for both all users and authenticated users. You can modify these sets at any time.

Access control lists

A namespace can be configured to allow users to associate ACLs with objects. An ACL consists of access control entries. Each access control entry grants a user or group of users (the grantee) one or more data access permissions for the applicable object.

ACL permissions

The permissions that can be included in an access control entry are:

Read
: Lets the grantee read and retrieve the object, including the system metadata and any custom metadata for the object, and list annotations for the object.
To read or retrieve the object through CIFS or NFS, the grantee must also have browse permission.

Read ACL
: Lets the grantee read and retrieve the object ACL.

Write
: Lets the grantee modify system metadata and add and replace custom metadata for the object.

Write ACL
: Lets the grantee add, replace, or delete the object ACL.

Delete
: Lets the grantee delete or purge the object and delete the object ACL.

Use of ACLs

When you create a namespace, the use of ACLs is disabled. You can enable this feature for the namespace at any time. However, once this feature is enabled, you cannot disable it.

Users can add and replace ACLs only with the HTTP protocol. Therefore, if you enable the use of ACLs for a namespace, you should also enable that protocol.

Enforcing ACLs

While the use of ACLs is enabled for a namespace, you can specify whether HCP should enforce ACLs in that namespace. While HCP is enforcing ACLs, the operations that a given user can perform on a given object are those permitted by any of:

- The data access permissions associated with the applicable user account or group accounts
- The applicable minimum data access permissions specified in the namespace configuration
- The object ACL

When not enforcing ACLs, HCP allows only the operations permitted by the first two items above.

You can change the specification of whether HCP should enforce ACLs at any time while the use of ACLs is enabled.

Replication

Replication is a process that supports configurations 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.

In addition to replicating objects, HCP replicates tenant and namespace configuration, user and group accounts, retention classes, content classes, all compliance log messages, and most other tenant log messages.

A *replication topology* is a configuration of HCP systems that are related to each other through replication. Typically, the systems in a replication topology 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*).

Clients can read from namespaces on all systems where those namespaces are replicated. The replication topology, which is configured at the system level, determines the systems on which clients can write to namespaces.

Replication benefits

Replication has several purposes:

- If a system in a replication topology becomes unavailable (for example, due to network issues), another system in the topology can provide continued data availability.
- If a system in a replication topology suffers irreparable damage, another system in the topology can serve as a source for disaster recovery.
- If multiple HCP systems are widely separated geographically, 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.
- If an enterprise has several satellite offices, an HCP system at a central facility can consolidate data from the HCP systems at those outlying locations.
- If an object cannot be read from one system in a replication topology (for example, because a node is unavailable), HCP can try to read it from another system in the topology. HCP tries to do this only if:
  - The namespace that contains the object is being replicated.
  - The namespace has the read-from-remote-system feature enabled.
  - The object has already been replicated. Users can check object metadata to determine whether an object has been replicated.
- If a system in a replication topology is unavailable, requests to that system that come through the REST, S3 compatible API can be automatically serviced by another system in the topology without the client needing to modify the target URL. The other system can service a request only if:
  - The namespace named in the URL is replicated on the other system
  - The namespace named in the URL is configured to accept requests redirected from other HCP systems
  - The HCP systems involved use DNS for system addressing

Replication implementation

Replication is implemented at the tenant and namespace level. When creating a tenant, the HCP system administrator specifies whether the tenant is eligible to be replicated. HCP system administrators can change this setting from not allowing replication to allowing it. However, they cannot do the reverse.

If the tenant is eligible for replication, you can choose whether to include each namespace in the replication of the tenant. You can change this setting for a namespace at any time.

If allowed by the tenant configuration, for each cloud-optimized namespace replicated with the tenant, you can specify whether HCP is allowed to use erasure coding to implement replication of the objects in that namespace. Erasure coding improves storage efficiency. However, read performance may be better for replicated namespaces that do not allow erasure coding.

System administrators can change a tenant from not being able to choose whether namespaces allow erasure coding to being able to do this. After this change occurs:

- Preexisting cloud-optimized namespaces with replication enabled are automatically reconfigured to allow erasure coding.
- When you enable cloud optimization for a preexisting namespace that had replication enabled but was not cloud optimized, the namespace is automatically configured to allow erasure coding.

The HCP system administrator selects tenants to be replicated from among those that are eligible. If a tenant has granted system-level administrative users access to itself, the system administrator can change the namespace selections for that tenant. HCP replicates the configuration of each selected tenant and the configuration and contents of all the namespaces selected for replication with the tenant.

Depending on the replication topology, you may not be able to make any configuration changes to the tenant or any of its namespaces on one or more systems in the topology. Clients cannot make any changes to namespace content on systems on which you cannot make configuration changes.

Replication is asynchronous with other HCP activity. If allowed by the system administrator, you can monitor replication progress in the Tenant Management Console.

Replication collision handling

If clients can write to multiple systems in a replication topology, collisions can occur when different changes are made to the same objects on different systems. Similarly, if you can make configuration changes to the tenant and its namespaces on multiple systems in a replication topology, configuration collisions can occur.

The way HCP handles collisions that occur due to replication depends on the type of collision. However, the general rule is that more recent changes have priority over conflicting less recent changes.

Object content collisions

An object content collision occurs when, for a namespace without versioning enabled, these events occur in the order shown:

1. An object is created with the same name in that namespace on two systems in a replication topology, but the object has different content on the two systems.
2. The object on one of the systems is replicated to the other system.

If versioning is enabled, no collision occurs. Instead, the less recently created of the two objects becomes an old version of the more recently created object.

When an object content collision occurs, the more recently created object keeps its name and location. The other object is either moved to the .lost+found directory in the same namespace or renamed, depending on the namespace configuration.

When HCP moves an object to the .lost+found directory, the full object path becomes .lost+found/replication/*system-generated-directory*/ *old-object-path*.

When renaming an object due to a content collision, HCP changes the object name to *object-name*.collision or *object-name*.*version-id*.collision, where *version-id* is the version ID of the object. HCP uses the second format only if versioning has ever been enabled for the namespace that contains the object but is not currently enabled.

If the new name is already in use, HCP changes the object name to *object-name*.1.collision or *object-name*.*version-id*.1.collision, as applicable. If that name is already in use, HCP successively increments the middle integer by one until a unique name is formed.

Objects that have been relocated or renamed due to content collisions are flagged as replication collisions in their system metadata. Clients can use the metadata query API to search for objects that are flagged as replication collisions.

If an object that's flagged as a replication collision changes (for example, if its retention period is extended), its collision flag is removed. If a client creates a copy of a flagged object with a new name, the collision flag is not set on the copy.

You can configure namespaces to have the DIsposition service automatically delete objects that are flagged as replication collisions. When selecting this option for a namespace, you specify the number of days the DIsposition service should wait before deleting such an object. The days are counted from the time the collision flag is set. If the collision flag is removed from an object, the object is no longer eligible for deletion by the DIsposition service.

System metadata collisions

A system metadata collision occurs when these events occur in the order shown:

1. Different changes are made to the system metadata for a given object on each of two systems in a replication topology.
2. The changed system metadata on one of the systems is replicated to the other system.

For example, suppose a user on one system changes the shred setting for an object while a user on the other system changes the index setting for the same object. When the object on either system is replicated to the other system, a system metadata collision occurs.

If a collision occurs when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- For changed system metadata other than the retention setting and hold status:
  - If the last change made on system A is more recent than the last change made on system B, HCP changes the system metadata on system B to match the system metadata on system A.
  - If the last change on system B is more recent than the last change on system A, HCP does not change the system metadata on system B.
- For a changed retention setting:
  - If the retention setting on system A specifies a longer retention period than does the retention setting on system B, HCP changes the retention setting on system B to match the retention setting on system A.
  - If the retention setting on system B specifies a longer retention period than does the retention setting on system A, HCP does not change the retention setting on system B.
- For a changed hold status:
  - If the object is on hold on system A but not on system B, HCP places the object on hold on system B.
  - If the object is on hold on system B but not on system A, HCP leaves the object on hold on system B.

Here are some examples of how HCP handles collisions when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology.

Example 1

The object starts out on both system A and system B with these system metadata settings:

- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the shred setting to true.
2. On system B, a client changes the index setting to true.
3. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
   - Shred: false

- Index: true

Example 2

The object starts out on both system A and system B with these system metadata settings:

- Retention: Initial Unspecified
- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the retention setting to Deletion Prohibited.
2. On system B, a client changes the retention setting to Deletion Allowed.
3. On system B, a client changes the index setting to true.
4. On system A, a client changes the shred setting to true.
5. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
   - Retention: Deletion Prohibited
   - Shred: true
   - Index: false

Example 3

The object starts out on both system A and system B with these system metadata settings:

- Retention: Initial Unspecified
- Hold: true
- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the retention setting to Deletion Allowed.
2. On system B, a client changes the retention setting to Deletion Prohibited.
3. On system B, a client changes the index setting to true.
4. On system A, a client changes the shred setting to true.
5. On system A, a client releases the object from hold.
6. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
   - Retention: Deletion Prohibited
   - Hold: true
   - Shred: true
   - Index: false
7. The changes on system B are replicated to system A. The resulting settings for the object on system A are:
   - Retention: Deletion Prohibited
   - Hold: true
   - Shred: true
   - Index: false

Custom metadata collisions

A custom metadata collision occurs when these events occur in the order shown:

1. One of these changes occurs:
   - An annotation is added with the same name to a given object on each of two systems in a replication topology, but the annotation has different content on the two systems.

     The addition of an annotation to a given object on only one of the systems does not result in a custom metadata collision if the object does not have an annotation with the same name on the other system. In this case, the new annotation is replicated without conflict.

   - Different changes are made to the content of a given annotation for a given object on each of the two systems in a replication topology.
   - A change is made to the content of a given annotation for a given object on one system in a replication topology, and the same annotation is deleted on another system in the topology.
2. The change made on one of the systems is replicated to the other system.

If a collision occurs when a custom metadata change for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change on system A is more recent than the last change on system B, HCP applies the change from system A to the custom metadata on system B
- If the last change on system B is more recent than the last change on system A, HCP does not change the custom metadata on system B

Here are two examples of how HCP handles collisions when custom metadata changes for a given object are replicated from one system (system A) in a replication topology to another system (system B) in the topology.

Example 1

The object starts out with annotations named a1 and a2 on both system A and system B.

The list below shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

1. On system B, a client changes the content of a1.
2. On system A, a client makes a different change to the content of a1.
3. On system A, a client adds annotation a3 to the object.
4. On system B, a client adds annotation a3 with different content from the a3 added on system A.
5. The changes on system A are replicated to system B. The resulting annotations for the object on system B are:
   - a1 with the changed content from system A
   - a2 (unchanged)
   - a3 with the content added on system B

6. The changes on system B are replicated to system A. The resulting annotations for the object on system A are:
    - a1 with the changed content from system A
    - a2 (unchanged)
    - a3 with the content added on system B

Example 2

The object starts out with the annotations named a1, a2, and a3 on both system A and system B.

The list below shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

1. On system B, a client changes the content of a1.
2. On system A, a client deletes a1.
3. On system A, a client changes the content of a2.
4. On system B, a client changes the content of a2.
5. On system A, a client deletes a3.
6. On system B, a client changes the content of a3.
7. The changes on system A are replicated to system B. The resulting annotations for the object on system B are:
    - a2 with the changed content from system B
    - a3 with the changed content from system B
8. The changes on system B are replicated to system A, the resulting annotations for the object on system A are:
    - a2 with the changed content from system B
    - a3 with the changed content from system B

Access control list collisions

An ACL collision occurs when these events occur in the order shown:

1. Different changes are made to the ACL for a given object on each of two systems in a replication topology.
2. The changed ACL on one of the systems is replicated to the other system.

An ACL is treated as a single unit. If a collision occurs when a changed ACL for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change to the ACL on system A is more recent than the last change to the ACL on system B, HCP changes the ACL on system B to match the changed ACL on system A
- If the last change to the ACL on system B is more recent than the last change to the ACL on system A, HCP does not change the ACL on system B

For example, suppose the ACL for a given object starts out with these grants on both system A and system B:

- All users: read
- User lgreen: write
- User mwhite: write, delete

The list below shows a sequence of events in which the ACL for the object is changed and the change is then replicated.

1. On system B, a client changes the grants in the ACL to:
    - All users: read
    - User lgreen: write, delete
    - User pdgrey: write
2. On system A, a client changes the grants in the ACL to:
    - All users: read
    - User mwhite: write
    - User pdgrey: write
3. The changed ACL on system A is replicated to system B. The resulting ACL for the object on system B contains these grants:
    - All users: read
    - User mwhite: write
    - User pdgrey: write

Configuration collisions

A configuration collision occurs when these events occur in the order shown:

1. Different changes are made to the same configuration property on each of two systems in a replication topology.
2. The changed property on one of the systems is replicated to the other system.

Examples of configuration properties are:

- The data access permission mask for a namespace
- The default shred setting for a namespace
- The HTTP protocol enabled setting for a namespace
- The default versioning setting for new namespaces
- The roles for a user account
- The data access permissions a group account has for a namespace
- The protocol optimization setting on a namespace

Certain groups of properties are treated as a single unit. Generally, these groups consist of properties that are updated by a single submission in the Tenant Management Console. Two notable exceptions to this rule are data access permissions for user accounts and content properties for content classes. In these cases, each set of data access permissions for a namespace and each content property is treated as an individual property.

If a collision occurs when a configuration change is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change to the configuration on system A is more recent than the last change to the configuration on system B, HCP changes the configuration on system B to match the configuration on system A
- If the last change to the configuration on system B is more recent than the last change to the configuration on system A, HCP does not change the configuration on system B

The rules above apply to all configuration collisions except collisions that occur when retention class properties are changed.

Here are two examples of how HCP handles collisions when configuration changes are replicated from one system (system A) in a replication topology to another system (system B) in the topology.

Example 1

A given namespace starts out on both system A and system B with these properties:

- Read from remote system: enabled
- Collision handling: move object

The list below shows a sequence of events in which the namespace configuration is changed and the change is then replicated.

1. On system B, an administrator disables read from replica for the namespace.
2. On system A, an administrator changes the collision handling option for the namespace to rename object.
3. The change on system A is replicated to system B. Because read from remote system and collision handling are properties in the same submission group, the resulting properties for the namespace on system B are:
    - Read from remote system: enabled
    - Collision handling: rename object

Example 2

A given user account starts out on both system A and system B with these roles and data access permissions:

- Roles: monitor, compliance
- Namespace-1 permissions: browse, read, write, delete

The list below shows a sequence of events in which the user account is changed and the changes are then replicated.

1. On system B, a security administrator adds the administrator role to the user account.
2. On system A, a security administrator removes the monitor role from the account.
3. On system B, an administrator removes the write permission from Namespace-1 and adds the purge permission.
4. On system A, an administrator adds the privileged permission to Namespace-1.
5. On system B, an administrator gives the user account browse and read permissions for Namespace-2.
6. On system A, an administrator gives the user account browse, read, and write permissions for Namespace-3.
7. The changes on system A are replicated to system B. Because roles and data access permissions are in separate submission groups, the resulting roles and data access permissions for the user account on system B are:
    - Roles: compliance
    - Namespace-1 permissions: browse, read, write, delete, privileged
    - Namespace-2 permissions: browse, read
    - Namespace-3 permissions: browse, read, write

Retention class collisions

A retention class collision occurs when these events occur in the order shown:

1. Different changes are made to the same retention class on each of two systems in a replication topology.
2. The changed retention class on one of the systems is replicated to the other system.

If a collision occurs when a change to a retention class is replicated from one system (system A) in a replication topology to another system (system B) involved in the topology:

- If the last change to the retention class on system A is more recent than the last change to the class on system B and:
    - The value of the class on system A is greater than the value of the class on system B, HCP changes the value of the class on system B to the value of the class on system A
    - The value of the class on system A is less than the value of the class on system B and:
        - System B is in enterprise mode, HCP changes the value of the class on system B to the value of the class on system A
          Note: An exception to this rule is when the value of the class on system A is -2 (Initial Unspecified) and the value of the class on system B is not 0 (Deletion Allowed). In this case, the value of the class on system B does not change.
        - System B is in compliance mode, HCP does not change the value of the class on system B
- If the last change to the retention class on system B is more recent than the last change to the class on system A, HCP does not change the value of the class on system B

Note: A retention class value of -1 (Deletion Prohibited) is greater than a value that's a specific duration. A retention class value of 0 (Deletion Allowed) or -2 (Initial Unspecified) is less than a value that's a specific duration.

Service plans

A *service plan* is a named option that can be associated with a namespace. This option determines how HCP manages the objects in that namespace. Service plan names are system specific.

When creating a tenant, the HCP system administrator specifies whether the tenant is allowed to associate service plans with namespaces. HCP system administrators can change this setting from not allowing these associations to allowing them. However, they cannot do the reverse.

The service plan you select for a namespace should match the expected usage pattern and properties for that namespace. For example, if the purpose of the namespace is to store objects that most likely will not be accessed again, you would choose a service plan with a description indicating that the plan is intended for archiving.

System-level administrative access

A tenant can optionally grant HCP system-level users administrative access to itself. This enables those users to access the Tenant Management Console for that tenant and perform the same management and monitoring activities as the tenant-level users. Additionally, it enables system-level users to search the namespaces owned by that tenant and perform all allowed operations on the objects they find.

General administrative information

As an HCP tenant administrator, you are responsible for managing a tenant and the namespaces it owns. Your primary job is to ensure that users and applications have the access they need to those namespaces.

The tool you use for this purpose is a web application called the Tenant Management Console. Depending on the permissions you have, you can use the Console to configure and monitor the tenant and its namespaces, as well as perform compliance activities.

Tenant Management Console

The Tenant Management Console is a tenant-specific web application that lets you manage tenants and namespaces. The Console shows you tenant and namespace status in real time, so you can effectively monitor activity and take action as needed.

Using the Console, you can modify tenant and namespace settings and perform compliance activities. Changes you make through the Console take effect immediately.

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

About the Console

Console access

To use the Tenant Management Console, you need either:

- A user account defined in HCP (either locally authenticated or RADIUS authenticated).
- If the tenant is configured to support Windows Active Directory (AD) authentication, an AD user account for a user that belongs to one or more AD groups for which corresponding group accounts are defined in HCP. In this book, such an Active Directory user account is referred to as a *recognized AD user account*.

The HCP user account or group accounts specify what you have permission to do in the Console. The menu options, pages, and panels you see in the Console depend on your permissions.

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 Tenant 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.

  For single sign-on to work, your web browser must be configured to support it.

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 exact amount of idle time allowed is configurable.

If you've granted HCP system-level users administrative access to the tenant, they can access the Tenant Management Console directly from the HCP System Management Console. Doing so does not start a Tenant Management Console session. Rather, it continues the current System Management Console session, and the configured idle time for that Console applies.

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 modify your tenant and create, modify, and delete namespaces, user and group accounts, and content classes for the tenant. Additionally, you can create, modify, and delete retention classes for the tenant's namespaces.

You use the Tenant Management Console to enable the management API at the tenant level. For the API to be available, however, it must also be enabled at the system level.

To use the management API, you need a user account that includes the applicable permissions for the actions you want to take.

If the tenant is configured to support Active Directory authentication, applications can also use recognized AD user accounts to access HCP through the management API. To do this, however, an application must use the SPNEGO protocol or the AD authentication header to negotiate the AD user authentication itself. For more information about SPNEGO, see http://tools.ietf.org/html/rfc4559. To provide credentials using the Active Directory authorization header, you use this format:

```
Authorization: ADAD-username:AD-password
```

Tenant Management Console URL

The URL for the Tenant Management Console has this format:

```
https://tenant-url-name.hcp-domain-name:8000
```

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

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

Using a hosts file

Typically, the HCP system uses DNS for system addressing. If this is not the case, you need to provide a mapping of the tenant hostname to an IP address for the HCP system.

You specify hostname mappings in the hosts file on the client. The location of this 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

Hostname mappings

Each entry in a hosts file maps one or more fully qualified hostnames to a single IP address. For example, if one of the IP addresses for the HCP system is 192.168.210.16, you would add this line to the hosts file on the client to enable access to the Tenant Management Console for the Finance tenant:

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

The following considerations apply to hosts file entries:

- Each entry must appear on a separate line.
- Multiple hostnames in a single line must be separated by white space. With some versions of Windows, these must be single spaces.
- Each hostname can map to multiple IP addresses.

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.

For the IP addresses for the HCP system, contact your HCP system administrator.

Hostname mapping considerations

An HCP system has multiple IP addresses. You can map the tenant hostname to more than one of these IP addresses in the hosts file. The way multiple mappings are used depends on the client platform. For information about how your client handles multiple mappings in a hosts file, see your client documentation.

If any of the IP addresses listed in the hosts file are unavailable, timeouts may occur when you use a hosts file to access the Tenant Management Console.

Logging in

Depending on the tenant configuration, you can log into the Tenant Management Console with a tenant-level user account or a recognized AD user account.

1. Open a web browser.
2. In the address field, enter the URL for your Tenant Management Console.
   Note: 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 Tenant Management Console, and the tenant Overview page appears:
     - You are currently logged in to Windows with a recognized AD user account.
     - The tenant is configured to support AD authentication.
     - Your web browser is configured to support single sign-on with AD.

     This is single sign-on. No further action is required.
   - If the tenant is configured to support AD authentication but any of the following apply, a message appears indicating that single sign-on was not possible:
     - Your web browser is not configured to support single sign-on.
     - You are not currently logged in to Windows with a recognized AD user account.
     - You are not on a Windows computer.

     In these cases, you need to click Console login page in the message to display the Tenant Management Console login page.
   - If the tenant is not configured to support AD authentication, the Tenant Management Console login page appears.
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 times in a row, you are locked out of the Console. The exact number of times is configurable.
   Note: AD can also be configured to disable user accounts after a given number of authentication attempts with an invalid password.
   Important: You should change your password as soon as possible the first time you log into the Tenant Management Console.
5. If the tenant is configured to support AD authentication, take either of these actions in the Domain field:
   - 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 tenant Overview page or, if you're using an HCP user account and are required to change your password, the Change Password page.

Using the Tenant Management Console

Tenant Management Console pages display information about the current tenant and its namespaces. Some pages also let you configure various aspects of the tenant and namespaces. (The *current tenant* is the one for which you're currently logged in to the Tenant Management Console.)

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

Refreshing pages

Tenant 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

Tenant Management Console pages and panels on which you can modify information have action buttons (such as Create Retention Class and Update Settings) 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 those 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.

Viewing HCP documentation

HCP documentation is available online in PDF format. To view a document from the Tenant Management Console:

1. In the top right corner of the Tenant Management Console window, hover over the documentation icon ( ) to open a dropdown menu of the available documents.
2. In the dropdown menu, click the document you want.

Changing your password

Depending on how your 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 Tenant 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 password using the Tenant Management Console.

1. Log into the Tenant 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

1. In the top right corner of the Tenant Management 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 Tenant Management Console using the credentials you used to log in.
   Tip: For extra security, clear the browser cache before closing the window.

Administrative responsibilities

You perform tenant-level administrative tasks by using the HCP Tenant Management Console.

Managing user and group accounts

HCP user and group accounts determine whether you can log into the HCP Tenant Management Console or Search Console and which operations you can perform in namespaces. For the Tenant Management Console, they also determine which actions you're allowed to perform after logging in.

You use the Tenant Management Console to create, modify, and delete user and group accounts. For each HCP user account, you specify whether it is authenticated locally or by RADIUS.

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

Maintaining the tenant

HCP system-level administrators create tenants and maintain certain aspects of their configuration. Other aspects of tenant configuration are maintained at the tenant level.

As a tenant administrator, you are responsible for configuring:

- Tenant contact information
- The tenant description
- The tenant permission mask
- System-level administrative access to the tenant
- Access to the Tenant Management Console
- Access to HCP through the management API
- Access to the Search Console for the tenant

You are also responsible for creating and managing content classes and content properties for the tenant.

Creating and maintaining namespaces

As a tenant administrator, you are responsible for creating and maintaining namespaces. After creating a namespace, you can change most of its properties. You are also responsible for managing search and indexing for the namespace.

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

Note: Users with the allow namespace management property can use the HCP management and S3 compatible APIs to create, view and change the versioning status of, and delete namespaces.

Monitoring the tenant and namespaces

HCP is a self-monitoring, self-healing system that automatically alerts you to any issues you may need to address, for example, a namespace running low on space. The Tenant Management Console enables you to review tenant and namespace activity and take action to address certain issues. Using the Console, you can view:

- Statistics and graphs showing namespace usage.
- Messages about tenant and namespace events, for example, configuration changes and searches performed from the Search Console.
- Messages about security events, for example, attempts to log into the Tenant Management Console with an invalid username.
- Messages about compliance events, for example, retention class activity and privileged delete operations.
- Reports of irreparable objects.

- Alerts warning you of conditions that may need your attention.
- The progress of replication activity.

You can also have HCP send tenant and namespace log messages to syslog servers, SNMP managers, and specified email addresses.

Additionally, you can generate chargeback reports that can be used as input to billing applications.

Managing namespace access

Managing namespace access entails:

- Setting the tenant and namespace data access permission masks
- Setting minimum data access permissions for authenticated and unauthenticated users
- Configuring the namespace access protocols for client access to each namespace
- Optionally, setting the IP addresses from which access to the Search Console is allowed or denied

Performing compliance activities

The Tenant Management Console enables you to perform certain activities required for compliance with some local regulations. Using the Console, you can:

- Create, modify, and delete retention classes
- Perform privileged delete operations

Managing accounts

As a tenant security administrator, you are responsible for creating and managing tenant-level user and group accounts. These accounts give users permission to use the Tenant Management Console and HCP management API and to access namespace content through namespace access protocols that require authentication, the Namespace Browser, the HCP metadata query API, and the HCP Search Console. These accounts also determine which actions the user is allowed to perform through the applicable interface.

Users with HCP user accounts are authenticated locally by HCP or remotely by RADIUS. Group accounts enable users defined in Active Directory to access HCP interfaces. These users are authenticated remotely by AD. The tenant configuration determines which types of authentication the tenant supports.

As an administrator with the security role, you can associate administrative roles with user and group accounts. To associate data access permissions with user and group accounts, you need the administrator role.

Different tenants have different user and group accounts. These accounts cannot be shared across tenants.

User and group accounts

User and group accounts control access to HCP interfaces. The administrative roles associated with these accounts allow users to use:

- The Tenant Management Console
- The HCP management API

You need the security role to create, modify, delete, and associate roles with user and group accounts.

The data access permissions associated with user and group accounts allow users to access namespace content through:

- Namespace access protocols that require authentication
- The Namespace Browser
- The HCP metadata query API
- The HCP Search Console

You need the administrator role to associate data access permissions with user and group accounts.

The allow namespace management property, which you can assign to a user or group account, allows users to use the HCP management and S3 compatible APIs to:

- Create namespaces
- List, view and change the versioning status of, and delete namespaces they own
- You need the administrator role to assign the allow namespace management property to a user or group account.

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 Tenant Management Console.

When you create a user account, you 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.

When you create a user account, you have the option of associating roles with it and assigning the allow namespace management property. You can change these properties as well associate data access permissions with the account at any time thereafter.

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.

Note: For HCP user accounts, HCP logs failed namespace access attempts with a given username once an hour. This prevents repeated log messages in the case where an application specifies invalid credentials. The message that’s logged indicates the number of failed attempts that occurred in the past hour.

A tenant can have at most 10,000 HCP 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 Tenant Management Console.

When you create a group account, you have the option of associating roles with it. You can change these associations and also associate data access permissions with the account at any time thereafter.

A tenant can have at most 100 group accounts.

Administrative roles and permissions

A *role* is a named collection of permissions that can be 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.

Tip: Before associating roles with a user or group account, make sure the permissions granted by those roles are consistent with job functions of the user or group for which you're creating the account.
Note: An AD user can be added to an AD group while that user is using the Tenant 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 Tenant Management Console and then log back in. If the user is also currently using the HCP System Management Console or the Namespace Browser, logging out of either of those interfaces has the same effect.

Available roles

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

Monitor
: Grants permission to use the Tenant Management Console to view the status of the tenant and its namespaces and most aspects of the tenant and namespace configurations. The monitor role does not grant permission to view user or group accounts.

Administrator
: Grants permission to use the Tenant Management Console to view the status of the tenant and its namespaces and perform most tenant and namespace configuration activities. The administrator role also grants permission to associate data access permissions with user and group accounts but not to view or manage any other aspects of user and group accounts.

Security
: Grants permission to use the Tenant Management Console to view the status of the tenant, configure Console and HCP management API security, and view security events in the tenant log. The security role also grants permission to create and manage user and group accounts, including associating roles with them but not viewing or managing their data access permissions.

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 view tenant status, namespace status, and compliance events in the tenant log.

Permissions granted by roles

In the table below, checkmarks indicate the permissions granted by each role.

Permission	Role			
	Monitor	Administrator	Security	Compliance
View the user account list	✓	✓	✓	•
View the full definition of individual user accounts	•		✓	•
View the description, allow namespace management property, and data access permissions for individual user accounts	✓	✓	•	•
Create, associate roles with, delete, and otherwise manage user accounts, except modifying the allow namespace management property and data access permissions	•	✓	✓	•
Modify the allow namespace management property and manage data access permissions for user accounts	•	✓	•	
View the group account list	✓	✓	✓	
View the full definition of individual group accounts	•	•	✓	
View the description, allow namespace management property, and data access permissions for individual group accounts	✓	✓	•	•
Create, associate roles with, and delete group accounts	•		✓	
Modify the allow namespace management property and manage data access permissions for group accounts	•	✓	•	
Specify message text for the Tenant Management Console and Search Console login pages	•		✓	
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	•	✓	•	•
View and modify Tenant Management Console security settings	•	•	✓	•

Permission	Role			
	Monitor	Administrator	Security	Compliance
View and modify HCP management API security settings	•	•	✓	•
View and modify Search Console security settings	•	•	✓	•
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	•	✓	•	•
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	✓	✓	•	•
Create and delete namespaces	•	✓	•	•
View the namespace list	✓	✓	•	✓
View namespace overviews	✓	✓	•	✓
Modify namespace names and quotas	•	✓	•	•
View namespace permission masks and descriptions	✓	✓	•	✓
Modify namespace permission masks and descriptions	•	✓	•	•
View namespace owners	✓	✓	•	✓
Change namespace owners	•	✓	•	•
View the tags associated with namespaces	✓	✓	•	•
Modify the tags associated with namespaces	•	✓	•	•
View namespace default retention settings	✓	✓	•	✓
Modify namespace default retention settings	•	•	•	✓
View namespace default shred settings	✓	✓	•	✓
Modify namespace default shred settings	•	•	•	✓
View namespace default index settings	✓	✓	•	•
Modify namespace default index settings	•	✓	•	•
View minimum data access permissions	✓	✓	•	•
Modify minimum data access permissions	•	✓	•	•
View namespace ACL settings (HCP tenants only)	✓	✓	•	•
Manage the use of ACLs in namespaces	•	✓	•	•
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	✓	✓	•	•
Configure object versioning in namespaces	•	✓	•	•
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	•	✓	•	•

Permission	Role			
	Monitor	Administrator	Security	Compliance
View namespace DPL settings	✓	✓	•	•
Modify namespace DPL settings	•	✓	•	•
View namespace retention modes	✓	✓	•	•
Modify namespace retention modes	•	✓	•	•
View default settings for namespace creation	✓	✓	•	•
Modify default settings for namespace creation	•	✓	•	•
View the maximum number of namespaces per user	✓	✓	•	•
Modify the maximum number of namespaces per user	•	✓	•	•
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	•	✓	•	•
Reindex namespaces	•	✓	•	•
Monitor replication	✓	✓	•	•
Select namespaces for replication	•	✓	•	•
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	✓	✓	✓	✓

Data access permissions

Data access permissions allow users to access namespace content and some information about namespaces. These permissions are granted separately for individual namespaces.

The data access permissions that can be associated with user and group accounts for any given namespace are:

Browse
: List directory contents.

Read
: View and retrieve objects, including the system and custom metadata for objects.
: View and retrieve previous versions of objects.
: Check the existence of objects.
: List annotations for objects.
: For this permission to be granted, users must also have browse permission.

Read ACL
: View and retrieve object ACLs.

Write
: Add objects to the namespace.
: Modify system metadata (except retention hold).
: Add or replace custom metadata.

Write ACL
: Add, replace, and delete object ACLs.

Change owner
: Change the owners of objects in the namespace.

Delete
: Delete objects, custom metadata, and ACLs from the namespace.

Purge
: Delete all versions of an object with a single operation. For this permission to be granted, users must also have delete permission.

Privileged
: Delete or purge objects that are under retention, provided the user also has delete or purge permission for the applicable namespace
: Hold or release objects, provided the user also has write permission for the applicable namespace

Search
: Use the HCP metadata query API and the HCP Search Console to query or search the namespace. For this permission to be granted, users must also have read permission.

Users with any data access permissions for a namespace can view information about that namespace.

Note: An Active Directory (AD) user can be added to an AD group while the user is using the Namespace Browser. However, if the AD group corresponds to an HCP group account, the data access permissions might not take effect immediately. It could take up to eight hours for the user to get the data access permissions associated with the group account. To get the data access permissions immediately, the user must log out of the Namespace Browser and then log back in. If the user is also currently using the HCP System Management Console or the Tenant Management Console, logging out of either of those interfaces has the same effect.

User authentication

To use these HCP Console and command-line interfaces, a user needs to supply a username and password for authentication:

- Console interfaces:
  - Tenant Management Console
  - Namespace Browser
  - Search Console
- Command-line interfaces:
  - HCP management API
  - Namespace access protocols that require authentication
  - HCP metadata query API

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*.

A tenant can support one or more of these authentication types. The types supported are set when the tenant is created. HCP system-level administrators can change these settings at any time.

Local authentication

For locally authenticated users, the user account password is stored in the HCP system. When a user submits the account username and password either on a login page for a Console or with a cookie in a command line, HCP checks the username and password internally.

HCP lets the user into the target Console or performs the requested operation if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- For the Tenant Management Console, the user account is associated with at least one role.
- For the Search Console, the user account is associated with the search permission.
- For the HCP management API, the user account is associated with a role that allows the requested operation.
- For a namespace access protocol, the user account is associated with permissions that allow the requested operation.
- For the metadata query API, the user account is associated with the search permission.

If any of these conditions is not true, HCP rejects the login or command-line request.

You can change the passwords of locally authenticated users in the Tenant Management Console. These users can also change their own passwords in the Tenant 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. When a user submits the account username and password either on a login page for a Console or with a cookie in a command line, 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 or performs the requested operation if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- For the Tenant Management Console, the user account is associated with at least one role.
- For the Search Console, the user account is associated with the search permission.
- For a command-line interface, the user account is associated with permissions that allow the requested operation.

If any of these conditions is not true, HCP rejects the login or command-line request.

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

Connections to RADIUS servers are configured at the HCP system level.

Note: RADIUS authentication is not supported for the namespace access protocols or for access to namespace content through any other interface.

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.
- For the Tenant Management Console, at least one such group account is associated with at least one role.
- For the Search Console, at least one such group account is associated with the search permission.

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

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

For the command-line interfaces, applications may use the SPNEGO protocol or the AD authentication header to negotiate the AD user authentication themselves. You cannot submit AD credentials with a cookie in a command line. For more information about SPNEGO, see http://tools.ietf.org/html/rfc4559. To provide credentials using the Active Directory authentication header, you use this format:

```
Authorization: AD ad-username:ad-password
```

Note: AD authentication is not supported for namespace creation through the S3 compatible API.
Tip: If the tenant supports both local and AD authentication, consider creating a locally authenticated user account with the security role. This ensures that you can still access the Tenant Management Console in the unlikely event that HCP cannot communicate with AD.

Starter account

When creating a tenant, the HCP system administrator defines either one locally authenticated HCP user account or one HCP group account for it. This starter account has only the security role and no data access permissions. It also does not have the allow namespace management property.

Before you can log into the Tenant Management Console:

- If the starter account is an HCP user account, you need to get the username and password for this account from the system administrator. The first time you log in with this account, you are immediately required to change your password.
- If the starter account is an HCP group account, you need to get the username and password of an AD user account for a user that belongs to the AD group that corresponds to the starter group account.

After you've logged in with the starter account, you can create new accounts as needed, including new accounts with the security role.

You can delete the starter account as long as at least one of these will still exist after you delete the account:

- A locally authenticated HCP user account that has the security role and is enabled
- An HCP group account that has the security role

Working with user accounts

To view, create, and manage HCP user accounts, you use the Users page in the Tenant Management Console. To display this page, in the top-level menu of the Tenant Management Console, select Security > Users.

Roles:

- View the user account list, you need the monitor, administrator, or security role
- View the full definitions of user accounts, you need the security role
- View the description, allow namespace management property, and data access permissions for user accounts, you need the monitor or administrator role
- Create, associate roles with, delete, and otherwise manage user accounts, except modifying the allow namespace management property and data access permissions, you need the security role
- Modify the allow namespace management property and data access permissions for user accounts, you need the administrator role

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 username
- 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 username.

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

1. On the Users page in the Tenant Management Console, click Create User Account.
2. In the Create User Account panel, in the Username field, type a login name for the user account.
   - 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.
   - User names are not case sensitive.
   - The user name must be unique for the current tenant. Different tenants can have user accounts with the same user name.
   - You can reuse user names that are not currently in use. For example, if you delete a user account, you can create a new account with the same user name.

   Tip: Consider using email addresses as usernames. This gives you easy access to email addresses should you need to contact users.
3. In the Full Name field, type the name of the person for whom you are creating the account.
   This name can be from one through 64 characters long and can contain any valid UTF-8 characters, including white space.
4. (Optional) Clear Enable account to have the user account initially disabled.
   A disabled user account cannot be used to access the Tenant Management Console or HCP Search Console. It can, however, be used for namespace access with the HTTP protocol and Namespace Browser.
5. For the Authentication option, select either Local or, for remote authentication, RADIUS.
   If you select Local, the panel displays the Password and Confirm Password fields and Force change on next login option. If you select RADIUS, these fields are hidden.

   For local authentication:

   a. In the Password field, type a password for the user account.
      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.
      Note: HCP does not save passwords in a recoverable format. If a user forgets his or her password, you need to assign a new one.
   b. In the Confirm Password field, retype the password.
   c. (Optional) Select Force change on next login.
      When this option is selected, the next time a user uses the account to log into the Tenant Management Console, the Console automatically displays the Change Password page. The user cannot do anything else in the Console until the password is changed.
      After the user changes the password, Force change on next login is automatically cleared.
6. In the Roles section, select any number of roles for the user account, or none.
7. (Optional) Specify a description for the user account.
   a. Click Description.
   b. In the Description field, type a description of the user account.
      This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
8. (Optional) If you have the administrator role, select Allow namespace management.
   If the account you are creating has the administrator role, this option is selected automatically and cannot be cleared.
9. (Optional) If you have the administrator role, click Assign Namespace Permissions. Then associate data-access permissions with the user account.
   You cannot associate data-access permissions with a RADIUS authenticated user account.
10. Click Create User Account.

Modifying a user account and its roles

As a user with the security role, you can change this information about a user account:

- The username.
- 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.
  Note: You can disable your own account. Once 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.

1. In the list of user accounts on the Users page, click the username 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 username 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 Tenant 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.

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.

Working with group accounts

To view, create, and manage HCP group accounts, you use the Groups page in the Tenant Management Console. This page is available only if the tenant supports AD authentication.

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

Roles: To:

- View the group account list, you need the monitor, administrator, or security role
- View the full definitions of groups accounts, you need the security role
- View the allow namespace management property and data access permissions for group accounts, you need the monitor or administrator role
- Create, associate roles with, and delete group accounts, you need the security role
- Modify the allow namespace management property and data access permissions for group accounts, you need the administrator 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. If you have the administrator role, you can also associate data access permissions with the 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 and data access permissions associated with existing group accounts. In this case, all the accounts involved end up with the same roles and permissions.

1. On the Groups page in the Tenant Management Console, click Add Active Directory Groups.
   The Find and Select Groups section lists all the AD groups HCP knows about. Groups for which HCP group accounts already exist for the tenant are marked with a checkmark ( ).
2. (Optional) 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 from which you can create HCP group accounts.
      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. Click the find control ( ).
   c. 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.
   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.
   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.
   The selected group rows turns green.
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. (Optional) If you have the administrator role, select Allow namespace management.
   This option is selected automatically and cannot be deselected if the account being created has the administrator role.
6. (Optional) If you have the administrator role, click Assign Namespace Permissions. Then associate data access permissions with the group accounts

7. Click Add Groups.

Modifying a group account

You can change the roles associated with 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.

1. In the list of group accounts on the Groups page in the Tenant 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 Settings in the Roles section.

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 and data access permissions granted by that group account.

If no existing HCP user account has the security role, you cannot delete the last group account with the security role.

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 Tenant Management Console may not immediately reflect the change to the HCP group account name.

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

Changing the allow namespace management property for a user or group account

As a user with the administrator role, you can change the allow namespace management property for a user or group account. However, if the account has the administrator role, you cannot remove the allow namespace management property from the account.

1. In the list of user or group accounts on the Users or Groups page, as applicable, select the user account or group account you want.
2. Select or deselect Allow namespace management, as applicable.
3. Click Update Settings.

Changing the data access permissions for a user or group account

As a user with the administrator role, you can change the data access permissions associated with a user or group account. For a user account, you do this on the Users page in the Tenant Management Console. For a group account, you do this on the Groups page.

You can make these changes to data access permissions for a user or group account:

- Specify permissions for any number namespaces in a single operation
- Change the permissions for an individual namespace for which the user or group account already has one or more permissions
- Dissociate a namespace from the user or group account, thereby removing all permissions for that namespace

You can change the data access permissions associated with multiple group accounts in a single operation.

Note: You cannot associate data access permissions with a RADIUS-authenticated user account.

Specifying permissions for any number of namespaces

You associate data access permissions with a user or group account by first displaying a list of namespaces and then selecting the ones for which you want to specify data access permissions. After selecting the namespaces you want, you select the permissions you want the user or group account to have for those namespaces.

You can specify permissions for any number of namespaces in a single operation. If the user or group account already has permissions for any of the selected namespaces, the set of permissions you select replaces the set of permissions already associated with each of those namespaces.

1. In the list of user or group accounts on the Users or Groups page, as applicable, select the user account or group account you want.
2. Click Assign Namespace Permissions.
   The Find and Select Namespaces section lists all the tenant's namespaces. Namespaces for which the user or group account already has any permissions are marked with a checkmark ( ).
3. (Optional) Filter the list of namespaces by name.
   a. In the Find and Select Namespaces field, type a text string 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.
   b. Click the find control ( ).
4. For each namespace from which you want to specify data access permissions, click the add control ( ) to select the group.
   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.
   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.
   The selected group rows turns green.
5. In the Assign Data Access Permissions for Selected Namespaces section, select the permissions you want the user or group account to have for the selected namespaces.
   Selecting Read automatically selects Browse. Selecting Search automatically selects Read and Browse. Selecting Purge automatically selects Delete.
   To select all the permissions, click Select all.
6. In the S3 Object Lock Permissions section, select the permissions you want to grant to the user or group account for the selected namespaces.
   Important: To use any of these permission settings, you must enable S3 Object Lock on the namespace. The following is a list of S3 Object Lock permissions, explaining when you would use each one
   - Bypass Governance Retention: Allows you to perform operations such as deletion, shortening the retention period, or removing the lock on object versions that are locked in governance mode.
   - Get Bucket Object Lock Configuration: Allows you to retrieve the Object Lock configuration for a bucket.
   - Get Object Legal Hold: Allows you to retrieve an object’s current legal hold status. The legal hold status indicates whether an object is locked and cannot be overwritten or deleted.

- Get Object Retention: Allows you to retrieve an object's retention settings. The retention settings indicate whether an object is locked and cannot be overwritten or deleted.
- Put Bucket Object Lock Configuration: Allows you to place an Object Lock configuration on the specified bucket.
- Put Object Legal Hold: Allows you to apply a legal hold configuration to the specified object. The legal hold status indicates whether an object is locked and cannot be overwritten or deleted.
- Put Object Retention: Allows you to apply an Object Retention configuration on an object.

To select all the permissions, click Select all.

7. Click Assign Namespaces.

Changing the permissions for an individual namespace

1. In the list of user or group accounts on the Users or Groups page, as applicable, click the name of the user account or group account you want.
   The panel that opens includes a list of the namespaces for which the user or group account already has data access permissions.
2. (Optional) Filter the list of namespaces.
   a. In the field above the Name column for the list of namespaces, select Name to filter the list by namespace name or Tag to filter the list by tag.
   b. In the next field, 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.
   c. Click the find control ( ).
3. In the list of namespaces, click the name of the namespace for which you want to change the data access permissions.
4. In the Data Access Permissions section, select the permissions you want the user or group account to have for the selected namespaces.
   Selecting Read automatically selects Browse. Selecting Search automatically selects Read and Browse. Selecting Purge automatically selects Delete.
   To select all the permissions, click Select all.
5. In the S3 Object Lock Permissions section, select the permissions you want to grant to the user or group account for the selected namespaces.
   Important: You will not see these permissions settings, if S3 Object Lock is not enabled on the namespace. The following is a list of S3 Object Lock permissions, explaining when you would use each one.
   - Bypass Governance Retention: Allows you to perform operations such as deletion, shortening the retention period, or removing the lock on object versions that are locked in governance mode.
   - Get Bucket Object Lock Configuration: Allows you to retrieve the S3 Object Lock configuration for a bucket.
   - Get Object Legal Hold: Allows you to retrieve an object's current legal hold status. The legal hold status indicates whether an object is locked and cannot be overwritten or deleted.
   - Get Object Retention: Allows you to retrieve an object's retention settings. The retention settings indicate whether an object is locked and cannot be overwritten or deleted.
   - Put Bucket Object Lock Configuration: Allows you to place an Object Lock configuration in the specified bucket.
   - Put Object Legal Hold: Allows you to apply a legal hold configuration to the specified object. The legal hold status indicates whether an object is locked and cannot be overwritten or deleted.
   - Put Object Retention: Allows you to apply an Object Retention configuration on an object. Setting retention periods ensures that objects remain locked for a specific duration.

   To select all the permissions, click Select all.
6. Click Update Settings.

Dissociating a namespace from a user or group account

1. In the list of user or group accounts on the Users or Groups page, as applicable, click the name of the user account or group account you want.
   The panel that opens includes a list of the namespaces for which the user or group account already has data access permissions.
2. (Optional) Filter the list of namespaces.
   a. In the field above the Name column for the list of namespaces, select Name to filter the list by namespace name or Tag to filter the list by tag.
   b. In the next field, 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.
   c. Click the find control ( ).
3. In the list of namespaces, click the delete control ( ) for the namespace for which you want to remove all data access permissions.
4. In response to the confirming prompt, click Delete.

User account and login settings

Several system settings affect user accounts and logins to the Tenant Management Console and Search Console. To view and change these settings, you use the Console Security page in the Tenant Management Console.

To display the Console Security page, in the top-level menu of the Tenant 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.
- 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 number of days after which locally authenticated users are automatically forced to change their passwords. Valid values are integers in the range zero through 999,999. The default is 180 days. A value of zero means users are never automatically forced to change their passwords.
  Note: Password expiration affects use of the System Management Console, Tenant Management Console, Search Console, and HCP management API only. Users with expired passwords can continue to use these passwords with the HCP metadata query API.

  Password changes affect all the HCP interfaces.

- 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 and no group accounts have the security role, the user account is reenabled automatically after one hour.

Note: A user account with both roles and data access permissions can be disabled by consecutive attempts to use the HTTP protocol or Namespace Browser with an invalid password. A user account with only data access permissions is not disabled by these actions.

- 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.

  If no group accounts have the security role, the last locally authenticated user account with the security role is not automatically disabled due to inactivity.

- The number of minutes a Tenant Management Console, Search Console, or Namespace Browser 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 sessions never time out due to inactivity.

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

  - If the user explicitly logged in, the Console or Browser login page appears
  - In the case of single sign-on, the Console or Browser displays the selected page in the Tenant Management Console or Namespace Browser or the Simple Search page in the Search Console.

  Tip: If the tenant supports AD authentication and has no HCP user accounts, the recommended session timeout interval is eight hours.

- Message text to appear on the login page of the Tenant Management Console and Search Console. 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 Finance Department HCP Management Console`.

Change one or more login settings

1. On the Console Security page, in the Login Settings section
   a. Make the changes you want.
   b. Click Update Settings.
2. In the Login Message section:
   a. Type the message you want.
   b. Click Modify Login Message.

Managing the current tenant

When you log into the Tenant Management Console, you do so for a particular tenant. You can then view all the available information about that tenant, change certain of its properties, and monitor its activity.

Tenant Overview page

When you log into the Tenant Management Console, the first page you see is the tenant Overview page. This page gives you a view of the tenant as a whole. It also shows the HCP system time.

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

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

Tenant statistics

The tenant Overview page shows three categories of statistics:

Storage
: This category shows:

  Quota
  : The total number of bytes available to the tenant for allocation to its namespaces. This is the hard quota for the tenant.

  Used
  : The total number of bytes currently occupied by stored data in all the tenant's namespaces. This includes object data, metadata (except ACLs), and any redundant data required to satisfy the namespace DPLs.
  Used storage includes storage occupied by the parts of in-progress multipart uploads that have already been written to the tenant's namespaces. Used storage does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.
  Note: Replaced parts, parts of aborted multipart uploads, and parts not included in completed multipart uploads are deleted automatically but not necessarily immediately.

  Available
  : The number of bytes still available for storing data in the tenant's namespaces.

Namespaces
: This category shows:

  Quota
  : The number of namespaces reserved for the tenant out of the total number of namespaces the system can have. This is also the maximum number of namespaces the tenant can own at any given time. If the tenant doesn't have a quota, this field displays `No Quota`.

  Used
  : The number of namespaces currently owned by the tenant.

  Available
  : The number of additional namespaces the tenant can own if the tenant has a quota. 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 with no quota.

  Objects 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 object versions that are delete markers or delete records.
  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.

  Objects Indexed

The total number of indexed objects in all the tenant's namespaces. This is the number of objects in the index maintained by the search facility that's currently selected for use with the Search Console.
This item appears only if the tenant has the search feature and a search facility is currently selected for use with the Search Console.

Accounts
This category shows:

- The numbers of locally authenticated and RADIUS-authenticated user accounts defined for the tenant. This information is shown only if the tenant supports local or RADIUS authentication.
- The number of group accounts defined for the tenant. This information is shown only if the tenant supports AD authentication and HCP support for AD is enabled at the system level.

Major tenant events

The Major Events section on the tenant Overview page lists log messages about major events related to the tenant and its namespaces (for example, the tenant permission mask was changed or a namespace was created). The list includes all such messages that have occurred since the tenant was created.

The list of messages in the Major Events section is a subset of the messages in the event log for the tenant. You can view all the tenant-level messages in the tenant event log in the All Events panel on the Tenant Events page.

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

If the Overview page shows alerts instead of log messages, click the Major Events tab to display the log messages.

Tenant alerts

The Alerts section on the tenant Overview page shows alerts that indicate tenant-related conditions that may require human intervention (for example, the tenant is running low on unused space). This section is visible only if alerts currently exist for the tenant.

Each alert is represented by an icon accompanied by descriptive text.

If the Overview page shows log messages instead of alerts, click the Alerts tab to display the alerts.

Note: If the tenant is read-only due to being a replication target or due to metadata unavailability, a notice of the situation appears at the top of every Tenant Management Console page. In this case, you cannot make any configuration changes to the tenant or to the namespaces it owns, nor can users and applications make any changes to namespace content. Additionally, in the case of metadata unavailability, statistics that describe namespace content may be inaccurate.

Tenant features

The Features section on the tenant Overview page shows which of these features the tenant has:

Replication
If this feature is present, the tenant is eligible for replication. Additionally, when you create a namespace, you have the option of selecting it to be replicated with the tenant. You can also select and deselect existing namespaces for replication.
If this feature is not present, the tenant cannot be replicated, and you cannot select or deselect namespaces to be replicated with it.

Retention Mode Selection
If this feature is present, you can set the retention mode to either enterprise or compliance when you create a namespace. You can also change the retention mode of an existing namespace from enterprise to compliance, but you cannot do the reverse.
If this feature is not present, you can create namespaces only in enterprise mode and cannot change the retention mode of an existing namespace.

Search
If this feature is present, you can create namespaces that support search. You can also enable and disable search for existing namespaces.
If this feature is not present, you cannot enable search for namespaces.

Service Plan Selection
If this feature is present, you can associate service plans with namespaces.
If this feature is not present, you cannot associate service plans with namespaces.

Versioning
If this feature is present, you can create namespaces with versioning enabled. You can also enable and disable versioning for existing namespaces.
If this feature is not present, you cannot enable versioning for namespaces.

Tenant contact information

You can view contact information for the current tenant from the tenant Overview page. To view this information, click Contact Information.

To view the contact information for a tenant, you need the administrator role.

The contact information for a tenant is visible not only in the Tenant Management Console but also in the system-level administrative interface to the HCP system. HCP system administrators can use this information to notify you about systemwide events (such as a system shutdown for maintenance). Therefore, you should keep this information up to date.

Tenant permission mask

The Permissions section on the tenant Overview page shows:

- The permissions included in the inherited permission mask, which is the systemwide permission mask. These permissions are indicated by gray dots.
- The permissions included in the tenant permission mask. These permissions are indicated by orange dots.
- The permissions included in the effective permission mask for the tenant. These permissions are indicated by checkmarks.

Tenant description

The Description section on the tenant Overview page shows the description of the tenant, if a description exists. This description is visible only in the Tenant Management Console. It is not visible to HCP system-level administrators who don't have administrative access to the tenant.

The tenant description appears below the tenant name on the login page for the Tenant Management Console.

Configuring the tenant

Changing the tenant contact information

When creating a tenant, the HCP system administrator has the option of entering contact information for it. Once the tenant exists, both system-level administrators and tenant-level administrators can modify this information.

To view or modify the tenant contact information, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Overview.
2. On the tenant Overview page, click Contact Information.
3. In the Contact Information window, fill in the contact information.
   The list below describes the values you can specify. Except as indicated, all fields are optional.

   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.

4. Click Update Contact Info.

Changing the tenant permission mask

When a tenant is created, its data access permission mask includes all permissions. You can change the permission mask for the current tenant at any time.

To change the tenant permission mask, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Overview.
2. On the tenant Overview page, click the edit link for the Permissions section.
   The Console displays a set of checkboxes for the possible permissions. The permissions that are currently in the tenant permission mask are selected.
3. Select or deselect permissions as needed to modify the permission mask.
   Selecting Purge automatically selects Delete. Selecting Search automatically selects Read.
4. Click Submit.

Changing the tenant description

The tenant description is optional. You can enter a description or modify the existing description at any time.

To change the tenant description, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Overview.
2. On the tenant Overview page, click the edit link for the Description section.
3. In the edit area for the description, type the new 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.
4. Click Submit.

Enabling or disabling system-level administrative access

You can choose whether to grant HCP system-level users administrative access to the current tenant. By default, when a tenant is created, this access is not enabled. You can change this at any time.

To enable or disable system-level administrative access to the tenant, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Overview.
2. On the tenant Overview page, take either of these actions:
   - To grant access, select Allow HCP system-level users to manage me and search across my space.
   - To deny access, deselect Allow HCP system-level users to manage me and search across my space.

Controlling access to the Tenant Management Console

You can choose to allow access to the Tenant Management Console only from specific IP addresses. Similarly, you can choose to deny access to the Console from specific IP addresses.

You use the Console Security page in the Tenant Management Console to configure access to the Console. To display this page, in the top-level menu of the Tenant Management Console, select Security > Console Security.

To view or modify the Console Security page, you need the security role.

To control access to the Tenant Management Console, on the Console Security page:

- Optionally, in the Allow/Deny section, specify IP addresses to be allowed or denied access to the Console.
- 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. Changes to this option take effect immediately.

Controlling access to HCP through the management API

For you to use the HCP management API with a tenant-level user account, the API must be enabled for both the HCP system and the tenant. Additionally, the API must be configured at the tenant level to allow access from your client IP address.

Enabling the management API also enables the use of the S3 compatible APIs to perform these bucket (S3 compatible API) and container activities:

- Create buckets or containers
- List the buckets or containers you own
- Enable, disable, or check the status of versioning for a bucket (S3 compatible API only)
- Add, retrieve (S3 compatible API only), or remove an access control list (ACL) for a bucket or container
- Delete a bucket or container

You use the Management API page in the Tenant Management Console to enable and configure the management API at the tenant level. To display this page, in the top-level menu of the Tenant Management Console, select Security > MAPI.

To view and modify the HCP management API configuration, you need the security role.

1. Enable the management API.
   In the Management API Settings section:
   a. Select Enable the HCP management API.
   b. Click Update Settings.
2. (Optional) In the Allow/Deny section, specify IP addresses to be allowed or denied access to HCP through the management API.
3. 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.
   Changes to this option take effect immediately.

Controlling access to the Search Console

To use the HCP Search Console to search one or more namespaces, users log into the Search Console for the tenant that owns those namespaces. You can choose to allow access to the Search Console only from specific IP addresses. Similarly, you can choose to deny access to the Search Console from specific IP addresses.

You use the Search Security page in the Tenant Management Console to configure access to the Search Console. To display this page, in the top-level menu of the Tenant Management Console, select Security > Search Security.

To view or modify the Search Security page, you need the security role.

To control access to the Search Console, on the Search Security page:

- Optionally, in the Allow/Deny section, specify IP addresses to be allowed or denied access to the Search Console.
- 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. Changes to this option take effect immediately.

Monitoring the tenant

While the tenant Overview page in the Tenant Management Console gives you a view of the tenant as a whole, the tenant log lets you monitor tenant and namespace activity on a more detailed level. The log records tenant and namespace events such as:

- Tenant Management Console logins
- Namespace creations
- Tenant and namespace configuration changes
- Creations, modifications, and deletions of retention classes
- Privileged delete operations
- Warnings about used storage approaching the hard quota

Each recorded entry about an event is called a *message*. The tenant log contains all the messages written to it since the tenant was created.

Viewing the complete tenant event log

The All Events panel on the Tenant Events page lists all messages recorded for the tenant and its namespaces. By default, the panel displays ten messages at a time in reverse chronological order.

Another way to manage the list of events displayed for the tenant is by using the Search option on the Tenant Events page. This option allows you to view All Events, Security Events, and Compliance Events based on a user-specified date range, event ID, or node.

To view the tenant All Events panel, you need the monitor, administrator, security, or compliance role. However, only users with the compliance role can see messages about events that require the compliance role. Only users with the security role can see messages about attempts to log into the Tenant Management Console with an invalid username.

1. In the top-level menu of the Tenant Management Console, select Monitoring > Tenant Events.
2. On the left side of the Tenant Events page, click All Events.

Viewing the tenant security log

The Security Events panel on the Tenant Events page lists all messages about attempts to log into the Tenant Management Console with an invalid username. By default, the panel displays ten messages at a time in reverse chronological order.

To view the tenant Security Events panel, you need the security role.

1. In the top-level menu of the Tenant Management Console, select Monitoring > Tenant Events.
2. On the left side of the Tenant Events page, click Security Events.

Viewing the tenant compliance log

The Compliance Events panel on the Tenant Events page lists all messages about events that require the compliance role across all the tenant's namespaces. This includes all retention class activity and privileged delete operations. By default, the panel displays ten messages at a time in reverse chronological order.

To view the tenant Compliance Events panel, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, select Monitoring > Tenant Events.
2. On the left side of the Tenant Events page, click Compliance Events.

Understanding log messages

Each message displayed in a view of the tenant log includes this information about an event:

- The username of the event initiator:
  - For user-initiated events, this is the username 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 username 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 username for the message is blank.
  - For system-initiated events, the username is `[internal]`.
  - For events initiated by HCP service or support personnel by means other than the Tenant Management Console, the username is `[service]`.

  Additionally, when the tenant is being replicated, messages for events initiated by a user who accessed the Tenant Management Console directly from the HCP System Management Console have a username of `[remote admin]` in the log messages on systems to which the tenant is replicated.

- 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:
  - Namespace created
  - Privileged delete requested

  Warning
  : The event is out of the ordinary and may require manual intervention.
  Examples are:
  - Namespace over soft quota
  - User account failed login

  Error
  : The event is serious and most likely requires manual intervention.
  Examples are:
  - HCP found an irreparable object
  - Object did not replicate

- The date and time at which the event occurred, shown in the time zone of the HCP system.
- 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 full text of the event message

Managing the message list

You can take the following actions in any of the views of the tenant log:

- To display details for all the listed events, click expand all. To hide all details, click collapse all.
- To view a different number of messages per page, select the number you want in the Items per page field.
- To page forward or backward, click the next (▶) or back (◀) control, respectively.
- To filter the events displayed for the tenant, you can use the Search option. This option allows you to view All Events, Security Events, and Compliance Events based on a user-specified date range, event ID, or node.

Viewing the Active Directory log

The Active Directory log lists the unassigned Service Principal Names of the tenant. If there are no SPNs or the system is not set to warn you about missing SPNs, the log states that the system is properly configured. If the tenant is missing an SPN, then it is listed here. This page is only visible if AD is enabled on both the System Management Console and Tenant Management Console.

Roles: To view the Active Directory log, you need the monitor, administrator, and security roles.

To display the Active Directory Status panel, in the top-level menu of the Tenant Management Console, select Security > Active Directory.

Enabling syslog logging

An HCP system can be configured to send system-level log messages to one or more specified syslog servers. You can choose to also send tenant log messages to those servers. The system-level configuration determines whether compliance and security messages are sent along with the other tenant log messages.

You use the Syslog page in the Tenant Management Console to enable or disable sending tenant log messages to the syslog servers. To display this page, in the top-level menu of the Tenant Management Console, select Monitoring > Syslog.

To view the Syslog page, you need the monitor or administrator role. To enable or disable syslog logging, you need the administrator role.

1. On the Syslog page, select (to enable) or deselect (to disable) Enable syslog logging.
   If the HCP system is not configured for syslog logging, selecting this option has no effect.

2. Click Update Settings.

Enabling SNMP logging

An HCP system can be configured to send system-level log messages to one or more specified SNMP managers. You can choose to also send tenant log messages to those managers. The system-level configuration determines whether compliance and security messages are sent along with the other tenant log messages.

You use the SNMP page in the Tenant Management Console to enable or disable sending tenant log messages to the SNMP managers. To display this page, in the top-level menu of the Tenant Management Console, select Monitoring > SNMP.

To view the SNMP page, you need the monitor or administrator role. To enable or disable SNMP logging, you need the administrator role.

1. On the SNMP page, select (to enable) or deselect (to disable) Enable SNMP logging.
   If the HCP system is not configured for SNMP logging, selecting this option has no effect.
2. Click Update Settings.

Configuring email notification

HCP can be configured at the system level to support the use of email to notify recipients about messages added to the system-level log. If the HCP system supports email notification, you can configure HCP to send email about tenant log messages to recipients that you specify.

You can configure each email recipient to receive notification of only selected messages based on the message importance, severity, and type. Important messages are those that appear in the Tenant Management Console. 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 tenant 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 Tenant Management Console to enable and configure email notification. To display this page, in the top-level menu of the Tenant Management Console, select Monitoring > Email.

Roles: To view the Email page, you need the monitor or administrator role. To configure email notification, you need the administrator role.

Enabling email notification

1. (Optional) Test whether email notification is supported.
2. Select Enable email notification.
3. (Optional) Change the format of the email to be sent.
4. Specify one or more recipients to receive email about log messages.

Testing email notification

HCP email notification works only if the HCP system has been configured to enable support for this feature. At any time, you can test the HCP system to determine whether it has been configured to support email notification.

Testing support for email notification 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`.

1. On the Email page, click Test.
2. In the Test Email Notification window, type the email address to which you want HCP to send the test email.
3. Click Send.

If support for email notification is not configured at the system level, the Tenant Management Console displays an error message. If the Console displays a success message but the email does not arrive, ensure that you've correctly specified the email address to which you want the email sent. If the email still doesn't arrive, contact your HCP system administrator for help.

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:

From
: 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.

Subject
: 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.

Body
: 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.

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 list below lists the variables you can use in the email template.

$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
: Either Tenant or Namespace

$severity
: The severity of the event that triggered the message

$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)

Modify the email notification template

Modify the template HCP uses for email notification about log messages.

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. 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.

Restoring the default template

The list below shows the format of the default email template.

From
: log@$location

Subject
: [$severity] $shortText

Body

```
The following event occurred on $date: $fullText

Reason:
$reason

Action:
$action

Details:
User: $user
Origin: $origin
```

1. On the Email page, click Reset.
2. 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.

Modifying rows in the recipients list

1. Add a row.
   a. (Optional) 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.
2. Modify a row.
   a. (Optional) 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.
   b. (Optional) 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.
3. To delete a row, click the delete control ( ) for the row.
   The row turns red.
4. Click Update Settings at the bottom of the page.

Monitoring and managing replication

The Replication page in the Tenant Management Console shows information about replication of the current tenant when both of these conditions are true:

- The tenant is eligible for and currently selected for replication.
- The HCP system is configured to show this information.

If the tenant is eligible for but not currently selected for replication, the page shows a replication status of `Not Replicating`.

You can use the statistics and graphs on the Replication page to monitor replication progress. You can also use the page to select and deselect namespaces to be replicated along with the tenant.

To display the Replication page, in the top-level menu of the Tenant Management Console, select Services > Replication.

Roles: To view the Replication page, you need the monitor or administrator role. To select and deselect namespaces for replication, you need the administrator role.

Tenant-level view of replication

At the tenant level, the Replication page shows:

- Only on an HCP system that's sending data for the tenant to other systems, the approximate number of objects and parts of multipart objects currently waiting to be replicated in all namespaces owned by the tenant.
- Only on an HCP system that's sending data for the tenant to other systems, the approximate amount of data currently waiting to be replicated in all namespaces owned by the tenant, in bytes.
- On an HCP system that's sending data for the tenant to other systems or receiving data for the tenant from other systems, the current rate of replication activity, expressed as operations per second and as bytes per second. An operation is the replication of a single item, such as the creation of a new object, a metadata change, or a namespace configuration change.

  These rates are the sums of the corresponding rates for the tenant's namespaces.

- A list of the namespaces selected for replication with the tenant. For each namespace, the list shows a progress bar that measures the up-to-date-as-of time for replication of that namespace, along with this time as a numeric value. The length of the progress bar represents 30 days, with the right end representing the current time.

  The up-to-date-as-of time is the difference between:

  - The time before which objects, object parts, metadata changes, and configuration changes are guaranteed to have been sent to other systems or received from other systems
  - The current time

Managing the namespace list

By default, the namespace list on the Replication page includes all the namespaces that are selected for replication. The namespaces are listed 20 at a time in ascending order by namespace name.

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

Paging

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

To page forward or backward through the namespace 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 namespace list in ascending or descending order by namespace name. To sort the list, 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 namespace list by namespace name or tag. The filtered list includes only those namespaces with a name or tag, as applicable, that begins with or is the same as a specified text string.

1. In the field above the Name column, select Name to filter by name or Tag to filter by tag.
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 ( ).

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

Namespace-level view of replication

To view more detailed information about the replication of an individual namespace listed on the Replication page, click the namespace name. The panel that opens shows:

- The date and time before which objects, parts of multipart objects, metadata changes, and configuration changes for the namespace are guaranteed to have been sent to other systems or received from other systems
- A graph of the history of the up-to-date-as-of time for replication of the namespace
- A graph of the history of the data transmission rate for replication of the namespace
- A graph of the history of the operation rate for replication of the namespace

On an HCP system that's sending data for the tenant to other systems, the panel also shows this information for the namespace:

- The approximate number of objects and parts of multipart objects currently waiting to be replicated
- The approximate amount of data currently waiting to be replicated

Up-to-date-as-of time

The Up to date as of section in the namespace replication panel contains a graph that shows the history of the up-to-date-as-of time for replication of the namespace. The section heading shows the current up-to-date-as-of time. If the graph is not currently visible, click Up to date as of to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication has been occurring for less than 30 days). The y-axis marks the up-to-date-as-of time in days, hours, or minutes. As the up-to-date-as-of time varies, the measurement unit for the y-axis grows or shrinks as needed (for example, from days to hours to minutes). The lower the up-to-date-as-of time, the closer replication is to being synchronized with current namespace activity.

Data transmission rate

The Transfer Rate section in the namespace replication panel contains a graph that shows the history of the rate of replication data transmissions for the namespace per second. The section heading shows the current data transmission rate. If the graph is not currently visible, click Transfer Rate to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication or recovery has been occurring for less than 30 days). The y-axis marks the data transmission rate in KB, MB, or GB. As the transmission rate varies, the measurement unit for the y-axis grows or shrinks as needed (for example, from KB to MB to GB).

Operation rate

The Operations per Second section in the namespace replication panel contains a graph that shows the history of the rate of replication operations for the namespace per second. The section heading shows the current operation rate. If the graph is not currently visible, click Operations per Second to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication or recovery has been occurring for less than 30 days). The y-axis marks the operation rate in tens, hundreds, or thousands. As the operation rate varies, the measurement unit on the y-axis grows or shrinks as needed (for example, from tens to hundreds to thousands).

Selecting or deselecting namespaces for replication

On the Replication page, at any time, you can change which namespaces are replicated with the tenant and, if allowed by the tenant configuration, specify whether those namespaces allow erasure coding. If you disable replication for a namespace that was already being replicated, replication of that namespace stops. If you subsequently enable replication for that namespace again, replication of the namespace starts again from where it stopped.

When you reenable replication of a namespace that has already been replicated, all operations that occurred in that namespace while replication was not happening, including object deletions, are replicated to the other system. During this replication, conflicts can occur between changes made on different systems while the namespace was not being replicated.

If you disable replication for a namespace that has already been replicated and then delete the namespace on one or more systems, the namespace deletions are not replicated. If you then reenable replication for that namespace and the namespace still exists on one or more systems, the namespace is replicated back to the systems where you deleted it.

You can also enable or disable replication for a namespace and specify whether the namespace allows erasure coding on the namespace Replication panel.

Depending on the current status of replication, if the tenant is being replicated, you may not be able to disable replication for namespaces that are being replicated.

Allowing erasure coding for a namespace that has shredding enabled as the default for new objects can significantly increase the load on all systems in the replication topology.

Important: Disabling replication for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

1. Click Namespace Selection for Replication.
   The Namespace Replication Selection section lists all the tenant's namespaces. For each namespace, the section shows whether the namespace is cloud optimized.
   The Namespace Replication Selection section has a column in which you can select or deselect namespaces for replication. If you can specify whether namespaces allow erasure coding, this section also has a column in which you can allow or disallow erasure coding for namespaces.
2. In the Namespace Replication Selection section:
   - To enable or disable replication for a namespace, select or deselect the namespace in the Replication column.
   - To enable or disable replication for all namespaces at the same time, select or deselect the Replication column heading.

     When you deselect Replication for a namespace, Allow Erasure Coding is automatically deselected for that namespace.

   - To allow or disallow erasure coding for a namespace, select or deselect the namespace in the Allow Erasure Coding column. This option is available only for cloud-optimized namespaces.
   - To allow or disallow erasure coding for all cloud-optimized namespaces at the same time, select or deselect the Replication column heading.

     When you select Allow Erasure Coding for a namespace, Replication is automatically selected for that namespace.

The Allow Erasure Coding column is present only if you're allowed to choose whether namespaces allow erasure coding.

3. Click Update Namespaces.

Generating chargeback reports

You can generate chargeback reports from the Tenant Management Console. A *chargeback report* contains current and historical statistics about the tenant and its namespaces, broken out by hour.

Chargeback reports are a good source of information for namespace 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.

About chargeback reports

A chargeback report contains statistics for each namespace owned by the current tenant. It also contains aggregated namespace statistics for the tenant. For example, the total number of reads for the tenant during a given reporting interval is the total number of successful read operations that occurred during that interval in each of the tenant's namespaces.

When generated from the Tenant Management Console, chargeback reports are in CSV format. Each line in a report contains the values for one namespace or for the tenant during one instance of the reporting interval.

The lines in a chargeback report are ordered alphabetically by namespace name. The lines for the tenant are at the end of the report. Multiple lines for a namespace or the tenant are ordered in ascending chronological order.

Roles: To generate chargeback reports, you need the monitor or administrator role.

Types of chargeback reports

You use the Chargeback page in the Tenant Management Console to generate chargeback reports. From this page, you can generate an hourly, daily, or monthly report:

Hourly report
: Includes statistics for the most recent full hour, plus the statistics accumulated so far for the current hour. For example, if you request the report at 2:30:15 p.m., it will contain one set of statistics for the period of time between 1:00:00 p.m. and 1:59:59 p.m. and another set of statistics for the period of time between 2:00:00 p.m. and 2:30:15 p.m.

Daily report
: Includes statistics for the most recent full day, plus the statistics accumulated so far for the current day. For example, if you request the report at 2:30:15 p.m. on October 7th, it will contain 24 sets of statistics for the period of time between 00:00:00 and 23:59:59 on October 6th and 15 sets of statistics for the period of time between 00:00:00 and 2:30:15 p.m. on October 7th.

Monthly report
: Includes statistics for the past 30 days, plus the statistics accumulated so far for the current day. For example, if you request the report at 2:30:15 p.m. on October 7th, it will contain 24 sets of statistics for each of the past 30 days and 15 sets of statistics for the period of time between 00:00:00 and 2:30:15 p.m. on October 7th.

The statistics reported for the current hour may not reflect some reads and writes that have already occurred during the hour. After the hour is past, however, the statistics reported for it are complete.

Tip: You can use the HCP management API to generate chargeback reports that cover longer time periods and are in XML, JSON, or CSV format. This allows you to create applications that generate chargeback reports at regular intervals and feed those reports to a billing system. For information about using the management API to generate chargeback reports, see HCP Management API Reference.

Generating a chargeback report

To generate a chargeback report, you need the monitor or administrator role.

1. In the top-level menu of the Tenant Management Console, select Monitoring > Chargeback.
2. On the Chargeback page:
   As applicable:
   - Click Hourly Chargeback Report.
   - Click Daily Chargeback Report.
   - Click Monthly Chargeback Report.
3. Select the browser-specific option for downloading the report.

By default, the name of the downloaded report file is either Hourly-Chargeback-Report.csv, Daily-Chargeback-Report.csv, or Monthly-Chargeback-Report.csv, as applicable.

Chargeback statistics collection

Chargeback statistics either reflect a 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 list below describes each of these values.

bytesIn
: Type: Dynamic
: The total number of bytes successfully written to the given namespace or to any of the namespaces owned by the tenant 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
: Type: Dynamic
: The total number of bytes read from the given namespace or from any of the namespaces owned by the tenant 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
: One of:

true
For a namespace only, the namespace was deleted after the statistics in the set were collected.
false
The namespace or tenant currently exists.
included
For a tenant only, the statistics in the set include values for one or more namespaces that were subsequently deleted.

deletes
Type: Dynamic
The total number of delete and purge operations successfully performed in the given namespace or in any of the namespaces owned by the tenant 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
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.

ingestedVolume
Type: Point in time
The total size of the stored data and custom metadata, in bytes, before the data and custom metadata were added to the given namespace or to any of the namespaces owned by the tenant.

multipartObject Bytes
Type: Point in time
The total number of bytes of object data in all the parts of multipart objects currently stored in the given namespace or in all the namespaces owned by the tenant.

multipartObject Parts
Type: Point in time
The total number of parts of multipart objects currently stored in the given namespace or in all the namespaces owned by the tenant.

multipartObjects
Type: Point in time
The total number of multipart objects currently stored in the given namespace or in all the namespaces owned by the tenant.

multipartUpload Bytes
Type: Point in time
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 or in all the namespaces owned by the tenant.
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
Type: Point in time
The total number of successfully uploaded parts of multipart uploads that are currently in progress in the given namespace or in all the namespaces owned by the tenant.
This number does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

multipartUploads
Type: Point in time
The total number of multipart uploads that are currently in progress in the given namespace or in all the namespaces owned by the tenant.

namespaceName
The name of the namespace to which the set of statistics in the line applies.
In lines that contain tenant statistics, this field has no value.

objectCount
Type: Point in time
The number of objects in the given namespace or in all the namespaces owned by the given tenant.
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.
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
Type: Dynamic
The total number of read operations performed in the given namespace or in any of the namespaces owned by the given tenant during the reporting interval.
A read of a multipart object counts as a single 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: 2010-10-07 14:00:00

storageCapacity Used
Type: Point in time
The total number of bytes occupied by stored data in the given namespace or in any of the namespaces owned by the given tenant. This includes object data, metadata, and any redundant data required to satisfy the applicable service plan.
Used storage capacity includes storage occupied by the parts of in-progress multipart uploads that have already been written to HCP. Used storage does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.

systemName
The HCP domain name used for access to the content of namespaces owned by the given tenant

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

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 a network failure or to other hardware issues.

writes
Type: Dynamic
The total number of write operations successfully performed in the given namespace or in any of the namespaces owned by the given tenant 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 europe tenant, which owns the finance and hr namespaces. The report is shown as it would appear in a spreadsheet.

systemName	tenantName	namespaceName	startTime	endTime	objectCount	IngestedVolume	storageCapacityUsed	bytesIn	bytesOut	reads	writes	deletes	multipa
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	2
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	3
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	87561	1	17	0	2
hcp.example.com	europe		2/18/2017 0:00:00	2/18/2017 23:59:59	30	206204134	206278656	62351045	0	0	20	0	3

Chargeback page graphs

The Chargeback page contains four graphs. These graphs show information about the usage of the tenant's namespaces 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 tenant's namespaces.
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 tenant's namespaces.
Each write 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 tenant's namespaces.

Reads (operations)
: Shows the number of read operations that targeted the tenant's namespaces.
A read of a multipart object counts as a single read operation.

Managing namespaces

When a tenant is first created, it has no namespaces. You use the Tenant Management Console to create them as needed.

After creating a namespace, you can view all the available information about it, change its properties, and monitor its activity. You can also delete namespaces that have no objects in them.

About the Namespaces page

o view, create, and manage namespaces, you use the Namespaces page in the Tenant Management Console. To display this page, in the top-level menu, click Namespaces.

The Create Namespace bar on the Namespaces page shows the number of bytes of storage used in all the tenant's namespaces, along with a graphical representation of the amount of storage used out of the hard quota for the tenant. It also shows the number of bytes of storage available for storing more objects in the tenant's namespaces.

The Namespaces page also lists the namespaces owned by the current tenant.

Roles: To view the Namespaces page, you need the monitor, administrator, or compliance role.

Understanding the namespace list

The Namespaces page contains a list of the namespaces owned by the current tenant. For each namespace, the list shows:

- The namespace name.
- The number of objects currently in the namespace. 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.

  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.

- Icons for any current alerts that apply to the namespace. Alerts indicate conditions that may need your attention. To see the text that accompanies an alert icon, hover over the icon.
- The number of bytes of storage used out of the hard quota for the namespace, along with a graphical representation of the amount of storage used.

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

Note: Replaced parts, parts of aborted multipart uploads, and parts not included in completed multipart uploads are deleted automatically but not necessarily immediately.

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

Managing the namespace list

By default, the namespace list on the Namespaces page includes all existing namespaces. The namespaces are listed 20 a time in ascending order by namespace name.

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

Paging

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

To page forward or backward through the namespace 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 namespace list in ascending or descending order by namespace name or by 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.

Filter using filter fields

You can filter the namespace list by namespace name or tag. The filtered list includes only those namespaces with a name or tag, as applicable, that begins with a specified text string.

You can filter the namespace list by name or by tag by using the fields above the list.

1. In the field above the Name column, select Name to filter by name or Tag to filter by tag.
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 ( ).

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

Filter using tag control

1. Click the tag control ( ) on the right above the namespace list.
   The Tags window opens. This window lists all the tags currently associated with the existing namespaces owned by the current tenant. For each tag, the window shows the number of associated namespaces.
2. Click the tenant-count icon ( ) for the tag you want.
   The namespace list shows only the namespaces that have the selected tag, and the fields above the Name column show the filter criteria.

Namespace Overview panel

The namespace Overview panel shows the current status of any given namespace.

Display the namespace Overview panel

To view the namespace Overview panel, you need the monitor, administrator, or compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.

To return to the namespace Overview panel from other namespace panels, click Overview in the row of tabs below the namespace name.

Namespace URL

The top of the namespace Overview panel shows the URL for access to the namespace content through the HTTP protocol. If the HTTP protocol is enabled for the namespace, this URL is a link that opens the Namespace Browser for the namespace.

A namespace URL has this format:

`https://`*`namespace-url-name.tenant-url-name.hcp-domain-name`*

For example, the URL for access to the content of the Accounts-Receivable namespace owned by the Finance tenant in the HCP system named hcp-ma.example.com is:

`https://accounts-receivable.finance.hcp-ma.example.com`

If SSL security is not enabled for the HTTP protocol, the URL contains http instead of https.

Note: The HCP domain name used for access to namespace content may not be the same as the domain name used for access to the tenant for management purposes. Be sure to give your namespace users the correct domain name.

Similarly, the IP addresses for the system may differ for these two purposes. For the IP addresses to use for namespace access, contact your HCP system administrator.

Namespace owner

The top right corner of the namespace Overview panel shows the namespace owner if the namespace has an owner:

- If the owner user account is an HCP account, the panel shows the account username.

  If the user account for the owner of a namespace is deleted, the namespace reverts to having no owner.

  - HCP can retrieve the user account information from AD, the panel shows the account username along with the name of the AD domain in which the account is defined, in this format: *username@ad-domain-name*
  - HCP cannot retrieve the user account information from AD, the panel shows the SID for the user account. This can happen if the AD user account was deleted or if HCP cannot communicate with AD.

In either case, the username or SID is a link that you can use to change the namespace owner. If the namespace has no owner, the top right corner of the panel shows the Modify Owner link, which you can use to assign an owner to the namespace.

Objects section

The Objects section in the namespace Overview panel contains a graph showing the number of objects in the namespace during the past 30 days (or since the namespace was created if that was less than 30 days ago).

Each version of an object counts as a separate object. However, the object count does not include object versions that are delete markers and delete records.

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 any of the search facilities is selected for use with the Search Console, the graph also shows the total number of indexed objects in the namespace 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 marks the number of objects. As the number of objects increases, the intervals on the y-axis get larger. The section heading indicates the current measurement unit (for example, thousands or millions).

The graph legend shows the most recent value for the number of objects stored (Ingested object count) and, if applicable, the number of indexed objects (Indexed object count).

Below the Usage section, which is below the Objects section, the Overview panel shows the date and time the Objects and Usage sections were last updated. To show the most current information in these sections, click Refresh Now.

Usage section

The Usage section in the namespace Overview panel contains a graph showing information about the namespace storage during the past 30 days (or since the namespace was created if that was less than 30 days ago).

The x-axis in the Usage graph marks the passage of time. The y-axis measures the amount of storage in gigabytes, terabytes, or petabytes, depending on the namespace size. The graph heading indicates the current measurement unit (gigabytes (GB), terabytes (TB), or petabytes (PB)).

The Usage graph shows:

Total storage capacity
: The hard quota for the namespace.

Used storage capacity
: The total amount of storage space currently occupied by all data stored in the namespace, including object data, metadata (except ACLs), and any redundant data required to satisfy the namespace service plan.
Used storage includes storage occupied by the parts of in-progress multipart uploads that have already been written to the namespace. Used storage does not include replaced parts of multipart uploads, parts uploaded for aborted multipart uploads, or unused parts of completed multipart uploads.
Note: Replaced parts, parts of aborted multipart uploads, and parts not included in completed multipart uploads are deleted automatically but not necessarily immediately.

Ingested volume
: The total size of the stored data and custom metadata before it was added to the namespace. This value tells you how much data you have stored.

The graph legend shows the current value for each item.

Below the Usage section, the Overview panel shows the date and time the Objects and Usage sections were last updated. To show the most current information in these sections, click Refresh Now.

Major namespace events

The Major Events section in the namespace Overview panel lists log messages about major events related to the namespace (for example, the amount of storage used by the namespace exceeds the namespace soft quota). The list includes all such messages that have occurred since the namespace was created.

The list of messages in the Major Events section is a subset of the messages in the event log for the namespace. You can view all the messages in the namespace event log in the All Events panel for the namespace.

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

If the Overview panel shows alerts instead of log messages, click the Major Events tab to display the log messages.

Namespace alerts

The Alerts section in the namespace Overview panel shows alerts that indicate namespace-related conditions that may require human intervention (for example, the namespace is running low on unused space). This section is visible only if alerts currently exist for the namespace.

Each alert is represented by an icon accompanied by descriptive text.

If the Overview panel shows log messages instead of alerts, click the Alerts tab to display the alerts.

Namespace features

The Overview panel for a namespace shows which of these features are currently enabled for the namespace:

Replication
: If this feature is present, the namespace is included in replication of its owning tenant. If this feature is not present, the namespace is not included in replication of its owning tenant.

Search
: If this feature is present, search is currently enabled for the namespace. The namespace is searchable if its effective permission mask includes search. If this feature is not present, the namespace is not searchable.

Versioning
: If this feature is present, users and applications can create multiple versions of objects in the namespace. If this feature is not present, the namespace does not support versioning.

Additionally, the Overview panel shows:

- The service plan in effect for the namespace.

  This feature is present only if the tenant is allowed to associate service plans with namespaces.

- The retention mode of the namespace depending on the retention type of the namespace.
  - **HCP Retention Mode**: Compliance or enterprise.

- **S3 Object Lock**: Disabled, governance, or compliance.
- The cryptographic hash algorithm for the namespace.
- The DPL for the namespace.

Namespace permission mask

The Permissions section in the namespace Overview panel shows:

- The permissions included in the inherited mask, which is the effective tenant permission mask.

  These permissions are indicated by gray dots.

- The permissions included in the namespace permission mask.

  These permissions are indicated by orange dots.

- The permissions included in effective permission mask for the namespace.

  These permissions are indicated by checkmarks.

Namespace description

The Description section in the namespace Overview panel shows the description of the namespace, if a description exists.

Creating a namespace

You create namespaces in the Tenant Management Console. When you create a namespace, you set some of its properties. Other namespace properties have default settings that you can change only after the namespace has been created.

You can change most of the properties for existing namespaces.

Note:

- If the tenant supports Active Directory authentication, you can create a namespace only while HCP can communicate with AD.
- Under certain circumstances, the current state of replication for the tenant may prevent namespace creation.

To create a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. On the Namespaces page, click Create Namespace.
   The Create Namespace panel opens. Below the Namespace Name field, this panel shows the number of namespaces the tenant currently owns and the number of additional namespaces currently available for the tenant to create.

   The default settings that appear in the Create Namespace panel are determined by the settings on the Namespace Defaults page.

3. In the Namespace Name field, type a name for the namespace.
   HCP derives the hostname for the namespace from this name. The hostname is used in URLs for access to the namespace.

   In English, the name you specify for a namespace must be from one through 63 characters long and can contain only alphanumeric characters and hyphens (-) but cannot start or end with a hyphen. In other languages, because the derived hostname cannot be more than 63 characters long, the name you specify may be limited to fewer than 63 characters.

   Namespace names cannot contain special characters other than hyphens and are not case sensitive. White space is not allowed.

   Namespace names cannot start with *xn*-- (that is, the characters *x* and *n* followed by two hyphens).

   The namespace name must be unique for the current tenant. Different tenants can have namespaces with the same name.

   You can change the namespace name any time after you create the namespace, except while the CIFS or NFS protocol is enabled for the namespace. However, when you change the name, the URL for the namespace may change as well.

   You can reuse namespace names that are not currently in use. So, for example, if you delete a namespace, you can give a new namespace the same name as the deleted namespace had.

4. (Optional) Specify an owner for the namespace:
   - If the owner has an HCP user account, select Local. Then type the username for the account in the Namespace Owner field.
   - If the owner has an AD user account, select Active Directory. Then, in the Namespace Owner field, type the account username along with the name of the AD domain in which the account is defined, in this format: *username@ad-domain-name*.
5. (Optional) In the Description field, type a description of the namespace.
   The description can be up through 1,024 characters long and can contain any valid UTF-8 characters, including white space. However, it must not include special characters such as *\n* (carriage return) and *\r* (line feed).
6. In the Hash Algorithm field, select the cryptographic hash algorithm for the namespace.
7. In the Hard Quota field, type the number of gigabytes or terabytes of storage to allocate to the namespace 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. The maximum value is the amount of space the tenant still has available to allocate to its namespaces.
   Tip: To the right of the Hard Quota field, the panel shows the amount of space the tenant has already allocated to its namespaces and the amount of space it still has available to allocate.
8. In the Soft Quota field, type the percent at which you want HCP to notify the tenant that free storage space for the namespace is running low.
   Valid values are integers in the range ten through 95.
9. (Optional) Associate tags with the namespace:
   a. Click Tags.
   b. 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.
   c. Click Add Tag.
10. Under Replication:
    - Select On to replicate the namespace along with the tenant.
    - Select Off to exclude it from replication.

    The Replication option is present only if the tenant is allowed to create namespaces with replication enabled.

Note: Depending on current replication requirements, if the tenant is being replicated, this option may be selected automatically. In this case, you cannot deselect it.

11. (Optional) If you selected On for Replication, select Allow erasure coding to allow HCP to use erasure coding to implement replication of the objects in the namespace.
    The Allow erasure coding option is present only while Replication is On and only if the tenant is allowed to manage erasure coding for namespaces.
    When you select Allow erasure coding, the Cloud Optimized option is automatically set to On.
12. Under Cloud Optimized:
    - Select On to optimize the namespace for cloud protocols only.
    - Select Off to optimize the namespace for all protocols.

    The Cloud Optimized option is present only if the tenant is allowed to create namespaces with replication enabled.
    When you select Off while Allow erasure coding is selected, that option is automatically deselected.
13. Under Directory Usage:
    - Select Balanced to configure the namespace for balanced directory usage.
    - Select Unbalanced to configure the namespace for unstructured data usage.
14. Under Retention Type, select either S3 Object Lock or HCP Retention to set the retention type for the namespace.
    The HCP Retention Mode option is present only if the Retention Mode Selection is enabled. You can enable S3 Object Lock only if versioning is enabled on the tenant.
    Note: When configuring namespaces that use S3 Object Lock, you cannot use existing retention related namespace configuration options that conflict with S3 Object Lock. For example, retention period values that Amazon S3 does not support, initial unspecified, event-based retention, and retention classes are not allowed.
15. Under Search:
    - Select On to enable search for the namespace.
    - Select Off to disable search.

    The Search option is present only if the tenant is allowed to create namespaces with search enabled.
16. In the Service Plan field, either type the name of an existing service plan or click the arrow control ( ).
    If you click the arrow control:
    a. In the Service Plans window, select the service plan you want.
    b. Click Apply Service Plan.

    The Service Plan field is present only if the tenant is allowed to associate service plans with namespaces.
17. Under Versioning:
    - Select On to enable object versioning in the namespace.
    - Select Off to disable object versioning in the namespace.

    The Versioning option is present only if the tenant is allowed to create namespaces with versioning enabled.
    When you select On, you can also enable version pruning and delete markers.
    a. In the Versioning Options section, select the Prune versions older than ... days option.
    b. In the option field, type the number of days old versions of objects must remain in the namespace before they are pruned.
       Valid values are integers from zero through 36,500 (that is, 100 years). A value of zero means prune immediately.
       If version pruning is enabled for a namespace, you can apply a backup policy to keep milestone versions for specified periods of time. You cannot delete versions that are under retention. The milestone versioning policy can apply to an object only when it is outside the retention policy of that object.
    c. In the Versioning Options section, select the Enable delete markers option.

       This option allows you to use the delete markers in Amazon S3 using Hitachi API for Amazon S3 and REST API. After you enable versioning and delete markers, you cannot disable them.

       When you delete an object in a version-enabled namespace, a delete marker is created. The delete marker then becomes the current version. The object behaves as if it is deleted. However, it automatically maintains previous versions of the object. The delete marker has the following characteristics:

       - Like in any other versioned object, the delete marker has a version ID associated with it.
       - Using an S3 DELETE request, you can delete the delete marker by specifying the version ID of the marker.
       - Using a GET bucket version request, you can retrieve a delete marker version ID.

       For non-versioned namespaces, allow object overwrites if desired. See Allowing object overwrites.
18. Click Create Namespace.
    If Versioning is set to On but Prune versions is not selected, a confirming message appears.
19. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
20. Click Update Settings.

Configuring a namespace

Changing the namespace name

You can change the name of a namespace any time, except while the S3 compatible, CIFS, or NFS protocol is enabled for the namespace. However, when you change the name, the URL for the namespace may change as well.

When you change the name of a namespace, AD single sign-on is automatically disabled for the REST API for that namespace. You can reenable it any time after the name change (as long as HCP can communicate with AD).

Tip: Be sure to notify the namespace users when you change the name of a namespace.
To change the name of a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Settings.
4. On the left side of the Settings panel, click Name.
5. In the New Namespace Name field in the Name panel, type the new name for the namespace.
6. Click Update Name.

Changing the namespace permission mask

When you create a namespace, its data access permission mask includes all permissions. Once the namespace exists, you can change its permission mask at any time.

To change a namespace permission mask, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the namespace Overview panel, click the edit link for the Permissions section.
   The Console displays a set of checkboxes for the permissions. The permissions that are currently in the namespace permission mask are selected.
4. Select or deselect permissions as needed to modify the permission mask.
   Selecting Purge automatically selects Delete. Selecting Search automatically selects Read.

5. Click Submit.

Changing the namespace description

The namespace description is optional. You can enter a description or modify the existing description at any time.

To change a namespace description, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the namespace Overview panel, click the edit link for the Description section.
4. In the edit area for the description, type the new description of the namespace.
   The description can be up through 1,024 characters long and can contain any valid UTF-8 characters, including white space.
5. Click Submit.

Changing the namespace storage quotas

You can change both the hard quota and soft quota for a namespace at any time.

To change namespace quotas, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the modify quotas control ( ) for the namespace whose quotas you want to change.
3. In the Modify Namespace Quota window, take either or both of these actions:
   - In the Hard Quota field, type the number of gigabytes or terabytes of storage to allocate to the namespace and select either GB or TB to indicate the measurement unit. Valid values are integers greater than or equal to one.
   - In the Soft Quota field, type a new soft quota for the namespace. Valid values are integers in the range ten through 95.
4. Click Update Quota.

Changing the namespace owner

You can change or remove the owner of a namespace at any time.

To change or remove the owner of a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In top right corner of the namespace Overview panel, click the Assign Owner link or the name of the current namespace owner, whichever is shown.
4. In the Modify Namespace Owner window that appears, type the name of the new owner in the New Namespace Owner field.
   Optionally, to remove the current owner of a namespace, leave the New Namespace Owner field empty.
5. Click Update Owner.

Changing the namespace tags

You can change the tags associated with a namespace at any time.

- To view the tags associated with a namespace, you need the monitor or administrator role.
- To change the tags associated with a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Settings.
4. On the left side of the Settings panel, click Tags.
5. Associate a new tag with the namespace.
   a. 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.
   b. Click Add Tag.
   The row with the new tag is highlighted in green.
6. (Optional) To remove a tag from the namespace, click the delete control ( ) for the tag.
   The row with the tag turns red.
7. Click Update Settings.

Changing the default HCP retention settings

When you create a namespace, its default HCP retention setting is Deletion Allowed. Once the namespace exists, you can change this setting at any time. Valid values for this setting are:

- An offset from the time the object is created.

  You specify an offset as numbers of years, months, and/or days. For example, you could specify an offset of two years. Then, an object added to the namespace on March 10, 2011, at 9:45 a.m. would expire on March 10, 2013, at 9:45 a.m.

- A retention class.
- One of these special values:

  Deletion Allowed
  : The object can be deleted at any time.

  Deletion Prohibited
  : The object can never be deleted by means of a normal delete operation. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.
  After an object has this retention setting, its retention setting cannot be changed.

  Initial Unspecified
  : The object cannot be deleted, but can have its retention setting changed to any other retention setting. This setting is useful for namespaces for which the only enabled namespace access protocol is SMTP.

- A fixed date in the future. In this case, the retention period for the object ends at the end of the specified day.

Tip: If you specify a fixed date, remember to change the default retention setting again before that date occurs. Otherwise, the default retention setting reverts to Deletion Allowed when the specified date arrives.

- To view the default retention setting for a namespace, you need the monitor, administrator, or compliance role.
- To change the default retention setting for a namespace, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Retention.
5. In the Default Retention Setting section in Retention panel, take one of these actions:
    - To make the default retention setting an offset: In the Retention Method field, select Offset, and then enter values in Years, Months, and Days. Possible values are integers in the range zero through 9,999.
    - To make the default retention setting a retention class: In the Retention Method field, select Retention Class, and then select the retention class you want.
    - To make the default retention setting a special value: In the Retention Method field, select Special Value, and then select the special value you want.
    - To make the default retention setting a fixed date: In the Retention Method field, select Fixed Date, and then either type a date or click the calendar control ( ) to select a date.
6. Click Update Settings in the Default Retention Setting section.

Changing the default shred setting

When you create a namespace, its default shred setting is not to shred. Once the namespace exists, you can change this setting at any time.

Once an object is marked for shredding, its shred setting cannot be changed.

Note: If HCP is allowed to use erasure coding to implement replication of a namespace, setting the default shred setting to shred for that namespace can significantly increase the load on all systems in the replication topology.

- To view the default shred setting for a namespace, you need the monitor, administrator, or compliance role.
- To change the default shred setting for a namespace, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Shredding.
5. In the Shredding panel:.
    - To enable secure deletion, select Shred on delete.
    - To disable secure deletion, deselect Shred on delete .
6. Click Update Settings.

Allowing object overwrites

When using HCP and the Hitachi API for Amazon S3, executing a PUT request for an object that has the same name as an existing object in a versioned namespace creates a new version of the object. For objects in non-versioned namespaces, you can enable an overwrite option to overwrite the prior contents of an object when executing a PUT request for an existing object. This option is available when creating or editing a non-versioned namespace.

Observe the following guidelines when using the overwrite option with objects in a non-versioned namespace:

- By default, the overwrite option is disabled. Executing a PUT request for an existing object results in a 409 Conflict error.
- If the overwrite option is enabled for a namespace, executing a PUT request for an existing object in that namespace succeeds and overwrites the previous contents of the object. This behavior is similar to issuing a DELETE request followed by a PUT request for an object in a non-versioned namespace.
- The overwrite option applies to the S3 compatible API only. It does not apply to REST or NFS/CIFS.
- For versioned namespaces, the overwrite option has no effect until versioning is disabled.
- If the overwrite option is selected and subsequent versioning is enabled for the namespace, the overwrite option remains selected and has no effect unless versioning is disabled.
- Objects under retention cannot be overwritten.
- Any custom metadata included with the overwrite PUT request is written with the object and any existing custom metadata associated with the prior instance of the object is deleted. If you add custom metadata with an overwrite PUT request, the custom metadata will be added to the object.
- The overwrite option is replicated to other HCP systems that support the overrite feature.
- If you replicate a namespace that suports the overwrite option to an HCP version that does not support this option, the overwrite option is not available for the earlier version. However, the object overwrite succeeds, and a DELETE request and a PUT request are sent to the replica system.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. Check Allow overwrite of objects via Hitachi API for Amazon S3 if versioning is disabled.

Changing the default index setting

When you create a namespace, its default index setting is to index. Once the namespace exists, you can change this setting at any time.

- To view the default index setting for a namespace, you need the monitor or administrator role.
- To change the default index setting for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Indexing.
5. In the Indexing panel:
    - To enable indexing, select Index objects.
    - To disable indexing, deselect Index objects.
6. Click Update Settings.

Changing minimum data access permissions

When you create a namespace, the set of minimum data access permissions is empty both for all users (that is, authenticated users and users that access the namespace anonymously) and for authenticated users. Once the namespace exists, you can modify these sets at any time.

- To view the minimum data access permissions for a namespace, you need the monitor or administrator role.
- To change the minimum data access permissions for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Protocols.
4. In the Protocols panel, click Minimum Data Access Permissions.
5. In the Minimum Data Access Permissions panel, select or deselect permissions, as applicable, for all users (Anonymous and Authenticated Access) and for authenticated users (Authenticated Access Only).
   Selecting Read automatically selects Browse. Selecting Search automatically selects Read and Browse. Selecting Purge automatically selects Delete.
   By default, selecting a permission in the Anonymous and Authenticated Access row automatically selects the same permission in the Authenticated Access Only row and prevents the permission from being deselected in that row. For information about changing this behavior, see the next step.
6. Click Advanced Configuration.
7. (Optional) Take either of these actions:
   - To ensure that authenticated users always have the minimum permissions for all users in addition to the minimum permissions for authenticated users regardless of whether the protocol they're using requires authentication, select Enforce anonymous permissions for authenticated users.

     Selecting this option causes permissions in the Authenticated Access Only row to be selected automatically when you select the corresponding permissions in the Anonymous and Authenticated Access row.

   - To allow unauthenticated users to have permissions that don't apply to authenticated users when those users are using a protocol that requires authentication, deselect Enforce anonymous permissions for authenticated users.

     Deselecting this option allows you to select permissions in the two rows independently of each other.
8. Click Update Settings.

Enabling the use of ACLs

When you create a namespace, the use of ACLs is disabled. Once the namespace exists, you can enable this feature. However, after enabling this feature, you cannot disable it.

To enable the use of ACLs for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Settings.
4. On the left side of the Settings panel, click ACLs.
5. In the ACLs panel, select Enable ACLs.
6. In response to the confirming prompt, click Enable ACLs.

Changing the option to enforce ACLs

By default, when you enable the use of ACLs for a namespace, the option to enforce ACLs is enabled. You can enable or disable this option at any time while the use of ACLs is enabled.

To view or change the option to enforce ACLs for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Settings.
4. On the left side of the Settings panel, click ACLs.
5. In the ACLs panel:
   - To have HCP enforce ACLs, select Enforce ACLs.
   - To have HCP not enforce ACLs, deselect Enforce ACLs.
6. Click Update Settings.

Changing HCP retention-related settings

When you create a namespace:

- Changes to POSIX UIDs and GIDs, POSIX permissions, and object owners are not allowed for objects under retention.
- Only add operations are allowed with custom metadata for objects under retention.

Once the namespace exists, you can change these settings at any time.

- To view retention-related settings for a namespace, you need the monitor, administrator, or compliance role.
- To change these settings for a namespace, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies pane, click Retention.
5. (Optional) In the Retention Options section in the Retention pane:
   - To allow changes for objects under retention, select Allow ownership and POSIX permission changes for objects under retention.
   - To allow the addition, deletion, and replacement of custom metadata for objects under retention, retention hold, and labeled retention hold, select Add, delete, and replace.
   - To allow only the addition of custom metadata for objects under retention, retention hold, and labeled retention hold, select Add only.
   - To disallow all custom metadata operations for objects under retention, retention hold, and labeled retention hold, select None.
6. Click Update Settings in the Retention Options section.
7. (Optional) In the Event-based Retention section in the Retention pane, set the Minimum Retention after Initial Unspecified value. Then, in the Event-based Retention section, click Update Settings.
   Similar to specifying an offset, you can specify this value as numbers of years, months, and/or days. The retention set on Initial Unspecified objects in the namespace must be greater than the Minimum Retention after Initial Unspecified value.

Enabling or disabling XML checking for custom metadata

When you create a namespace, custom metadata XML checking is enabled. You can change this setting at any time.

- To view the custom metadata XML checking setting for a namespace, you need the monitor or administrator role.
- To change the custom metadata XML checking setting for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Metadata.
5. In the Metadata panel, take one of these actions:
    - To enable custom metadata XML checking, select Check on ingestion that XML in custom metadata files is well-formed.
    - To disable custom metadata XML checking, deselect Check on ingestion that XML in custom metadata files is well-formed.
6. Click Update Settings.

Configuring object versioning

When you create a namespace, you specify whether versioning is enabled or disabled for it. Once the namespace exists, you can change this setting at any time except while the WebDAV, CIFS, NFS, or SMTP protocol is enabled for the namespace.

If a tenant is not allowed to create namespaces with versioning enabled, the versioning setting is not available for its namespaces.

When you enable versioning, you can also enable version pruning. If versioning has ever been enabled for a namespace, you can change the pruning settings for the namespace at any time regardless of whether versioning is currently enabled.

Tip: To immediately remove old versions of objects, set the number of days to keep them to zero.

HCP maintains a transaction log in which it records 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.

For any given namespace, you can choose whether HCP should keep records of deletion operations (delete, purge, prune, and disposition) if the namespace has ever had versioning enabled. The amount of time for which HCP keeps deletion records is determined by the system configuration.

In a namespace that was replicated but is not currently selected for replication, the following sequence of actions can cause objects that were deleted to reappear:

1. You deselect the option to keep records of deletion operations.
2. You reselect the namespace for replication.

- To view the versioning settings for a namespace, you need the monitor or administrator role.
- To change the versioning settings for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Versioning.
5. In the Versioning panel:
    - To enable or disable versioning, select or deselect the Enable versioning option, respectively.
    - To enable or disable version pruning, select or deselect the Prune versions older than ... days option, respectively.

      If you select this option, in the option field, type the number of days old versions of objects must remain in the namespace before they are pruned. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means prune immediately.

      This option is available only if you select the Enable versioning option or if versioning has ever been enabled.

    - To keep or not keep deletion records, select or deselect the Keep deletion records for versioned objects option, respectively.
6. Click Update Settings.
   If the version pruning option is unselected, a confirming message appears.
7. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
8. Click Update Settings.

Changing the compatibility setting

When you create a namespace, atime synchronization is disabled. You can change this setting at any time.

- To view the compatibility setting for a namespace, you need the monitor or administrator role.
- To change the compatibility setting, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Settings.
4. On the left side of the Settings panel, click Compatibility.
5. In the Compatibility panel, select or deselect the Synchronize POSIX atime values and object retention settings.
6. Click Update Settings.

Changing disposition settings

When you create a namespace, disposition is disabled for both objects with expired retention periods and objects flagged as replication collisions. Once the namespace exists, you can change these settings at any time.

- To view the disposition settings for a namespace, you need the monitor, administrator, or compliance role.
- To change the disposition settings for a namespace, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Services.
4. On the left side of the Services panel, click Disposition.
5. In the Disposition panel:
    - To enable or disable disposition for objects with expired retention periods, select or deselect Automatically delete objects with expired retention periods, respectively.

- To enable or disable disposition for objects flagged as replication collisions, select or deselect Automatically delete replication collision objects after ... days, respectively.

  If you select this option, in the option field, type the number of days objects flagged as replication collisions must remain in the namespace before they are automatically deleted. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means delete immediately.

6. Click Update Settings.

Changing the automatic abort time for multipart uploads

The automatic abort time for a namespace determines how long multipart uploads can remain incomplete before they are automatically aborted.

You can change the automatic abort time for a namespace at any time while the namespace is cloud optimized. You cannot change the automatic abort time for a namespace that is not cloud optimized.

- To view the automatic abort time for a namespace, you need the monitor or administrator role.
- To change the automatic abort time for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Multipart Upload.
5. In the Abort incomplete multipart uploads field, type the number of days after which HCP should automatically abort incomplete multipart uploads in the namespace. Valid values are integers in the range zero through 180. A value of zero means multipart uploads are never automatically aborted.
6. Click Update Settings.

Changing replication options

You can enable or disable replication for a namespace on the namespace Replication panel. While replication is enabled for the namespace, you can change options that relate to replication. While replication is disabled for the namespace, these options are hidden.

The replication options you can change are:

- Read from remote system.

  By default, when you create a namespace, this option is enabled.

  Important: Do not disable the read-from-remote-system option unless you have a specific reason to do so.
- Accept REST, S3 compatible requests redirected from other HCP systems.

  By default, when you create a namespace, this option is enabled.

  You may want to disable this option if your applications cannot tolerate stale data or metadata. One way to get stale data would be to request an object for which two versions exist but for which the current version hasn't been replicated yet. In this case, the system targeted by the request would retrieve the old version from another system in the replication topology and return that version to the application.

- Collision handling.

  By default, when you create a namespace, this option is set to move objects.

- Allow erasure coding.

  If allowed by the tenant configuration and if you make the namespace cloud optimized, when you create a namespace, you can choose whether the namespace allows erasure coding.

  Allowing erasure coding for a namespace that has shredding enabled as the default for new objects can significantly increase the load on all systems in the replication topology.

  You can also enable or disable replication for namespaces and, if allowed, manage erasure coding on the Replication page.

  While the tenant is being replicated, if you disable replication for a namespace that has already been replicated and then delete the namespace on one or more systems, the namespace deletions are not replicated. If you then reenable replication for that namespace and the namespace still exists on one or more systems, the namespace is replicated back to the systems where you deleted it.

  Important: Disabling replication or the read-from-remote-system option for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

- To view the replication options for a namespace, you need the monitor or administrator role.
- To change the replication options for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the namespace you want.
3. In the row of tabs below the namespace name, click Services.
4. On the left side of the Services panel, click Replication.
5. To enable or disable replication, select or deselect Replication.
6. (Optional) If Enable replication is selected, take one or more of these actions:
   - To enable or disable the read-from-remote-system feature, select or deselect Enable read from remote system.
   - To allow or disallow HCP to service redirected REST, S3 compatible requests that target the namespace, select or deselect Accept requests redirected from other systems in the replication topology.
   - For cloud-optimized namespaces only, to allow or disallow erasure coding for the namespace, select or deselect Allow erasure coding.
   - To change the collision handling option, click Collision Handling. Then, in the Collision Handling section:
     - To have HCP move objects flagged as replication collisions to the .lost+found directory, select Move object to the .lost+found directory.
     - To have HCP rename objects flagged as replication collisions, select Rename object and store in the same location.
7. Click Update Settings.
   Note: Removing a tenant from an Active-Passive replication link on the Active site followed by its deletion from the Passive site can result in lost data if, in the future, an Active/Active replication link is created between the same clusters and the same tenant is added to that link.

Changing the service plan

The service plan for a namespace is set when the namespace is created. You can change this setting at any time.

- To view the service plan for a namespace, you need the monitor or administrator role.
- To change the service plan for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Services.
4. On the left side of the Services panel, click Service Plan.
5. In the list of service plans, select the service plan you want.
   Note: HCP system administrators can delete service plans regardless of whether they're associated with any namespaces. In this case, the service plan name remains associated with the applicable namespaces, but the service plan is not available to be selected for any namespaces. HCP uses the Default service plan for the namespaces associated with that service plan name.

   In the list of service plans, a deleted service plan has no description.

6. Click Update Settings.

Changing the HCP retention mode

The HCP retention mode of a namespace is either enterprise or compliance. You can change a namespace in enterprise mode to compliance mode, but you cannot do the reverse.

If a tenant is not allowed to create namespaces in compliance mode, the retention mode setting is not available for its namespaces.

When you change the HCP retention mode of a namespace from enterprise to compliance, you have no guarantee that objects that should have been retained were not already deleted.

Important: Changing the retention mode of a namespace may violate local regulations regarding data retention. Before taking this action, be sure you understand the implications.

- To view the retention mode setting for a namespace, you need the monitor or administrator role.
- To change the retention mode of a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Retention.
5. In the Retention Mode panel, select Compliance.
6. Click Update Settings.
   A confirming message appears.
7. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
8. Click Update Settings.

Configuring S3 Object Lock

Configuring an S3 Object Lock namespace allows you to apply retention periods or legal holds to your objects, ensuring that they remain locked for a specified period of time.

- To view the S3 Object Lock settings for a namespace, you need the monitor, administrator, or compliance role.
- To change the default S3 Object Lock settings for a namespace, you need the administrator role.
- To configure S3 Object Lock, you must enable it when you create the namespace. For more information about enabling S3 Object Lock, see Creating a namespace.
- You must enable versioning at the tenant level.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Policies.
4. On the left side of the Policies panel, click Retention.
5. In the Default Retention section in the Retention pane:
   a. Select Enabled to enable Default Retention.
   b. Select Disabled to disable Default Retention.
      The default retention mode determines the level of protection applied to objects placed in the namespace. When you create a new namespace with S3 Object Lock enabled, you can choose to configure a default retention mode. If you disable default retention, objects will not have an active retention period and can be deleted.
6. In the Default Retention Mode section in the Retention pane:
   a. Select Governance to enable governance mode.

      In S3 Object Lock governance mode, users with the necessary permissions can change the retention settings or delete objects.

   b. Select Compliance to enable compliance mode.
      In compliance mode, users and administrators cannot delete objects or modify the retention settings to reduce or remove retention time. However, users and administrators can extend the retention time as needed.
   c. In the Default Retention Period field, type the number of days or years that you want to retain the object.
      The minimum duration is 1 day from the current date and the maximum duration is 100 years. If you choose compliance mode, neither users nor administrators can change retention settings or delete objects..
7. Click Update Settings.

Namespace-level CORS rules configuration

You can use the Tenant Management Console to configure CORS rules for a namespace.

Alternatively, you can use either the Hitachi API for Amazon S3 or the HCP management API to configure CORS rules at the namespace level.

You can also configure CORS rules at the tenant level to serve as the default CORS configuration for all namespaces owned by a tenant. To configure CORS settings at the tenant level, use either the System Management Console or the HCP management API. Note that you must have the administrator role to modify a tenant.

This section of the help describes how to use the Tenant Management Console to configure CORS settings at the namespace level.

Request elements (CORS rules)

A CORS rules configuration uses the request elements described in the next table. Some of the request elements are optional.

CORSConfiguration
: Container for CORSRules elements.

Type: Container
Children: `CORSRules`
Ancestor: None
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.
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.

```
<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 for a namespace

You can use the Tenant Management Console to configure CORS settings for a namespace.

- 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 Tenant Management Console, click Namespaces.
2. On the Namespaces page, click the right arrow next to the namespace for which you want to configure CORS settings.
   The namespace 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 CORS settings to use for the namespace.
5. Click Update Settings.
   A message is displayed above the CORS Configuration field indicating whether the update was successful.

Your configuration is saved and persists in HCP.

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"?>
```

Configuring namespace access protocols

HCP supports the REST, S3 compatible, WebDAV, CIFS, NFS, and SMTP protocols for access to namespaces. You use these protocols to add, view, modify, and delete namespace content. Additionally, you can use the S3 compatible API to create, view or change the versioning status of, and delete namespaces.

Each protocol is configured separately for each namespace. Any given protocol can be enabled on some namespaces and disabled on others unless protocol optimization is configured for cloud-only protocols.

This section of the help provides instructions for enabling and configuring each of the supported protocols.

Namespace access protocol configuration

Users and applications have access to the content stored in namespaces through these industry-standard protocols: REST, S3 compatible API, WebDAV, CIFS, NFS, and SMTP. By default, when a namespace is created, the REST API is enabled. The other protocols are initially disabled. For any namespace access to occur, at least one protocol must be enabled.

For enhanced security, keep unused namespace access protocols disabled.

When you enable a namespace access protocol, you also need to configure it. Each protocol, with the exception of the REST, S3 compatible, and WebDAV protocols, has its own set of configuration options. REST, the S3 compatible API, and WebDAV share a set of these options. Some configuration options are common to multiple protocols; others are protocol specific.

Note: If your system administrator has configured new namespaces to be optimized for cloud protocols only, you cannot configure new namespaces to use CIFS, NFS, WebDAV or SMTP without first disabling cloud optimization for the namespace. If you have already begun ingesting data in the namespace, you cannot disable cloud optimization. Similarly, NFS, CIFS, and WebDAV cannot be enabled if the namespace assigned to a service plan has HCP S Series Nodes set as the ingest tier. To allow enabling of CIFS, NFS, WebDAV, or SMTP, see the topic *Modifying a service plan* in the Administering HCP online help and select Primary Running as the ingest tier for the service plan to which the namespace is assigned.

For namespaces configured with S3 Object Lock, only the S3 gateway protocol is supported.

Display the Protocols panel

To enable and configure the protocols for a namespace, you use the Protocols panel for that namespace in the Tenant Management Console. This panel has separate tabs for each protocol except REST, the S3 compatible API, and WebDAV, which share a tab.

- To view the Protocols panel, you need the monitor or administrator role.
- To enable, disable, and configure namespace access protocols, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want to configure.
3. In the row of tabs below the namespace name, click Protocols.

Changing the protocol optimization for a namespace

A namespace can be optimized for all namespace access protocols or for cloud protocols only. Optimization for all protocols is required if clients will be using the WebDAV, CIFS, NFS, or SMTP protocol to access the namespace.

Optimization only for cloud protocols increases the ingest rate for the namespace but also configures the namespace to ingest objects exclusively through the cloud protocols (REST and the S3 compatible API). This setting is recommended if clients will be using only cloud protocols to access the namespace.

Only cloud-optimized namespaces can allow erasure coding. Also, only cloud-optimized namespaces support multipart uploads with the S3 compatible API.

You can change the protocol optimization setting for a namespace from optimized only for cloud protocols to optimized for all protocols only if all of these are true:

- The namespace does not contain any objects.
- The namespace does not allow erasure coding.
- The namespace is not configured for unbalanced directories.
- The namespace is not configured to use S3 Object Lock.

You can change the protocol optimization setting from optimized for all protocols to optimized only for cloud protocols only if the namespace doesn't have any noncloud protocols enabled.

A system administrator can change a tenant from not being able to choose whether namespaces allow erasure coding to being able to do this. After this change occurs, when you enable cloud optimization for a preexisting namespace that was not cloud optimized and that did not allow erasure coding, the namespace is automatically configured to allow erasure coding.

Note: You cannot make protocol optimization changes while an HCP system upgrade is in progress.

- To view the protocol optimization setting for a namespace, you need the monitor or administrator role.
- To change the protocol optimization setting for a namespace, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the namespace, click the Settings tab.
4. In the namespace left-hand navigation bar, click Optimization.
5. In the Optimization panel, select Optimized for all protocols or Optimized for cloud protocols only.
6. Click Update Settings.
   If you selected Optimized for cloud protocols only, a confirming message appears.

7. In the field in the message window, type YES (this is case sensitive) to confirm that you understand the consequences of your action.
8. Click Update Settings.

IP addresses for namespace access

For each namespace access protocol, you have the option of allowing access only from specific IP addresses. For all but NFS, you can also deny access to the namespace from specific IP addresses.

Tip: For enhanced security, restrict access to namespaces to as few IP addresses as possible.

The Tenant Management Console panels for the namespace access protocols each contain an Allow list and, except for the NFS panel, a Deny list. Each list has an associated field in which you type entries for it.

Add entries in Allow and Deny lists

Changes you make to either list of IP addresses take effect immediately.

1. In the field above the list, type the entry you want.
2. Click Add.

Remove entries in Allow and Deny lists

To remove a single entry, click the delete control ( ) for that entry.

To remove all entries, click Delete All.

Changes you make to either list of IP addresses take effect immediately.

Valid Allow and Deny list entries

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.

Allow and Deny list handling

IP addresses can be included in neither, one, or both of the Allow and Deny lists for REST, the S3 compatible API, WebDAV, CIFS, and SMTP. They can be included or not included in the Allow list for the NFS protocol. The way HCP handles allowed and denied IP addresses differs depending on the protocol.

Allow and Deny list handling for REST, the S3 compatible API, and WebDAV

For HTTP and WebDAV, you can choose how HCP handles Allow and Deny list entries by selecting or deselecting Allow request when same IP is used in both lists in the HTTP(S) panel. The table below describes the effects of selecting or deselecting this option. Either action takes effect immediately.

Allow requests when same IP is used in both lists		
List entries	Selected	Not selected
Allow list: empty Deny list: empty	All IP addresses can access the namespace through REST, the S3 compatible API, and WebDAV.	No IP addresses can access the namespace through REST, the S3 compatible API, or WebDAV.
Allow list: at least one entry Deny list: empty	All IP addresses can access the namespace through REST, the S3 compatible API, and WebDAV.	Only IP addresses in the Allow list can access the namespace through REST and WebDAV.
Allow list: empty Deny list: at least one entry	All IP addresses not in the Deny list can access the namespace through REST, the S3 compatible API, and WebDAV. IP addresses in the Deny list cannot.	No IP addresses can access the namespace through REST, the S3 compatible API, or WebDAV.
Allow list: at least one entry Deny list: at least one entry	IP addresses appearing in both or neither of the lists can access the namespace through REST, the S3 compatible API, and WebDAV.	Only IP addresses appearing in the Allow list and not in the Deny list can access the namespace through REST, the S3 compatible API, or WebDAV.

Allow and Deny list handling for CIFS

For CIFS, HCP handles Allow and Deny list entries as described in the table below.

List entries	Effect
Allow list: empty Deny list: empty	All IP addresses can access the namespace through the CIFS protocol.
Allow list: at least one entry Deny list: empty	Only IP addresses in the Allow list can access the namespace through the CIFS protocol.

List entries	Effect
Allow list: empty Deny list: at least one entry	All IP addresses that are not in the Deny list can access the namespace through the CIFS protocol. IP addresses in the Deny list cannot.
Allow list: at least one entry Deny list: at least one entry	IP addresses that appearing in the Allow list and the Deny list cannot access the namespace through the CIFS protocol.

Allow list handling for NFS

For NFS, if the Allow list in the NFS panel includes one or more IP addresses, those addresses have access to the namespace through NFS and all others don't. If the list is empty, all IP addresses can access the namespace through NFS.

Allow and Deny list handling for SMTP

For SMTP, HCP handles Allow and Deny list entries as described in the table below.

List entries	Effect
Allow list: empty Deny list: empty	All IP addresses can access the namespace through the SMTP protocol.
Allow list: at least one entry Deny list: empty	Only IP addresses in the Allow list can access the namespace through the SMTP protocol.
Allow list: empty Deny list: at least one entry	No IP addresses can access the namespace through the SMTP protocol.
Allow list: at least one entry Deny list: at least one entry	Only IP addresses appearing in the Allow list and not in the Deny list can access the namespace through the SMTP protocol.

User authentication options

The REST, S3 compatible, and CIFS protocols have the option to either require user authentication or support both authenticated and unauthenticated (anonymous) access. If a protocol requires authentication, users must present valid credentials in order to use the protocol. If a protocol supports both types of access, users can present credentials but are not required to.

With the REST, S3 compatible, or CIFS protocol configured to support both authenticated and anonymous access:

- If a user presents credentials, HCP tries to authenticate the user. If the credentials are valid, HCP continues processing the request. If the credentials are invalid, HCP rejects the request.
- With REST and CIFS, if a user does not present credentials, HCP continues processing the request.
- With the S3 compatible API, if a user presents the clear-text username all_users, HCP continues processing the request. If the user does not present either credentials or all_users, HCP rejects the request.

Configuring the REST, S3 compatible, and WebDAV APIs

With the REST and S3 compatible APIs, users and applications can add, view, and delete objects and modify object metadata through a RESTful API. With the WebDAV API, users and applications can perform these activities through familiar directory structures.

REST, S3 compatible, and WebDav API configuration

You use the HTTP(S) panel to enable and configure the REST, S3 compatible, and WebDAV APIs for a namespace. To display this panel, on the left side of the Protocols panel, click HTTP(S).

Although you use a single panel to enable these protocols, you enable or disable them independently of each other.

Before you can enable the S3 compatible API for a namespace, ACLs must be enabled for the namespace.

The top of the HTTP(S) panel shows the URL for access to the namespace through the REST API. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with https. If only the HTTP port is open, the URL starts with http.

Note: Certain countries prohibit the export of encryption technology. HCP systems shipped to restricted countries have the HTTPS option on the namespace protocols page disabled. If you do not see the checkbox to enable HTTPS and you are in a country where SSL encryption is permitted, please contact your HCP system administrator.

The HTTP(S) panel lets you:

- Enable the REST API.
- Enable the S3 compatible API.
- Enable the WebDAV API.
- Specify whether the REST, S3 compatible, and WebDAV APIs require the use of SSL security.
- Specify whether the REST, S3 compatible APIs require user authentication for access to the namespace.
- If the tenant supports user authentication with Active Directory, specify whether HCP supports AD single sign-on for REST and S3 compatible APIs access to the namespace. This affects the Namespace Browser, HCP Search Console, and other HTTP-based applications that support Integrated Windows authentication.
- Specify whether the WebDAV API requires basic authentication for access to the namespace.

- If WebDAV basic authentication is enabled, specify the username and password against which HCP authenticates WebDAV access to the namespace.

  The username and password you specify for WebDAV basic authentication has no relationship to HCP or AD user accounts.

  Tip: Be sure to give WebDAV users the specified username and password.
- Specify whether WebDAV dead properties can be stored as custom metadata. If they can be, they are stored in the annotation named default.
- Specify the client IP addresses that have access to the namespace through the REST, S3 compatible, and WebDAV APIs.

By default, when a namespace is first created, the REST API is enabled with authentication required. If the HCP system supports the use of SSL for data access, the REST API also requires the use of SSL security by default.

Considerations for the S3 compatible API

The following considerations apply to using the S3 compatible API:

- You can enable the S3 compatible API for a namespace only while ACLs are enabled for the namespace.
- For users and applications to be able to perform most bucket-level operations with the S3 compatible API, the HCP management API must be enabled for the tenant.
- For a user or application to be able to create and manage namespaces with the S3 compatible API, the applicable user or group account must have the allow namespace management property enabled.
- Only cloud-optimized namespaces support the use of multipart uploads with the S3 compatible API.

Enabling REST, S3 compatible, and WebDAV access to a namespace

The HTTP(S) panel has two sections for enabling and configuring the REST, S3 compatible, and WebDAV APIs. This procedure is for the Settings section.

Note: REST and WebDAV are not supported on the namespaces that are configured to use S3 Object Lock.

1. Take either or both of these actions:
   - To open the HTTPS port for REST, S3 compatible, and WebDAV access to the namespace with SSL security, select Enable HTTPS.

     Certain countries prohibit the export of encryption technology. HCP systems shipped to restricted countries have the HTTPS option on the namespace protocols page disabled. If you do not see the checkbox to enable HTTPS and you are in a country where SSL encryption is permitted, please contact your HCP system administrator.

   - To open the HTTP port for REST, S3 compatible, and WebDAV access to the namespace without SSL security, select Enable HTTP.

   These two options are independent of each other. If you select only Enable HTTPS, data sent through the REST, S3 compatible, and WebDAV APIs is always secure. If you select both options, users and applications can send both secure and unsecure data through the REST, S3 compatible, and WebDAV APIs.
   Note: To enable access to the namespace through the REST, S3 compatible, or WebDAV API, you also need to select Enable REST API, Enable Hitachi API for Amazon S3, or Enable WebDAV API, respectively. Opening the HTTPS and HTTP ports does by itself enable these protocols.
2. Enable the REST API.
   a. Select Enable REST API.
   This option is available only if Enable HTTP or Enable HTTPS is already selected.

   Above the Enable REST API option, the panel shows the URL for access to the namespace through the REST API. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with https. If only the HTTP port is open, the URL starts with http.

   b. To specify REST authentication requirements, below the Enable REST API option, select either Authenticated access only or Anonymous and authenticated access.
   c. (Optional) Select or deselect Enable Active Directory single sign-on to allow or disallow, respectively, single sign-on to the namespace with Active Directory authentication.
   This option appears only if the tenant supports AD for user authentication.

   The option to enable AD single sign-on for REST is synchronized with the same option for the S3 compatible API. Enabling or disabling either enables of disables the other, respectively.

   To help ensure that AD single sign-on is available for those namespaces that need it, enable it only for those namespaces.

   After this option is disabled, you can reenable it only while HCP can communicate with AD.

3. Enable the S3 compatible API.
   a. Select Enable Hitachi API for Amazon S3.
   This option is available only if Enable HTTP or Enable HTTPS is already selected.

   Above the Enable Hitachi API for Amazon S3 option, the panel shows the URL for access to the namespace through the S3 compatible API. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with https. If only the HTTP port is open, the URL starts with http.

   b. To specify S3 compatible authentication requirements, below the Enable Hitachi API for Amazon S3 option, select either Authenticated access only or Anonymous and authenticated access.
   c. Optionally, select or deselect Enable Active Directory single sign-on to allow or disallow, respectively, single sign-on to the namespace with Active Directory authentication.
   This option appears only if the tenant supports AD for user authentication.
4. Enable the WebDAV API.
   a. Select Enable WebDAV API.
   This option is available only if Enable HTTP or Enable HTTPS is already selected.

   Above the Enable WebDAV API option, the panel shows the URL for access to the namespace through the WebDAV API. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with https. If only the HTTP port is open, the URL starts with http.

   b. Select Enable WebDAV basic authentication.
   c. In the Username field, type the user name to use for basic authentication.
   User names must 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. User names are not case sensitive.
   d. In the Password field, type the password to use for basic authentication.
   Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters, including white space. The minimum password length is the same as the minimum password length for HCP user accounts, which is configurable. To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

   If you’re modifying settings in the HTTP(S) panel and you leave the Password field empty, the previously set password remains in effect.

   e. In the Confirm Password field, type the password again.

Tip: Be sure to tell WebDAV users the username and password you specify.

f. (Optional) Enable WebDAV users to store dead properties as custom metadata by selecting Use custom metadata to store WebDAV properties.

5. Click Update Settings.
   If you selected Enable HTTP and also selected Enable REST API, Enable Hitachi API for Amazon S3, or Enable WebDAV API, a confirming message appears.
6. Click Update Settings.

Set the IP addresses to be allowed or denied access

The HTTP(S) panel has two sections for enabling and configuring the REST, S3 compatible, and WebDAV APIs. This procedure is for the Allow/Deny section.

- Optionally, in the Allow/Deny section, specify IP addresses to be allowed or denied access to the namespace through the REST, S3 compatible, and WebDAV APIs.
- 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. Changes to this option take effect immediately.

Configuring the CIFS protocol

With the CIFS protocol, users and applications can add, view, and delete objects and modify object metadata through familiar directory structures.

CIFS protocol configuration

You use the CIFS panel to enable and configure the CIFS protocol for a namespace. To display this panel, on the left side of the Protocols panel, click CIFS.

The top of the CIFS panel shows the string to use to identify the namespace when mapping it to a network drive or adding it as a network place on a CIFS client.

The CIFS panel lets you:

- Enable the CIFS protocol.
- Specify whether the CIFS protocol requires user authentication for access to the namespace. HCP uses Active Directory to authenticate CIFS users. This authentication is possible only if the tenant is configured to support AD authentication.
  Note: If the HCP system does not support Active Directory and CIFS is enabled for the namespace, the namespace is exposed as a share in the Windows workgroup specified in the HCP system configuration. However, if the CIFS protocol is configured to require authentication, the namespace cannot be accessed through the workgroup.
- Specify the client IP addresses that have access to the namespace through CIFS.
- Change CIFS case sensitivity

When you reconfigure the CIFS protocol while it’s already enabled, the changes you make don’t affect current CIFS mounts of the namespace. To force the changes to take effect, you can take either of these actions:

- Disable and then reenable the protocol. This causes all CIFS clients to lose their connections to the namespace. When they reconnect, the changes will be in effect.
- Direct all clients with current CIFS mounts to disconnect from the namespace and then to either reboot or wait five minutes for cached connections to be released before reconnecting.

CIFS case sensitivity

The Windows operating system is case preserving but not case sensitive. The HCP CIFS implementation, by default, is both case preserving and case sensitive. One result of this discrepancy is that Windows applications that do not observe differences in case may not be able to access HCP objects by name.

For example, suppose a Windows application adds a file named File.txt to the namespace by using the CIFS protocol. CIFS preserves case, so the namespace then contains an object named File.txt. Now suppose the application tries to retrieve that object using the name file.txt. CIFS is case sensitive, so it passes the request to HCP with only the name file.txt. It doesn’t include any case variations on the name, such as File.TXT, FILE.txt, or File.txt. As a result, HCP cannot find the object.

If you have Windows applications that ignore case, you may want HCP to ignore case as well. You can change the CIFS protocol configuration in either of two ways to meet this need:

Make CIFS case forcing
: With this behavior, CIFS changes names to all upper- or lowercase in the requests it passes to HCP. To Windows applications, then, HCP appears to be case-insensitive. An application that stores File.txt and then retrieves File.TXT will get the right object back.
  The drawback to this method is that applications using other namespace access protocols must accommodate this behavior. For example, suppose CIFS changes names to all uppercase. If an application using the CIFS protocol stores an object named File.txt, applications using the case-sensitive HTTP, WebDAV, and NFS protocols need to retrieve the object as FILE.TXT.

Make CIFS case insensitive
: With this behavior, CIFS preserves case as objects are stored in the namespace but passes through every case variation possible when applications make other requests for objects.
  For example, suppose an application using the CIFS protocol requests an object named FILE.txt. CIFS passes the request through with the names File.txt, FILE.txt, fiLe.TXT, and so on. HCP then returns the first object it finds with a name that matches any of these.
  The major drawback to this method is that performance is slowed by the need to check for matches to multiple case variations. A second drawback is that if the namespace contains multiple objects with names that vary only in case, HCP may return the wrong object.

If you make CIFS both case forcing and case insensitive, it is case forcing when storing objects and case insensitive on requests for existing objects.

Enabling CIFS access to a namespace

The CIFS panel has three sections for enabling and configuring the CIFS protocol.

Settings section

1. Select Enable CIFS.
2. To specify CIFS authentication requirements, select either Authenticated access only or Anonymous and authenticated access.
3. Click Update Settings in the Settings section.

Allow/Deny section

Optionally, in the Allow/Deny section, specify IP addresses to be allowed or denied access to the namespace through CIFS.

CIFS case sensitivity

The Windows operating system is case preserving but not case sensitive. The HCP CIFS implementation, by default, is both case preserving and case sensitive. One result of this discrepancy is that Windows applications that do not observe differences in case may not be able to access HCP objects by name.

For example, suppose a Windows application adds a file named File.txt to the namespace by using the CIFS protocol. CIFS preserves case, so the namespace then contains an object named File.txt. Now suppose the application tries to retrieve that object using the name file.txt. CIFS is case sensitive, so it passes the request to HCP with only the name file.txt. It doesn't include any case variations on the name, such as File.TXT, FILE.txt, or File.txt. As a result, HCP cannot find the object.

If you have Windows applications that ignore case, you may want HCP to ignore case as well. You can change the CIFS protocol configuration in either of two ways to meet this need:

Make CIFS case forcing
: With this behavior, CIFS changes names to all upper- or lowercase in the requests it passes to HCP. To Windows applications, then, HCP appears to be case-insensitive. An application that stores File.txt and then retrieves File.TXT will get the right object back.
The drawback to this method is that applications using other namespace access protocols must accommodate this behavior. For example, suppose CIFS changes names to all uppercase. If an application using the CIFS protocol stores an object named File.txt, applications using the case-sensitive HTTP, WebDAV, and NFS protocols need to retrieve the object as FILE.TXT.

Make CIFS case insensitive
: With this behavior, CIFS preserves case as objects are stored in the namespace but passes through every case variation possible when applications make other requests for objects.
For example, suppose an application using the CIFS protocol requests an object named FILE.txt. CIFS passes the request through with the names File.txt, FILE.txt, fiLe.TXT, and so on. HCP then returns the first object it finds with a name that matches any of these.
The major drawback to this method is that performance is slowed by the need to check for matches to multiple case variations. A second drawback is that if the namespace contains multiple objects with names that vary only in case, HCP may return the wrong object.

If you make CIFS both case forcing and case insensitive, it is case forcing when storing objects and case insensitive on requests for existing objects.

Configuring the NFS protocol

With the NFS protocol, users and applications can add, view, and delete objects and modify object metadata through familiar directory structures.

NFS protocol configuration

You use the NFS panel to enable and configure the NFS protocol for a namespace. To display this panel, on the left side of the Protocols panel, click NFS.

The top of the NFS panel shows the string to use to identify the namespace when mounting it on an NFS client.

The NFS panel lets you:

- Enable the NFS protocol.
- Specify default values for POSIX UIDs and GIDs.
- Specify the client IP addresses that have access to the namespace through NFS.

Enabling NFS access to a namespace

The NFS panel has two sections for enabling and configuring the NFS protocol.

Settings section

1. Select Enable NFS.
2. (Optional) In the UID field, type a different UID to be displayed for objects that don't have an explicit POSIX UID.
   Valid values are integers greater than or equal to zero.
3. (Optional) In the GID field, type a different GID to be displayed for objects that don't have an explicit POSIX GID.
   Valid values are integers greater than or equal to zero.
4. Click Update Settings.

Allowed IP Addresses section

To set the IP addresses to be allowed access to the namespace through NFS, optionally, specify IP addresses in the Allowed IP Addresses section.

Configuring the SMTP protocol

With the SMTP protocol, HCP can automatically archive emails forwarded by email servers.

SMTP protocol configuration

HCP provides SMTP support for Microsoft® Exchange email servers. For information about which Microsoft Exchange email servers are qualified for use with the SMTP protocol, check the HCP release notes for the version of HCP that you have installed.

You use the SMTP panel to enable and configure the SMTP protocol for a namespace. To display this panel, on the left side of the Protocols page, click SMTP.

The top of the SMTP panel shows the string to use to identify the namespace when configuring Microsoft Exchange to archive email to the namespace.

The SMTP panel lets you:

- Enable the SMTP protocol
- Specify the email server IP addresses that have access to the namespace through SMTP
- Specify where and in what format email objects are stored
- Specify whether to store email attachments separately

The SMTP protocol always stores attachments along with the email they accompany. The metadata query engine index the attachments along with the email.

You can choose to additionally store attachments separately from the email they accompany. With this option, searches return not only the original email with the attachments but also the attachments as separate objects.

When attachments are stored only with the email they accompany, searches return only the email objects. You then need to retrieve the email objects and separate the attachments yourself.

Storing attachments as separate objects can have a significant impact on performance and storage space.

Enabling SMTP access to a namespace

The SMTP panel has three sections for enabling and configuring the SMTP protocol.

Settings section

1. Select Enable SMTP.
2. Click Update Settings in the Settings section.

Allow/Deny section

Optionally, in the Allow/Deny section, specify IP addresses of email servers to be allowed or denied access to the namespace through SMTP.

Emails section

1. Click Emails.
2. In the Email Location field, type the path for the directory in which you want email objects stored.
   This is the full path starting after the root directory (that is, rest or data). Be sure to start and end the path with a forward slash (/), like this:

   ```
   /email/company_all/
   ```

   If any part of the specified directory path doesn't exist, HCP creates it.
3. In the Format field, select either .eml or .mbox.
   The one you choose depends on the application you use to read the stored email.
4. To store email attachments separately from the emails they're attached to, select Separate attachments from parent email.
   Important: Storing attachments separately from the email they accompany can have a significant impact on performance and storage space. Unless you have a specific reason to do so, do not enable this option.
5. Click Update Settings in the Emails section.

Changing the default settings for namespace creation

When you open the Create Namespace panel to create a namespace, the panel shows default settings for many of the namespace properties. You can change the defaults for these settings at any time. Changing the default settings for namespace creation has no effect on existing namespaces.

- To view the default settings for namespace creation, you need the monitor or administrator role.
- To change the default settings for namespace creation, you need the administrator role.

1. In the top-level menu of the Tenant Management Console, select Configuration > Namespace Defaults.
2. (Optional) In the Description field, type a new description.
   The description can be up through 1,024 characters long and can contain any valid UTF-8 characters, including white space. By default, this field is blank.
3. (Optional) In the Hash Algorithm field, select a different cryptographic hash algorithm.
   The default is SHA-256.
4. (Optional) In the Hard Quota field, type a new number of gigabytes or terabytes of storage to allocate to the namespace and select either GB or TB to indicate the measurement unit.
   The default is 50 GB. The maximum value you can specify is equal to the hard quota for the tenant.
5. (Optional) In the Soft Quota field, type a new percent at which you want HCP to notify the tenant that free storage space for the namespace is running low.
   The default is 85.
6. (Optional) Under Replication, change the selection.
   The default is Off. The Replication option is present only if the tenant is allowed to create namespaces with replication enabled.
7. (Optional) If you selected On for replication, select Allow erasure coding to allow HCP to use erasure coding to implement replication of the objects in the namespace.
   The Allow erasure coding option is present only if the tenant can manage erasure coding for namespaces.
   When you select Allow erasure coding, if the Cloud Optimized setting is currently set to Off, the setting automatically changes to On.
8. Under Cloud Optimized:
   - Select On to optimize the namespace for cloud protocols only.
   - Select Off to optimize the namespace for all protocols.

     When you select Off while Allow erasure coding is selected, that option is automatically deselected.

   - Select System default to use the system-level default protocol optimization setting that's current when you create a namespace.

   The Cloud Optimized option is present only if the tenant is allowed to create namespaces with replication enabled.
9. Under Directory usage:
   - Select Balanced to configure the namespace for balanced directory usage.
   - Select Unbalanced to configure the namespace for unstructured data usage. It is applicable only for cloud-optimized namespaces.
   - Select System default to use the system-level default directory usage setting that's current when you create a namespace.
10. Under HCP Retention Type, change the selection.
    - Select S3 Object Lock to configure the namespace for S3 Object Lock. If you choose S3 Object Lock, versioning, delete markers, and cloud-optimized protocols must be enabled.
    - Select HCP Retention to configure the namespace for HCP Retention.
11. (Optional) Under HCP Retention Mode, change the selection.
    - Select Enterprise to configure the namespace for enterprise mode The default is enterprise mode.
    - Select Compliance to configure the namespace for compliance mode.

    Note: This option is visible only if you have selected HCP Retention. The HCP Retention Mode option is present only if the tenant is allowed to create namespaces in compliance mode.
12. (Optional) Under Search, change the selection.
    The default is Off. The Search option is present only if the tenant is allows to create namespaces with search enabled.
13. (Optional) In the Service Plan field, type the name of or select a different service plan.
    The default is the Default service plan. The Service Plan field is present only if the tenant is allowed to associate service plans with namespaces.
14. (Optional) Under Versioning, change the selection.
    The default is Off. The Versioning option and the pruning options below are present only if the tenant is allowed to create namespaces with versioning enabled.
15. (Optional) Change the selection for the Prune versions older than ... days option.
    By default, this option is unselected. If you select this option, in the option field, type the number of days old versions of objects must remain in the namespace before they are pruned. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means prune immediately.
16. Click Update Settings.
    If the version pruning option is unselected, a confirming message appears.
17. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.

18. Click Update Settings.

Setting the maximum number of namespaces per user

You can limit the number of namespaces that can be owned by a single user. By default, this limit is 100. You can change the limit at any time.

Changing this limit does not affect current namespace ownership. For example, if a user owns seven namespaces and you change the limit to five, that user still owns those seven namespaces even though that exceeds the new limit. However, the user cannot own any additional namespaces, and if namespaces are taken away from the user, the limit of five applies.

- To view the limit on namespace ownership, you need the monitor or administrator role.
- To change the limit on namespace ownership, you need the administrator role.

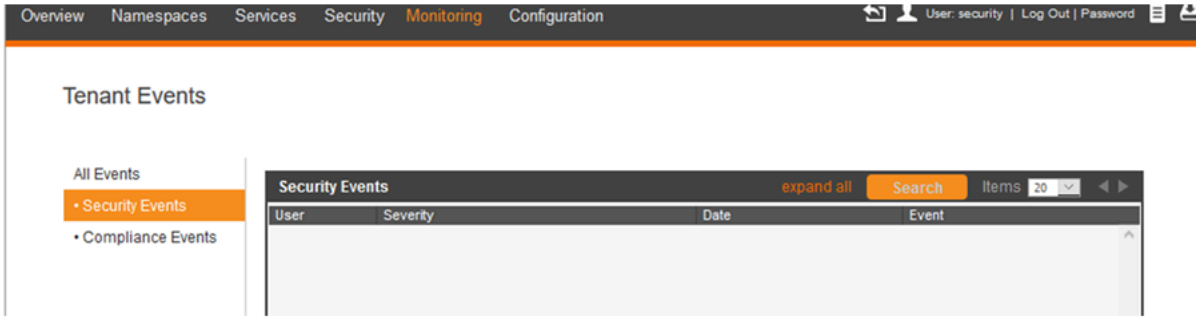
1. In the top-level menu of the Tenant Management Console, select Configuration > Miscellaneous.
2. In the Maximum Number of Namespaces per User field, type the new limit.
   Valid values are integers in the range zero through 10,000.
3. Click Update Settings.

Monitoring a namespace

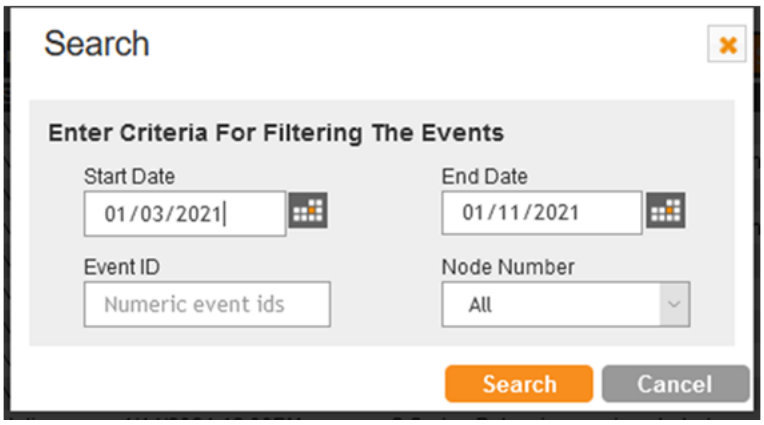
While the namespace Overview panel in the Tenant Management Console gives you a view of a namespace as a whole, these namespace views of the tenant log let you monitor namespace activity on a more detailed level:

- The namespace-level all-events view shows all log messages for a given namespace.
- The namespace-level compliance view shows all log messages about events that require the compliance role for a given namespace.

Although unlikely, if HCP finds a broken object it cannot repair, it reports the event in the tenant log. In the Tenant Management Console, you can see a list of the irreparable, unavailable, and nonreplicating objects in any given namespace.



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.

Viewing the complete namespace event log

The namespace All Events panel lists all namespace-specific log messages. By default, the panel displays ten messages at a time in reverse chronological order.

To view the namespace All Events panel, you need the monitor, administrator, or compliance role. However, only users with the compliance role can see messages about events that require the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click All Events.

Viewing the namespace compliance log

The namespace Compliance Events panel lists all namespace-specific log messages about events that require the compliance role. This includes all retention class activity and privileged delete operations. By default, the panel displays ten messages at a time in reverse chronological order.

To view the namespace Compliance panel, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click Compliance Events.

Working with unavailable objects

HCP keeps track of objects that are unavailable. You can view a list of these objects for any given namespace in the Tenant Management Console.

To view the Unavailable Objects panel, you need the monitor or administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click Unavailable Objects.
   For each object it lists, the Unavailable Objects panel shows the date that the HCP system discovered the unavailable object, the name of the object, and the reason why it is unavailable.

   If an object subsequently becomes available again, the object is removed from the list.

   By default, the objects in the Unavailable Objects panel are listed ten at a time in reverse chronological order by discovery time:

   - To view a different number of objects, select the number of objects you want in the Items per page field. The options are 10, 20, 50, and 100.
   - To page forward or backward, click the next ( ) or back ( ) control, respectively.

Working with irretrievable objects

HCP keeps track of objects that are irretrievable. You can view these objects for any given namespace in the Tenant Management Console.

Displaying irretrievable objects

The HCP system keeps track of the irretrievable objects it finds. You can view a list of these objects for any given namespace in the Tenant Management Console.

To view the Irretrievable Objects in the events panel, you need the monitor or administrator role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click All Events.

About irretrievable objects

The HCP system classifies an object as irretrievable when it encounters issues with accessing the object on primary storage and cannot access any other copies available in alternative storage locations.

In the All Events panel, each irretrievable object displays its full path and the date and time at which HCP discovered that the object was irretrievable. If versioning has been enabled for the namespace, the list also displays the version ID of each object. An object listed as irretrievable is not replicated. If HCP subsequently repairs a listed object, the object is removed from the list.

You can delete irretrievable objects from a namespace using standard delete operations, provided they are not under retention (or via privileged delete if the objects are under retention). When an object is deleted, HCP removes it from the irretrievable object list.

- To view a different number of objects, select the number of objects you want in the Items per page field. The options are 10, 20, 50, and 100.
- To page forward or backward, click the next ( ) or back ( ) control, respectively.

Working with irreparable objects

To view the Irreparable Objects panel, you need the monitor or administrator role. To acknowledge irreparable objects, you need the administrator role.

Displaying irreparable objects

The HCP system keeps track of the irreparable objects it finds. You can view a list of these objects for any given namespace in the Tenant Management Console.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click Irreparable Objects.

About irreparable objects

For each object it lists, the Irreparable Objects panel shows the full path to the object (starting after `rest` or `data`) and the date and time at which HCP discovered that the object was irreparable. If the namespace has ever had versioning enabled, the list also shows the version ID of each object.

If HCP subsequently repairs a listed object, the object is removed from the list.

You can acknowledge irreparable objects in the Irreparable Objects panel. Acknowledging an object leaves a checkmark in the object row. You can use this option to distinguish objects you've already seen from objects that have recently become irreparable.

You can delete irreparable objects from a namespace through normal delete operations as long as the objects are not under retention (or by using privileged delete if the objects are under retention). When you delete an object, HCP removes it from the list of irreparable objects.

Note: Acknowledging that an object is irreparable does not delete the object from the namespace.

By default, the objects in the Irreparable Objects panel are listed ten at a time in reverse chronological order by discovery time:

- To view a different number of objects, select the number of objects you want in the Items per page field. The options are 10, 20, 50, and 100.
- To page forward or backward, click the next ( ) or back ( ) control, respectively.

Acknowledge irreparable objects

To acknowledge all objects, whether selected or not, on all pages in a single operation, click Acknowledge All.

1. In the Irreparable Objects panel, individually select the objects you want to acknowledge, or click select all to select all the unacknowledged objects on the current page.
2. Click Acknowledge Selected.

Working with nonreplicating objects

To view the Nonreplicating Objects panel, you need the monitor or administrator role.

Displaying nonreplicating objects

HCP keeps track of objects and parts of multipart objects that cannot be replicated. You can view a list of these objects and object parts for any given namespace in the Tenant Management Console.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Monitoring.
4. On the left side of the Monitoring panel, click Nonreplicating Objects.

About nonreplicating objects

For each listed object or object part, the Nonreplicating Objects panel shows the date and time when HCP discovered the nonreplicating object or object part, the version number of the object or object part, the reason why the object or object part was not replicated, and the name of the object or object part.

The possible reasons why an object or object part is nonreplicating are:

Object is not completely written
: The object or object part is nonreplicating because the write operation used to create the object was never completed.

Object is temporarily nonreplicating
: The object or object part is nonreplicating, but the situation that's causing it to be nonreplicating is most likely temporary. This state is typically due to a system-level issue such as a node becoming unavailable. HCP usually resolves these issues on its own within 24 to 48 hours. If the object or object part remains in this state for more than 48 hours, contact your HCP system administrator.

Object is unavailable or irreparable
: The object or object part is nonreplicating because it is unavailable or irreparable.

If HCP subsequently replicates a listed object or object part, the object or object part is removed from the list.

By default, the objects and object parts in the Nonreplicating Objects panel are listed ten at a time in reverse chronological order by discovery time:

- To view a different number of objects, select the number of objects you want in the Items per page field. The options are 10, 20, 50, and 100.
- To page forward or backward, click the next ( ) or back ( ) control, respectively.

Deleting a namespace

You can delete a namespace that does not contain any objects.

If a namespace is being replicated, you may not be able to delete it directly on all the HCP systems in the replication topology. However, if you delete it on one system, the deletion is replicated to the other systems.

Important: If the namespace you want to delete is being replicated, do not clear it from replication before deleting it. If you clear it first, the deletion is not replicated and the namespace remains on the other systems where it was replicated. Depending on the replication topology, you may not be able to delete the namespace on one or more of those other systems.

When a namespace is deleted, the chargeback statistics for it become unavailable. Therefore, before deleting a namespace for which you need these statistics, generate a chargeback report.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the delete control ( ) for the namespace you want to delete.
3. In response to the confirming message, click Delete.
   Important: Removing a tenant from an Active-Passive replication link on the Active site followed by its deletion from the Passive site can result in lost data if, in the future, an Active/Active replication link is created between the same clusters and the same tenant is added to that link.

Managing search and indexing

You manage search and indexing for namespaces at both the tenant and namespace level. At the tenant level, you create content classes and content properties. At the namespace level, you enable search and indexing options.

The discussion of content properties in this chapter assumes a basic understanding of XML.

Search and indexing

For a namespace to be searchable through either the metadata query API or the Search Console, it must be search enabled, and its effective permission mask must include the read and search permissions. Additionally, to get results from object-based queries through the metadata query API and from searches through the Search Console with any search facility, the namespace must be indexed by the applicable search facility.

You can enable search for your namespaces only if allowed to do so by the tenant configuration. HCP system-level administrators can change this configuration from not allowing you to enable search to allowing it. However, they cannot do the reverse.

Metadata query engine and HCP search facility indexing

The metadata query engine and the HCP search facility index each namespace that has both search and indexing enabled. When you first enable search for a namespace, indexing is enabled by default.

The metadata query engine index is based on system metadata, ACLs, and, optionally, custom metadata that is well-formed XML. The HCP search facility index is based on object data, system metadata, and, optionally, custom metadata.

You can enable or disable indexing for a namespace at any time while search is enabled for the namespace. Disabling indexing for a namespace prevents the metadata query engine and HCP search facility from updating their indexes with new objects and metadata changes in that namespace. When indexing is reenabled, these facilities update their indexes with the backlogged objects and changes and continue indexing from there.

You can enable or disable indexing of custom metadata for a namespace at any time while indexing is enabled for the namespace. Because indexing custom metadata can significantly increase the size of the indexes, you should enable it only if users need to perform searches based on custom metadata.

Indexing can be disabled for the metadata query engine or HCP search facility at the HCP system level. If this indexing is disabled at the system level, enabling it at the namespace level has no effect.

Similarly, custom metadata indexing can be disabled for the metadata query engine or HCP search facility at the HCP system level. If this indexing is disabled at the system level, enabling it at the namespace level has no effect.

You can reduce the amount of custom metadata the metadata query engine indexes by creating content properties. Content properties not only decrease the size of the index but also enable users to query for objects more easily and intuitively.

You can also reduce the size of the metadata query engine index by excluding selected custom metadata annotations from being indexed.

Content properties and annotation exclusions affect only metadata query engine indexing.

When indexing custom metadata, the HCP search facility indexes only annotations named default.

Disabling search

You can disable and reenable search for a namespace at any time. When you disable search, indexing is automatically disabled for all three search facilities.

Disabling search also removes objects in the namespace from the metadata query engine and HCP search facility indexes. If you subsequently reenable search for the namespace, the namespace must be completely reindexed. The amount of time required to rebuild the indexes depends on the amount of data in the namespace. With a very large amount of data, this process can take several days.

Content classes and content properties

A *content class* is a named construct that is used to characterize objects in one or more namespaces. Content classes use object metadata to impose structure on unstructured namespace content. They do this through content properties.

A *content property* is a named construct used to extract an element or attribute value from custom metadata that's well-formed XML. Content properties use XPath expressions to identify the metadata of interest. When content properties are indexed, users can use them to find unstructured content that matches structured patterns.

For example, consider the following XML structure that could occur in the custom metadata for multiple objects in a namespace that contains medical data:

```
<doctor>
    <name>doctor-name</name>
</doctor>
<patient>
    <name>patient-name</name>
</patient>
```

The information of interest in this custom metadata consists of the doctor’s name and the patient’s name.

Based on the metadata structure above, you could create content properties named Doctor_Name and Patient_Name that extract the doctor’s name and patient’s name from the custom metadata XML for each object. The metadata query engine could then index objects with this metadata structure by those property values. Using the metadata query API or the Metadata Query Engine Console, users could query for objects that have Doctor_Name or Patient_Name equal to a specific value.

Content properties belong to content classes. Both content classes and content properties are defined at the tenant level. Content classes are optionally associated with namespaces. Through this association, content properties are associated with namespaces.

Metadata query engine indexing of custom metadata

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 content properties (that is, it’s not associated with any content classes that have content properties), no custom metadata is indexed.

You can choose to have the metadata query engine index the full text of custom metadata. If you enable this option, the metadata query engine indexes both content properties, if any exist, and the full text of custom metadata.

With content properties, the metadata query engine indexes only the values that you determine are of interest. When indexing the full text of custom metadata, the metadata query engine indexes each word individually.

For example, suppose an object has this XML in its custom metadata:

```
<doctor>
    <name>Lee Green</name>
</doctor>
<patient>
    <name>Paris Black</name>
</patient>
```

If you’ve defined the Doctor_Name and Patient_Name properties, the metadata query engine index includes:

```
Lee Green
Paris Black
```

If full text indexing is enabled, the metadata query engine index includes:

```
doctor name Lee Green name doctor patient name Paris Black name patient
```

In this case, to use the metadata query API to find the objects that have a doctor named Lee Green, users would need to query for custom metadata containing “doctor.name.Lee Green.name.doctor”. This kind of query can become very complex when elements are nested to deeper levels or when they have attributes.

Content class and content property workflow

Here’s the basic procedure for working with content classes and content properties:

1. Create one or more content classes for the tenant. Give each class a meaningful name. For example, if a class will contain object properties that pertain to medical images, you could name it DICOM. (DICOM is a standard for managing medical images.)

   A tenant can have at most 25 content classes.

2. Create content properties for each content class. Create only the content properties that will be useful to metadata query API and Search Console users. Creating content properties that won’t be used unnecessarily increases the size of the metadata query engine index.

   A content class can have at most 100 content properties.

3. If custom metadata indexing isn’t already enabled for the namespaces you plan to associate with the content classes, enable it.
4. Associate namespaces with the applicable content classes. For clarity, associate a namespace with a content class only if the namespace contains objects that can be characterized by the content properties in the content class.

   You can associate any number of namespaces with a content class. Additionally, a namespace can be associated with any number of content classes.

5. Optionally, reindex some or all of the namespaces associated with the content classes. You would reindex a namespace if you want objects that were already in the namespace to be indexed by the new content properties.

   You can reindex namespaces starting from the time they were created or starting from a specific date. When reindexing a namespace, the metadata query engine reindexes all objects with a change time that’s equal to or later than the time you specify.

Tip: Because reindexing can take a long time, before reindexing a namespace:

- Create all the content properties you want for the namespace
- Associate all the content classes containing those properties with the namespace

Content property definitions

The definition of a content property consists of:

- A name for the property.
- The XPath expression that identifies the property values.
- The data type of the property values.
- For numeric and datetime data types, the format of the property values.
- An indication of whether the property is single-valued or multivalued. A multivalued property can have multiple values for any given object.
- The examples of content property definitions in the following sections are based on this sample custom metadata XML:

```
<?xml version="1.0" ?>
<dicom_image>
    <image type="MRI">
        <date>09/27/2012</date>
        <technician>Morgan Grey</technician>
    </image>
    <doctor>
        <name>Lee Green</name>
        <office>ABC Oncology</office>
        <address>
            <address1>Anytown Medical Building</address1>
            <address2>1 Main Street</address2>
            <city>Anytown</city>
            <state>MA</state>
            <zip>02000</zip>
        </address>
        <specialties>
            <specialty primary="true">Oncology</specialty>
            <specialty>Internal Medicine</specialty>
        </specialties>
    </doctor>
    <patient>
        <id>243789</id>
        <name>Paris Black</name>
        <address>
            <address1>10 Elm Street</address1>
            <address2/>
            <city>Anytown</city>
            <state>MA</state>
            <zip>02000</zip>
       </address>
    </patient>
    <followup_needed>true</followup_needed>
</dicom_image>
```

Content property names

When you define a content property, you specify a name for it. Content property names must be from one through 25 characters long, can contain only alphanumeric characters and underscores (_), and are case sensitive. White space is not allowed.

Content property names should be intuitive for users of the metadata query API and Metadata Query Engine Console. For example, for the property that extracts the name of the doctor from the sample custom metadata, you should use a name like Doctor_Name rather than a name like dname.

Content properties with the same name

You can use the same name for multiple content properties as long as those properties have the same data type. For example, suppose the custom metadata for some objects includes a physician element instead of a doctor element, like this:

```
<physician>
        <name>Lee Green</name>
         <office>ABC Oncology</office>
        <address>
             <address1>Anytown Medical Building</address1>
             <address2>1 Main Street</address2>
            <city>Anytown</city>
            <state>MA</state>
             <zip>02000</zip>
        </address>
        <specialties>
            <specialty primary="true">Oncology</specialty>
            <specialty>Internal Medicine</specialty>
        </specialties>
    </physician>
```

You could define two content properties named Doctor_Name, one with an XPath expression that includes the `doctor` element, the other with an XPath expression that includes the `physician` element.

Within a content class, content properties with the same name must have the same data type.

Reserved words

The following words are reserved and cannot be used as content property names:

- accessTime
- accessTimeString
- acl
- changeTimeMilliseconds
- changeTimeString
- customMetadata
- customMetadataAnnotation
- dpl
- gid
- hash
- hashScheme
- hold
- index
- ingestTime
- ingestTimeString
- namespace
- objectPath
- operation
- owner
- permission
- replicated
- retention
- retentionClass
- retentionString
- shred
- size
- type
- uid
- urlName
- updateTime
- updateTimeString
- utf8Name
- version

Content property expressions

For each content property you create, you specify an XPath expression. An XPath expression is an instruction for navigating an XML document to find an element or attribute value.

XPath expressions use the XPath language. HCP supports the full syntax of this language. The examples in this section illustrate only a small part of the XPath syntax.

XPath expressions that find element values

Here's a simple XPath expression that finds the value of the `followup_needed` element:

```
/dicom_image/followup_needed
```

The forward slash (/) at the beginning of the expression means that the first element is the root element in the XML. The element after the second forward slash is a child of the root element.

Here's another simple XPath expression:

```
//name
```

This expression is probably not very useful. The double slash at the beginning means find the value of any `name` element, regardless of whether that element is a child of the `doctor` element or the `patient` element.

A more useful XPath expression specifies a path to the `name` element:

```
/dicom_image/doctor/name
```

This expression means start at the root element, find the `doctor` element that's the child of the root element, and then find the `name` element that's the child of the `doctor` element. A content property with this expression finds only the name of the doctor, not the name of the patient.

A different content property with this Xpath expression finds only the patient's name:

```
/dicom_image/patient/name
```

The element path in an XPath expression can go deeper than the three levels shown above. Here's an XPath expression that's four levels deep and finds the city in which the doctor's office is located:

```
/dicom_image/doctor/address/city
```

XPath expressions that find attribute values

To find the value of an attribute, you include an at sign (@) followed by the attribute name at the end of the XPath expression. For example, here's an XPath expression that finds the value of the type attribute of the image element:

```
/dicom_image/image@type
```

Complex XPath expressions

XPath expressions can be much more complex than the ones shown so far. For example, an XPath expression can navigate XML based on the values of elements and attributes. Here's an expression that finds the name of a doctor whose primary specialty is oncology:

```
/dicom_image/doctor/specialties/specialty[@primary='true' and text()='Oncology']/
ancestor::doctor/name
```

This expression navigates down from the doctor element to the specialty elements and finds the one that has both a value of Oncology and a primary attribute with a value of true. The expression then navigates back up to the same doctor element and from there down to the name element that's the child of the doctor element.

Annotation-specific content properties

You can associate content properties with annotation names. When a content property is associated with an annotation name, the metadata query engine indexes the value of that property only when the value occurs in an annotation with the specified name.

To associate a content property with an annotation name, you specify the case-sensitive annotation name in front of the XPath expression for the property, in this format:

```
@annotation-name:xpath-expression
```

For example, suppose:

- The objects in a namespace can have either of two annotations — one named dicom, the other named appointment
- Both of these annotations have a `date` element
- Depending on who created the dicom annotation, the `date` element in it might be a child of the root element or a child of the `image` element

To find the value of the `date` element in the dicom annotation, you would need to use this XPath expression:

```
//date
```

This expression means find a `date` element that occurs anywhere in the XML. Without more context, it applies equally to the dicom and appointment annotations.

To have the content property with this XPath expression apply only to the dicom annotation, you would specify the expression this way:

```
@dicom://date
```

Content property data types

Each content property has a data type that determines how the property values are treated by the metadata query engine. The possible data types are:

String
: The metadata query engine indexes the value as a text string. The value is handled as a single unit, even if it contains white space. Users cannot base queries on individual terms within a string value.

Tokenized
: The metadata query engine indexes the value as a text string after breaking it into tokens. A token is a string of either alphabetic or numeric characters. For example, the value SSN12345789 becomes this string of two tokens: ssn 123456789. Tokens are not case sensitive.
The metadata query engine treats white space and special characters as token separators. For example, the value 12A Elm Street, apt. 2D becomes this string of seven tokens: 12 a elm street apt 2 d.
Users can base queries on any individual token or sequence of tokens within a tokenized string.

Boolean
: The metadata query engine indexes the value as true or false. Values that start with 1, t, or T are treated as true. Any other values are treated as false.

Integer
: The metadata query engine indexes the value as an integer. Users can base queries on comparative numeric values.
The metadata query engine indexes values for a content property with a data type of integer only if the values conform to the format for the property.

Float
: The metadata query engine indexes the value as a decimal number with or without an exponent, depending on the value. Users can base queries on comparative numeric values.
The metadata query engine indexes values for a content property with a data type of float only if the values conform to the format for the property.

Datetime
: The metadata query engine indexes the value as a date and time. Users can base queries on comparative datetime values.
The metadata query engine indexes values for a content property with a data type of date only if the values conform to the format for the property.

Format for the integer and float data types

For a content property with the integer or float data type, you can specify a format that values needs to match in order to be indexed. The following sections include basic information about these formats. You can find more information at:

```
http://docs.oracle.com/javase/6/docs/api/java/text/DecimalFormat.html
```

Integer data type formats

The basic format for a content property with the integer data type is:

```
optional-prefixnumber-patternoptional-suffix
```

A number pattern for the integer data type consists of any number of number signs (#), followed by any number of zeroes. Both number signs and zeroes represent any number of digits, including none. The metadata query engine does not consider the length of the number pattern when matching values.

A number pattern can include a thousands separator. With the integer data type, the metadata query engine recognizes either commas (,) or periods (,) as the thousands separator.

For example, a value of 1234 matches any of these number patterns:

```
0
000
##
###0000
0,0
##,000
```

If a content property value contains a thousands separator, the value matches only number patterns that contain the same thousands separator. For example, the value `1,234` matches the last two patterns above, but not the first four. It also does not match 0.0 or ##.000.

The prefix or suffix in the format for the integer data type can be any character string, with a few exceptions. For example, a prefix or suffix cannot include a period (.) or percent sign (%). The format must include white space between the integer pattern and the suffix, if used.

For example, for the metadata query engine to index the value `$1234` as an integer, the format for the content property must have a dollar sign ($) in front of the integer pattern, with no space between them.

Here are some examples of integer formats with examples of values that match them:

```
Format        Example
$ 0,0                 $ 1,234
###0 AD            2012 AD
~# mph                            ~55 mph
```

If you don't specify a format for a content property with the integer data type, the metadata query engine indexes only sequences of digits with no special characters.

Float data type formats

For the format for a content property with the float data type, you can use any of the formats for the integer data type. However, with the float data type, the thousands separator, if used, must be a comma (,).

You can include a period as a decimal separator in the number pattern for the float data type, although this is not required. If you do include it, any number signs (#) must come after any zeroes in the part following separator.

For example, a value of `1234.5` matches any of these number patterns:

```
0
00.0
.0
#0.0#
##,000
0,0
#,0.0#
```

You can also include an exponent character (E) followed by one or more zeroes in the number pattern for the float data type. However, values with an exponent character also match patterns that don't include the exponent character, and values without an exponent character also match patterns with an exponent character.

For example, a value of 1234E5 matches any of these number patterns:

```
0
00.0
.0E0
#0.0#E000
##,000E0
0,0
#,0.0E00
```

You can use a percent sign (%) by itself as the prefix or suffix in the format for the float data type. Before indexing values with a matching percent sign, the metadata query engine converts them to their decimal equivalents. For example, a value of `1234%` matches a format of 0% and is indexed as `12.34`.

White space is not required between the number pattern and a suffix that's a percent sign.

If you don't specify a format for a float data type, the metadata query engine indexes only sequences of digits that optionally include one decimal point.

Datetime data type formats

For a content property with the datetime data type, you can specify a format that values needs to match in order to be indexed. The format consists of a pattern of letters, optional separators, and optional quoted text. The letters represent date or time components, as outlined in the list below. Letters can be repeated, which can affect their meaning.

G

Represents a valid era indicator, such as AD, BC, or BCE. Repetition has no effect.
If a datetime pattern doesn't include any occurrences of G, the metadata query engine assumes an era of AD for matching values.

y
: Represents a year. For matching values with a two-digit year, a pattern that includes y more than twice in a row causes the metadata query engine to interpret the two digits as being preceded by two zeroes rather than by the number that indicates the current century.
If a datetime pattern doesn't include any occurrences of y, the metadata query engine assumes a year of 1970 for matching values.

M
: Represents a month. Values that include the month as a number match a pattern that includes M or MM. Values that include the name of the month, either in full or as a three-letter abbreviation, match a pattern that includes three or more occurrences of M in a row.
If a datetime pattern doesn't include any occurrences of M, the metadata query engine assumes a month of January for matching values.

w
: Represents the number of the week into the year. Repetition has no effect.

W
: Represents the number of the week into the month, where the first week is the week that includes the first day of the month. Repetition has no effect.

D
: Represents the number of the day into the year. Repetition has no effect.

d
: Represents the number of the day into the month. Repetition has no effect.

F
: Represents the number of the week into the month, where the first week starts with the first Sunday in the month. Repetition has no effect.

E
: Represents the day of the week. Matching values include the name of the day in full or as a three-letter abbreviation. Repetition has no effect.

a
: Represents a valid morning or afternoon indicator, such as AM or pm. Repetition has no effect.

H
: Represents the hour on a 24-hour clock, where midnight is represented by zero. Repetition has no effect.

k
: Represents the hour on a 24-hour clock, where midnight is represented by 24. Repetition has no effect.

K
: Represents the hour on a 12-hour clock, where midnight and noon are represented by zero. Repetition has no effect.

h
: Represents the hour on a 12-hour clock, where midnight and noon are represented by 12. Repetition has no effect.

m
: Represents the minute into the hour. Repetition has no effect.
If a datetime pattern doesn't include any occurrences of m, the metadata query engine assumes that the number of minutes is zero for matching values.

s
: Represents the second into the minute. Repetition has no effect.
If a datetime pattern doesn't include any occurrences of s, the metadata query engine assumes that the number of seconds is zero for matching values.

S
: Represents a number of milliseconds past the applicable second. Repetition has no effect.

z
: Represents a valid time zone specified as text, such Eastern Standard Time, EDT, or GMT. Repetition has no effect.

Z
: Represents a valid time zone specified as an offset from GMT, formatted as (+|-)nnnn, such as +0500 or -0200. Repetition has no effect.

If a datetime format doesn't include a representation for:

- A day, the metadata query engine assumes that the day is the first day of the applicable month for matching values
- An hour, the metadata query engine assumes that the hour is midnight
- A time zone, the metadata query engine assumes that the time is in the HCP system time zone

The separators in a datetime format can be any of several different special characters, including forward slashes (/), hyphens (-), colons (:), semicolons (;), at signs (@), and spaces.

To include text in a datetime format, enclose the text in single quotation marks ('). To include a single quotation mark, specify two single quotation marks in a row.

Here are some examples of datetime formats with examples of values that match them:

Format	Example
MM/dd/yy HH:mm:ss z	03/19/12 14:35:27 EST
hh 'o''clock' a, zzz	2 o'clock PM, Eastern Standard Time
yyyy-MM-dd'T'HH:mm:ss.SSSZ	2012-03-19T14:35:27.236-0400
E., MMM d, yyyy 'at' k:s	Mon., March 19, 2012 at 14:35

If you don't specify a format for a content property with the datetime data type, the metadata query engine indexes only values that match patterns such as MM/dd/yyyy, MM-dd-yyyy, yyyy-MM-dd, or yyyy-MM-dd'T'HH:mm:ssZ.

Multivalued content properties

A content property is defined as either single-valued or multivalued:

- If you define a content property as single-valued, the metadata query engine indexes only the first occurrence of it for any given object, regardless of how many times it occurs in the custom metadata XML for that object.
- If you define a content property as multivalued, the metadata query engine indexes all occurrences of it in the custom metadata XML for an object.

For example, based on the sample custom metadata XML, you would define as multivalued a content property that extracts the value of the specialty element.

With the metadata query API, users can sort query results based on single-valued content properties but not on multivalued properties.

Content properties extracted from sample XML

When working with content properties in the Tenant Management Console, you can supply sample well-formed XML and have HCP extract content properties from that XML. You can then select which of those properties you want to add to a content class.

HCP extracts only content properties for XPath expressions that follow a straight path from the root element. These conventions apply to the content property definitions:

- The XPath expression always starts from the root element.
- The name of a content property that extracts an element value is the name of the element preceded by the name of the parent element.
- The name of a content property that extracts an attribute value is the name of the attribute preceded by the name of the element the attribute applies to.
- Content property names that would exceed 25 characters in length are truncated to 25 characters, starting from the beginning.
- The definitions do not include formats.
- The definitions are listed alphabetically by XPath expression.

When adding extracted content properties to a content class, you can change any parts of their definitions.

The table below shows the definitions of the content properties HCP extracts from the sample custom metadata XML.

XPath expression	Name	Data type	Multivalued
/dicom_image/doctor/address/address1	addressAddress1	String	No
/dicom_image/doctor/address/address2	addressAddress2	String	No
/dicom_image/doctor/address/city	addressCity	String	No
/dicom_image/doctor/address/state	addressState	String	No
/dicom_image/doctor/address/zip	addressZip	Integer	No
/dicom_image/doctor/name	doctorName	String	No
/dicom_image/doctor/office	doctorOffice	String	No
/dicom_image/doctor/specialties/specialty	specialtiesSpecialty	String	Yes
/dicom_image/doctor/specialties/specialty/@primary	specialtyPrimary	Boolean	No
/dicom_image/followup_needed	icom_imageFollowup_needed	Boolean	No
/dicom_image/image/@type	imageType	String	No
/dicom_image/image/date	imageDate	String	No
/dicom_image/image/technician	imageTechnician	String	No
/dicom_image/patient/address/address1	addressAddress1	String	No
/dicom_image/patient/address/address2	addressAddress2	String	No
/dicom_image/patient/address/city	addressCity	String	No
/dicom_image/patient/address/state	addressState	String	No
/dicom_image/patient/address/zip	addressZip	Integer	No
/dicom_image/patient/id	patientId	Integer	No
/dicom_image/patient/name	patientName	String	No

Content property files

You can export the content properties for a content class to a file that you can then use to import the properties to another class. The exported file contains XML definitions of the content properties in this format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<contentClass>
    <contentProperties>
        <contentProperty>
             <name>property-name</name>
            <expression>xpath-expression</expression>
            <type>data-type</type>
            <multivalued>true-or-false</multivalued>
            <format>format</format>
        </contentProperty>
        .
        .
        .
    </contentProperties>
</contentClass>
```

Using the same format, you can also create content property files yourself.

Here's an example of XML that defines some content properties based on the sample custom metadata XML:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<contentClass>
    <contentProperties>
        <contentProperty>
            <name>Doctor_City</name>
            <expression>/dicom_image/doctor/address/city</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Doctor_State</name>
            <expression>/dicom_image/doctor/address/state</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
```

```
            <format />
        </contentProperty>
        <contentProperty>
            <name>Doctor_Name</name>
            <expression>/dicom_image/doctor/name</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Doctor_Office</name>
            <expression>/dicom_image/doctor/office</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Doctor_Specialty</name>
            <expression>/dicom_image/doctor/specialties/specialty</expression>
            <type>STRING</type>
            <multivalued>true</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Followup_Needed</name>
            <expression>/dicom_image/followup_needed</expression>
            <type>BOOLEAN</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Image_Type</name>
            <expression>/dicom_image/image/@type</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Image_Date</name>
            <expression>/dicom_image/image/date</expression>
            <type>DATE</type>
            <multivalued>false</multivalued>
            <format>MM/dd/yyyy</format>
        </contentProperty>
        <contentProperty>
            <name>Patient_City</name>
            <expression>/dicom_image/patient/address/city</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Patient_State</name>
            <expression>/dicom_image/patient/address/state</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Patient_ID</name>
            <expression>/dicom_image/patient/id</expression>
            <type>INTEGER</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
        <contentProperty>
            <name>Patient_Name</name>
            <expression>/dicom_image/patient/name</expression>
            <type>STRING</type>
            <multivalued>false</multivalued>
            <format />
        </contentProperty>
    </contentProperties>
</contentClass>
```


About the Search page

To manage search and indexing, including viewing, creating, and managing content classes and content properties, you use the Search page in the Tenant Management Console. To display this page, in the top-level menu, select Services > Search.

The Search page is available only if the tenant is configured to allow search and index management.

To view existing content classes and content properties, you need the monitor or administrator role. To create, modify, and delete content classes and content properties and reindex namespaces associated with content classes, you need the administrator role.

Managing the content class list

The Search page lists existing content classes. For each content class, the list shows the content class name.

By default, the content class list includes all existing content classes. The content classes are listed 20 at a time in ascending order by name.

You can page through, sort, and filter the list of content classes. The Search page indicates which content classes are shown out of the total number of content classes in the current list.

Paging

You can change the number of content classes shown at a time on the Search 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 content class list in ascending or descending order by content class 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 content class list by content class name. The filtered list includes only those content classes 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 ( ).

Understanding the content property list for a content class

To view the content properties defined for a content class, click the content class name in the content class list. The panel that opens (the Settings panel) contains a list of the content properties in that content class. The properties are listed in alphabetical order by name.

For each content property, the list shows:

Name
: The content property name

Expression
: The XPath expression for the content property, with an annotation prefix if applicable

Type
: The data type of the content property

Format
: The format for the content property

: An indication of whether the content property is multivalued

Creating a content class

When you create a content class, you can create content properties for it at the same time. Alternatively, you can create a content class with no properties and add properties to it later.

1. On the Search page, click Create Content Class.
2. In the Name field, type a name for the content class.
   Content class names must be from one through 64 characters long, can contain any valid UTF-8 characters, including white space, and are not case sensitive.
3. (Optional) Define one or more content properties to be added to the content class.
4. (Optional) If you defined content properties, test or export them.
5. Click Create Content Class.

Managing content properties for a content class

You can add, modify, and delete content properties for a content class at any time. You can also test the properties against XML that you supply. Additionally, you can export the properties to a content property file.

Workflow for adding, modifying, and deleting content properties

1. On the Search page, in the list of content classes in the Settings panel, click the name of the content class for which you want to add, modify, or delete content properties.
2. Add, modify, or delete a content property.
   - Add one or more properties individually
   - Extract one or more properties from XML that you supply
   - Import properties from a content property file
   - Modify a content property by making the changes you want in the row for the property.
   - Delete an existing content property by clicking the delete control ( ) for the row containing the property.

   New content properties appears in the list of content properties for the content class. The new rows are highlighted in green. Deleted properties are highlighted in red.
3. Test or export all the listed content properties.
4. Click Update Settings.

If you also typed a new name for the content class in the Name field, clicking Update Settings changes the content class name.

Adding content properties individually

1. Above the content property list, click Add.
2. In the new row that appears in the content properties list, fill in the definition for the new content property.

Extracting content properties from sample XML

1. In the Sample Custom Metadata field, type or paste the well-formed XML from which you want to extract properties.
2. Above the content property list, click Extract.
   The Extract Content Properties window opens. The window lists all the content properties HCP was able to extract from the sample XML.
3. Select each content property you want to add to the content class.
   To select all the listed content properties, click in the checkbox at the top of the list. To deselect all the properties after selecting all, click in the checkbox again.
4. Click Add Selected.
   A row for each content property you selected appears in the list of content properties for the content class.
5. (Optional) Modify the definitions of the new content properties.

Importing content properties from a content property file

1. Above the content property list, click Import.
2. In the Import Content Properties window, click Browse. Then select the content property file you want.
3. Click Import.
   A row for each content property defined in the content property file appears in the list of content properties for the content class.
4. (Optional) Modify the definitions of the new content properties.

Testing content properties

You can test the definitions of the content properties for a content class at any time. You do this by having HCP extract content property values from sample XML that you supply. The test applies to all the content properties in the content property list, including those that have not yet been committed.

1. On the Search page, in the list of content classes, click the name of the content class with the content properties you want to test.
2. In the Sample Custom Metadata field in the Settings panel, type or paste the well-formed XML you want to use for the test.
3. Above the content property list, click Test.

HCP extracts the values it can find for the content properties in the content property list. The extracted values appear in the Test Value column in the content property list.

Exporting content properties

You can export the definitions of the content properties for a content class to a content property file at any time. The resulting file includes the definition of each property in the list, including those that have not yet been committed.

1. On the Search page, in the list of content classes, click the name of the content class with the content properties you want to export.
2. Above the content property list in the Settings panel, click Export.
3. When prompted, save the content property file to the location of your choice.

Changing the namespaces associated with a content class

You can change the associations between namespaces and content classes at any time. However, only namespaces that are search enabled can be associated with content classes.

When you change the namespaces associated with a content class, you have the option of reindexing all the affected namespaces. If you choose to do this, the metadata query engine reindexes each of those namespaces starting from the time the namespace was created.

1. On the Search page, in the list of content classes, click the name of the content class with for which you want to change namespace associations.
2. In the row of tabs below the content class name, click Namespaces.
   In the Namespaces panel, the Associate Namespaces with Content Class section lists namespaces that are enabled for search and are not already associated with the content class.
   If any namespaces are already associated with the content class, they are listed in the Content Class Namespaces section.
3. (Optional) Filter the list of namespaces in the Associate Namespaces with Content Class section by namespace name.
   a. In the Associate Namespaces with Content Class field, type a text string 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. You cannot filter the namespace list while any of the namespaces in it are selected for association.
   b. Click the find control ( ).
4. For each namespace you want to associate with the content class, click the add control ( ) for the namespace in the Associate Namespaces with Content Class section.
   - To select all the namespaces listed in the Associate Namespaces with Content Class list, click Select All.
   - To deselect a namespace, click the remove control ( ) for it.
   - To deselect all the selected namespaces, click Clear.

   The row containing the namespace turns green.
5. For each namespace in the Content Class Namespaces section that you want to dissociate from the content class, click the remove control ( ) for the namespace in that section.
   - To select all the namespaces listed in the Content Class Namespaces section, click Select All.
   - To deselect a namespace, click the add control ( ) for it.
   - To deselect all the selected namespaces, click Clear.

   Tip: You can filter the list of namespaces in the Content Class Namespaces section by namespace name to include only those namespaces you want to remove from replication.
   The row containing the namespace turns red.
6. (Optional) Reindex all the namespaces you are associating with or dissociating from the content class by selecting Reindex all objects in added/removed namespaces.
7. Click Update Content Class.

Reindexing namespaces associated with a content class

You can reindex the namespaces associated with a content class at any time. You might do this for example, if you add a new content property to the content class.

1. On the Search page, in the list of content classes, click the name of the content class with the namespaces you want to reindex.
2. In the row of tabs below the content class name, click Reindex.
   The Content Class Namespaces section in the Reindex panel displays a list of the namespaces that are associated with the content class.
3. (Optional) Filter the list of namespaces by namespace name.
   a. In the Content Class Namespaces field, type a text string 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. You cannot filter the namespace list while any of the namespaces in it are selected for reindexing.
   b. Click the find control ( ).
4. For each namespace you want to reindex, click the add control ( ) to select the namespace.
   - To select all the namespaces in the list, click Select All.
   - To deselect a selected namespace, click the remove control ( ) for the namespace.
   - To deselect all the namespaces after selecting all, click Clear.

   The namespace row turns green.
5. In the Reindex Selected Namespaces section, select either All objects or Objects modified after.
   - If you select Objects modified after, either type a date in the associated field or click the calendar control ( ) to select a date. If you type a date, use this format: mm/dd/yyyy
   - If you enter an invalid date using the correct date format, HCP tries to convert it to a real date. For example, if you enter 11/31/2012, HCP converts it to 12/01/2012.
6. Click Reindex Namespaces.
   If you selected All objects, a confirming message appears.
7. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
8. Click Reindex Namespaces.

Renaming a content class

You can rename a content class at any time. Renaming a content class has no effect on the associations between namespaces and that class.

1. On the Search page, in the list of content classes, click the name of the content class you want to rename.
2. In the Name field in the Settings panel, type a new name for the content class.
3. Click Update Settings.
   If you also modified the list of content properties for the content class, clicking Update Settings commits those changes as well.

Deleting a content class

You can delete a content class at any time. When you delete a content class, you have the option of reindexing all the namespaces associated with that class. If you choose to do this, the metadata query engine reindexes each of those namespaces starting from the time the namespace was created.

1. On the Search page, in the list of content classes in the Settings panel, click the delete control ( ) for the content class you want to delete.
2. In response to the confirming message:
   a. (Optional) To reindex all namespaces associated with the content class you're deleting, select Reindex all objects in associated namespaces.
   b. Click Delete.

Managing search and indexing for an individual namespace

You can change the search and indexing settings for an individual namespace at any time. You can:

- Enable or disable search.

  Disabling search also:

  - Disables all indexing for the namespace
  - Removes the objects in the namespace from the metadata query engine and HCP search facility indexes
  - Deletes the list of excluded annotations for the namespace
  - Deletes all associations the namespace has with any content classes
- If search is enabled:
  - Enable or disable indexing. Disabling indexing also disables custom metadata indexing for the namespace. However, it does not remove objects in the namespace from the indexes.

    By default, when you create a namespace with search enabled, indexing is also enabled.
  - Add or delete associations between content classes and the namespace.
- If indexing is enabled, enable or disable indexing of custom metadata. Disabling custom metadata indexing also disables metadata query engine indexing of the full text of custom metadata.

  If you disable custom metadata indexing after it has been enabled, custom metadata that has already been indexed is not removed from the index.

  By default, when you create a namespace with search enabled, indexing of custom metadata is disabled.

- If indexing of custom metadata is enabled:
  - Enable or disable metadata query engine indexing of the full text of custom metadata. If you disable this option after it has been enabled, custom metadata text that has already been indexed is not removed from the index.
  - Specify annotations to be excluded from metadata query engine indexing of custom metadata. Annotations are excluded by name. So, for example, you could exclude all annotations named miscellaneous. Users cannot query for objects based on the content of excluded annotations.

You can also reindex an individual namespace at any time. You might do this, for example, if you associate additional content classes with the namespace.

Displaying the namespace Search panel

To manage search and indexing for an individual namespace, you use the namespace Search panel in the Tenant Management Console.

While the metadata query engine or HCP search facility is selected for use with the Search Console, the Search panel shows the date and time before which eligible objects in the namespace are guaranteed to be included in the applicable index.

- To view the search and indexing settings for a namespace, you need the monitor or administrator role.
- To modify the search and indexing settings for a namespace or to reindex a namespace, you need the administrator role.

1. In the top-level menu, click Namespaces.
2. In the list of namespace on the Namespaces page, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Services.
4. On the left side of the Services panel, click Search.

Setting search and indexing options

1. In the Search panel for the namespace, select or deselect Enable search to enable or disable search, respectively.
2. If Enable search is selected:
   - Select or deselect Enable indexing to enable or disable indexing, respectively.
   - In the Content Classes list, select or deselect content classes to associate them with or dissociate them from the namespace, respectively.

     To select all the listed content classes, click in the checkbox at the top of the list. To deselect all the content classes after selecting all, click in the checkbox again.
3. If Enable indexing is selected, select or deselect Enable indexing of custom metadata to enable or disable indexing of custom metadata, respectively.
4. If Enable indexing of custom metadata is enabled:
   - Select or deselect Enable full custom metadata indexing to enable or disable metadata query engine indexing of the full text of custom metadata, respectively.
   - In the Exclude Annotations from Indexing field, specify the names of one or more annotations to be excluded from custom metadata indexing. Use a comma to separate each annotation name from the next.

   Instead of explicit 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 asterisk can occur anywhere in the pattern. Annotation names are case sensitive.
5. Click Update Settings.
   If you deselected Enable search, HCP displays a confirming message.
6. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
7. Click Update Settings.

Reindexing an individual namespace

1. In the Search panel for the namespace, in the Reindex section of the Search panel, in the first field, select either:
   - Metadata Query Engine to have the metadata query engine reindex the namespace
   - HCP Search Facility to have the HCP search facility reindex the namespaces

   The Reindex section displays either `Namespace indexed` or `Namespace not indexed` to indicate whether the namespace is currently included in the index for the selected search facility.
2. Select either All objects or Objects modified after.
   If you select Objects modified after, either type a date in the associated field or click the calendar control ( ) to select a date. If you type a date, use this format: mm/dd/yyyy
   If you enter an invalid date using the correct date format, HCP tries to convert it to a real date. For example, if you enter 11/31/2015, HCP converts it to 12/01/2015.
3. Click Reindex Objects.
   If you selected All objects, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action.
5. Click Reindex Objects.

If indexing is disabled for the namespace, the procedure above does not by itself start the reindexing process. To start reindexing the namespace, you need to reenable indexing.

Working with retention classes

Retention classes provide a means to consistently manage data that must remain in a namespace for a specific amount of time. For example, if local law requires that medical records be kept for a specified number of years, you can use a retention class to enforce that requirement.

Retention classes are defined on a per-namespace basis. The classes you create for one namespace are not visible in any other namespace.

You create retention classes in the Tenant Management Console. Users and applications can then use those classes as retention settings for objects.

This chapter describes retention classes and explains how to create, modify, and delete them.

Note: Retention classes apply only to HCP namespaces.

About retention classes

A *retention class* is a named value that, when used as the retention setting for an object, specifies how long the object must remain in its namespace. This value can be:

- An offset from the time the object is created. You specify an offset as numbers of years, months, or days.

  For example, you could create a retention class named HlthReg-107 with an offset of 21 years. Then, all objects assigned HlthReg-107 as their retention setting could not be deleted for 21 years after they're created.

- One of these special values:

  Deletion Allowed
  : The object can be deleted at any time.

  Deletion Prohibited
  : The object can never be deleted by means of a normal delete operation. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.

  Initial Unspecified
  : The retention period for the object is unspecified. The object cannot be deleted by means of a normal delete operation while it has this retention setting. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.

- A fixed future date that the object will be deleted.

The retention period for an object assigned to a retention class is calculated from the value of that class. So, for example, if an object stored on October 8, 2011, is assigned to a retention class with an offset value of seven years, the retention period for that object expires on October 8, 2018.

You can choose to have HCP automatically delete the objects assigned to a retention class when they expire. This applies only to retention classes with a value that's an offset. It does not apply to retention classes with special values.

Automatic deletion of expired objects in retention classes occurs only if disposition is enabled.

Display the Retention Classes panel

To view, create, and manage retention classes for a namespace, you use the Retention Classes panel for that namespace.

- To view retention classes, you need the monitor, administrator, or compliance role.
- To create, modify, and delete retention classes, you need the compliance role.

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Compliance.
4. On the left side of the Compliance panel, click Retention Classes.

Understanding the retention class list

The Retention Classes panel lists the retention classes defined for a namespace. For each class, the list shows:

- The retention class name.
- Whether the retention class value is an offset, special value, or fixed date.
- The retention class value.

  A value that's an offset has this format:

  ```
  A+ny+nm+nd
  ```

  In this format, y is the number of years, m is the number of months, and d is the number of days. Only the measurement units with nonzero values are shown. For example, an offset of two years and 5 days looks like this:

  ```
  A+2y+5d
  ```

- Whether expired objects in the retention class are automatically deleted (Allow Disposition).

To view the description of a listed retention class, click the class name.

Creating a retention class

1. In the Retention Classes panel, click Create Retention Class.
2. In the Retention Class Name field, type a name for the retention class.
   Retention class names must be from one through 64 characters long, can contain only alphanumeric characters, hyphens (-), and underscores (_), and are not case sensitive.
3. Take one of these actions:
   - To make the retention class value an offset, in the Retention Method field, select Offset. In the Years field, type a number of years. In the Months field, type a number of months. In the Days field, type a number of days.

     Valid values are integers in the range zero through 9,999.

   - To make the retention class value a special value, in the Retention Method field, select Special Value. In the Special Value field, select the special value you want.
   - To make the retention class a fixed date, in the Retention Method field, select Fixed Date. In the Fixed Date field, type the date you want. The date format is mm/dd/yyyy.
4. (Optional) In the Description field, type a description of the retention class.
   The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
5. (Optional) Select Allow Disposition service to delete objects when expired to have HCP automatically delete expired objects in the retention class.
   This option is present only when the retention method is offset.
6. Click Create Retention Class.

Modifying a retention class

You can increase the value of a retention class at any time. These changes increase the value:

- From an offset to a larger offset
- From Deletion Allowed to an offset or Deletion Prohibited

If the namespace is in enterprise mode, you can decrease the value of a retention class at any time. These changes decrease the value:

- From an offset to a smaller offset
- From an offset to Deletion Allowed
- From Deletion Prohibited to an offset or Deletion Allowed

If the value of a retention class is Initial Unspecified, you can change it to any other value at any time. You can change the value to Initial Unspecified only from Deletion Allowed.

You can enable or disable the autodeletion feature at any time. You can also change the class description at any time.

1. In the Retention Classes panel, in the list of retention classes, click the edit control ( ) for the retention class you want to modify.
2. In the Edit Retention Class window, make the changes you want.
3. Click Update Settings.

Deleting a retention class

You can delete a retention class only if the namespace in which the class is defined is in enterprise mode. You cannot delete a retention class in a namespace that's in compliance mode.

When you delete a retention class, the retention setting of each object in the class changes to Deletion Prohibited.

1. In the Retention Classes panel, in the list of retention classes, click the delete control ( ) for the retention class you want to delete.
2. In response to the confirming message, click Delete Retention Class.

Using privileged delete

Namespaces configured to use HCP retention enterprise mode support privileged delete operations. However, S3 Object Lock doesn't support privileged delete.

Users and applications with the applicable data access permissions can perform privileged delete operations through the HTTP namespace access protocol, and the HCP Search Console. If you have the compliance role through your HCP user account or group accounts, you can perform these operations through the Tenant Management Console.

About privileged delete

Privileged delete is an HCP feature that enables you to delete objects even if they are under retention. This feature is available only for namespaces in enterprise mode. If a namespace is in compliance mode, you cannot delete objects that are under retention.

Privileged delete supports government regulations that require the destruction of certain types of data in response to changing circumstances. For example, companies may be required to destroy particular information about employees who leave. If that data is under retention, it cannot be deleted through normal delete operations.

If the namespace supports versioning, you can turn a privileged delete operation into a privileged purge operation. This deletes all versions of the target object.

When using privileged delete, you need to specify a reason for the deletion. The tenant log records all privileged delete operations, including the specified reasons, thereby creating an audit trail.

Using privileged delete, you can also delete objects that are not under retention. You would do this, for example, if you wanted to record the reason for an object deletion.

You cannot use privileged delete to delete objects that are on hold, regardless of their retention settings.

To perform a privileged delete operation through the Tenant Management Console, you need the compliance role.

Object specification

With privileged delete, you can delete only one object at a time. To specify the object, you need to include the full path to it in its namespace (starting after `rest` or `data`). The path must begin with a forward slash (/).

For example, to delete the `Lee_Green_1254` object from the `Corporate/Employees` directory, you would specify:

```
/Corporate/Employees/Lee_Green_1254
```

Directory and object names are case sensitive. The separator is the forward slash (/).

Non-UTF-8 characters in directory and object names must be percent encoded. To avoid ambiguity, you should also percent-encode the characters listed in the table below.

Character	Percent-encoded value
Space	%20
Tab	%09
New line	%0A
Carriage return	%0D
+	%2B
%	%25
#	%23
?	%3F
&	%26
\	%5C

Percent-encoded values are not case sensitive.

Performing a privileged delete

1. In the top-level menu of the Tenant Management Console, click Namespaces.
2. In the list of namespaces, click the name of the namespace you want.
3. In the row of tabs below the namespace name, click Compliance.
4. On the left side of the Compliance panel, click Privileged Delete.
   Note: This option is present only if the namespace is configured to use HCP retention, enterprise mode and your user account includes the compliance role.
5. In the Privileged Delete panel:
   a. In the Object to Delete field, type the path to and name of the object you want to delete.
   b. (Optional) Select Purge all versions of this object to change the delete operation to a purge operation.
      This option appears only if versioning is enabled for the namespace.
   c. In the Reason for Deletion field, type the reason why you're deleting the object.
      This text must be from one through 1,024 characters long and can contain any valid UTF-8 characters, including white space.
6. Click Delete This Object.
7. In response to the confirming message, click Delete Object.

Tenant Management Console alerts

The Tenant Management Console uses icons to report tenant and namespace status on the tenant Overview, Namespaces, and Search pages and on the namespace Overview panel. The Console also uses icons to report conflicting user accounts on the Users page. These icons, called alerts, are accompanied by text on the tenant Overview page and namespace Overview panel. On all pages on which they appear, alerts have text that's displayed when you hover over them.

This appendix describes the alerts that can appear on the Console pages and shows the hover text for each alert. Where applicable, the appendix also tells you how to respond to the alerts.

The alerts in each table in this appendix are listed alphabetically by their hover text.

Tenant Overview page alerts

Conflicting user accounts

Two or more user accounts have the same username. This can happen after an upgrade if, before the upgrade occurred, a user account and a data access account (created in an HCP release earlier than 5.0) had the same username. Resolve the conflict by merging or separating the conflicting accounts on the Users page in the Tenant Management Console.

Irreparable and unavailable objects

One or more of the tenant's namespaces contain irreparable objects, and one or more of the tenant's namespaces contain unavailable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the applicable namespaces.

Irreparable objects

One or more of the tenant's namespaces contain irreparable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the applicable namespaces.

Nonreplicating objects

The namespace contains objects that are not replicating. Please contact your HCP system administrator.

Soft quota exceeded

The amount of storage used by all the tenant's namespaces exceeds the soft quota configured for the tenant. Consider deleting some objects from the namespaces or requesting an increase in 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 with DPL 1 namespaces that are not replicating

The tenant owns one or more namespaces that have a DPL of 1 (one) and are not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the DPL of the affected namespaces.

This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.

Unavailable objects

One or more of the tenant's namespaces contain unavailable objects. Please contact your HCP system administrator.

Namespaces page alerts

AD single sign-on access disabled.

Active Directory single sign-on is currently not working with the HTTP protocol. Please contact your HCP system administrator.

Anonymous access allowed

One or more enabled protocols allow clients to access the namespace without presenting user credentials for authentication.

Content classes but no custom metadata indexing

The namespace is associated with one or more content classes, but custom metadata indexing is disabled for the namespace. The metadata query engine is not indexing content properties for objects in the namespace.

DPL 1 namespace is not replicating

The namespace has a DPL of 1 (one) and is not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the namespace DPL.

This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.

Hard quota exceeded

The amount of storage used by the namespace exceeds the hard quota configured for the namespace. Clients will not be able to add data to the namespace until either some existing objects are deleted or you increase the hard quota.

Namespace *namespace-name* has *irreparable-object-count* irreparable objects

The namespace contains the indicated number of irreparable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the namespace.

Namespace *namespace-name* has *irreparable-object-count* irreparable objects and *unavailable-object-count* unavailable objects

The namespace contains the indicated number of irreparable objects and the indicated number of unavailable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the namespace.

Namespace *namespace-name* has *unavailable-object-count* unavailable objects

The namespace contains the indicated number of unavailable objects. Please contact your HCP system administrator.

Namespace setting for CIFS authenticated access not supported by system configuration

The namespace requires authentication for CIFS-based data access. However the system is currently not configured to support the use of authenticated CIFS.

Nonreplicating objects

The namespace contains objects that are not replicating. Please contact your HCP system administrator.

Soft quota exceeded

The amount of storage used by the namespace exceeds the soft quota configured for the namespace. Consider deleting some objects from the namespace or increasing its hard quota.

Versioning without REST API

The namespace has versioning enabled, but the REST API is not enabled. Versioning works only with the REST API.

Namespaces Overview panel alerts

Anonymous access allowed

One or more enabled protocols allow clients to access the namespace without presenting user credentials for authentication.

DPL 1 namespace is not replicating

The namespace has a DPL of 1 (one) and is not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the namespace DPL.

This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.

Hard quota exceeded

The amount of storage used by the namespace exceeds the hard quota configured for the namespace. Clients will not be able to add data to the namespace until either some existing objects are deleted or you increase the hard quota.

Irreparable and unavailable objects

The namespace contains irreparable objects and unavailable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the namespace.

Irreparable objects

The namespace contains irreparable objects. Please contact your HCP system administrator.

To see which objects are irreparable, go to the Irreparable Objects panel for the namespace.

Namespace setting for CIFS authenticated access not supported by system configuration

The namespace requires authentication for CIFS-based data access. However the system is currently not configured to support the use of authenticated CIFS.

Nonreplicating objects

The namespace contains objects that are not replicating. Please contact your HCP system administrator.

Soft quota exceeded

The amount of storage used by the namespace exceeds the soft quota configured for the namespace. Consider deleting some objects from the namespace or increasing its hard quota.

Unavailable objects

The namespace contains unavailable objects. Please contact your HCP system administrator.

Versioning enabled without REST API

The namespace has versioning enabled, but the REST API is not enabled. Versioning works only with the REST API.

Search page alert

Namespaces without custom metadata indexing

The content class is associated with one or more namespaces for which custom metadata indexing is disabled. The metadata query engine is not indexing content properties for objects in those namespace.

Users page alert

Conflicting user accounts

Another user account has the same username as this account. Resolve the conflict by merging or separating the conflicting accounts.

Tenant log messages

Tenant log messages

The tenant log contains messages about events that happen at the tenant and namespace levels. The table in this appendix lists the messages HCP can write to the tenant log. The messages are listed in order by event ID.

ID	Event	Explanation	Action	Severity
2005	HCP found an unavailable object	HCP could not repair an object because the object was unavailable.	Contact your HCP system administrator.	Warning
2006	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
2028	HCP found an irreparable object	HCP was unable to repair the object. The repair may be retried at a later time.	Contact your HCP system administrator.	Error
2044	HCP found an unavailable object	HCP could not repair an object because the object was unavailable.	Contact your HCP system administrator.	Warning
2046	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
2070	Object has been shredded	An object was shredded.	No action is required.	Notice
2087	Disposition service stopped: run complete	The Disposition service finished successfully.	No action is required.	Notice
2088	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
2089	Disposition service stopped: run complete	The Disposition service finished successfully.	No action is required.	Notice
2090	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
2092	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
2093	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
2154	Additional namespaces included in tenant replication	The indicated namespaces were selected to be included in replication of the tenant.	No action is required.	Notice
2155	One or more namespaces removed from tenant replication	The indicated namespaces were removed from replication of the tenant.	No action is required.	Notice
2156	Replication automatically paused for this tenant	Replication of the tenant was automatically paused 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

ID	Event	Explanation	Action	Severity
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
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
2343	Successfully added Service Principal Name to Active Directory	HCP successfully added a Service Principal Name to Active Directory.	No action is required.	Notice
2345	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
2347	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
2351	Group account created	A user created a group account.	No action is required.	Notice
2353	Group account updated	A user updated a group account.	No action is required.	Notice
2355	Group account deleted	A user deleted a group account.	No action is required.	Notice
2396	Successfully removed Service Principal Name from the Active Directory	Successfully removed Service Principal Name from the Active Directory.	No action is required.	Notice
2398	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
2637	Syslog disabled for a tenant.	Syslog has been disabled for a tenant.	No action is required	Notice
2638	Syslog enabled for a tenant.	Syslog has been enabled for a tenant.	No action is required	Notice
2900	Privileged delete requested	A user requested a privileged delete operation.	No action is required.	Notice
2901	Privileged delete succeeded	A privileged delete operation succeeded.	No action is required.	Notice
2902	Privileged delete failed	A privileged delete operation failed.	No action is required.	Notice
2903	Retention class created	A user created a retention class.	No action is required.	Notice
2904	Retention class updated	A user updated a retention class.	No action is required.	Notice

ID	Event	Explanation	Action	Severity
2905	Retention class deleted	A user deleted a retention class.	No action is required.	Notice
2906	Retention mode set	The namespace retention mode has been changed.	No action is required.	Notice
2907	Privileged purge requested	A user requested a privileged purge operation.	No action is required.	Notice
2908	Privileged purge succeeded	A privileged purge operation succeeded.	No action is required.	Notice
2909	Privileged purge failed	A privileged purge operation failed.	No action is required.	Notice
2911	Retention class missing	HCP system detected a missing retention class.	Contact your HCP system administrator.	Error
2912	Privileged delete failed	A user updated Minimum Retention after Initial Unspecified setting.	No action is required.	Notice
3004	Namespace created	A user created a namespace.	No action is required.	Notice
3005	Namespace updated	A user updated a namespace.	No action is required.	Notice
3006	Namespace deleted	A user deleted a namespace.	No action is required.	Notice
3011	User account created	A user created a user account.	No action is required.	Notice
3012	User account updated	A user updated a user account.	No action is required.	Notice
3013	User account deleted.	A user deleted a user account.	No action is required.	Notice
3014	User account is disabled	A user tried to log in with a disabled user account.	Reenable the user account to allow the user to log in.	Warning
3015	User account disabled.	A user account has been disabled.	No action is required.	Notice
3016	User account enabled	A user account has been enabled.	No action is required.	Notice
3017	User account password changed	A user changed the password for a user account.	No action is required.	Notice
3018	User account failed login	A user tried to log in with a username and password that are not valid for any user account.	Have the user log in with a username and password that are valid for a user account.	Warning
3019	Failed login to the Search Console	A user tried to log into the Search Console with a username and password that are not valid for any user account.	Have the user log into the Search Console with a username and password for that are valid for a user account.	Warning
3020	Namespace over hard quota	The amount of storage used by the namespace exceeds the configured hard quota.	Delete some objects from the namespace or increase the hard quota.	Warning
3021	Namespace under hard quota	The amount of storage used by the namespace is under the configured hard quota	No action is required.	Warning
3022	Namespace over soft quota	The amount of storage used by the namespace exceeds the configured soft	Consider deleting some objects from the	Warning

ID	Event	Explanation	Action	Severity
		quota.	namespace or increasing the hard quota for the namespace.	
3023	Namespace under soft quota	The amount of storage used by the namespace is under the configured soft quota.	No action is required.	Warning
3024	Tenant over soft quota	The amount of storage used by all namespaces owned by the tenant exceeds the soft quota configured for the tenant.	Consider deleting some objects from the namespaces or requesting an increase in the hard quota for the tenant.	Warning
3025	Tenant under soft quota	The amount of storage used by all namespaces owned by the tenant is under the soft quota configured for the tenant.	No action is required.	Warning
3028	Failed user account login attempt	An attempt to log into a tenant failed because the user account could not be authenticated.	No action is required.	Warning
3032	Tenant at namespace quota	The number of namespaces is equal to the maximum allowed for this tenant.	No action is required.	Warning
3033	Tenant over namespace quota	The number of namespaces is greater than the maximum allowed for this tenant.	Either delete one or more namespaces or have your HCP system administrator increase the namespace quota.	Warning
3037	Username conflict	Multiple user accounts have the same username. All user accounts must have a unique username.	Rename one account or merge duplicate accounts together.	Warning
3508	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
3998	Search enabled or disabled	A user enabled or disabled search.	No action is required.	Notice
3999	Search indexing enabled or disabled	A user enabled or disabled search indexing.	No action is required.	Notice
4000	HCP search facility indexing failure	The HCP search facility encountered an object it could not index.	Contact your HCP system administrator.	Error
4002	User account created	A user created a user account.	No action is required.	Notice
4003	User account updated	A user updated a user account.	No action is required.	Notice
4004	User account deleted	A user deleted a user account.	No action is required.	Notice
4005	User authenticated	A user login to the Tenant Management Console was successfully authenticated.	No action is required.	Notice
4006	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
4007	Account reenabled by timer	A disabled security user account has been automatically reenabled.	No action is required.	Notice
4008	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.

ID	Event	Explanation	Action	Severity
4009	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.
4010	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.
4011	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.
4012	Remote authentication server error	The login for a remotely authenticated user failed due to an error communicating with a RADIUS server.	Contact your HCP system administrator.	Warning.
4013	Password changed	A user changed the password for a user account.	No action is required.	Notice.
4014	Account enabled	A user account has been enabled.	No action is required.	Notice.
4015	Account disabled	A user account has been disabled.	No action is required.	Notice.
4016	Account disabled due to too many failed logins	A user account has been 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
4017	Account will be reenabled	A security user account will be reenabled automatically after a waiting period.	No action is required.	Warning.
4018	User authenticated	A user login to the Search Console was successfully authenticated.	No action is required.	Warning.
4019	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Warning.
4020	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Warning.
4021	Irreparable object acknowledged	A user acknowledged an irreparable object.	No action is required.	Warning.
4022	All irreparable objects acknowledged	A user acknowledged all irreparable objects.	No action is required.	Warning.
4023	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
4024	User account created	A user created a user account.	No action is required.	Notice.
4025	User account updated	A user updated a user account.	No action is required.	Notice.
4026	User account deleted	A user deleted a user account.	No action is required.	Notice.
4027	User account is disabled	A user tried to log in with a disabled user account.	Reenable the user account to allow the user to log in.	Warning
4028	User account disabled due to too many failed logins	A user account has been automatically disabled due to too many failed login attempts.	Reenable the user account to allow the account user to log in.	Warning

ID	Event	Explanation	Action	Severity
4029	User account disabled	A user account has been disabled.	No action is required.	Notice.
4030	User account password changed	A user changed the password for a user account.	No action is required.	Notice.
4031	User accounts merged	A user merged multiple user accounts with the same username into a single account.	No action is required.	Notice.
4100	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
4101	Object did not replicate	An object was not replicated.	Contact your HCP system administrator.	Error
4102	Object did not replicate; will retry later	An object was not replicated. Replication of the object will be retried later.	Monitor the replica to see whether this object is eventually replicated. If the object does not replicate within one week, contact your HCP system administrator.	Warning.
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.	No action is required. If this situation persists, 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.
4114	Metadata query engine indexing failure	The metadata query engine encountered an object it could not index.	If this situation persists, contact your HCP system administrator.	Warning.
4115	Metadata query engine checkpoint reset	A user reset the metadata query engine checkpoint for the indicated namespace.	No action is required.	Warning.
4122	Failure adding namespace to the search index.	The HCP search facility could not create the index for a namespace because the system limit was reached.	No action is required. If this situation persists, contact your authorized service provider.	Warning.
4123	Namespace was successfully added to index	Namespace was added to the index	No action is required.	Notice.
4124	Content class created	A user created a content class.	No action is required.	Notice.
4125	Content class updated	A user updated a content class.	No action is required.	Notice.
4126	Content class deleted	A user deleted a content class.	No action is required.	Notice.
4127	Namespaces associated with content class	A user associated namespaces with a content class.	No action is required.	Notice.
4128	Content classes associated with namespace	A user associated content classes with a namespace.	No action is required.	Notice.

ID	Event	Explanation	Action	Severity
4220	Namespace tags updated	A user updated the tags for a namespace.	No action is required.	Notice.
4225	Namespace default settings updated	A user updated the namespace default settings.	No action is required.	Notice.

Browser configuration for single sign-on with Active Directory

If a tenant is configured to support AD authentication, you can use a recognized AD user account to access the Tenant Management Console with single sign-on. However, for this to work, the web browser you use to access the Console must be configured to support single sign-on.

This appendix contains instructions for configuring Windows Internet Explorer® and Mozilla® Firefox® to support single sign-on.

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.

Replicating tenants and namespaces

Geographically distributed data protection

An individual Hitachi Content Platform (HCP) system maintains a repository of objects in one or more namespaces. To ensure data availability and protect against data corruption, namespaces can be configured (using service plans) to store multiple copies of each object. However, storing multiple copies of objects on only one system does not provide protection against the unavailability or loss of that system.

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. Depending on the number of systems and how you configure the relationships between them, data could even be protected against the concurrent unavailability or loss of more than one 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*). You have multiple options for implementing geo-protection, each with its own benefits and drawbacks.

This section of the Help provides an overview of how geo-protection works and how it supports business continuity and disaster recovery.

About geo-protection

Geo-protection is implemented by the HCP Replication service. The Replication service is responsible for keeping tenants and namespaces on two or more HCP systems in sync with each other. Replication entails sending information from the system where the service is running to one or more other systems. The information sent includes tenant and namespace configuration information, metadata and data for newly created objects, metadata changes for existing objects, and instructions to perform delete operations.

The Replication service works on the systems in a replication topology. A *replication topology* is a configuration of HCP systems wherein each system is related to each other system through a path of one or more replication relationships. The HCP system from which you are viewing the replication topology is called the *local system*. Any other system in the replication topology is called a *remote system*.

You select the tenants to be replicated in a replication topology. For each tenant, the tenant administrator selects the namespaces to be replicated. If the tenant administrator has granted system-level users access to the tenant, you also can select namespaces for replication.

Geo-protection offers several benefits:

- If a system in a replication topology becomes unavailable, a remote system can provide continued data availability. A system is unavailable if it is not running or is unreachable.
- If a system in a replication topology suffers irreparable damage, a remote system can serve as a source for disaster recovery.
- If the Content Verification or Protection service discovers objects it cannot repair on a system in a replication topology, the service can use object data and metadata from a remote system to make the needed repairs.
- If an object cannot be read from a system in a replication topology, for example, because a node is unavailable, HCP can try to read it from a remote system. HCP tries to do this only if:
  - The namespace that contains the object is involved in replication.
  - The namespace has the read-from-remote-system feature enabled.
  - The object has already been replicated. Users can check object metadata to determine whether an object has been replicated.
  - The replication networks for the local and remote systems can both use the same IP mode (IPv4 or IPv6).
- If a system in a replication topology is unavailable, requests to that system that come through the REST, S3 compatible namespace access protocol can be automatically serviced by a remote system without the client needing to modify the target URL. A remote system can service a request only if:
  - The namespace named in the URL is replicated to the remote system.
  - The namespace named in the URL is configured to accept requests redirected from other HCP systems.
  - The HCP systems involved use a shared DNS for system addressing.
  - Both the DNS and the unavailable system are configured to support DNS failover. (This condition is not a requirement if you're using a load balancer that can target the requests to a remote system.)
- If multiple HCP systems are widely separated geographically, 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.
- If an enterprise has several satellite offices, an HCP system at a central facility can consolidate data from the HCP systems at those outlying locations.

Protection types

HCP supports two types of geo-protection: *whole-object protection* and *erasure-coded protection*.

Whole-object protection

With whole-object protection, all the data for each object in a replicated namespace is maintained on each HCP system in a replication topology, except on systems where the object is on a metadata-only storage tier. In response to a client request for an object on a metadata-only storage tier on the target HCP system, HCP retrieves the object data from another system in the replication topology.

In case of system unavailability or loss, whole-object protection ensures continued data availability when at least one of the systems with the object data remains available. If an object is metadata-only on all the available systems, the object data is inaccessible.

The service plan associated with a namespace determines whether and when objects in that namespace move to a metadata-only storage tier.

Erasure-coded protection

With erasure-coded protection, 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.

For the purpose of erasure coding, parts of multipart objects are each treated as an individual object.

To implement erasure-coded protection, you create an *erasure coding topology*. An erasure coding topology is a named replication topology in which object data is protected by erasure coding. The total number of chunks for an erasure-coded object is equal to the number of systems in the erasure coding topology, where each system stores one chunk.

An erasure-coded object can be read from any system in the erasure coding topology. In response to a client read request, HCP reconstructs the object data on the fly by retrieving the chunks stored on the other systems. If any one system in an erasure coding topology is unavailable, the data for an erasure-coded object can be completely reconstructed from the chunks on the remaining systems.

If more than one system in an erasure coding topology is unavailable, HCP cannot reconstruct the erasure-coded objects. In this case, HCP marks the erasure-coded objects as unavailable or irreparable, depending on the reasons why they cannot be reconstructed.

An erasure coding topology does not necessarily include all the HCP tenants that are replicated in the underlying replication topology. You need to explicitly select the tenants to be included. You cannot include the default tenant in an erasure coding topology.

An erasure coding topology has properties that control which objects are erasure coded and when those objects are erasure coded.

Protection types for namespaces

Protection types apply to individual namespaces. Only cloud-optimized namespaces support erasure-coded protection.

When you create a replication-enabled tenant, you choose between:

- Allowing erasure-coded protection for all cloud-optimized namespaces owned by the tenant.
- Allowing the tenant administrator to allow erasure-coded protection for selected cloud-optimized namespaces.

  If the tenant administrator has granted system-level users access to the tenant, you also can allow erasure-coded protection for selected namespaces.

Objects in a replicated namespace that allows erasure-coded protection are erasure coded only if the tenant that owns the namespace is included in an erasure coding topology. If the tenant is not in an erasure coding topology, the namespace uses whole-object protection.

Objects in a replicated namespace that does not allow erasure-coded protection use whole-object protection, even if the tenant that owns the namespace is included in an erasure coding topology.

Note: Regardless of protection type, namespaces obey the DPL specified by their associated service plans. That is, on any given system:

- A namespace that uses whole-object protection maintains DPL copies of the complete data for each object
- A namespace that uses erasure-coded protection maintains DPL copies of the chunk for each object

Distribution methods for erasure-coded protection

HCP supports two distribution methods for erasure-coded protection: *chunk distribution* and *full-copy distribution*.

Chunk distribution

With chunk distribution, after an object is ingested, the chunks for the object are calculated and distributed among the systems in the erasure coding topology. Only the system where the object was ingested has a full copy of the object data.

After all of the chunks have been successfully distributed and a specified amount of time has elapsed, the HCP Geo-Distributed Erasure Coding service reduces the object on the ingest system to a chunk. The amount of time that the service waits before reducing an object to a chunk is called the *erasure coding delay*.

Full-copy distribution

With full-copy distribution, after an object is ingested, full copies of the object data are distributed to the systems in the erasure coding topology. After the erasure coding delay expires, the Geo-Distributed Erasure Coding service on each system reduces the full copy of the object data on that system to a chunk.

Metadata-only considerations for objects subject to erasure coding

For an erasure-coded object to be protected properly, each system in the erasure coding topology must have a chunk for the object. Therefore, even if the object should be metadata-only on one or more systems, those systems must each store a chunk for the object:

- With chunk distribution, each system receives a chunk for an erasure-coded object, regardless of whether the object should be metadata-only on that system.
- With full-copy distribution, each system receives a full copy of the object data unless the object should be metadata-only on that system. After the erasure coding delay expires, each system where the object should be metadata-only receives a chunk for the object, and the Geo-Distributed Erasure Coding service on each system with a full copy of the object data reduces that full copy to a chunk.

Object counts

An HCP system keeps track of the total number of objects stored on it and, separately, the number of erasure-coded objects stored on it:

- The total number of objects stored on a system includes whole objects, metadata-only objects, and objects that are subject to erasure coding, regardless of whether the system currently has a full copy of the object data or a chunk for the object.
- The number of erasure-coded objects stored on a system includes only objects for which the system currently has a chunk.

HCP also tracks both of these object counts by tenant and namespace. You can view system-level and tenant-level object counts in the System Management Console, through the management API, and in system-level chargeback reports. For tenants to which you have administrative access, you can also view namespace-level object counts through the management API and in chargeback reports.

Tenant administrators can view total object counts for the applicable tenant and its namespaces in the Tenant Management Console, through the management API, and in tenant-level chargeback reports. Tenant administrators cannot see counts of erasure-coded objects.

Choosing a protection type

The two protection types, whole-object protection and erasure-coded protection, each have their own benefits and limitations. The following sections describe factors you should consider when choosing the protection type for a namespace.

Storage efficiency

With whole-object protection, all the data for an object in a replicated namespace is stored on each system that has that namespace, except on systems where the object is on a metadata-only storage tier. This means that the total storage used for the object data is at most the size of the data times the number of systems in the replication topology. (The storage used can be less due to compression/encryption, duplicate elimination, and metadata-only storage tiers.)

Note: This discussion assumes a data protection level (DPL) of one. As the DPL increases, the amount of storage needed to store the data for an object also increases, regardless of the protection type.

For example, in a three-system replication topology in which the object is not metadata-only on any system, the storage used for a 1 MB object is, at most, 3 MB. Having the object be metadata-only on one or two of the systems increases storage efficiency but decreases the level of data protection.

With erasure-coded protection, each system in the erasure coding topology 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.

For example, each object in an erasure coding topology with three systems has two data chunks and one parity chunk, so the size of each chunk of a one-megabyte object is .5 MB. As a result, the total storage used for the object is, at most, 3 × 0.5 MB, which is 1.5 MB.

The greater the number of systems in an erasure coding topology, the greater the storage efficiency. The maximum number of systems that can be in an erasure coding topology is six. With six systems, the total storage used for a one-megabyte object is, at most, 1.2 megabytes.

Data availability

Whole-object protection can provide better protection from system unavailability than erasure-coded protection provides. With whole-object protection, clients can access objects in a replicated namespace if at least one of the systems where the object data is stored is available. (HCP does not store data for objects on metadata-only storage tiers.)

With erasure-coded protection, all but one of the systems in the erasure coding topology must be available for clients to access objects in a namespace that's replicated on those systems.

Disaster recovery

Both whole-object protection and erasure-coded protection provide support for disaster recovery in case of catastrophic system failure. Disaster recovery entails reprotecting objects in replicated namespaces to their prefailure protection level by recovering them to a replacement system.

With whole-object protection, if a single system fails, the object data can be recovered to the replacement system from any remaining system where the replicated objects are not metadata-only. If two or more systems fail concurrently, whole-object protection can still provide support for disaster recovery. However, as the level of protection increases, the number of systems that must store the complete object data also increases, thereby decreasing storage efficiency.

With erasure-coded protection, if a single system fails, object data can be reconstructed on the replacement system from the chunks on all the remaining systems in the erasure coding topology. If two or more systems fail concurrently, object data cannot be reconstructed and may be permanently lost.

Read performance

With whole-object protection, a client read request for a replicated object results in a single read operation when the request is issued against a system that has the object data. If the object is metadata-only on the target system, that system must retrieve the object data from another system in the replication topology, which may increase the response time.

With erasure-coded protection, a client read request for a single erasure-coded object causes the system that's servicing the request to reconstruct the object from multiple chunks. Only one of those chunks is stored on that system. Therefore, a client read request for an erasure-coded object results in multiple read operations. These operations can be concurrent or sequential, depending on the replication topology on which the erasure coding topology is based. If sequential reads are required, the response time may be longer than if all the reads are concurrent.

Rehydration with whole-object protection and restore periods with erasure-coded protection can decrease read response times.

These considerations apply to choosing a protection type for a replicated namespace when read performance is a factor:

- If objects are likely to be read frequently throughout their lifespans and read performance is more important than storage efficiency, consider using whole-object protection for the namespace.
- If objects are unlikely to be read and storage efficiency is important, consider using erasure-coded protection for the namespace.
- If objects are likely to be read only for a limited amount of time in the short term and read performance is important, consider using erasure-coded protection with an erasure coding delay that's equal to or greater than the amount of time objects will be read for.
- If objects are likely to be read frequently but only for limited periods throughout their lifespans and read performance is important, consider using erasure-coded protection with a restore period. With a restore period, after an object is read, a full copy of the object data is placed on the ingest tier for the containing namespace and is kept there for a configured amount of time.

  The ingest tier for a namespace is the storage tier where objects in the namespace are stored when the object data is first written to HCP. The ingest tier is determined by the service plan currently associated with the namespace.

Network bandwidth usage

For namespaces that use whole-object protection, replication entails sending the complete data for an object to each system in the replication topology, except to systems where the object should be metadata-only. Similarly, for namespaces that use erasure-coded protection with full-copy distribution, the complete object data is sent to each system in the erasure coding topology, except to systems where the object should be metadata-only.

For namespaces that use erasure-coded protection with chunk distribution, only object chunks are sent throughout the erasure coding topology. As a result, replication with this type of protection typically requires less network bandwidth than is required for whole-object protection and for erasure-coded protection with full-copy distribution.

On the other hand, with whole-object protection, a client read request against a system that has the object data results in a single data transfer operation. With erasure-coded protection, a client read request results in at least one data transfer operation for each required chunk that's not on the target system in addition to the data transfer operation between the system servicing the request and the client. Therefore, read requests with erasure-coded protection typically use more network bandwidth than is used for read requests with whole-object protection.

Additionally, the chunks for erasure-coded objects are transferred between systems on the replication network. Because servicing read requests takes precedence over replication processing, while any replicated namespaces are experiencing a high read rate, replication may be slow.

Rehydration with whole-object protection and restore periods with erasure-coded protection can affect network bandwidth usage for read operations.

PUT copy operations

For a PUT copy operation where the source object is erasure coded, the new object must be reconstructed from the chunks for the source object. For a large object, this reconstruction can take a long time, increasing the potential for the PUT copy operation to time out.

If large objects in a replicated namespace are likely to be sources for PUT copy operations, whole-object protection may be a better choice for the namespace than erasure-coded protection.

How replication works

To enable replication between two HCP systems, you create a *replication link* between the two systems. A replication link is a secure, trusted relationship between two systems. The link determines what is replicated and how data is transmitted between the systems.

Link types

A replication link can be active/active or active/passive:

- With an *active/active* link, the HCP tenants and namespaces and default-namespace directories being replicated are read-write on both systems, and data is replicated in both directions between the two systems. Active/active links are designed for use in environments where applications need seamless access to namespaces regardless of

where those applications are located. All links in an erasure coding topology must be active/active links.

With an active/active link, HCP gives preference to synchronizing object metadata between the two systems, followed by data synchronization. This preferential treatment enables the fastest access to objects regardless of which system they were created on. If a full copy of the data for an object or a chunk for the object has not yet been replicated to the system targeted by a client request, HCP can read all the object data from a remote system. Additionally, synchronizing metadata first ensures that object names are reserved as quickly as possible.

Note: Until a full copy of the data for an object or a chunk for the object is replicated to a given system, the object is metadata-only on that system.

- With an *active/passive link*, the HCP tenants and namespaces and default-namespace directories being replicated are read-write on one system, called the *primary system*, and read-only on the other system, called the *replica*. In this case, data is replicated in one direction only: from the primary system to the replica. Active/passive links are designed to support read-only content sharing and disaster recovery.

  With an active/passive link, HCP replicates object data and metadata together, thereby ensuring that objects are complete on the replica and can be recovered should that become necessary. However, this approach means that the replica cannot service requests for an object until that object is fully replicated.

To a primary system, an active/passive link is an *outbound link*; that is, the system is sending data through the link. To a replica, an active/passive link is an *inbound link*; that is, the system is receiving data through the link. To both systems involved in an active/active link, the link functions as both an outbound link and an inbound link.

Link security

Replication relies on SSL to ensure the integrity and security of transmitted data. Before you can create a replication link, the two systems involved in the link must each have a valid SSL server certificate. Each system must also have the server certificate from the other system installed as a *trusted replication server certificate*.

Replication priority

Replication is asynchronous with object ingest. An HCP system can, therefore, develop a backlog of objects to be replicated.

You can choose to have the Replication service work on objects with the oldest changes first, regardless of which namespaces they're in. Alternatively, you can have the service balance its processing time evenly across the namespaces being replicated. In this case, the service may replicate recent changes in some namespaces before older changes in others.

What is replicated?

Replication works by tenant. For each replication link, you can select HCP tenants to be replicated on that link. If you have administrative access to the tenant, you can also select the namespaces to include in replication of that tenant. To replicate the default tenant, you select the default-namespace directories to be replicated.

Regardless of the system on which you create the link:

- For an active/active link, you can select items to be replicated from both systems involved in the link
- For an active/passive link, you can select items to be replicated only from the primary system

You can select the HCP tenants to include in an erasure coding topology from any system in the topology. Each tenant you select is automatically added to every link in the underlying replication topology. You cannot include the default tenant in an erasure coding topology.

What is replicated for each tenant differs between HCP tenants and the default tenant.

Replication of HCP tenants

When creating a tenant, you specify whether it can be replicated. After creating the tenant, you can change this setting from not allowing replication to allowing replication. You cannot do the reverse.

A replication link or erasure coding topology can include only HCP tenants that are configured to allow replication.

Replicated tenants and namespaces

When an HCP tenant is replicated, the Replication service works only on selected namespaces owned by that tenant. The tenant administrator can select and deselect namespaces for replication at any time. If the tenant is being replicated, the tenant and its selected namespaces are replicated on each link that includes the tenant. If the tenant is not being replicated, the selected namespaces are not replicated either.

If an HCP tenant has granted system-level users administrative access to itself, you can select and deselect its namespaces for replication when you create the replication link or by modifying the link at a later time. You should coordinate namespace selection with the tenant administrator to ensure that you both have the same understanding of what should be replicated.

Tenants can be replicated from one HCP system to another regardless of the number of tenants that already exist on the other system. However, you can create a new tenant on a system only if the total number of tenants on the system is less than 1,000.

Similarly, namespaces can be replicated from one HCP system to another regardless of the number of namespaces that already exist on the other system. However, you can create a new namespace on a system only if the total number of namespaces on the system is less than ten thousand.

HCP tenants created on different systems can have the same names as each other. However, every tenant has a unique internal ID, so HCP can distinguish tenants with the same name from one another. You cannot replicate a tenant from one system to another if the second system has a different tenant with the same name. To replicate the tenant in this case, you first need to change the name of the tenant on one of those systems.

Replicated items

The Replication service replicates these items for an HCP tenant:

- The tenant configuration
- The configuration of each namespace being replicated
- Existing objects, object creations, object deletions, and metadata changes in the namespaces being replicated
- Old versions of objects in the namespaces being replicated
- Retention class creations, modifications, and deletions for the namespaces being replicated
- Content class and content property creations, modifications, and deletions
- All tenant-level log messages
- All namespace-level log messages for the namespaces that are being replicated
- User accounts defined for the tenant
- Group accounts defined for the tenant

Replicated changes

With an active/active link, replicated HCP tenants are read-write on both systems involved in the link. Administrators can make changes to the configuration of the replicated tenants and namespaces on either system, and users and applications can make changes to the content of the replicated namespaces on either system. All changes made on each system are replicated to the other system.

With an active/passive link, replicated HCP tenants are read-write on the primary system and read-only on the replica. Administrators cannot make any configuration changes to the replicated tenants or to any of their namespaces on the replica, nor can users and applications make any changes to the content of the replicated namespaces on the replica. However, all changes made on the primary system are replicated to the replica.

Note: Although you cannot make any changes to the configuration of a replicated namespace on a replica, you can reindex the namespace.

Replication of the default tenant

For the default tenant, the Replication service works on one or more selected directories directly under `fcfs_data` in the default namespace. The service replicates the entire directory hierarchy under each selected directory.

Default namespace properties

Directories in the default namespace on one system involved in a replication link can be replicated only to the default namespace on the other system involved in the link. They cannot be replicated to HCP namespaces.

Additionally:

- Before you can include any default-namespace directories in a replication link, the default namespace must exist on both systems involved in the link.
- The default namespaces in the two systems must have the same cryptographic hash algorithm and retention mode.

The default namespace can be configured to prevent writes and deletes. This configuration can differ between the default namespace on the two systems involved in a link. However, even if the system receiving data is configured to prevent these actions, changes to namespace content on the sending system are replicated.

Replicated directories

You select directories for replication when you create the replication link. You can select additional directories or deselect directories by modifying the link at a later time. A replication link can include, at most, 256 directories.

Directories can be created in the default namespace on both of the systems involved in a replication link, so the two systems can have directories with the same name. You cannot replicate a directory created on one of the systems if a locally created directory with the same name already exists on the other system.

The one exception to this is the directory used for email archiving through SMTP. You can replicate the email directory if the email directory name is the same on both systems.

Replicated changes

With an active/active link, replicated directories are read-write on both systems involved in the link. All changes made to the content of those directories on either system are replicated to the other system.

With an active/passive link, the replicated directories are read-write on the primary system and read-only on the replica. Users and applications cannot make any changes to the content of the replicated directories on the replica. However, all changes made on the primary system are replicated to the replica.

Replicated items

The Replication service replicates these items for the default tenant:

- Existing objects, object creations, object deletions, and metadata changes in the directories being replicated
- Retention class creations, modifications, and deletions for the default namespace
- Content class and content property creations, modifications, and deletions
- All log messages relating to retention classes and privileged delete operations

Replication service processing

With an active/active link, the Replication service runs on both HCP systems involved in the link. With an active/passive link, the Replication service runs only on the primary system.

Each replication link has a schedule that specifies when the Replication service should run. By default, when you create a link, the link schedule has the service running 24 hours a day, seven days a week.

The Replication service starts sending information on a link the first time you add HCP tenants and/or default-namespace directories to that link, as long as the link schedule has the service running at that time. If the service is not scheduled to run at that time, the service starts sending information as soon as the next scheduled run period starts.

Configuration information first

When you first add HCP tenants, namespaces, and/or default-namespace directories to a replication link, the Replication service replicates the configuration of those items as soon as possible. The service then starts replicating objects in those namespaces and default-namespace directories. The service replicates objects in chronological order either across all namespaces or within each namespace in turn, depending on the link configuration. The chronological order is oldest-first based on the time of the last metadata change to the object.

Whenever you add a new item to a replication link or change the configuration of an item already included on the link, the Replication service replicates the configuration of the new item or the configuration change as soon as possible. This ensures the correct behavior of objects on the receiving system.

Whole-object protection with unavailable systems

With whole object protection, the Replication service on the system where an object is ingested sends a full copy of the data for the object to the available systems to which the ingest system is directly connected by a replication link and on which the object is not supposed to be metadata-only. If a system is unavailable, the Replication service sends the full copy of the object data to that system when the system becomes available.

Chunk distribution with unavailable systems

For erasure-coded protection with chunk distribution, the Replication service on the system where an object is ingested sends a chunk for the object to each available system in the erasure coding topology. When an unavailable system becomes available, the Replication service on the ingest system sends a chunk to that system. After all the systems that were

unavailable have chunks and the erasure coding delay has expired, the Geo-distributed Erasure Coding service reduces the full copy of the object data on the ingest system to a chunk.

A system in an erasure coding topology can suffer a catastrophic failure after ingesting data while another system in the topology is unavailable. If this happens with a topology that's configured for chunk distribution, the data that was ingested on the failed system while the other system was unavailable is lost.

To minimize the risk of data loss, if an erasure coding topology is configured for chunk distribution:

- Any upgrade of a system in the topology should be performed while the system is online
- Planned system unavailability (due, for example, to a system shutdown for maintenance or to a loss of connectivity during a network upgrade) should be scheduled for times when data ingest is at a minimum

Tip: To protect newly ingested objects during a period of planned system unavailability, take these actions before making the system unavailable:

1. For each namespace that's owned by a tenant included in the erasure coding topology and that allows erasure coding, ensure that the service plan associated with that namespace does not include a metadata-only storage tier on at least two of the systems that will remain available. If an applicable service plan includes a metadata-only storage tier, you can temporarily either modify the service plan or associate the namespace with a different service plan.
2. Disable the erasure coding service.
3. Reconfigure the erasure coding topology to use full-copy distribution.

After making the system available again:

1. Reconfigure the erasure coding topology to use chunk distribution.
2. Enable the erasure coding service.

Full-copy distribution with unavailable systems

For erasure-coded protection with full-copy distribution, when an object is ingested, each available system in the erasure coding topology, except systems where the object should be metadata-only storage tier, receives a full-copy of the object data. When an unavailable system becomes available:

- If the erasure coding delay has not expired and the object is not supposed to be metadata-only, the system receives a full copy of the object data. If the object should be metadata-only, the system does not receive either a full copy or a chunk.

  After all the systems in the topology are available, when the erasure coding delay expires, each system where the object should be metadata-only receives a chunk for the object, and all full copies of the object data are reduced to chunks.

- If the erasure coding delay has expired, the system receives a chunk for the object regardless of whether the object should be metadata-only. After all the systems in the topology are available, full copies of the object data are reduced to chunks.

Geo-Distributed Erasure Coding service processing

The Geo-Distributed Erasure Coding service is responsible for ensuring that objects that are or have ever been subject to erasure coding are in the correct state at any given time.

On any given HCP system, the Geo-Distributed Erasure Coding service runs according to a system-specific schedule. Therefore, the service is not necessarily running at the same time on any set of systems. However, the service on one system can query other HCP systems for the state of the objects on those systems even when the service is not running on those systems.

While running, the Geo-Distributed Erasure Coding service examines each object individually. If the system in which the service is running has a full copy of the data for an object and should not, the service reduces the data to a chunk. If the system has a chunk for the object and should not, the service restores the chunk to a full copy. If the object is in the state it should be in, the service takes no action on the object.

To have sufficient information to restore a chunk for an object to a full copy of the object data, the Geo-Distributed Erasure Coding service can ask other systems to send the chunks they have for that object. Alternatively, if any of those systems has a full copy of the object data, the service can ask for the full copy.

During a scheduled run time, the Geo-Distributed Erasure Coding service actually runs only if the system is part of an active erasure coding topology or if the system contains erasure-coded objects. An active erasure coding topology is one that is currently being used for geo-protection. A system can participate in only one active erasure coding topology.

If the Geo-Distributed Erasure Coding service doesn't have sufficient run time on a system that's receiving full copies of object data, those full copies may not be reduced to chunks in a timely manner. When scheduling the service, keep in mind that full copies of object data use the full storage required by the object data until they are reduced to chunks.

The Geo-Distributed Erasure Coding service cannot restore a chunk for an object to a full copy of the object data if the system where the service is running doesn't have enough space for the complete object data. In this case, the service leaves the chunk on the system as is.

Note: The Geo-Distributed Erasure Coding service is automatically added to the HCP Default Schedule service schedule when HCP is upgraded to release 8.x from a release earlier than 8.0. You need to schedule the service yourself in any user-created service schedules in which you want the service to have run time.

Determining what the state of an object should be

Several factors determine whether a system should have a chunk or a full copy of the data for a given object:

1. First, the Geo-Distributed Erasure Coding service on the system must determine whether the namespace containing the object has erasure coding allowed.
2. Then, if erasure coding is allowed, the service must determine whether the tenant that owns the namespace is currently included in an active erasure coding topology.
3. Finally, if the tenant is included in an active erasure coding topology, the service must determine:
   - What the state of the object should be with respect to these properties of the erasure coding topology: distribution method, erasure coding delay, restore period, and minimum size for erasure coding.
   - What the state of the object is on the other systems in the erasure coding topology.

Keeping objects sufficiently protected

An object that is subject to erasure coding:

- Is sufficiently protected as long as all the systems in the erasure coding topology are available or as long as at least two systems in the topology have a full copy of the object data
- Is insufficiently protected if the object would become unavailable due to a system in the erasure coding topology becoming unavailable

The Geo-Distributed Erasure Coding service never reduces a full copy of the data for an object to a chunk if doing so would cause the object to be insufficiently protected.

Namespace configuration changes

Erasure coding can be disallowed for a namespace that previously had erasure coding allowed. Similarly, replication can be disabled for a namespace that was previously selected for replication.

If erasure coding is disallowed or replication is disabled for a namespace that contains erasure-coded objects, the Geo-Distributed Erasure Coding service on each system that contains those objects is responsible for:

- Restoring the chunks for the objects to full copies of the object data on HCP systems where the object is not supposed to be metadata-only. The service can restore the object data as long as no more than one system in the erasure coding topology is unavailable or at least one system in the topology has a full copy of the object data.
- Deleting chunks for the objects on HCP systems where the object should be metadata-only.

Before disallowing erasure coding or disabling replication for a namespace that contains erasure-coded objects, you need to ensure that each system where the chunks for the objects will be restored to full copies of the object data has sufficient storage to accommodate that data.

Replication Verification service processing

The HCP **Replication Verification service** is responsible for checking whether the Replication service missed replicating or was unable to replicate any objects that should have been replicated. If the Replication Verification service encounters such an object, the service tries to replicate the object.

If either the Replication service or the Replication Verification service encounters an object it cannot replicate, the service marks the object as nonreplicating. If the Replication Verification service replicates a nonreplicating object, the service removes the nonreplicating mark from the object.

The Replication Verification service is not a scheduled service. The service runs only when you:

- Set the service to run continuously while the Replication service is running.
- Set the service to run once. In this case, if the Replication service is running, the Replication Verification service starts immediately. Otherwise, the Replication Verification service waits to start until the next time the Replication service runs.

You can also disable the service so that it doesn't run at all.

While running, the Replication Verification service may degrade HCP system performance. Normally, you run the service only when directed to do so by your authorized HCP service provider.

The Overview panel for a replication link indicates whether any tenants on the link have namespaces with nonreplicating objects.

Tenant administrators can view the list of nonreplicating objects in a namespace in the Tenant Management Console.

Unavailable and irreparable erasure-coded objects

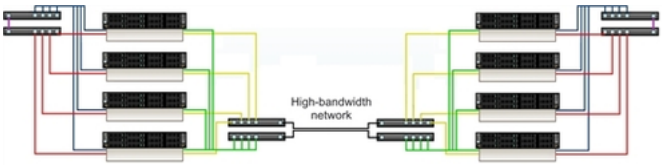
The status of an erasure-coded object can differ among the systems in an erasure coding topology:

- An erasure-coded object is unavailable on a system if all of these are true:
  - One or more systems in the erasure coding topology are inaccessible. The object data cannot be reconstructed from the available chunks.
  - No accessible system has a good full copy of the object data.
- An erasure-coded object is irreparable on a system if all of these are true:
  - All systems in the erasure coding topology are accessible.
  - The object data cannot be reconstructed from the available chunks.
  - No system in the topology has a good full copy of the object data.

Replicated systems

Replication on each link in a replication topology occurs between two separate HCP systems, each of which is complete in its own right. Because replication is a software function, the two systems can have entirely different hardware configurations, including differing amounts of storage.

The two systems in a replicated pair are connected through the front-end network infrastructure, as shown in the following figure. Replication traffic from each system must be routable to the network selected for replication on the other system.



Replication is a network bandwidth-intensive process. To ensure sufficient front-end network capacity when replicating, you must give extra consideration to planning the front-end infrastructure.

Replication and Active Directory authentication

An HCP system can be configured to support Windows® Active Directory® (AD) for user authentication. Part of this configuration is the specification of an AD domain. The domain determines the AD groups from which HCP group accounts can be created.

If HCP is configured to support AD, HCP tenants can be configured to allow access by users authenticated by AD. For this access to work, the AD user must belong to one or more AD groups for which corresponding group accounts are defined for the tenant.

For the same AD users to be able to access a given tenant on both systems involved in a replication link, the group accounts on each system must correspond to the same AD groups as they do on the other system. To make this happen, support for AD must be enabled on both systems, and either of these must be true:

- The same domain is specified in the AD configuration on both systems.
- The domain specified in the AD configuration on one system is trusted by the domain specified in the AD configuration on the other system.

Similarly, for the same AD users to be able to access the default namespace on two systems involved in a replication link, the system-level group accounts on each system must correspond to the same AD groups as they do on the other system.

Replication and RADIUS authentication

An HCP system can be configured to support RADIUS for user authentication. If HCP is configured this way, HCP tenants can be configured to allow access by RADIUS-authenticated users. Also, if HCP is configured this way, RADIUS-authenticated users with system-level user accounts can access the default namespace.

For the same RADIUS-authenticated users to have access to both systems involved in a replication link, the HCP RADIUS configuration on the two systems must specify the same RADIUS servers.

Replication topologies

An HCP system can have up to five outbound links and up to 20 inbound links. An active/active link counts as both an outbound link and an inbound link. The ability for a single system to participate in multiple links enables HCP to support various replication topologies.

Replication can occur:

- In two directions on a single link between two HCP systems (active/active replication)
- In one direction on a single link between two HCP systems (active/passive replication)
- From multiple HCP systems to a single HCP system (many-to-one replication)
- From one HCP system to a second HCP system and from that second system to a third HCP system, such that the same HCP tenants and namespaces and default-namespace directories that are replicated to the second system are then replicated to the third system (chained replication)
- From one HCP system to multiple other HCP systems (one-to-many replication)

These configurations can be combined to form complex replication topologies.

Note: A replication topology can include one or more HCP systems where the occurrences of a given namespace can contain metadata-only objects. If the service plan associated with the namespace does not include a metadata-only storage tier on only one system in the topology and the topology is being used for production purposes, the topology should include a disaster recovery system where the service plan associated with the namespace also does not include a metadata-only storage tier.

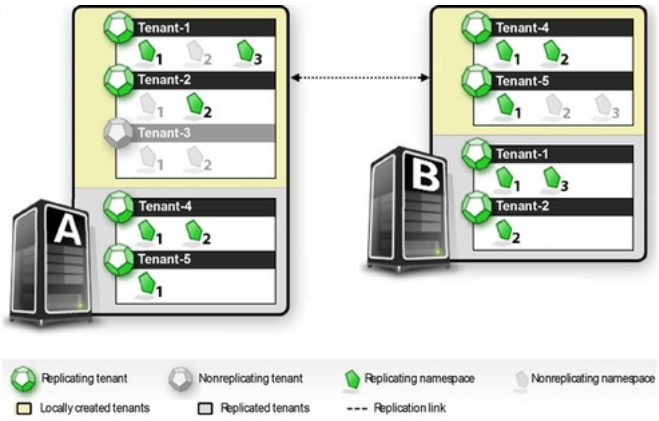
Simple active/active replication

In an *simple active/active replication topology*, two HCP systems replicate the same HCP tenants and namespaces and default-namespace directories to each other over an active/active link. The items being replicated can be created originally on either system. The items are read-write on the system in which they were created and, after being replicated, are also read-write on the other system.

With active/active replication, client requests can be directed to either system. All changes made on each system, including both configuration changes and changes to namespace content, are replicated to the other system.

What this looks like

The following figure shows a simple active/active replication topology in which two HCP systems (A and B) are replicating to each other.



In this figure:

- Two of three HCP tenants created locally in system A are being replicated between system A and system B. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- Two tenants created locally in system B are being replicated between system A and system B. In the first tenant, two namespaces are selected for replication. In the second tenant, one of three namespaces is selected for replication.

Uses

The active/active replication topology supports a cloud storage model, where any type of client request can be serviced equally by either HCP system involved in the replication link. With this topology, if one system becomes unavailable (for example, either unexpectedly or for scheduled maintenance), the other system can still provide all the required functionality.

With an active/active replication topology, the processing load can be distributed between the two systems. This distribution can be accomplished in two ways:

- By having some applications direct requests to one system and other applications direct requests to the other system. Typically, the assignment of applications to systems is based on geographic location.

  With this configuration, a single shared DNS can enable requests to be redirected automatically from one system to the other in case one of the systems becomes unavailable.

- By using a load balancer to divide requests between the two systems. For each client request, the decision as to which system to target can be based on several factors, such as the current load on each system and the geographical distance between the client and each system.

With this configuration, if one system becomes unavailable, the load balancer simply directs all requests to the other system.

Active/active replication ring

In an active/active replication ring topology, four or more HCP systems are connected by active/active links, where:

- Each system has exactly two active/active links that connect that system to two other systems in such a way that all the systems are linked in the form of a ring
- The same HCP tenants and namespaces and default-namespace directories are replicated on each link

With an active/active replication ring topology, changes made on one system travel around the ring in both directions from that system until they reach a system where those changes have already occurred.

Configuring an active/active replication ring

To configure an active/active replication ring topology:

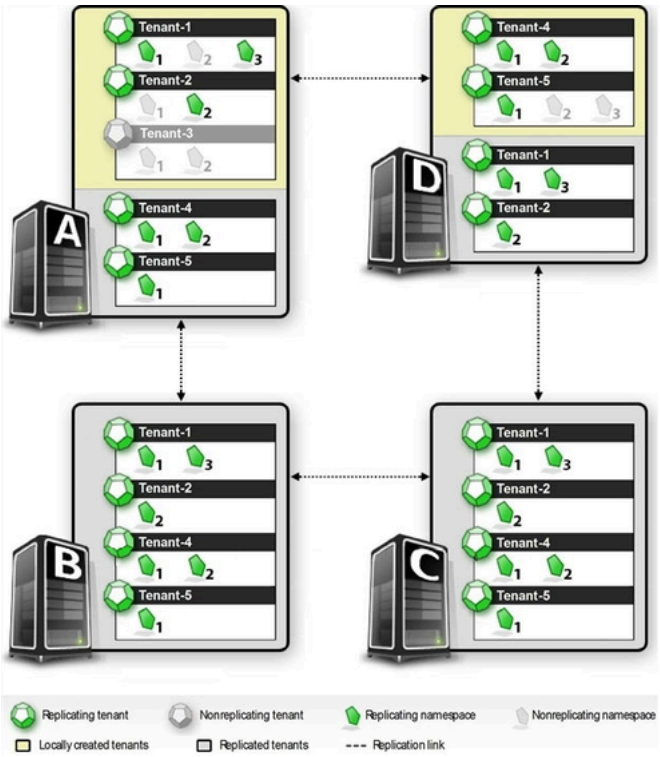
1. Create an active/active link between each pair of systems to be connected in the ring.
2. For each system that has locally created tenants, namespaces, and directories that you want to replicate, add those items to one of the links connected to that system.
3. After those tenants, namespaces, and directories have been replicated, add them to the second link that's connected to the system to which the items have been replicated.
4. After the items have been replicated to that system, add them to the next link in the ring.
5. Continue adding the replicated items to successive links until you have added them to the second link that connects to the system where the items were originally created.

Active/active replication ring topology

An active/active replication ring topology that includes four, five, or six HCP systems can be used as the basis for an erasure coding topology. When you add a tenant to the erasure coding topology, if the tenant is not already being replicated in the ring topology, HCP automatically adds that tenant to all the links in the ring topology.

What this looks like

The following figure below shows an active/active replication ring topology that includes four systems (A, B, C, and D).



In this figure:

•Two of three HCP tenants created locally in system A are being replicated around the ring. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.

•Two tenants created locally in system D are being replicated around the ring. In the first tenant, two namespaces are selected for replication. In the second tenant, one of three namespaces is selected for replication.

Using active/active replication ring topology

The active/active replication ring topology supports increasingly large storage clouds. The HCP systems included in the ring are typically in geographically disperse locations, with each system providing the same functionality as all the others. Changes made on any one system are propagated to all the other systems, effectively enabling shared read-write access to the same HCP tenants and namespaces and default-namespace directories regardless of where the client applications are located.

New HCP systems can be added to an active/active replication ring topology at any time. To add a new system (for example, system X) to the topology:

1. Create a new active/active link between any system already in the topology (for example, system B) and system X.
2. Add the tenants, namespaces, and directories already being replicated around the ring to the new link.
3. Create a new link between system X and one of the other systems with which system B participates in a link (for example, system C).
4. Add the tenants, namespaces, and directories already being replicated around the ring to that new link.

5. Delete the link between system B and system C.

Fully connected active/active replication

In a fully connected active/active replication topology, multiple HCP systems are connected by active/active links, where:

- Each system in the topology is connected to each other system in the topology by an active/active link
- The same HCP tenants and namespaces and default-namespace directories are replicated on each link

Because each system can participate in at most five active/active links, a fully connected active/active replication topology can have up to six systems.

Configuring a fully connected active/active replication topology

To configure a fully connected active/active replication topology:

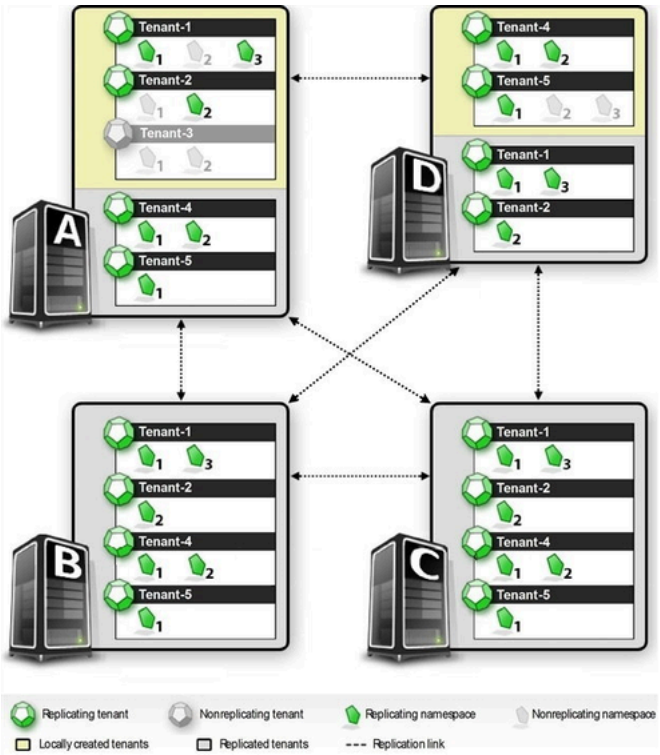
1. Create an active/active link between each pair of systems to be included in the topology.
2. For each system that has locally created tenants, namespaces, and directories you want to replicate, add those items to each of the links connected to that system.
3. After those tenants, namespaces, and directories have been replicated, add them to each of the other links in the topology.

Fully connected active/active replication topology as erasure coding topology

A fully connected active/active replication topology can be used as the basis for an erasure coding topology. When you add a tenant to the erasure coding topology, if the tenant is not already being replicated on the links in the fully connected active/active topology, HCP automatically adds that tenant to all the links in the fully connected active/active topology.

What this looks like

The following figure shows a fully connected active/active replication topology that includes four systems (A, B, C, and D).



In this figure:

- Two of three HCP tenants created locally in system A are being replicated throughout the topology. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- Two tenants created locally in system D are being replicated throughout the topology. In the first tenant, two namespaces are selected for replication. In the second tenant, one of three namespaces is selected for replication.

Uses

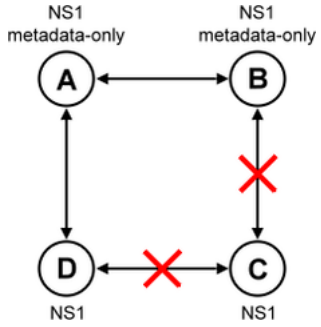
The fully connected active/active replication topology is an alternative to the active/active ring topology for maintaining the same namespaces on multiple HCP systems in a storage cloud.

A fully connected topology provides better protection from system unavailability and nonfunctioning replication links than a ring topology provides. The network of links in a fully connected topology ensures that each system has multiple paths to each other system, thereby preventing individual systems from becoming isolated from the rest.

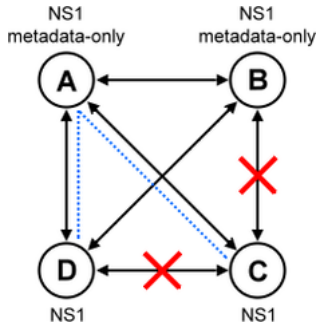
For example, suppose that the following conditions are true:

- Namespace NS1 is being replicated in a replication topology that includes systems A, B, C, and D
- The service plan associated with NS1 includes a metadata-only storage tier on A and B
- Object O1 is metadata-only on both A and B

With a ring topology, if the replication links between B and C and between C and D are broken, system C is isolated. Because no path connects system D to system C, system D cannot retrieve data for O1 from the only other system that has the data (for example, in a situation in which read from remote is required).



Given the same circumstances with a fully connected topology, system D can still read data for O1 from system C by using the links between D and A and between A and C.



A fully connected topology requires more maintenance than a ring topology. In the worst case, with six systems in a fully connected topology, you must maintain 15 replication links. With six systems in a ring topology, you need to maintain only six links.

Additionally, the more systems you have in a fully connected topology, the less the ability to replicate other tenants to systems outside the topology. For example, in a five-system fully connected topology, any system could have one additional link on which to replicate tenants that are not in the topology to a system outside the topology. In a six-system fully connected topology, the systems cannot have any additional links.

A typical use for a fully connected active/active replication topology is as the basis for an erasure coding topology.

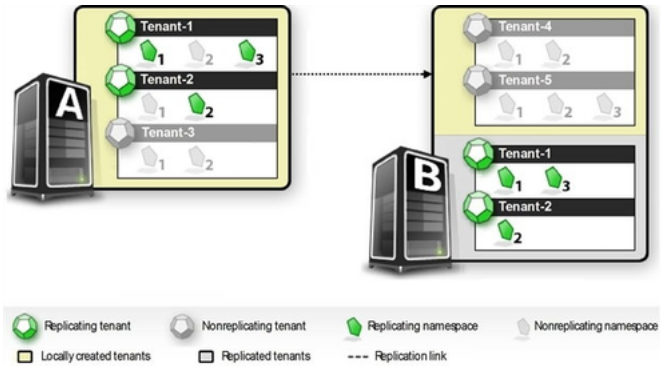
Responses to read requests for erasure-coded objects are faster with a fully connected topology than with a ring topology because all chunks not on the target system can be retrieved from directly connected systems. In comparison, with an erasure coding topology based on a ring replication topology, responses to read requests are slower because some chunks can be retrieved only through paths consisting of more than one replication link. Also, the use of the additional links increases network bandwidth usage.

Simple active/passive replication

In a *simple active/passive replication topology*, one HCP system, the primary system, replicates HCP tenants and namespaces and default-namespace directories to another HCP system, the replica, over an active/passive link. The items being replicated are originally created only in the primary system. The items are read-write on the primary system and, after being replicated, read-only on the replica.

What this looks like

The figure below shows a simple active/passive replication topology in which one HCP system (A) is replicating to a second HCP system (B).



In this figure:

- From system A, two of three locally created tenants are being replicated to system B. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- In system B, no locally created tenants are being replicated.

Uses

The main purpose of a simple active/passive replication topology is to have a backup of the primary system for use in disaster recovery. However, this topology also supports a scenario in which some applications need read-write access to the replicated items while other applications need only read access. By directing requests from the latter to the replica, you can reduce the load on the primary system.

Active/passive many-to-one replication

In an *active/passive many-to-one replication topology*, multiple HCP systems replicate to a single other HCP system. Each of the replicating systems is the primary system for an active/passive replication link. The other system is the replica for each of those links.

In this topology, the replica is like a hub, with the primary systems being at the ends of spokes connected to that hub. The spokes themselves are the replication links. The hub can have up to five spokes.

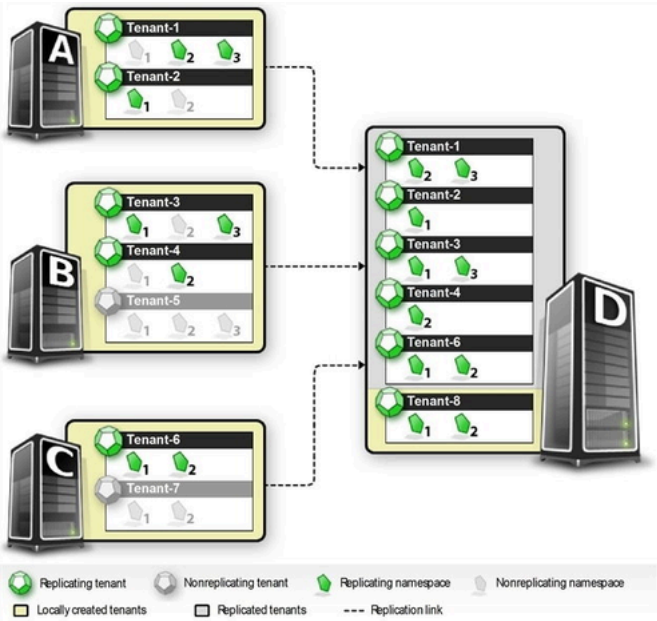
Each HCP tenant and default-namespace directory selected for replication on a primary system must be unique on the replica. For example, if two of the primary systems each have a tenant named Finance, the Finance tenant can be replicated from only one of the systems. For both tenants to be replicated, they must have different names.

Similarly, before you can have an email directory in the default namespace on multiple primary systems replicated, the SMTP protocol on each system must specify a different email directory name.

Note: You can also create a many-to-one replication topology that consists of a combination of active/passive and active/active links or even active/active links only.

What this looks like

The figure below shows an active/passive many-to-one replication topology in which three primary systems (A, B, and C) are replicating to a single replica (D).



In this figure:

- From system A, two HCP tenants are being replicated to system D. In the first tenant, two of three namespaces are selected for replication. In the second tenant, one of two namespaces is selected for replication.
- From system B, two of three HCP tenants are being replicated to system D. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- From system C, one of two HCP tenants is being replicated to system D. In that tenant, both namespaces are selected for replication.
- System D has one HCP tenant of its own that is not the result of replication. This tenant has two namespaces.

Uses

In an active/passive many-to-one replication topology, the replica is typically the largest HCP system. The data center in which it resides is usually fully staffed with IT personnel. The primary systems typically are smaller. Because replication links can be created and managed from either side, the data centers where these systems reside can be minimally staffed with less experienced people.

Active/passive many-to-one replication supports a scenario in which the outlying sites are branch offices of an enterprise that has an HCP system at a primary data center. Applications running at each of those offices connect over a local area network (LAN) to an HCP system at the local data center. Because they are close to the storage they use, the applications perform better than they would if they were using a wide area network (WAN) to connect to the HCP system at the hub. Also, the distribution of the network load among the outlying sites further enhances application performance.

With active/passive many-to-one replication, you can consolidate similar data from multiple sources in a single HCP system. Using a search application, you can then perform federated queries across the replicated namespaces on that system. For example, suppose each of the branch offices of an enterprise stores completed orders in a namespace in its own HCP system. If each of those namespaces is replicated to a single HCP system, you could query that system to find all orders placed for a specific product at any of the branch offices.

Active/passive many-to-one replication enables a single HCP system to be used for backup and recovery of multiple other HCP systems, so the outlying sites don’t need backup systems of their own. For additional data protection, the hub system can be backed up, for example, to tape or to another HCP system .

Active/passive chained replication

In an *active/passive chained replication topology*, HCP tenants and namespaces and default-namespace directories in one HCP system (A) are replicated to a second HCP system (B) and then from the second system to a third HCP system (C). Both the replication link from A to B and the replication link from B to C are active/passive links.

Configuring an active/passive chained replication

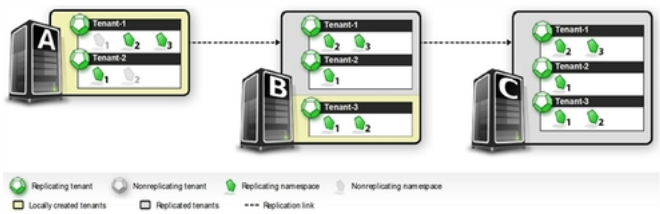
To configure an active/passive chained replication topology:

1. When you create the replication link from A to B, select the tenants, namespaces, and directories you want to replicate. In this link, A is the primary system and B is the replica.
2. When you create the replication link from B to C, select the link from A to B to be included in that link. This causes the HCP tenants, namespaces, and directories replicated on the link from A to B to be replicated again from B to C.
   In this link, B is the primary system and C is the replica.
   The link from B to C can also include tenants, namespaces, and directories that were originally created on B.
   You cannot individually select the replicated tenants, namespaces, and directories on B for inclusion in the link from B to C.
   In an active/passive chained replication topology with the configuration A > B > C, B is the replica for the link from A to B. Therefore, in B, the tenants and directories that were replicated from A are read-only, even though B is also the primary system for the link from B to C.
   HCP supports replication chains that consist of three HCP systems. Longer chains are not supported.
   Note:
   - You can also create a chained replication topology in which the first link is active/active and the second link is active/passive. You cannot, however, create a chained replication topology in which the first link is active/passive and the second link is active/active or in which both links are active/active.
   - In a replication chain A > B > C, in which the objects in a namespace on system B are supposed to be metadata-only, HCP does not remove data from those objects until that data has been replicated to system C.

Active/passive chained replication topology details

What this looks like

The following figure shows an active/passive chained replication topology in which system A is replicating to system B and system B is replicating to system C.



In this figure:

- From system A, two HCP tenants are being replicated to system B. In the first tenant, two of three namespaces are selected for replication. In the second tenant, one of two namespaces is selected for replication.
- From system B, the tenants and namespaces created by replication from system A are being replicated to system C because the link from A to B is included in the link from B to C.
- One tenant that was originally created on system B is also being replicated to system C. Both the namespaces in that tenant are selected for replication.

Uses

In an active/passive chained replication topology, all three HCP systems typically are located at full-scale data centers. For example, suppose a corporation has three major locations: New York, Los Angeles, and Tokyo. Each of these locations runs an application that is vital to the corporation, but only New York generates the data for these applications. Replicating the data from New York to Los Angeles and from Los Angeles to Tokyo enables applications at each location to access the data through a local area network. Because those applications are not accessing the data on the HCP system in New York, this topology also reduces the load on that system.

Active/passive chained replication helps ensure continuous data availability. If any one or even two of the HCP systems in the chain become unavailable, applications still have access to the stored data.

In an active/passive replication chain, the third HCP system provides disaster recovery functionality for the second system, and the second system provides disaster recovery functionality for the first system.

With an active/passive chained replication topology, you can create and manage both replication links from the HCP system in the middle of the chain. To this system, the link from the first system is an inbound link, and the link to the third system is an outbound link.

Active/passive one-to-many replication

In an *active/passive one-to-many replication topology*, one HCP system replicates to two or more other HCP systems using separate active/passive replication links. The replicating system is the primary system for each link. The other systems are replicas.

Typically, in an active/passive one-to-many replication topology, the replication links include different HCP tenants and namespaces and default-namespace directories.

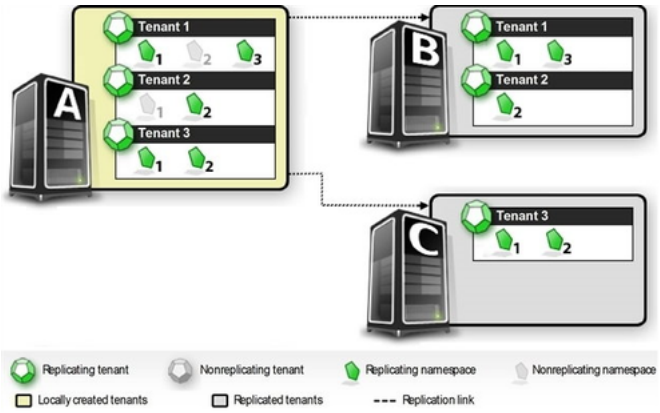
If three systems need to have the same tenants, namespaces, and directories as each other, consider using a chained topology for them rather than a one-to-many topology. The one-to-many topology puts greater load on the single primary system than does a chained topology, which splits the load between the first and second systems in the chain.

In some cases, however, replicating the same tenants and namespaces to two different replicas in a one-to-many topology may be appropriate.

Note: You can also create a one-to-many replication topology that consists of a combination of active/passive and active/active links or even only active/active links.

What this looks like

The figure below shows an active/passive one-to-many replication topology in which one primary system (A) replicates to two replicas (B and C) over two separate replication links.



In this figure:

- Two of three HCP tenants in system A are being replicated to system B. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- The third HCP tenant in system A is being replicated to system C. This tenant has two namespaces, both of which are selected for replication.

Using active/passive one-to-many replication topology to upgrade HCP systems from HCP with internal storage to HCP with SAN-attached storage

An *active/passive one-to-many replication topology* lets you replicate different tenants and default-namespace directories from a single primary system to multiple different replicas. You might do this, for example, if the replicas are at sites where users need read access to only a limited number of namespaces. Those sites can then have HCP systems that use smaller amounts of storage.

You can also use an active/passive one-to-many replication topology to upgrade your HCP systems from HCP with internal storage to HCP with SAN-attached storage. This scenario assumes you currently have a HCP with internal storage primary system replicating to a HCP with internal storage replica on an active/passive link. A HCP with SAN-attached storage primary system must replicate to a HCP with SAN-attached storage replica. To make this happen:

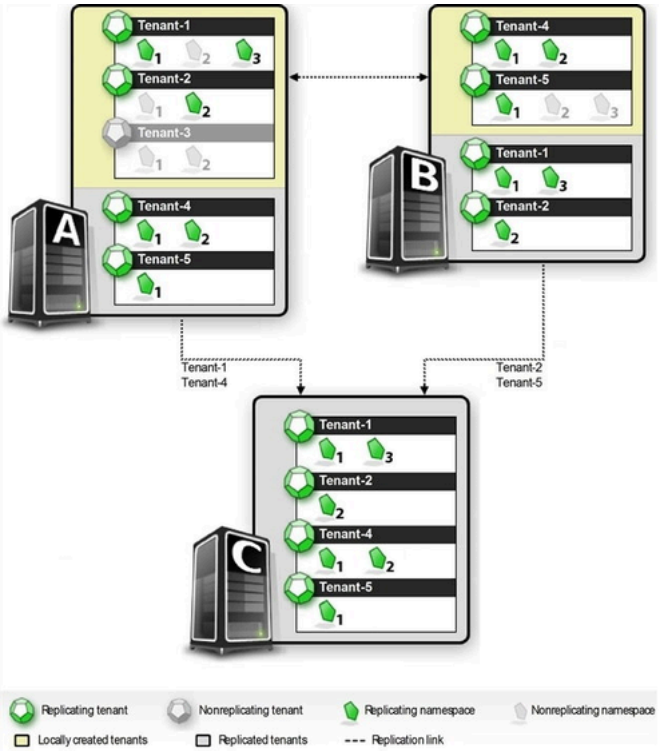
1. Create a second active/passive link from the HCP with internal storage primary system to the HCP with SAN-attached storage system that will be the primary system after the upgrade.
   Use this link to replicate all the HCP tenants, HCP namespaces, and default-namespace directories in the HCP with internal storage system.
2. Create a replication link from the new HCP with SAN-attached storage primary system to the second HCP with SAN-attached storage system.
   Include the link created in Step 1 above in this link to create a replication chain.
3. When replication is completely up to date, fail over the link from the HCP with internal storage system to the HCP with SAN-attached storage system.
   To enable replication to become completely up to date, you may need to stop clients from writing to the HCP with internal storage system before you fail over the link.
4. Delete the link from the HCP with internal storage system to the HCP with SAN-attached storage system.
5. Decommission the two HCP with internal storage systems.

Active/active replication with disaster recovery support

You can combine active/active replication with active/passive replication to create a topology in which a third system provides disaster recovery support for the two systems that participate in an active/active link. In this topology, a set of HCP tenants and namespaces and default-namespace directories is replicated on an active/active link between two systems (A and B). Some of those items are also replicated on an active/passive link from A to a third system (C). The rest of the items are also replicated on an active/passive link from system B to system C.

The choice of which items to replicate on each active/passive link is independent of which system the items were initially created on. For example, an HCP tenant created locally on system A could be included on the active/passive link from B to C.

The following figure shows a simple active/active replication topology with disaster recovery support.



In this figure:

- Two of three HCP tenants created locally in system A are replicated between system A and system B. In the first tenant being replicated, two of three namespaces are selected for replication. In the second tenant being replicated, one of two namespaces is selected for replication.
- Two HCP tenants created locally in system B are replicated between system A and system B. In the first tenant, two namespaces are selected for replication. In the second tenant, one of three namespaces is selected for replication.
- From system A, one HCP tenant initially created on system A and one HCP tenant initially created on system B are replicated to system C.
- From system B, one HCP tenant initially created on system A and one HCP tenant initially created on system B are replicated to system C.

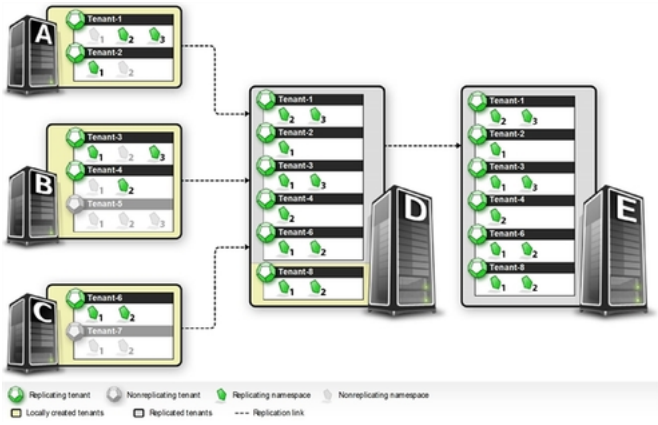
Many-to-one replication with disaster recovery support

You can combine the many-to-one and chained replication topologies to create a configuration in which multiple HCP systems replicate to a single HCP system (many-to-one), which, in turn, replicates to another HCP system (chained). The last system provides additional assurance of continuous data availability for all the HCP tenants and namespaces and default-namespace directories originally selected for replication. It also provides disaster recovery functionality for the HCP system to which those tenants, namespaces, and directories are initially replicated.

Creating many-to-one replication with disaster recovery support

In this example, HCP systems A, B, and C replicate to system D, which replicates to system E. To create this combined topology:

1. When you create the replication links from A to D, from B to D, and from C to D, select the tenants, namespaces, and directories you want to replicate.
2. When you create the replication link from D to E, select the links from A to D, from B to D, and from C to D to be included in that link.
   This causes the tenants, namespaces, and directories replicated on all three of those links to be replicated again from D to E. In effect, you're creating three replication chains: A → D → E, B → D → E, and C → D → E. The following below shows a many-to-one replication topology with disaster recovery support.

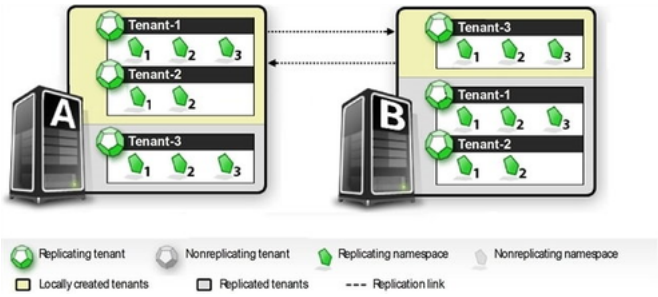


Bidirectional active/passive replication

For any given pair of HCP systems, each system can serve as both a primary system and a replica for the other system, as long as different HCP tenants and different default-namespace directories are being replicated in each direction. A system that serves as both a primary system and a replica at the same time has two active/passive links: one outbound and one inbound. This topology is called *bidirectional active/passive replication*.

What this looks like

The following figure shows a bidirectional active/passive replication topology in which two systems (A and B) are each replicating to the other system.



In this figure:

- From system A, two locally created tenants are being replicated to system B. In both tenants, all namespaces are selected for replication.
- From system B, one locally created tenant is being replicated to system A. In this tenant, all namespaces are selected for replication.

Uses

For each link in a bidirectional active/passive replication topology, the tenants, namespaces, and directories being replicated are read-write on the primary system and read-only on the replica. Therefore, a bidirectional active/passive replication topology supports a scenario like this:

- Application 1 running in a data center in New York needs read-write access to Tenant-1, which was created locally in the HCP system (A) in New York.
- Application 2 running in a data center in Tokyo needs read-write access to Tenant-2, which was created locally in the HCP system (B) in Tokyo.
- Application 1 needs only read access to Tenant-2.
- Application 2 needs only read access to Tenant-1

To meet these needs, you could:

- Create an active/passive link from system A to system B that includes Tenant-1. System A sends Tenant-1 to system B, where the tenant is in read-only mode. Application 2 can access the tenant more efficiently on system B than on system A.
- Create an active/passive link from system B to system A that includes Tenant-2. System B sends Tenant-2 to system A, where the tenant is in read-only mode. Application 1 can access the tenant more efficiently on system A than on system B.

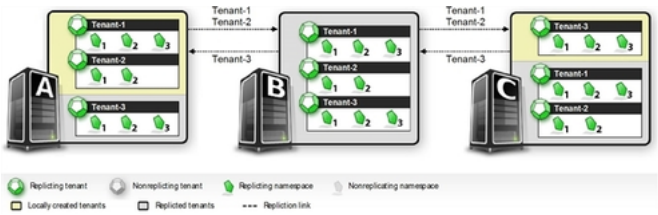
Bidirectional active/passive chained replication

In a **bidirectional active/passive chained replication** topology, three HCP systems participate in two active/passive replication chains, with each chain going in a different direction. That is, given three HCP systems A, B, and C:

- In one chain, system A replicates to system B, which replicates to system C.
- In the other chain, system C replicates to system B, which replicates to system A.

What this looks like

The following figure shows a bidirectional active/passive chained replication topology in which the replication chains are A → B → C and C → B → A.



In this figure:

- From system A, Tenant-1 and Tenant-2 are being replicated to system B. In both tenants, all namespaces are selected for replication.
- From system C, Tenant-3 is being replicated to system B. This tenant has three namespaces, all of which are selected for replication.
- From system B:
  - The tenants and namespaces created by replication from system A (that is, Tenant-1 and Tenant-2 and their namespaces) are being replicated to system C because the link from A to B is included in the link from B to C.
  - The tenant and namespaces created by replication from system C (that is, Tenant-3 and its namespaces) are being replicated to system A because the link from C to B in included in the link from B to A.

Uses

A bidirectional active/passive chained replication topology lets clients write to selected HCP tenants, namespaces, and default-namespace directories on three different systems while reading from all those tenants, namespaces, and directories on all those systems. In this example, data centers are in New York, Los Angeles, and Tokyo, and:

- The HCP system in New York has a locally created HCP tenant named Tenant-1
- The HCP system in Los Angeles has a locally created HCP tenant named Tenant-2
- The HCP system in Tokyo has a locally created HCP tenant named Tenant-3
- At each data center, a locally running application needs write access to the namespaces owned by the locally created tenant
- Clients at all three locations need read access to the namespaces owned by all three HCP tenants

To meet these needs, you could:

- Create an active/passive link (Link-1) from the New York system to the Los Angeles system that includes Tenant-1, which is writable in New York. The New York system sends Tenant-1 to the Los Angeles system, where the tenant is in read-only mode.
- Create an active/passive link (Link-2) from the Los Angeles system to the Tokyo system that includes Link-1 and Tenant-2, which is writable in Los Angeles. The Los Angeles system sends both Tenant-1 and Tenant-2 to the Tokyo system, where the tenants are in read-only mode.
- Create an active/passive (Link-3) from the Tokyo system to the Los Angeles system that includes Tenant-3, which is writable in Tokyo. The Tokyo system sends Tenant-3 to the Los Angeles system, where the tenant is in read-only mode.
- Create an active/passive link (Link-4) from the Los Angeles system to the New York system that includes Link-3 and Tenant-2. The Los Angeles system sends both Tenant-3 and Tenant-2 to the New York system, where the tenants are in read-only mode.

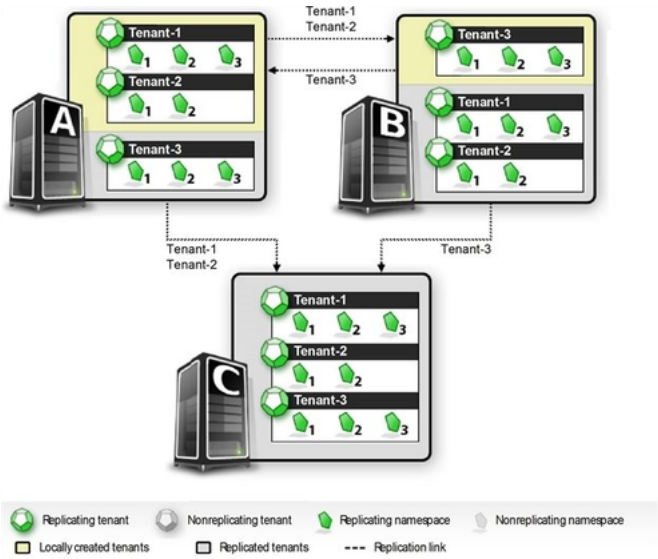
Bidirectional active/passive replication with disaster recovery support

You can combine the bidirectional and one-to-many replication topologies to create a configuration in which each of two systems replicates its locally created HCP tenants and namespaces and default-namespace directories to both the other system and a third system. This third system then provides each of the first two systems with both additional assurance of continuous data availability and disaster recovery functionality.

For example, HCP systems A and B each replicate their locally created HCP tenants and namespaces and default-namespace directories to each other, and a third system, C, provides disaster recovery functionality for each of those systems. To create this combined topology:

- Create a link from A to B that includes all the HCP tenants and namespaces and default-namespace directories that were originally created on system A.
- Create a link from A to C that includes the same tenants, namespaces, and directories as the link from A to B.
- Create a link from B to A that includes all the HCP tenants and namespaces and default-namespace directories that were originally created on system B.
- Create a link from B to C that includes the same tenants, namespaces, and directories as the link from B to A.

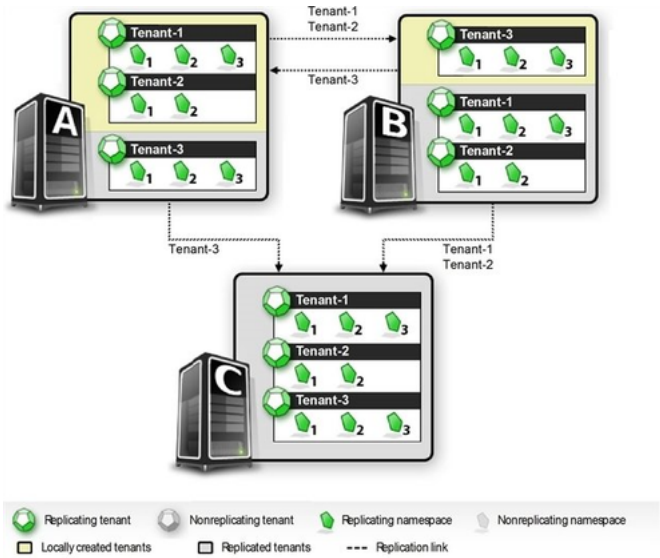
The following figure shows a bidirectional replication topology with disaster recovery support.



You can combine the bidirectional and chained replication topologies to have the same result as the topology described above, which involves the bidirectional and one-to-many topologies. That is, the replicated items in the link from A to B also end up on C, and the replicated items in the link from B to A also end up on C.

In this case, however, instead of the link from A to C replicating the same items as the link from A to B, the link from A to C would include the link from B to A. Likewise, instead of the link from B to C replicating the same items as the link from B to A, the link from B to C would include the link from A to B.

The following figure shows this topology.



This topology provides better performance than does the first topology described above. Additionally, if you need to add a tenant to the link from A to B, for example, you don't need to also add it to the link from A to C. Instead, the tenant is automatically replicated to C because the link from A to B is included in the link from B to C.

On the other hand, the first topology described above is better for assuring continuous data availability in case system A or B fails. For example, if system A is replicating to systems B and C and system B fails, the items being replicated from system A are still making it to system C. In the second topology, if system B fails, the items from system A are not replicated to system C because the replication chain is broken.

Failover and failback

Failover is a process that stops replication on a link and results in a situation in which, for read-write access:

- For an active/active link, applications should use only the HCP system to which the link was failed over
- For an active/passive link, applications should use only the replica

Typically, you fail over a link when one of the systems involved in the link becomes unavailable. With an active/passive link, this system must be the primary system. You don't need to fail over the link when the replica fails.

You can fail over a link while both systems are available. You might do this, for example, if you need to shut down one of the systems for maintenance.

Depending on the link configuration, failover either is a manual procedure or occurs automatically. When automatic failover is enabled for a link, the link fails over automatically after the applicable system is unavailable for a specified amount of time.

You enable or disable automatic failover separately for each system involved in an active/active link. For an active/passive link, you enable or disable automatic failover only for the replica.

Failback is the process that restarts replication on a link that has been failed over and returns the HCP systems involved in the link to normal operation. Typically, you fail back a link when an unavailable system becomes available again.

If connectivity was lost between the two systems involved in a failed-over link, before failback can occur, connectivity must be restored. Connectivity exists when the network infrastructure through which the two systems communicate is healthy and the applicable SSL server certificates have been shared between the two systems.

In a disaster recovery situation in which the system that became unavailable has been rebuilt, the link no longer exists on that system. In this case, before failback can occur, the link must be restored to the rebuilt system.

With an active/active link, failback is a manual procedure. With an active/passive link, the failback procedure can be partially automated.

Failover and failback with active/active links

The effects of failing over and failing back an active/active link differ depending on whether DNS failover was enabled for the system that became unavailable. In all cases, however, when the link fails over, replication on that link stops. When the link fails back, normal replication restarts.

Failover with an active/active link

With an active/active link, failover can occur in either direction between the two systems involved in the link. While the link is failed over, the replicated HCP tenants and namespaces and default-namespace directories remain read-write on both systems. However, because failover normally occurs when one system is unavailable, to avoid wasting resources, neither system tries to read or repair objects from the other system.

With DNS failover enabled, when an active/active link fails over from one of the HCP systems involved in the link (system A) to the other system involved in the link (system B), system B broadcasts a new configuration to the DNS. This new configuration causes client requests targeted to system A by domain name to be redirected to system B when the request is for an HCP namespace or default-namespace directory that was being replicated on the failed-over link.

Note: System B can service redirected namespace access requests only if the applicable namespace is configured to allow service by remote systems.

If a client request targeted to system A is for an HCP namespace or default-namespace directory that was not being replicated on the failed-over link, the request is not redirected to system B. Client requests that target system A by IP address are also not redirected to system B.

Client requests that use a domain name to target the Tenant Management Console for a replicated HCP tenant on system A are redirected to system B, but system B cannot process such requests. Instead, system B returns a 403 error code.

While the link is failed over, system A does not broadcast any configuration information to the DNS.

With DNS failover disabled, failing over an active/active link stops replication on the link but does not cause any other changes. Clients can still access system A by domain name (if system A is available).

Failback with an active/active link

Failing back an active/active link entails a single action, fail back. When an active/active link fails back:

- Replication immediately restarts in both directions on the link. With DNS failover enabled, each HCP system involved in the link broadcasts its own configuration to the DNS. From that point on, client requests that target either system by domain name are directed to the specified system.

Failover and failback with active/passive links

The effects of failing over and failing back an active/passive link differ depending on whether DNS failover was enabled for the system that became unavailable. In all cases, however, when an active/passive link fails over, replication on that link stops. When the link fails back, normal replication restarts.

Failover with an active/passive link

Failover with an active/passive link occurs only from the primary system to the replica. When an active/passive link fails over to the replica, the replicated HCP tenants and namespaces and default-namespace directories become read-write on the replica.

With DNS failover enabled, when an active/passive link fails over, the replica broadcasts a new configuration to the DNS. This new configuration causes client requests targeted to the primary system by domain name to be redirected to the replica when the request is for an HCP namespace or default-namespace directory that was being replicated on the failed-over link.

Note: A replica can service redirected namespace access requests only if the applicable namespace is configured to allow service by remote systems.

If a client request targeted to the primary system is for an HCP namespace or default-namespace directory that was not being replicated on the failed-over link, the request is not redirected to the replica. Client requests that target the primary system by IP address are also not redirected to the replica.

Client requests that use a domain name to target the Tenant Management Console for a replicated HCP tenant on the primary system are redirected to the replica, but the replica cannot process such requests. Instead, the replica returns a 403 error code.

If the primary system is still available when an active/passive link is failed over and the primary system and the replica can communicate with each other, the replicated HCP tenants and namespaces and default-namespace directories become read-only on the primary system. Also, while the link is failed over, the primary system does not broadcast any configuration information to the DNS.

If the two systems cannot communicate with each other when the link is failed over, the replicated items remain read-write on the primary system, and the primary system continues to broadcast its configuration information to the DNS. If DNS failover is disabled, clients can still access the primary system by domain name.

If clients are allowed to write to both the primary system and the replica while an active/passive link is failed-over, configuration conflicts and conflicts in namespace content may occur when the link is failed back. Although HCP resolves such conflicts in a predictable manner, the recommended practice is to avoid them in the first place. Therefore, when you fail over an active/passive link without DNS failover enabled, you should tell the applicable tenant administrators to direct all client access requests to the replica.

Failover with bidirectional active/passive links

With bidirectional active/passive links, failover is a independent process for each of the two links. If one of the HCP systems involved in the links becomes unavailable, failover needs to occur only on the link for which that system is the primary system. The link for which that system is the replica does not need to be failed over, and the status of the HCP tenants and namespaces and default-namespace directories on that link does not change.

Failback with an active/passive link

Failing back an active/passive link has two phases, begin recovery and complete recovery. The begin recovery phase is always started manually. The complete recovery phase can be started manually or automatically.

When recovery begins on a link, the replica starts sending configuration changes and changes to namespace content back to the primary system. The replicated HCP tenants and namespaces and default-namespace directories remain read-write on the replica and read-only on the primary system.

The complete recovery phase is designed to allow data recovery to catch up to the current time before normal replication restarts. At the beginning of this phase, the replicated items change to read-only on the replica and remain read-only on the primary system. The replica continues to send data to the primary system until the two HCP systems involved in the link are in sync with each other. Within a minute after that point:

- Normal replication restarts on the link.
- With DNS failover enabled, each system involved in the link broadcasts its own configuration to the DNS. From that point on, client requests that target either system by domain name are directed to the specified system.

Before starting the complete recovery phase manually, you should wait until data recovery is caught up with the current time. When you configure automatic failback for an active/passive link, you specify how up to date data recovery must be before the complete recovery phase begins.

Replication collisions

With an active/active link, clients can make configuration changes and changes to namespace content on both HCP systems involved in the link. This situation can result in configuration and content collisions.

With an active/passive link, if clients are allowed to make changes on both HCP systems involved in the link while the link is failed over to the replica, configuration and content collisions can occur on failback. Collisions can also occur on failback if changes made on the replica while a link is failed over conflict with configuration or content that was not yet replicated at the time of failover.

The way HCP handles collisions that occur due to replication depends on the type of collision. The general rule for namespace content is that more recent changes have priority over conflicting less recent changes. If conflicting changes occur at exactly the same time, HCP gives priority to the change that occurred on the system where the link was created.

When configuration changes result in a conflict, the Replication service pauses replication or recovery of the tenant, as applicable.

Note: If the system time is not in sync on the two systems involved in a replication link, replication collision handling may have unexpected results.

Object content collisions

An object content collision occurs when:

- For an HCP namespace without versioning enabled, these events occur in the order shown:
  1. An object is created with the same name in that namespace on both systems involved in a replication link, but the object has different content on the two systems.
  2. The object on one of the systems is replicated to the other system.

  If versioning is enabled for the namespace, no collision occurs. Instead, the less recently created of the two objects becomes an old version of the more recently created object. If the two objects were created at exactly the same time, the object that was created on the system where the link was created is treated as the newer version.

- For a default-namespace folder, these events occur in the order shown:
  1. An object is created with the same name in that folder on both systems involved in a replication link, but the object has different content on the two systems.
  2. The object on one of the systems is replicated to the other system.

When an object content collision occurs, the more recently created object keeps its name and location. The other object is either moved to the .lost+found folder in the same namespace or renamed, depending on the namespace configuration. If the two objects were created at exactly the same time, the object that was created on the system where the link was created keeps its name and location.

When HCP moves an object to the .lost+found folder, the full object path becomes .lost+found/replication/*link-id*/*old-object-path*.

When renaming an object due to a content collision, HCP changes the object name to *object-name*.collision or *object-name.version-id.*collision, where *version-id* is the version ID of the object. HCP uses the second format only if versioning has ever been enabled for the namespace that contains the object but is not currently enabled.

If the new name is already in use, HCP changes the object name to *object-name.*1.collision or *object-name.version-id.*1.collision, as applicable. If that name is already in use, HCP successively increments the middle integer by one until a unique name is formed.

Objects that have been relocated or renamed due to content collisions are flagged as replication collisions in their system metadata. Clients can use the metadata query API to search for objects that are flagged as replication collisions.

If an object that has been flagged as a replication collision changes (for example, if its retention period is extended), its collision flag is removed. If a client creates a copy of a flagged object with a new name, the collision flag is not set on the copy.

Namespaces can be configured to have the DIsposition service automatically delete objects that are flagged as replication collisions. When selecting this option for a namespace, the tenant administrator specifies the number of days the DIsposition service should wait before deleting such an object. The days are counted from the time the collision flag is set. If the collision flag is removed from an object, the object is no longer eligible for deletion by the DIsposition service.

System metadata collisions

A system metadata collision occurs when these events occur in the order shown:

1. Different changes are made to the system metadata for a given object on each of two systems in a replication topology.
2. The changed system metadata on one of the systems is replicated to the other system.

For example, suppose a user on one system changes the shred setting for an object while a user on the other system changes the index setting for the same object. When the object on either system is replicated to the other system, a system metadata collision occurs.

If a collision occurs when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- For changed system metadata other than the retention setting and hold status:
  - If the last change made on system A is more recent than the last change made on system B, HCP changes the system metadata on system B to match the system metadata on system A.
  - If the last change on system B is more recent than the last change on system A, HCP does not change the system metadata on system B.
- For a changed retention setting:
  - If the retention setting on system A specifies a longer retention period than does the retention setting on system B, HCP changes the retention setting on system B to match the retention setting on system A.
  - If the retention setting on system B specifies a longer retention period than does the retention setting on system A, HCP does not change the retention setting on system B.
- For a changed hold status:
  - If the object is on hold on system A but not on system B, HCP places the object on hold on system B.
  - If the object is on hold on system B but not on system A, HCP leaves the object on hold on system B.

Here are some examples of how HCP handles collisions when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology.

Example 1

The object starts out on both system A and system B with these system metadata settings:

- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the shred setting to true.
2. On system B, a client changes the index setting to true.
3. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
   - Shred: false
   - Index: true

Example 2

The object starts out on both system A and system B with these system metadata settings:

- Retention: Initial Unspecified
- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the retention setting to Deletion Prohibited.
2. On system B, a client changes the retention setting to Deletion Allowed.

3. On system B, a client changes the index setting to true.
4. On system A, a client changes the shred setting to true.
5. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
    - Retention: Deletion Prohibited
    - Shred: true
    - Index: false

Example 3

The object starts out on both system A and system B with these system metadata settings:

- Retention: Initial Unspecified
- Hold: true
- Shred: false
- Index: false

The list below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

1. On system A, a client changes the retention setting to Deletion Allowed.
2. On system B, a client changes the retention setting to Deletion Prohibited.
3. On system B, a client changes the index setting to true.
4. On system A, a client changes the shred setting to true.
5. On system A, a client releases the object from hold.
6. The changes on system A are replicated to system B. The resulting settings for the object on system B are:
    - Retention: Deletion Prohibited
    - Hold: true
    - Shred: true
    - Index: false
7. The changes on system B are replicated to system A. The resulting settings for the object on system A are:
    - Retention: Deletion Prohibited
    - Hold: true
    - Shred: true
    - Index: false

Custom metadata collisions

A custom metadata collision occurs when these events occur in the order shown:

1. One of these changes occurs:
    - An annotation is added with the same name to a given object on each of two systems in a replication topology, but the annotation has different content on the two systems.

      The addition of an annotation to a given object on only one of the systems does not result in a custom metadata collision if the object does not have an annotation with the same name on the other system. In this case, the new annotation is replicated without conflict.

    - Different changes are made to the content of a given annotation for a given object on each of the two systems in a replication link.
    - A change is made to the content of a given annotation for a given object on one system in a replication link, and the same annotation is deleted on another system in the link.
2. The change made on one of the systems is replicated to the other system.

For a default-namespace directory, these events occur in the order shown:

1. One of these changes occurs:
    - Custom metadata is added to a given object on both systems involved in a replication link, but the added custom metadata is different on the two systems.

      The addition of custom metadata to an object on only one of the systems involved in a replication link does not result in a custom metadata collision. Instead, the new custom metadata is replicated from that system to the other system involved in the link without conflict.

    - The custom metadata for a given object is replaced on both systems involved in a replication link, but the replacement custom metadata is different on the two systems.
    - The custom metadata for a given object is replaced on one of the systems involved in a replication link, and the same custom metadata is deleted on the other system involved in the link.
2. The change made on one of the systems is replicated to the other system.

If a collision occurs when a custom metadata change for a given object is replicated from one system (system A) in a replication link to another system (system B) in the link:

- If the last change on system A is more recent than the last change on system B, HCP applies the change from system A to the custom metadata on system B
- If the last change on system B is more recent than the last change on system A, HCP does not change the custom metadata on system B

Here are some examples of how HCP handles collisions when custom metadata changes for a given object are replicated from one system (system A) in a replication link to another system (system B) in the link.

Example 1

In an HCP namespace, the object starts out with annotations named a1 and a2 on both system A and system B.

The following list shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

1. On system B, a client changes the content of a1.
2. On system A, a client makes a different change to the content of a1.
3. On system A, a client adds annotation a3 to the object.
4. On system B, a client adds annotation a3 with different content from the a3 added on system A.
5. The changes on system A are replicated to system B. The resulting annotations for the object on system B are:
    - a1 with the changed content from system A
    - a2 (unchanged)
    - a3 with the content added on system B
6. The changes on system B are replicated to system A. The resulting annotations for the object on system A are:

    - a1 with the changed content from system A
    - a2 (unchanged)
    - a3 with the content added on system B

Example 2

The object starts out with the annotations named a1, a2, and a3 on both system A and system B.

The following list shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

1. On system B, a client changes the content of a1.
2. On system A, a client deletes a1.
3. On system A, a client changes the content of a2.
4. On system B, a client changes the content of a2.
5. On system A, a client deletes a3.
6. On system B, a client changes the content of a3.
7. The changes on system A are replicated to system B. The resulting annotations for the object on system B are:
    - a2 with the changed content from system B
    - a3 with the changed content from system B
8. The changes on system B are replicated to system A, the resulting annotations for the object on system A are:
    - a2 with the changed content from system B
    - a3 with the changed content from system B

Example 3

In a default-namespace directory, the object starts out with same custom metadata on system A and system B.

The following list shows a sequence of events in which the custom metadata for the object is changed and the change is then replicated.

1. On system B, a client replaces the custom metadata for the object with new custom metadata.
2. On system A, a client replaces the custom metadata for the object with different custom metadata from the custom metadata used on system B.
3. The change on system A is replicated to system B. The resulting custom metadata for the object on system B is the new custom metadata from system A.

Access control list collisions

An ACL collision occurs when these events occur in the order shown:

1. Different changes are made to the ACL for a given object on each of two systems in a replication link.
2. The changed ACL on one of the systems is replicated to the other system.

An ACL is treated as a single unit. If a collision occurs when a changed ACL for a given object is replicated from one system (system A) in a replication link to another system (system B) in the link:

- If the last change to the ACL on system A is more recent than the last change to the ACL on system B, HCP changes the ACL on system B to match the changed ACL on system A
- If the last change to the ACL on system B is more recent than the last change to the ACL on system A, HCP does not change the ACL on system B

For example, suppose the ACL for a given object starts out with these grants on both system A and system B:

- All users: read
- User lgreen: write
- User mwhite: write, delete

The following list shows a sequence of events in which the ACL for the object is changed and the change is then replicated.

1. On system B, a client changes the grants in the ACL to:
    - All users: read
    - User lgreen: write, delete
    - User mwhite: write, delete, read ACL
2. On system A, a client changes the grants in the ACL to:
    - All users: read
    - User mwhite: write
    - User pdgrey: write
3. The changed ACL on system A is replicated to system B. The resulting ACL for the object on system B contains these grants:
    - All users: read
    - User mwhite: write
    - User pdgrey: write

Configuration collisions

A configuration collision occurs when these events occur in the order shown:

1. Different changes are made to the same configuration property on each of two systems in a replication link.
2. The changed property on one of the systems is replicated to the other system.

Examples of configuration properties include:

-
    - The namespace quota for a tenant
    - The data access permission mask for a namespace
    - The versioning setting for a namespace
    - The default shred setting for a namespace
    - The roles for a user account
    - The data access permissions a group account has for a namespace
    - The protocol optimization setting on a namespace

Certain groups of properties are treated as a single unit. Generally, these groups consist of properties that are updated by a single submission in the System Management Console or Tenant Management Console. Two notable exceptions to this rule are data access permissions for user accounts and content properties for content classes. In these cases, each

set of data access permissions for a namespace and each content property is treated as an individual property.

If a collision occurs when a configuration change is replicated from one system (system A) in a replication topology to another system (system B) involved in the link:

- If the last change to the configuration on system A is more recent than the last change to the configuration on system B, HCP changes the configuration on system B to match the configuration on system A
- If the last change to the configuration on system B is more recent than the last change to the configuration on system A, HCP does not change the configuration on system B

The rules above apply to all configuration collisions except collisions that occur when retention class properties are changed.

Here are two examples of how HCP handles collisions when configuration changes are replicated from one system (system A) in a replication topology to another system (system B) involved in the link.

Example 1

A given tenant starts out on both system A and system B with these properties:

- Namespace quota: 5
- Versioning: disabled

The following list shows a sequence of events in which the tenant configuration is changed and the change is then replicated.

1. In the System Management Console on system B, an administrator changes the namespace quota for the tenant to 10.
2. In the System Management Console on system A, an administrator enables versioning for the tenant.
3. The change on system A is replicated to system B. Because namespace quota and versioning are properties in the same submission group, the resulting properties for the tenant on system B are:
    - Namespace quota: 5
    - Versioning: enabled

Example 2

A given tenant-level user account starts out on both system A and system B with these roles and data access permissions:

- Roles: monitor, compliance
- Namespace-1 permissions: browse, read, write, delete

The following list shows a sequence of events in which the user account is changed and the changes are then replicated.

1. In the System Management Console on system B, an administrator changes the namespace quota for the tenant to 10.
2. In the System Management Console on system A, an administrator enables versioning for the tenant.
3. The change on system A is replicated to system B. Because namespace quota and versioning are properties in the same submission group, the resulting properties for the tenant on system B are:
    - Namespace quota: 5
    - Versioning: enabled
4. In the Tenant Management Console on system A, an administrator adds the privileged permission to Namespace-1.
5. In the Tenant Management Console on system B, an administrator gives the user account browse and read permissions for Namespace-2.
6. In the Tenant Management Console on system A, an administrator gives the user account browse, read, and write permissions for Namespace-3.
7. The changes on system A are replicated to system B. Because roles and data access permissions are in separate submission groups, the resulting roles and data access permissions for the user account on system B are:
    - Roles: compliance
    - Namespace-1 permissions: browse, read, write, delete, privileged
    - Namespace-2 permissions: browse, rea
    - Namespace-3 permissions: browse, read, write

Retention class collisions

A retention class collision occurs when these events occur in the order shown:

1. Different changes are made to the same retention class on each of two systems in a replication link.
2. The changed retention class on one of the systems is replicated to the other system.

If a collision occurs when a change to a retention class is replicated from one system (system A) in a replication link to another system (system B) involved in the link:

- If the last change to the retention class on system A is more recent than the last change to the class on system B and:
    - The value of the class on system A is greater than the value of the class on system B, HCP changes the value of the class on system B to the value of the class on system A
    - The value of the class on system A is less than the value of the class on system B and:
        - System B is in enterprise mode, HCP changes the value of the class on system B to the value of the class on system A
          Note: An exception to this rule is when the value of the class on system A is -2 (Initial Unspecified) and the value of the class on system B is *not* 0 (Deletion Allowed). In this case, the value of the class on system B does not change.
        - System B is in compliance mode, HCP does not change the value of the class on system B
- If the last change to the retention class on system B is more recent than the last change to the class on system A, HCP does not change the value of the class on system B

A retention class value of -1 (Deletion Prohibited) is greater than a value that's a specific duration. A retention class value of 0 (Deletion Allowed) or -2 (Initial Unspecified) is less than a value that's a specific duration.

Considerations for cross-release replication

HCP release 9.x systems support replication with other release 9.x systems and with release 8.x systems. HCP does not support replication between 9.x systems and systems earlier than 8.0.

Cross-release replication and erasure coding topologies

Erasure coding topologies cannot include HCP systems at a release earlier than 8.0.

Cross-release replication and multipart objects

HCP cannot replicate multipart objects between a 9.x system and an 8.x system. As a result:

- When you add a tenant to a cross-release replication link, HCP automatically pauses replication of that tenant if both of the following are true for any of the tenant's namespaces:
  - The namespace has replication enabled.
  - The namespace contains one or more multipart objects.
- When you select a namespace for replication, HCP automatically pauses replication of the tenant that owns that namespace if both of the following are true for any of the tenant's namespaces:
  - The namespace has replication enabled.
  - The namespace contains one or more multipart objects.
- When you select a namespace for replication, HCP automatically pauses replication of the tenant that owns that namespace if both of the following are true:
  - The replication link on which the tenant is being replicated is a cross-release link.
  - The namespace contains one or more multipart objects.
- When a multipart upload is completed on a namespace, HCP automatically pauses replication of the tenant that owns that namespace if both of the following are true:
  - The namespace has replication enabled.
  - The replication link on which the tenant is being replicated is a cross-release link.

Configuring SSL for replication

Before replication can occur between two HCP systems, the systems involved must have a trust relationship with each other. This trust is based on shared SSL server certificates.

This section of the Help provides instructions for downloading, uploading, and deleting SSL server certificates for replication.

To view the SSL configuration for replication, you need the monitor or administrator role. To configure SSL for replication, you need the administrator role.

Sharing SSL server certificates

Before replication can occur on a replication link, the two systems involved in the link each need to have installed at least one valid replication SSL server certificate. Each system also needs to have installed at least one valid replication SSL server certificate from the other system as a trusted replication server certificate.

A valid replication SSL server certificate on any given HCP system is one that:

- Is associated with the domain that’s associated with the network that’s selected for replication on that system
- Has already reached its start date
- Has not expired

To share a certificate, the HCP administrator for the system in which the certificate is installed needs to download the certificate and give it to the administrator for the other system. That administrator then needs to upload the certificate as a trusted replication server certificate on the other system. Because what’s downloaded is only the public portion of each server certificate, you can transfer the certificate unsecured.

For any given replication link, the two systems directly involved must share certificates. In a replication chain, for example, from system A to system B to system C, systems A and B must share certificates, and systems B and C must share certificates, but systems A and C don’t need to do this.

If you take any of these actions on one of the systems in a replication pair, the replication certificate on that system automatically changes:

- Delete the certificate that’s currently being used for replication
- Associate a different domain with the network that’s selected for replication
- Select a different network for replication, where that network is associated with a different domain from the previously selected network
- Install a new valid certificate for the applicable domain where that certificate has an earlier start date than the certificate that’s currently being used for replication

The replication certificate also automatically changes if:

- The certificate that’s currently being used for replication expires and the applicable domain has at least one other certificate that’s valid
- A future certificate for the applicable domain becomes valid and the domain has no other valid certificates

In any of these cases, when the certificate changes, HCP automatically suspends replication or recovery activity on all links in which the system participates. At that point, you need to download the new certificate and upload it to the other system for each link. After you upload the new certificate, activity on the link resumes automatically.

Downloading an SSL server certificate

To view the SSL configuration for replication, you need the monitor or administrator role. To configure SSL for replication, you need the administrator role.

1. In the top-level menu of the HCP System Management Console, select Services > > Replication.
2. On the left side of the Replication page, click Certificates.
   On the replication Certificates page, the Replication Server panel is displayed. The panel shows this information about each currently installed replication SSL server certificate, regardless of whether it’s expired:

   Server Certificate Domain
   : The distinguished name for the certificate

   Valid On
   : The date and time at which the certificate goes (or went) into effect

   Expires On
   : The date and time at which the certificate expires (or expired)

3. Click the download control ( ) for the certificate you want to download. Then save the downloaded certificate in the location of your choice.

Uploading a trusted replication server certificate

To view the SSL configuration for replication, you need the monitor or administrator role. To configure SSL for replication, you need the administrator role.

1. In the top-level menu of the HCP System Management Console, select Services > > Replication.
2. On the left side of the Replication page, click Certificates.
3. On the replication Certificates page, click Trusted Replication.
   The Trusted Replication panel shows this information about each trusted replication server certificate:

Server Certificate Domain
The distinguished name for the certificate
Valid On
The date and time at which the certificate goes (or went) into effect
Expires On
The date and time at which the certificate expires (or expired)

4. In the Trusted Replication section, click Browse. Then select the file containing the downloaded SSL server certificate.
5. Click Upload Certificate.

The Trusted Replication section displays the uploaded certificate.

Note: You can also download a trusted replication server certificate. To do this, click the download control ( ) for the certificate in the Trusted Replication section.

Deleting a trusted replication server certificate

You can delete trusted replication server certificates. You may want to do this, for example, with certificates that become invalid.

You can delete a trusted replication server certificate only while all links in which the system participates are suspended.

To view the SSL configuration for replication, you need the monitor or administrator role. To configure SSL for replication, you need the administrator role.

1. In the top-level menu of the HCP System Management Console, select Services > > Replication.
2. On the left side of the Replication page, click Certificates.
3. On the replication Certificates page, click Trusted Replication.
4. In the Trusted Replication panel, click the delete control ( ) for the certificate you want to delete.
5. In response to the confirming message, click Remove Certificate.

Working with replication links

A replication link provides all the information the Replication service needs to perform its functions. You can create a link in the HCP System Management Console for either of the systems involved in the link.

When you create a link, you specify whether it is active/active, the outbound side of an active/passive link (that is, the primary system), or the inbound side of an active/passive link (that is, the replica). Once a link exists, you can select HCP tenants, default-namespace directories, and, for active/passive links only, other links to replicate on the link.

You can modify replication links at any time. You can also delete replication links. However, this action should be taken only with a full understanding of the consequences.

This section of the Help contains considerations and instructions for performing the activities mentioned above.

To view a replication link, you need the monitor or administrator role. To create, manage, modify, or delete a replication link, you need the administrator role.

You can also use the HCP management API to create, manage, modify, and delete replication links.

Link properties

You create a replication link on either one of the systems you want to participate in the link. When you first create the link, you set these properties:

- The link name.
- Optionally, a description of the link.
- The link type. This can be active/active, outbound (for an active/passive link you're creating on the primary system), or inbound (for an active/passive link you're creating on the replica).
- Whether HCP should compress and/or encrypt data before transmitting it to the other system. For an active/active link, these settings apply to data being replicated in both directions on the link.
- Whether priority should be given to objects with the oldest changes, regardless of namespace, or processing should be balanced across namespaces. For an active/active link, this setting applies to both systems involved in the link.
- The identity of the other system you want to participate in the link. You can identify the other system either by domain name or by the IP addresses of storage nodes in that system.
- The port on which the other system will listen for transmissions from the system where you're creating the link. Typically, you accept the default of 5748.
- If the system where you're creating the link uses network address translation (NAT):
  - The domain name or IP addresses the other system should use to communicate with the system where you're creating the link
  - The port on which the system where you're creating the link will listen for transmissions from the other system

  Note: If either or both of the systems involved in a link use a NAT, the NAT or NATs must be configured for port forwarding.

When you create a link, the automatic failover and failback properties default to disabled. You cannot modify these properties during link creation.

Considerations for creating a replication link

There are several considerations when you create a replication link.

- You cannot create a replication link between a release 9.x HCP system and a system earlier than release 8.0.
- You can create a replication link only after you have installed the required SSL certificates.
- You can create multiple replication links between the same two systems. However, the links cannot include the same HCP tenants and default-namespace directories. Also, only one of the links can be used in an erasure coding topology.
- If you do not want HCP tenant-level users to see replication details, you should clear the option that allows this behavior before you create the replication link.

Creating a replication link

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click Create Link.
   The link creation wizard opens.
3. On the wizard Name page:
   a. In the Name field, type a name for the link.
      Link names must be from one through 64 characters long and can contain any valid UTF-8 characters, including white space. Link names are not case sensitive.
      Link names must be unique within a replication topology.

b. (Optional) n the Description field, type a description for the link.
The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

4. Click Next.
5. On the wizard Settings page:
   - In the Link Type section:
     - To create an active/active link, select Active/Active.
     - To create an active/passive link for which the system where you're creating the link is the primary system, select Outbound.
     - To create an active/passive link for which the system where you're creating the link is the replica, select Inbound.
   - In the Data Transfer section:
     - Optionally, to compress data before it's transmitted from one system to the other, select Compress data.

       Compressing data increases network throughput but also increases processing time. Therefore, because compression applies to all transmitted data, you should enable compression only if most of the data being replicated is compressible.

     - To enable or disable the encryption of data before it's transmitted from one system to the other, select or deselect Encrypt data.

       By default, data encryption is enabled on replication links. Encryption keeps the data confidential during transmission. The transmitted data is automatically decrypted on the target system. If you have disabled encryption on replication links and want to enable it again, select Encrypt data.

       If you have disabled encryption on replication links, data is transmitted unencrypted, even if the data is encrypted on the system sending the data. Regardless of whether the data is encrypted before transmission, the data is still secured by SSL during transmission.

       If the HCP system does not support HTTPS for data transmission, the Encrypt data option is not present.

   - In the Replication Priority section:
     - To have the Replication service balance its processing time evenly across the namespaces being replicated, select Balanced across namespaces.
     - To replicate objects with the oldest changes first, regardless of which namespaces they're in, select Oldest object first.
6. Click Next.
7. On the wizard Connection page:
   - In the Remote Hostname or IP Addresses field, type either the domain name of the other system you want to participate in the link or one or more comma-separated IP addresses of storage nodes in that system. For the domain name, use either of these formats:

     `replication.`*`hcp-domain-name`*

     `replication.admin.`*`hcp-domain-name`*

     In these formats, hcp-domain-name must be the name of the domain associated with the network that's selected for replication on the other system. For example, if the domain name is hcp-ca.example.com, you specify this in the Remote Hostname or IP Addresses field when using the second format shown above:

     `replication.admin.hcp-ca.example.com`

     If you specify IP addresses for one or more nodes, they must be IP addresses in the network that's selected for replication on the other system.

     Note: If you specify a domain name, the system where you're creating the link transmits data to all storage nodes in the other system. If you specify IP addresses, the system where you're creating the link transmits data to only those nodes. Therefore, you should specify IP addresses only if you have a compelling reason to do so (for example, HCP is not using DNS, or you need to reduce the processing load on some number of nodes).
   - (Optional) To specify a different port for the other system to listen on or to specify network address translation (NAT) information for the system where you're creating the link, click Advanced Configuration. Then, in the Advanced Configuration section, as applicable:
     - In the Remote Port field, type the number of the port on which the other system will listen for data from the system where you're creating the link. The default port is 5748. Typically, you specify a different port only if other port usage makes using a different port necessary.
     - If the system where you're creating the link uses NAT for communication with the other system, specify the target for data transmissions from the other system:
       - In the Local Hostname or IP Addresses field, type either the name of the domain associated with the network that's selected for replication on the system where you're creating the link (as that name is known to the other system) or one or more comma-separated IP addresses of storage nodes in that network (as those addresses are known to the other system). For the domain name, use either of these formats:

         `replication.`*`hcp-domain-name`*

         `replication.admin.`*`hcp-domain-name`*

         Make sure the other system can resolve the domain name you specify.

         Note: The other system will transmit data only to the nodes identified by the domain name or IP addresses you specify. Therefore, if you're using IP addresses, you should specify the addresses of all the storage nodes in the system.
       - In the Local Port field, type the number of the port on which the system where you're creating the link will listen for data from the other system. This is the port that's exposed to the other system.
         Note: For network configurations that use NAT, multiple IP addresses must be configured to expose the HCP nodes. You cannot use multiple ports on the same IP address.
8. Click Next.
9. On the wizard Review page, review the link configuration.
10. If the link configuration is what you want, click Finish to create the link.
    If the link configuration is not what you want, use the Previous button in the wizard to return to pages on which you want to make corrections. Alternatively, press Cancel to leave the wizard without creating the link.
    Tip: If HCP cannot create the configured link, check that the other system is healthy and that you've correctly shared SSL server certificates between the two systems.

Considerations for specifying link content

These considerations apply to specifying the content for replication links:

- The content for a replication link (that is, what is replicated on the link) consists of any number of:
  - HCP tenants
  - HCP namespaces
  - Directories defined in the default namespace
  - For active/passive links only, chained links
- You can add a tenant to a replication link only if the tenant is configured to allow replication.
- You cannot add a tenant to a replication link between two systems if another link between the same two systems already includes that tenant.

- You can choose which namespaces to replicate for any given HCP tenant only if the tenant has granted system-level users administrative access to itself. Namespaces that are selected for replication are replicated on every link that includes the owning tenant.
- To select and deselect HCP namespaces for replication, you can use any link that includes the owning tenant.
- You can add and remove HCP tenants, default-namespace directories, and chained links from a replication link at any time, except during an upgrade of either system involved in the link, while the link is failed over, while data recovery is occurring on the link, or while the two systems involved in the link cannot communicate with each other.
- When you add an HCP tenant to an erasure coding topology, the tenant is automatically added to every link in that topology.
- When you add an HCP tenant to a replication link without adding the tenant to an erasure coding topology, all replication-enabled namespaces owned by the tenant use whole-object protection regardless of whether they are configured to allow erasure coding.
- You cannot add an HCP tenant to a replication link while that tenant is included in an active, retiring , or retired erasure coding topology that includes one or both of the systems involved in the link but not the link itself.
- You cannot remove an HCP tenant from a replication link that's part of an active erasure coding topology.
- You cannot remove an HCP tenant from a replication link if that tenant was previously removed from the active erasure coding topology and any of the tenant's namespaces still contain chunks for erasure-coded objects.
- You cannot remove an HCP tenant from a replication link that's part of a retiring erasure coding topology if any of the tenant's namespaces still contain chunks for erasure-coded objects.
- You can select HCP namespaces for replication at any time, except during an upgrade of either system involved in the link you started from. You can deselect HCP namespaces from replication at any time, except during an upgrade of either system involved in the link you started from, while a link that includes the owning tenant is failed over, or while data recovery is occurring on a link that includes the owning tenant.
- After removing an HCP tenant or default-namespace directory from an active/active replication link, you can add the tenant or directory back to that link. While the tenant or directory is not on the link, operations on that tenant or directory, on replicated namespaces owned by that tenant, or on objects in those replicated namespaces or in that directory can occur on both systems involved in the link.

  Similarly, after deselecting a namespace for replication, you can select it again. If the tenant that owns the namespace is on an active/active link, while the namespace is deselected, operations on objects in the namespace can occur on both systems involved in the link.

  These considerations apply:

  - When you add a replicated tenant back to a link:
    - If you deleted the tenant on either system involved in the link while the tenant was not on the link, the tenant is replicated back to that system
    - If you deleted any of the tenant's replicated namespaces on either system involved in the link while the tenant was not on the link but you did not delete the tenant, those namespaces are replicated back to that system
    - If you deleted any objects in any of the tenant's replicated namespaces on either system involved in the link while the tenant was not on the link but you did not delete the tenant or those namespaces, those objects are deleted on the other system
  - When you add a replicated directory back to a link:
    - If you deleted the directory on either system involved in the link while the directory was not on the link, the delete operation is replicated to the other system
    - If you deleted any objects in the directory on either system involved in the link while the directory was not on the link but you did not delete the directory, those objects are deleted on the other system.
  - When you add a replicated tenant or directory back to a link or reselect a replicated namespace for replication, all operations that occurred in that tenant, directory, or namespace on either system while replication was not happening are replicated to the other system (except for the deletion of the tenant or namespace). During this replication, conflicts can occur between changes made on different systems while the tenant, directory, or namespace was not being replicated.
- After removing an HCP tenant or default-namespace directory from an active/passive link, you cannot add the tenant or directory back to that link unless you first delete the tenant or directory from the replica. This is because the tenant or directory now already exists on the replica.
- When you add one or more default-namespace directories to a link, some objects in directories that were already on the link may be reprocessed. This can increase the replication backlog for the default namespace.
- You cannot add an HCP tenant to an active/passive link if the same tenant already exists on the replica. Two tenants are the same as each other if they have the same internal ID.

  The only way the same tenant can exist on two systems is if it was created on one system and then replicated to the other system. Changing the name of the tenant on either of the systems does not make the two tenants different from each other.

- You cannot add an HCP tenant to any type of replication link if a different tenant with the same name already exists on the other system involved in the link. In this case, however, if you change the name of the tenant on either of the systems involved, you can add the tenant to the link.
- You cannot add a default-namespace directory to an active/passive link if a directory with the same name already exists on the replica. If the directory is empty on the primary system or the replica, you can change the directory name on that system. Then you can add the directory to the link.
- You cannot chain a replication link between system A and system B into an active/passive link between system B and system C if an HCP tenant on the first link has the same name as a different tenant that already exists on system C. However, if you change the name of the tenant on system A or system C, you chain the first link into the second link.
- You cannot chain a replication link between system A and system B into an active/passive link between system B and system C if an HCP tenant on the first link is the same as a tenant that already exists on system C, regardless of whether the tenant names are the same.
- You cannot chain a replication link between system A and system B into an active/passive link between system B and system C if a default-namespace directory on the first link has the same name as a default-namespace directory that already exists on system C.
- In a replication chain with the configuration A > B > C, if you add an HCP tenant to the link from system A to system B and the same tenant already exists on system C, replication of that tenant from system B to system C is automatically paused. To recover from this situation:
  1. Either delete the tenant on system C, or remove the tenant from the link from system A to system B.
  2. Resume replication of the tenant on the link from system B to system C.
- In a replication chain with the configuration A > B > C, if you add an HCP tenant to the link from system A to system B and a different tenant with the same name already exists on system C, replication of that tenant from system B to system C is automatically paused. To recover from this situation:
  1. Either rename the tenant on system C, delete the tenant on system C, or remove the tenant from the link from system A to system B.
  2. Resume replication of the tenant on the link from system B to system C.
- In a replication chain with the configuration A > B > C, if you add a default-namespace directory to the link from system A to system B and a default-namespace directory with the same name already exists on system C, replication of the default tenant from system B to system C is automatically paused. To recover from this situation:
  1. Either rename the directory on system C, delete the directory on system C, or remove the directory from the link from system A to system B. The first two options are possible only if the directory is empty on system C.
  2. Resume replication of the default tenant on the link from system B to system C.
- In a replication chain with the configuration A > B > C, if you add a default-namespace directory to the link from system A to system B and either of these is true, replication of the default tenant from system B to system C is automatically paused:
  - The default namespace doesn’t exist on system C. To recover from this situation:
    1. Create the default namespace on system C with the same retention mode and cryptographic hash algorithm as the default namespaces on systems A and B have.
    2. Resume replication of the default tenant on the link from system B to system C.
  - The default namespace exists on system C but has a different retention mode or cryptographic hash algorithm from the default namespaces on systems A and B. To recover from this situation:
    1. Delete the default-namespace directory from the link from system A to system B.

2. Resume replication of the default tenant on the link from system B to system C.

- On the Replication page in the System Management Console, each panel in which you can add and remove items of a specific type to and from a replication link includes a list of the items of the applicable type that are already included on the link. In those lists, rows containing items that have been deleted from HCP are highlighted in red and have a trash can icon ( ) on the right.

  HCP automatically removes each deleted namespace from a link after the deletion has been replicated. You need to remove deleted tenants and directories yourself.

  Important: Do not remove a deleted item from a replication link until after the deletion has been replicated.
- If you deselect a namespace from replication, any further action on that namespace, including deletion of the namespace, is not replicated. This enables a situation in which the owning tenant can end up with more namespaces than are allowed by its namespace quota and/or using more storage than is allowed by its hard quota.

  For example, consider the following scenario for a tenant has reached its namespace quota of five:

  1. The tenant is selected for replication on an active/passive link, along with all five of its namespaces.

     The tenant now has five namespaces on both the primary system and the replica.
  2. One of the namespaces is removed from the replication link.
  3. On the primary system, the tenant empties and deletes the removed namespace.

     The tenant now has four namespaces on the primary system and five namespaces on the replica.
  4. On the primary system, the tenant creates a new namespace.

     The tenant now has five namespaces on the primary system and five namespaces on the replica, but the namespaces on the two systems are not the same ones.
  5. The new namespace is added to the replication link.

     The tenant now has five namespaces on the primary system and six namespaces on the replica.

- A namespace can contain metadata-only objects on one or more HCP systems in a replication topology. If such a system is involved in only one replication link that includes the tenant that owns the namespace, the following actions can result in the data for those metadata-only objects becoming inaccessible from that system, possibly permanently:
  - You remove the tenant that owns the namespace from the link. In this case, to make the data accessible again:
    - If the link is active/active, add the tenant back into the link.
    - If the link is active/passive, either change the link to active/active, or create a new active/active link between the same two systems. Then add the tenant back to the changed link or to the new link, as applicable.
  - You deselect the namespace from replication. In this case, to make the data accessible again, reselect the namespace.
  - The tenant that owns the namespace is included on the first link in a replication chain, the namespace with the metadata-only objects is on the third HCP system in the chain, and you remove the first link from the link to the third system. In this case, to make the data accessible again:
    1. If the first link in the chain is active/passive, change the link to active/active.
    2. Either change the link to the third system to active/active, or create a new active/active link between the second and third systems in the chain.
    3. Add the tenant back to the changed link to the third system or to the new link, as applicable.
  - The namespace with the metadata-only objects is on the third HCP system in a replication chain, and you remove the tenant that owns the namespace from the first replication link in the chain. In this case, to make the data accessible again:
    1. Create a new active/active link between the first and second systems in the replication chain.
    2. Add the tenant to the new link.

    HCP displays a warning about metadata-only objects when you submit a request to delete an active/passive link or to remove a tenant from an active/passive link while any of the namespaces being replicated on the link contain metadata-only objects.

- You can add an HCP tenant to a replication link on one of the systems involved in the link even if the management and data access networks associated with that tenant aren't defined on the other system involved in the link. However, if these networks are not defined on the other system, the tenant and its namespaces will be inaccessible on that system.

  If a network associated with a tenant is undefined in a given system, the tenant list on the Tenants page in the System Management Console for that system shows this alert for the tenant:

Specifying link content

1. In the top-level menu of the HCP System Management Console for either system involved in the link, select Services > Replication.
2. On the replication Links page, click the link for which you want to specify content.
3. On the replication link details page, click Content.

Specifying link content for an active/active link

Adding HCP tenants in an active/active link

The link content Tenants panel for an active/active link has these sections:

Tenants Replicating
: Lists the HCP tenants already included on the link.

Local Tenants
: Lists the HCP tenants on the local system that are eligible for replication but not currently included on the link. This list does not include tenants that are read-only on the local system due to replication.

Remote Tenants
: Lists the HCP tenants on the other system involved in the link that are eligible for replication but not currently included on the link. This list does not include tenants that are read-only on the other system due to replication.

If a tenant has granted system-level users administrative access to itself, the row for the tenant in the applicable list shows the number of the tenant's namespaces that are selected for replication. On the primary system for an active/passive link, the row shows this number out of the total number of namespaces owned by the tenant.

1. (Optional) Filter the list from which you want to select one or more tenants to add to the link.
2. In the applicable list, select the tenants you want to add to the link.
   - To select all the tenants in the list, click Select All above the list.
   - To deselect all the selected tenants, click Clear above the list.

3. Click Add Selected Tenants below the applicable list.

Removing HCP tenants in an active/active link

The link content Tenants panel for an active/active link has these sections:

Tenants Replicating
: Lists the HCP tenants already included on the link.

Local Tenants
: Lists the HCP tenants on the local system that are eligible for replication but not currently included on the link. This list does not include tenants that are read-only on the local system due to replication.

Remote Tenants
: Lists the HCP tenants on the other system involved in the link that are eligible for replication but not currently included on the link. This list does not include tenants that are read-only on the other system due to replication.

If a tenant has granted system-level users administrative access to itself, the row for the tenant in the applicable list shows the number of the tenant's namespaces that are selected for replication. On the primary system for an active/passive link, the row shows this number out of the total number of namespaces owned by the tenant.

1. (Optional) In the Tenants Replicating section, filter the list of tenants that are currently included on the link.
2. In the tenants replicating list, select the tenants you want to remove from the link.
   - To select all the tenants in the list, click Select All above the list.
   - To deselect all the selected tenants, click Clear above the list.
3. Click Remove Selected Tenants.

Selecting HCP namespaces for tenants in an active/active link

You select and deselect HCP namespaces for replication in the Manage Namespaces window for the tenant that owns the namespaces. To open this window, in the link content Tenants panel, click the manage namespaces control ( ) for the owning tenant. This control is present only if the tenant has granted system-level users administrative access to itself.

When you start from an active/active link, the Manage Namespaces window has these sections:

Namespaces Selected for Replication
: Lists the tenant's namespaces that are currently selected for replication
Important:

- In the Namespaces Selected for Replication section, rows containing namespaces that have been deleted from HCP are highlighted in red and have a trash can icon ( ) on the right. HCP automatically removes each deleted namespace from this list after the deletion has been replicated.

  Do not manually remove deleted namespaces from this list. If you do, the deletion will not be replicated.

- Disabling replication for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

Local Namespaces
: Lists the namespaces that are owned by the tenant on the local system and that are not currently selected for replication

Remote Namespaces
: Lists the namespaces that are owned by the tenant on the other system involved in the link and that are not currently selected for replication

To close the Manage Namespaces window without taking any action, click the close control ( ) in the upper right corner.

1. (Optional) Filter the list from which you want to select one or more namespaces for replication.
2. For each listed namespace you want to select for replication, click in the namespace row.
   The namespace is selected, and the namespace row changes color.
   - To select all the namespaces in the list, click Select All above the list.
   - To deselect a selected namespace, click in the namespace row.
   - To deselect all the selected namespaces, click Clear.
3. Click Add Selected Namespaces below the list.

Deselecting HCP namespaces for tenants in an active/active link

You select and deselect HCP namespaces for replication in the Manage Namespaces window for the tenant that owns the namespaces. To open this window, in the link content Tenants panel, click the manage namespaces control ( ) for the owning tenant. This control is present only if the tenant has granted system-level users administrative access to itself.

When you start from an active/active link, the Manage Namespaces window has these sections:

Namespaces Selected for Replication
: Lists the tenant's namespaces that are currently selected for replication
Important:

- In the Namespaces Selected for Replication section, rows containing namespaces that have been deleted from HCP are highlighted in red and have a trash can icon ( ) on the right. HCP automatically removes each deleted namespace from this list after the deletion has been replicated.

  Do not manually remove deleted namespaces from this list. If you do, the deletion will not be replicated.

- Disabling replication for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

Local Namespaces
: Lists the namespaces that are owned by the tenant on the local system and that are not currently selected for replication

Remote Namespaces
: Lists the namespaces that are owned by the tenant on the other system involved in the link and that are not currently selected for replication

To close the Manage Namespaces window without taking any action, click the close control ( ) in the upper right corner.

1. (Optional) In the Namespaces Selected for Replication section, filter the list of namespaces that are currently selected for replication.
2. For each listed namespace you want to deselect from replication, click in the namespace row.

The namespace is selected, and the namespace row changes color.
- To select all the namespaces in the list, click Select All above the list.
- To deselect a selected namespace, click in the namespace row.
- To deselect all the selected namespaces, click Clear.

3. Click Remove Selected Namespaces below the list.

Adding default-namespace directories in an active/active link

The link content Default Tenant panel for an active/active link has these sections:

Directories Replicating
: Lists the HCP default-namespace directories already included on the link.

Local Directories
: Lists the default-namespace directories on the local system that are not currently included on the link. This list does not include directories that are read-only on the local system due to replication.

Remote Directories
: Lists the default-namespace directories on the other system involved in the link that are not currently included on the link. This list does not include directories that are read-only on the other system due to replication.

1. (Optional) Filter the list from which you want to select one or more directories to add to the link.
2. In the applicable directory list, select the directories you want to add to the link.
   - To select all the directories in the list, click Select All above the list..
   - To deselect all the selected directories, click Clear above the list.
3. Click Add Selected Directories below the applicable list.

Removing default-namespace directories in an active/active link

The link content Default Tenant panel for an active/active link has these sections:

Directories Replicating
: Lists the HCP default-namespace directories already included on the link.

Local Directories
: Lists the default-namespace directories on the local system that are not currently included on the link. This list does not include directories that are read-only on the local system due to replication.

Remote Directories
: Lists the default-namespace directories on the other system involved in the link that are not currently included on the link. This list does not include directories that are read-only on the other system due to replication.

1. (Optional) In the Directories Replicating section, filter the list of directories that are currently on the link.
2. In the list of replicating directories, select the directories you want to remove from the link.
   - To select all the directories in the list, click Select All above the list.
   - To deselect all the selected directories, click Clear above the list.
3. Click Remove Selected Directories below the list.

Specifying link content for an active/passive link

Adding HCP tenants in an active/passive link

The link content Tenants panel for an active/passive link has these sections:

Tenants Replicating
: Lists the HCP tenants already included on the link.

Local Tenants
: For outbound links only, lists the HCP tenants on the local system that are eligible for replication but not currently included on the link. This list does not include tenants that are either:

  - Read-only on the local system due to replication
  - Included on a link that is chained into the current link

  This section is not present for inbound links.

Remote Tenants
: For inbound links only, lists the HCP tenants on the other system involved in the link that are eligible for replication but not currently included on the link. This list does not include tenants that are either:

  - Read-only on the other system due to replication
  - Included on a link that is chained into the current link

  This section is not present for outbound links.

If a tenant has granted system-level users administrative access to itself, the row for the tenant shows the number of the tenant's namespaces that are selected for replication.

1. (Optional) Filter the list of tenants in the Local Tenants or section, as applicable.
2. In the applicable list, select the tenants you want to add to the link.
   - To select all the tenants in the list, click Select All above the list.
   - To deselect all the selected tenants, click Clear above the list.
3. Click Update Link.
   If you're removing tenants from the link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.

Removing HCP tenants in an active/passive link

The link content Tenants panel for an active/passive link has these sections:

Tenants Replicating
: Lists the HCP tenants already included on the link.

Local Tenants

For outbound links only, lists the HCP tenants on the local system that are eligible for replication but not currently included on the link. This list does not include tenants that are either:

- Read-only on the local system due to replication
- Included on a link that is chained into the current link

This section is not present for inbound links.

Remote Tenants

For inbound links only, lists the HCP tenants on the other system involved in the link that are eligible for replication but not currently included on the link. This list does not include tenants that are either:

- Read-only on the other system due to replication
- Included on a link that is chained into the current link

This section is not present for outbound links.

If a tenant has granted system-level users administrative access to itself, the row for the tenant shows the number of the tenant's namespaces that are selected for replication.

1. (Optional) Filter the list of tenants in the Tenants Replicating section.
2. In the list of replicating tenants, select the tenants you want to remove from the link.
   - To select all the tenants in the list, click Select All above the list.
   - To deselect all the selected tenants, click Clear above the list.
3. Click Update Link.
   If you're removing tenants from the link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.
   Important: Removing a tenant from an Active-Passive replication link on the Active site followed by its deletion from the Passive site can result in lost data if, in the future, an Active/Active replication link is created between the same clusters and the same tenant is added to that link.

Selecting HCP namespaces for tenants in an active/passive link

You select and deselect HCP namespaces for replication in the Manage Namespaces window for the tenant that owns the namespaces. To open this window, in the link content Tenants panel, click the manage namespaces control ( ) for the owning tenant. This control is present only if the tenant has granted system-level users administrative access to itself.

When you start from an active/passive link, the Manage Namespaces window has these sections:

Namespaces Selected for Replication

Lists the tenant's namespaces that are currently selected for replication.
Important:

- In the Namespaces Selected for Replication section, rows containing namespaces that have been deleted from HCP are highlighted in red and have a trash can icon ( ) on the right. HCP automatically removes each deleted namespace from this list after the deletion has been replicated.

  Do not manually remove deleted namespaces from this list. If you do, the deletion will not be replicated.

- Disabling replication for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

Select Namespaces for Replication

Lists the tenant's namespaces that are not currently selected for replication.

To close the Manage Namespaces window without taking any action, click the close control ( ) in the upper right corner.

1. (Optional) Filter the list of namespaces in the Select Namespaces for Replication section.
2. For each listed namespace you want to select for replication, click in the namespace row.
   The namespace is selected, and the namespace row changes color.
   - To select all the namespaces in the list, click Select All above the list.
   - To deselect a selected namespace, click in the namespace row.
   - To deselect all the selected namespaces, click Clear.
3. Click Update.

Deselecting HCP namespaces for tenants in an active/passive link

You select and deselect HCP namespaces for replication in the Manage Namespaces window for the tenant that owns the namespaces. To open this window, in the link content Tenants panel, click the manage namespaces control ( ) for the owning tenant. This control is present only if the tenant has granted system-level users administrative access to itself.

When you start from an active/passive link, the Manage Namespaces window has these sections:

Namespaces Selected for Replication

Lists the tenant's namespaces that are currently selected for replication.
Important:

- In the Namespaces Selected for Replication section, rows containing namespaces that have been deleted from HCP are highlighted in red and have a trash can icon ( ) on the right. HCP automatically removes each deleted namespace from this list after the deletion has been replicated.

  Do not manually remove deleted namespaces from this list. If you do, the deletion will not be replicated.

- Disabling replication for a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more systems in the replication topology.

Select Namespaces for Replication

Lists the tenant's namespaces that are not currently selected for replication.

To close the Manage Namespaces window without taking any action, click the close control ( ) in the upper right corner.

1. (Optional) Filter the list of namespaces in the Namespaces Selected for Replication section.
2. For each listed namespace you want to deselect from replication, click in the namespace row.

The namespace is selected, and the namespace row changes color.
- To select all the namespaces in the list, click Select All above the list.
- To deselect a selected namespace, click in the namespace row.
- To deselect all the selected namespaces, click Clear.

3. Click Update.

Adding default-namespace directories in an active/passive link

The link content Default Tenant panel for an active/passive link has these sections:

Directories Replicating
: Lists the default-namespace directories already included on the link.

Local Directories
: For outbound links only, lists the default-namespace directories on the local system that are not currently included on the link. This list does not include directories that are either:

- Read-only on the local system due to replication
- Included on a link that is chained into the current link

This section is not present for inbound links.

Remote Directories
: For inbound links only, lists the default-namespace directories on the other system involved in the link that are not currently included on the link. This list does not include directories that are either:

- Read-only on the other system due to replication
- Included on a link that is chained into the current link

This section is not present for outbound links.

1. Optionally, filter the list of directories in the Local Directories or Remote Directories section, as applicable.
2. In the applicable directory list, select the directories you want to add to the link.
   - To select all the directories in the list, click Select All above the list.
   - To deselect all the selected directories, click Clear above the list.
3. Click Update Link.
   If you're removing directories from the link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.

Removing default-namespace directories in an active/passive link

The link content Default Tenant panel for an active/passive link has these sections:

Directories Replicating
: Lists the default-namespace directories already included on the link.

Local Directories
: For outbound links only, lists the default-namespace directories on the local system that are not currently included on the link. This list does not include directories that are either:

- Read-only on the local system due to replication
- Included on a link that is chained into the current link

This section is not present for inbound links.

Remote Directories
: For inbound links only, lists the default-namespace directories on the other system involved in the link that are not currently included on the link. This list does not include directories that are either:

- Read-only on the other system due to replication
- Included on a link that is chained into the current link

This section is not present for outbound links.

1. (Optional) Filter the list of directories in the Directories Replicating section.
2. In the list of replicating directories, select the directories you want to remove from the link.
   - To select all the directories in the list, click Select All above the list.
   - To deselect all the selected directories, click Clear above the list.
3. Click Update Link.
   If you're removing directories from the link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.

Adding chained links in an active/passive link

The link content Chained Links panel for an active/passive link has these sections:

Links Replicating
: Lists the links already included in the current link.

Local Links
: For outbound links only, lists the active/active links in which the current link participates and the active/passive links for which the current system is the replica.
This section is not present for inbound links.

Remote Links
: For inbound links only, lists the active/active links in which the other system involved in the current link participates and the active/passive links for which the other system involved in the current link is the replica.
This section is not present for outbound links.

1. (Optional) Filter the list of links in the Local Links or Remote Links section, as applicable.
2. In the applicable list, select the links you want to add to the current link.
   - To select all the links in the list, click Select All above the list.
   - To deselect all the selected links, click Clear above the list.
3. Click Update Link.

If you're removing chained links from the current link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.

Removing chained links in an active/passive link

The link content Chained Links panel for an active/passive link has these sections:

Links Replicating
: Lists the links already included in the current link.

Local Links
: For outbound links only, lists the active/active links in which the current link participates and the active/passive links for which the current system is the replica.
This section is not present for inbound links.

Remote Links
: For inbound links only, lists the active/active links in which the other system involved in the current link participates and the active/passive links for which the other system involved in the current link is the replica.
This section is not present for outbound links.

1. (Optional) Filter the list of links in the Links Replicating section.
2. In the list of replicating links, select the links you want to remove from the current link.
   - To select all the links in the list, click Select All above the list.
   - To deselect all the selected links, click Clear above the list.
3. Click Update Link.
   If you're removing chained links from the current link, a confirming message appears.
4. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Update Link.

Filtering item selection lists

By default, the lists you use to add and remove items in replication links contain all of the applicable items. You can filter any of these lists to display a subset of the applicable items. A filtered list contains only those items with a name that begins with or is the same as a specified text string.

You cannot filter a list while any of the items in it are selected.

1. In the field above the list, 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, and is not case sensitive. White space is allowed.
2. Click the find control ( ).

To redisplay the entire list, click the clear filter control ( ).

Considerations for modifying a replication link

These considerations apply to modifying replication links:

- You can modify a replication link in the HCP System Management Console for either system involved in the link.
- You can modify a replication link at any time.
- You can change an active/passive link to an active/active link, but you cannot change an active/active link to an active/passive link.
- When changing an active/passive link to active/active, you need to ensure that replication checkpoints are up to date before converting, otherwise you risk losing directory metadata.
- You cannot change the direction of an active/passive link.
- If you change the domain name or IP addresses for either system involved in a link, the new domain name or IP addresses must identify the same system. The exception to this is when you're reconfiguring the link before restoring it to a new or rebuilt system.
- When you change an active/passive link to an active/active link, HCP suspends activity on the link. You need to resume activity on the link manually.
- While updating link properties other than the link type, HCP temporarily suspends activity on the link.

Modifying a replication link

You use separate procedures to modify the link properties you can set when you create a link and to modify the automatic failover and failback settings for a link.

Changing link properties

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the name of the link you want to modify.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Settings tab.
5. In the link Settings panel, make the changes you want.
6. Click Update Link.

Changing automatic failover and failback settings

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the name of the link you want.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Failover tab.
5. In the Failover panel, click Automatic Failover Settings.
6. In the Automatic Failover Settings section:
   - For an active/active link or an inbound active/passive link, in the Local System section:
     - To enable automatic failover to the current system, select Fail over automatically. Then, in the Automatically fail over link after loss of connectivity for field, type the number of minutes HCP should wait before automatically failing over the link after a loss of connectivity to the other system involved in the link. Valid values are integers in the seven through 9,999.
     - To disable automatic failover to the current system, deselect Fail over automatically.
     - For active/passive links only, to enable automatic failback to the other system involved in the link, select Complete recovery automatically. Then, in the Automatically complete recovery when synchronization is less than field, type the number of minutes the up-to-date-as-of time for the link must be less than before HCP should automatically fail back the link. Valid values are integers in the one through 9,999.
     - For active/passive links only, to disable automatic failback to the other system involved in the link, deselect Complete recovery automatically.

- For an active/active link or an outbound active/passive link, in the Remote System section:
  - To enable automatic failover to the other system involved in the link, select Fail over automatically. Then, in the Automatically fail over link after loss of connectivity for field, type the number of minutes HCP should wait before automatically failing over the link after a loss of connectivity to the current system. Valid values are integers in the seven through 9,999.
  - To disable automatic failover to the other system involved in the link, deselect Fail over automatically.
  - For active/passive links only, to enable automatic failback to the current system, select Complete recovery automatically. Then, in the Automatically complete recovery when synchronization is less than field, type the number of minutes the up-to-date-as-of time for the link must be less than before HCP should automatically fail back the link. Valid values are integers in the one through 9,999.
  - For active/passive links only, to disable automatic failback to the current system, deselect Complete recovery automatically.

7. Click Update Settings.

Considerations for deleting a replication link

These considerations apply to deleting replication links:

- You can delete a replication link in the HCP System Management Console for either system involved in the link.
- You can delete a replication link only while activity on the link is suspended.
- When you delete a replication link, replication on that link immediately stops. The HCP tenants and default-namespace directories on the link remain or become read-write on both systems involved in the link.
- You can delete a replication link that's included as a chained link in a second replication link. When you do this, the HCP tenants and default-namespace directories that were on the deleted link are automatically included individually in the second link.
- After deleting an active/passive link, you can no longer replicate the HCP tenants and default-namespace directories included on that link to the same replica on an active/passive link unless you first delete them on the replica. If you don't delete them, when you create a new active/passive link with the same replica, HCP doesn't let you include them because they now exist on both systems.

  If the possibility exists that you will want to replicate those tenants and directories again to the same replica on an active/passive link, you should either pause replication for the individual tenants or suspend activity on the link instead of deleting the link.

- After deleting an active/passive link, you can include the HCP tenants and default-namespace directories that were included on the deleted link in a new or existing active/active link. In this case, you do not need to delete those tenants and directories from the system that was the replica for the deleted link.
- A namespace can contain metadata-only objects on one or more systems in a replication topology. If you delete the only replication link that involves such a system, the data for those metadata-only objects becomes inaccessible from that system. In this case, to make the data accessible again:
  - If the deleted link was active/active, recreate the link.
  - If the deleted link was active/passive, recreate the link as an active/active link.
- You cannot delete a replication link that's part of an active or retiring erasure coding topology.
- You can delete a link that's part of a retired erasure coding topology.

Deleting a replication link

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the name of the link you want to delete.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Management tab.
5. In the Management panel, click Delete Replication Link.
6. In the Delete Replication Link section, click Delete.
7. In response to the confirming message:
   - If any namespace being replicated on the link contains metadata-only objects on either of the systems involved in the link or if the two systems involved in the link cannot communicate with each other:
     a. In the field in the message window, type `YES`. This value is case sensitive.
     b. Click Delete Link.
   - If no namespaces being replicated on the link contain metadata-only objects on either of the systems involved in the link and the two systems involved in the link can communicate with each other, click Delete Link.

Working with erasure coding topologies

An erasure coding topology provides all the information the Replication service and Geo-distributed Erasure Coding service need to implement erasure-coded protection. You can create and manage an erasure coding topology in the HCP System Management Console from any of the HCP systems included in the topology.

To create an erasure coding topology, you select the HCP systems and replication links to include in the topology. You also set the topology properties. After you create the topology, you add HCP tenants to it. If the tenants you add are not already on the replication links in the erasure coding topology, they are automatically added to those links.

You can modify the properties of an erasure coding topology at any time. You can also replace the systems in a topology, but you cannot replace the links.

You can retire and delete erasure coding topologies. However, these actions should be taken only with a full understanding of the consequences.

This section of the Help contains considerations and instructions for performing the activities mentioned above.

To view an erasure coding topology, you need the monitor or administrator role. To create, specify tenants for, modify, retire, or delete an erasure coding topology, you need the administrator role.

You can also use the HCP management API to create, specify tenants for, modify, retire, and delete erasure coding topologies.

About erasure coding topologies

An erasure coding topology consists of a set of HCP systems and active/active replication links that connect those systems. Within an erasure coding topology, each system must have at least two paths to each other system. Each path can consist of any number of systems and links, but the paths cannot have any systems or links in common.

When you create an erasure coding topology, you select the systems to include in it. The systems you select must be part of an existing active/active replication ring topology or fully connected active/active replication topology.

For each pair of selected systems that are connected to each other in the underlying replication topology, if the pair has only one active/active replication link between them, that link is automatically included in the erasure coding topology. If any pair of the selected systems is connected by more than one active/active link, you select which one of those links to include in the erasure coding topology.

An erasure coding topology does not automatically include the tenants on the links in the underlying replication topology. Instead, you select the tenants to include in an erasure coding topology from all the replication-enabled tenants defined on the systems in the topology. Each tenant you select is automatically added to each link in the erasure coding topology.

When you create an erasure coding topology, it's in the active state. If you want to stop using the active topology for erasure-coded protection, you need to retire the topology.

Retiring an erasure coding topology causes the Geo-distributed Erasure Coding service to restore object chunks to full-copies or, on systems where the objects are on metadata-only storage tiers, delete the chunks. While the chunks are being restored or deleted, the topology is in the retiring state.

When all the systems in a retiring erasure coding topology have no more chunks that are the result of that topology, the state of the topology changes to retired. Once a topology is retired, you can delete it. Deleting an erasure coding topology does not cause any systems, links, tenants, namespaces, or objects to be deleted.

A system can be in at most five erasure coding topologies concurrently. Only one of those topologies can be active. The rest must be either retiring or retired.

Erasure coding topology properties

An erasure coding topology has these properties:

- A name and, optionally, a description.
- The number of HCP systems in the erasure coding topology. A topology can have from three through six systems.
- For an erasure coding topology with four or more systems, the type of the underlying replication topology: ring or fully connected. The topology type for three systems is always fully connected.
- A distribution method — chunk or full copy.
- A minimum size for erasure coding objects and object parts — 4 KB, 16 KB, 32 KB, 64 KB, 128 KB, 256 KB, 512 KB, or 1 MB. HCP erasure-codes only objects and object parts with a size greater than or equal to the minimum size you select. HCP uses whole-object protection for objects and parts below the minimum size, regardless of whether the containing namespace is using erasure-coded protection.
  Note: The service plan associated with a namespace can include a metadata-only storage tier on all the systems in an erasure coding topology. With this configuration, objects and parts in the namespace that are smaller than the minimum size for erasure coding may have data on only one of those systems. As a result, those objects and parts are not protected against a single system failure.
- An erasure coding delay. This is the amount of time the Geo-distributed Erasure Coding service waits before reducing a full copy of the data for an object or object part to a chunk. With full-copy distribution, this is also the amount of time the service waits on systems where the object or part is metadata-only before requesting a chunk for the object.
- Optionally, a restore period. If an erasure coding topology has a restore period, after an object or object part that's subject to erasure coding is read from a system in the topology, a full copy of the object or part data is kept on that system at least until the restore period expires.

When setting the minimum size, erasure coding delay, and restore period, consider the tradeoffs with respect to storage efficiency and read performance.

Erasure coding delay

The erasure coding delay is counted from the time the ingest system receives the object or part data. You specify the delay as a number of days.

Even if the erasure coding delay has expired for an object, the Geo-distributed Erasure Coding service does not reduce a full copy of the data for the object or part to a chunk if doing so would leave the object or part insufficiently protected.

Restore period

You specify the restore period for an erasure coding topology as a number of days. If the specified number is zero, the topology does not have a restore period.

When an object or part that's subject to erasure coding is read from a given system, where that system is in an erasure coding topology with a restore period:

- If the system currently has a full copy of the object or part data, the restore period applies to that full copy.
- If the system currently has a chunk for the object or part on primary running storage, on an S Series Node, or on spindown storage and the chunk has never been tiered to extended storage, a full copy of the object or part data is restored on the current tier, and the chunk is deleted. The restore period applies to the restored full copy.
- While the system has only a full copy of the object or part data, the object or part is not counted as an erasure-coded object on that system.
- If the system currently has a chunk for the object or part and the chunk is or ever was on an extended storage tier, a full copy of the object or part data is restored on the highest storage tier that could have had a full copy of the data, and the chunk is deleted. The restore period applies to the restored full copy.
  Note: For objects and parts that are subject to erasure coding, the storage tiers that can have a full copy of the object or part data are primary running storage, HCP S Series Node, and primary spindown storage. HCP never tiers a full copy of the object or part data to extended storage. Instead, when the Geo-distributed Erasure Coding service on a system reduces a full copy of object or part data to a chunk, if the object or part is due to be tiered, that service puts the chunk on the applicable storage tier.

The restore period for an object or part starts when the object or part is read. If the object or part is read again during the restore period, the restore period restarts from the time of that read operation.

The restore period for an object or part can restart only once on any given day. After the first restart on a day, subsequent reads on the same day do not cause the restore period to restart.

The restore period for an object or part can start before the erasure coding delay has expired. If the erasure coding delay then expires before the restore period expires, the full copy of the object or part data is not reduced to a chunk until the restore period expires. If the restore period expires before the erasure coding delay expires, the full copy of the object or part data is not reduced to a chunk until the erasure coding delay expires.

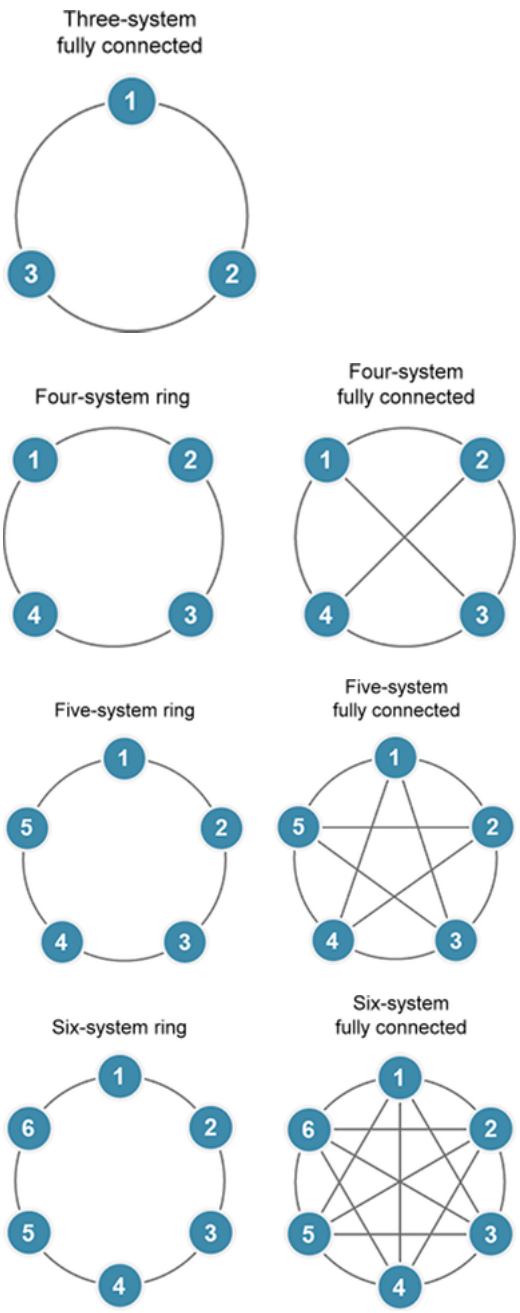
Note: Internal reads (for example, by an HCP service) do not cause object or part chunks to be restored to full copies of the object or part data and do not start or restart restore periods.

Supported replication topologies

An erasure coding topology can include from three through six HCP systems. An erasure coding topology with four, five, or six systems can be based on either an active/active replication ring topology or a fully connected active/active replication topology. A three-system erasure coding topology is always based on a fully connected active/active replication topology.

Before you can create an erasure coding topology, the underlying replication topology must already exist.

The figures below show all the replication topologies on which an erasure coding topology can be based.



Erasure coding topology retirement

When you retire an erasure coding topology, the protection type for any namespaces that were using erasure-coded protection changes to whole-object protection. This change causes the Geo-distributed Erasure Coding service to, for any given object:

- Restore the chunk for the object to a full copy of the object data on HCP systems where the object is not supposed to be metadata-only. As the service restores chunks to full copies, the use of storage on those systems increases.
- Delete the chunk for the object on HCP systems where the object should be metadata-only. The service does not delete the chunk for an object until a full copy of the object data exists either on at least two systems in the topology or on one system if the object should have data on only one system.

  For any given erasure-coded object, if the object should be metadata-only on every system in the topology, the Geo-distributed Erasure Coding service on one system restores the chunk to a full copy. The system where this occurs varies depending on when the service processes the object on each system in the topology.

The number of concurrent system failures HCP can tolerate for a replicated namespace with whole-object protection is one less than the number of systems where the namespace contains object data. Therefore, to maintain at least the same protection level with whole-object protection as the protection level maintained by erasure-coded protection, the underlying replication topology must include at least two systems where the replicated namespaces contain object data.

Before retiring an erasure coding topology, you need to ensure that any system where object chunks will be restored to full copies of the object data has sufficient storage to accommodate that data.

Tip: To estimate the amount of storage required on a given system:

1. For each tenant included in the retiring erasure coding topology, use the management API to get the value of the `erasureCodedSize` property of the /tenants/tenant-name/statistics resource. This value is the total amount of storage, in bytes, occupied by chunks for erasure-coded objects in all the tenant's namespaces.
2. Add together the numbers of bytes occupied by chunks for erasure coded objects for all the tenants. The total is the number of bytes occupied by chunks for all erasure-coded objects on the system.
3. Multiply the total number of bytes by the number of data chunks in the topology protection level. The result is an estimate of the required amount of storage, in bytes.

Also before retiring an erasure coding topology, if you don't want chunks for objects in a namespace restored to full copies of the object data on a given system, ensure that, on that system, the namespace is already associated with a service plan that keeps all objects in the namespace on a metadata-only storage tier. That way, chunks are not unnecessarily restored to full copies on systems where the objects should be metadata-only.

As the Geo-distributed Erasure Coding service on a system processes the chunks for a retiring erasure coding topology, the number of erasure-coded objects for that topology on that system decreases. When that number reaches zero on all the systems in the topology, the state of the topology changes to retired.

For any given system in an erasure coding topology, you can use the erasure coding topology details page in the HCP System Management Console to monitor the count of erasure-coded objects for that topology on that system.

You can also view counts of erasure-coded objects for all active and retiring erasure coding topologies:

- The storage Overview page shows the total number of erasure-coded objects currently stored on the system.
- The tenant Overview panel shows the total number of erasure-coded objects in all the tenant's namespaces.

These counts are not specific to an erasure coding topology. If an active erasure coding topology exists, these numbers do not go down to zero when an erasure coding topology has finished retiring.

Chargeback reports also contain erasure-coded object counts for the system, tenants, and, if you have administrative access to a tenant, the namespaces owned by that tenant.

Erasure coding topology replacement

You cannot add or remove HCP systems in an erasure coding topology. You also cannot add, remove, or replace replication links in an erasure coding topology. If you want to change a topology in any of these ways, you need to retire the topology and create a new one to replace it.

After you retire an erasure coding topology, you cannot make it active again. If you inadvertently retire a topology, you can replace it with a new topology that includes the same systems and links.

To replace a system in an active erasure coding topology, you don't need to create a new topology. Instead, you use the procedure for replacing a failed system. At the end of this procedure, replication restarts with the replacement system, and the replacement system receives full copies of object data or chunks for objects, as determined by the erasure coding topology.

Note: To replace a system in an active erasure coding topology with a system that has a different domain name or different IP addresses, you need to reconfigure the replication links that connect other systems in the topology to the system you're replacing. When reconfiguring the links, ensure that they all connect to the same replacement system. If the links connect to different systems, the erasure coding topology will no longer be functional.

Erasure coding topology replacement process

When replacing an erasure coding topology, you don't need to wait for the old topology to finish retiring before you create the new topology. During the replacement process, the Geo-distributed Erasure Coding service on each system in the retiring topology determines what to do with each object affected by that topology based on:

- The current state of the object on the system (full copy or chunk).
- The state the object should be in with the new topology. (Until you create the new topology, the object is subject to whole-object protection.)
- The requirement that the object always be protected against a single system failure.

During the topology replacement process, the Geo-distributed Erasure Coding service on any given system in the retiring topology can take any of these actions on an object:

- If the system is part of the new topology:
  - Reduce a full copy of the object data to the chunk for the new topology
  - Replace an existing chunk for the object with the chunk for the new topology
  - Restore an existing chunk for the object to a full copy of the object data and, some time later, reduce the full copy to the chunk for the new topology
  - Restore an existing chunk for the object to a full copy of the object data and, if the object is smaller than the minimum size for erasure coding with the new topology, leave the full copy as is
  - Make no change if the existing full copy of the object data or chunk for the object is the same as it should be with the new topology
- If the system is not part of the new topology but should contain data for the object, restore an existing chunk for the object to a full copy of the object data
- Regardless of whether the system is part of the new topology:
  - Delete the existing chunk or full copy of the object data if the system should not contain data for the object (that is, the object should be metadata-only).
  - Completely delete the object (that is, delete both the data and metadata for the object).

    During the topology replacement process, the Geo-distributed Erasure Coding service deletes an object only on detecting that the object has been deleted on another system in the retiring topology. The service can delete the object even if replication is paused on the link over which the service detected the deletion.

For systems that are in both the retiring and new topologies, you cannot predict on which systems the service will try to restore chunks to full copies of object data. Therefore, to facilitate the topology replacement, you should ensure that each system in the topology you're retiring has significantly more free space than the space required for the addition of a full copy of the data for the largest object that was erasure coded.

Systems in the retiring topology that are not also in the new topology must have enough free space to accommodate full copies of the object data for all erasure-coded objects that are not supposed to be metadata-only.

During the topology replacement process, the number of erasure-coded objects for the retiring topology only decreases on each system. However, the total number of erasure-coded objects on each system can increase or decrease unpredictably until the topology replacement is complete.

Considerations for replacing an erasure coding topology

You can replace an erasure coding topology with a topology that includes some but not all of the HCP systems in the old topology. When you add a tenant in the old topology to the new topology, replication of that tenant is automatically paused on each link where:

- The link is not in the new topology
- One or both of the systems involved in the link are in the new topology

Although replication of the tenant is paused on those links, the tenant, its replicated namespaces, and the objects in those namespaces still exist on systems in the old topology that are not in the new topology.

In this situation, you may want to sever the relationship between the tenant on systems in the new topology and the tenant on systems that are not in the new topology. Severing this relationship lets you:

- Delete the tenant either on systems in the new topology or on systems that are not in the new topology but not on both
- Delete one or more of the tenant's replicated namespaces either on systems in the new topology or on systems that are not in the new topology but not on both
- Delete one or more objects in the tenant's replicated namespaces either on systems in the new topology or on systems that are not in the old topology but not on both

Before you sever the tenant relationship, do not let clients access the tenant or its replicated namespaces on systems where you plan to delete that tenant or those namespaces . Disallowing access prevents situations such as this, where these events occur in the order shown:

1. A client makes a change to an object on a system where the tenant or containing namespace will be deleted.
2. You sever the tenant relationship before the change is replicated to a system where the tenant or namespace will not be deleted.

To sever the tenant relationship:

1. Wait for each system in the old topology to have no objects that are erasure coded according to that topology.

   You can see the number of objects that are erasure coded according to a given topology on the details page for that topology in the HCP System Management Console.

2. When the state of the old topology changes to retired, delete that topology.
   Important: Do not resume replication of the tenant on the links where replication of the tenant is paused.
3. Remove the tenant from each link between a system in the new topology and a system that's not in the new topology.

After severing a tenant relationship, you can add the tenant back to the links from which you removed that tenant only if the tenant is not in the erasure coding topology (either because you removed the tenant from the topology or because you deleted the tenant from the systems in the topology).

Erasure coding topology replacement procedure

When replacing an erasure coding topology, use this procedure to ensure that the replacement process occurs in the most efficient manner:

1. Disable the Geo-distributed Erasure Coding service on each system in the topology you're replacing.
   Doing this will prevent the service from restoring chunks for objects to full copies that will later need to be reduced to chunks.
   Note: Services can be disabled from the system Overview page in the System Management Console. To disable services, you need the service role.
2. Disable the Storage Tiering service on each system in the topology you're replacing.
   Doing this will prevent the service from tiering full copies of object data that will later need to be reduced to chunks.
3. If all of the following are true for any given namespace on any given system, ensure that the service plan associated with that namespace keeps all objects in the namespace on a metadata-only storage tier on that system:
   - The system will be included in the new erasure coding topology.
   - The namespace has erasure coding allowed, and the tenant that owns the namespace will be included in the new topology.
   - You want each object in the namespace to use whole-object protection until the erasure coding delay specified by the new topology expires.
   - You want objects in the namespace to be metadata-only on the system while they are subject to whole-object protection.

     With whole-object protection, HCP does not store data for objects on metadata-only storage tiers. However, if an object should be on a metadata-only storage tier on all the systems in the topology, one system in the topology will store data for that object.

   Keeping objects on a metadata-only storage tier on one or more systems will prevent full copies of object data from being distributed to those systems:

   - Between the retirement of the existing topology and the creation of the new topology
   - Before the expiration of the erasure coding delay for the new topology

   Note: To keep objects protected during the replacement procedure, ensure that the service plan associated with each applicable namespace does not include a metadata-only storage tier on at least two of the systems in the topology you're replacing. To distribute the storage load, on any given system, configure the applicable service plans such that some include a metadata-only storage tier and some do not.
4. Retire the existing erasure coding topology.
   Newly ingested objects are now replicated using whole-object protection. Objects that are already erasure coded remain erasure coded.
5. Create any new replication links you need for the new erasure coding topology.
   Do not add tenants to the new links at this point. The tenants will be added to the links automatically when you add the tenants to the new topology.
6. Create the new erasure coding topology and then add tenants to it.
   The tenants you add are automatically added to any replication links in the topology that do not already include them.
   The tenants you add to the new erasure coding topology may already be included on links not in the topology, where one of the systems involved in the link is in the topology. When this is the case, replication or recovery of those tenants is automatically paused on those links.
7. Reenable the Geo-distributed Erasure Coding service.
   The service starts processing objects again.
8. Reenable the Storage Tiering service.
   The service starts tiering object chunks that are the result of the new erasure coding topology.
9. When the state of the retiring erasure coding topology changes to retired, delete that topology.

Considerations for creating an erasure coding topology

These considerations apply to creating an erasure coding topology:

- Before you can create an erasure coding topology:
  - All the HCP systems to be included in the erasure coding topology must be at release 8.0 or later.
  - All the HCP systems to be included in the erasure coding topology must be available.
  - The underlying replication topology must already exist.
  - Each system in the underlying replication topology must be able to recognize each other system in the topology through a path of one or more active/active replication links. However, these links do not need to be the links you include in the erasure coding topology.
- All replication links to be included in an erasure coding topology must be active/active.
- You can create an erasure coding topology from any HCP system to be included in the topology. You cannot create an erasure coding topology from a system that will not be part of the topology.
- You cannot create an erasure coding topology while any HCP systems to be included in the topology are being upgraded.
- Each link to be included in an erasure coding topology can include any number of tenants, including none. Those tenants do not need to be included in the erasure coding topology.
- The links to be included in an erasure coding topology can include different tenants from each other.
- Two systems to be connected by a replication link in a new erasure coding topology can already be connected by a link in a retiring or retired topology. If this is the case, the new topology must include that link. You cannot use a different link to connect the two systems in the new topology.

Creating an erasure coding topology

1. In the top-level menu of the HCP System Management Console for any system you want to include in the erasure coding topology, select Services > Geo-distributed EC.
2. On the EC Topologies page, click Create Erasure Coding Topology.
   The erasure coding topology creation wizard opens.

3. Review the information on the wizard Overview page. Then click Next.
4. On the wizard Name page:
   a. In the Name field, type a name for the erasure coding topology.
      The name must be from one through 64 characters long and can contain any valid UTF-8 characters, including white space. Erasure coding topology names are not case sensitive.
      Erasure coding topology names must be unique for each HCP system in the topology. That is, you cannot use the name of a retiring or retired topology as the name for a new topology that will include any of the same systems as the retiring or retired topology. You can reuse the name of a deleted topology.
   b. (Optional) In the Description field, type a description for the erasure coding topology.
      The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
5. Click Next.
6. On the wizard HCP System Selection page:
   a. In the Number of HCP Systems field, select the number of systems to be included in the erasure coding topology.
   b. If you selected 4, 5, or 6 for the number of systems, for Topology Type, select Ring or Fully connected.
   c. In each numbered field in the HCP Systems section, select an HCP system to be included in the erasure coding topology:
      - For a ring topology, the order of the systems in the numbered fields must correspond to the arrangement of the systems in the topology diagram displayed on the page, with your choice of system as number one.
      - For a fully connected topology, the systems can be in any order in the numbered fields.

   If you don't see all the systems you want to include in the erasure coding topology, check that all required links exist and are healthy.

   In the process of creating the erasure coding topology, HCP may change which system is associated with each number. However, this change in no way affects the topology itself.

7. Click Next.
8. On the wizard Link Selection page, for each pair of HCP systems connected by more than one replication link, select the link you want to include in the erasure coding topology.
   For each pair of systems connected by a single link, that link is automatically included in the erasure coding topology. These pairs on not listed on the Link Selection page.
9. Click Next.
10. On the wizard Settings page:
    a. For Distribution Method, select Chunk distribution or Full-copy distribution.
    b. In the Minimum Object or Object Part Size for Erasure Coding field, select the minimum size for objects and parts of multipart objects to be erasure coded.
       The options are 4 KB, 16 KB, 32 KB, 64 KB, 128 KB, 256 KB, 512 KB, and 1 MB.
    c. In the Erasure Coding Delay field, type the number of days after ingest that full copies of object or part data should be reduced to chunks.
       Valid values are integers in the range zero through 3,650.
    d. In the Restore Period field, type the number of days that full copies of object or part data should remain on the ingest after being restored from chunks due to a read operation.
       Valid values are integers in the range zero (no restore period) through 180.
11. Click Next.
12. On the wizard Review page, review the erasure coding topology configuration.
    - If the erasure coding topology configuration is what you want, click Finish.
    - If the erasure coding topology configuration is not what you want, use the Previous button in the wizard to return to pages on which you want to make corrections. Alternatively, press Cancel to leave the wizard without creating the erasure coding topology.

Considerations for specifying the tenants for an erasure coding topology

These considerations apply to specifying the content for an erasure coding topology:

- When you add a tenant to an erasure coding topology, that tenant is automatically included on all the replication links in the underlying replication topology. Therefore, all the considerations that apply to adding a tenant to a replication link apply to adding a tenant to an erasure coding topology.
- An erasure coding topology can include at most one thousand tenants.
- You cannot add default-namespace directories to an erasure coding topology.
- You cannot add or remove tenants from a retiring or retired erasure coding topology.
- You can use the System Management Console for any system in an erasure coding topology to add tenants to that topology.
- You choose tenants to add to an erasure coding topology from a list of tenant candidates. This list includes only tenants for which all of these are true:
  - Replication is enabled for the tenant.
  - The tenant exists on at least one system in the topology.
  - For at least one such system, either:
    - The tenant is not on any links in which that system participates.
    - The tenant is on one or more links in which that system participates, and each of those links is in an active, retiring, or retired topology.

    If, for every such system, the tenant is on one or more links that are not in an active, retiring, or retired topology, the tenant is not included in the candidate list. In this case, to have HCP include the tenant in the candidate list, for at least one of the systems, remove the tenant from all links not in an active, retiring, or retired topology.

- You cannot add a listed tenant candidate to an erasure coding topology if either of these is true:
  - A different tenant with the same name exists on one or more other systems in the topology.

    To add a tenant with a name conflict to the topology, you first need to either rename that tenant or rename the other tenants that have the same name.

  - The tenant is on a link that's not in the topology, and both of these are true:
    - One or both of the systems involved in the link are in the topology.
    - The link is not in an active, retiring, or retired topology.

    To add a tenant with a link conflict to the topology, you first need to remove the tenant from all the links that satisfy the above criteria for at least one system in the topology.

  In the tenant candidate list, tenants with a name conflict or link conflict are accompanied by an icon ( ) indicating that an issue exists. The hover text for the icon identifies the issue.

- When you add a tenant to an erasure coding topology, namespaces owned by the tenant use erasure-coded protection only if they are configured to allow erasure coding. Namespaces that are not configured this way use whole-object protection.
- If you have administrative access to a tenant:
  - You can use the System Management Console to select namespaces for replication by starting from a replication link that includes the owning tenant
  - You can use the Tenant Management Console to select namespaces for replication and, at the same time, configure them to be cloud optimized and to allow erasure coding
- When you add tenants to an erasure coding topology, the process of including those tenants on the all the replication links in the topology can take up to five minutes.

- When you add a tenant to an erasure coding topology, replication of that tenant is automatically paused on all links for which all of these are true:
  - The tenant is on the link.
  - The link is not in the topology.
  - One or both of the systems involved in the link are in the topology.
- When you remove a tenant from an erasure coding topology, the tenant remains on all the links in the underlying replication topology, but the tenant's namespaces that allow erasure coding change from using erasure-coded protection to using whole-object protection. The effect of this change is the same as the effect of retiring an erasure coding topology.
- You cannot remove a tenant from a retiring erasure coding topology if any objects in any of the tenant's namespaces still contain objects that were erasure coded according to that topology.
- You can add and remove tenants in an erasure coding topology while one or more systems in the topology are unreachable from other systems in the topology. If conflicting changes are made during this period (for example, the same tenant is added on two different systems and then removed on one of those systems), the most recent change is the one that takes effect when communication between the systems is restored.
- While a system in an erasure coding topology is being upgraded, you cannot use that system to add or remove tenants in that topology.

Specifying the tenants for an erasure coding topology

You use the Tenants panel for an erasure coding topology to specify the tenants for the topology. This panel contains two sections:

Tenants in This Erasure Coding Topology
: Lists the tenants that are currently included in the erasure coding topology. The tenants are listed in alphanumeric order by name.

Tenant Candidates
: Lists the tenants from which you can choose tenants to be added to the erasure coding topology. The tenants are listed in alphanumeric order by name.

Each listed tenant with a name conflict or link conflict is accompanied by this icon: . The hover text for the icon identifies the issue.

Adding and removing tenants

1. In the top-level menu of the HCP System Management Console, select Services > Geo-distributed EC.
2. On the EC Topologies page, click the topology for which you want to specify the tenants.
3. On the erasure coding topology details page, click Tenants.
4. Take either or both of these actions:
   - To add tenants to the erasure coding topology:
     a. (Optional) In the Tenant Candidates section, filter the list of tenants that are eligible to be included in the topology.
     b. In the tenant candidate list, select the tenants you want to add to the topology.
        - To select all the tenants in the list, click Select All above the list.
        - To deselect all the selected tenants, click Clear above the list.
     c. Click Add Selected Tenants.
   - To remove tenants from the erasure coding topology:
     a. (Optional) In the Tenants in This Erasure Coding Topology section, filter the list of tenants that are currently included in the topology.
     b. In the list of tenants in the topology, select the tenants you want to remove from the topology.
        - To select all the tenants in the list, click Select All above the list.
        - To deselect all the selected tenants, click Clear above the list.
     c. Click Remove Selected Tenants.

Filtering the tenant lists

By default, each tenant list in the Tenants panel contains all the applicable tenants. You can filter the list in either section to display a subset of the applicable tenants. A filtered list contains only those items with a name that begins with or is the same as a specified text string.

You cannot filter a list while any of the tenants in it are selected.

Filtering

You can filter the tenant list by tenant name or tag. The filtered list includes only those tenants with a name or tag, as applicable, that begins with or is the same as a specified text string.

1. In the field above the Name column, select Name to filter by name or Tag to filter by tag.
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 ( ).

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

Considerations for modifying an erasure coding topology

These considerations apply to modifying an erasure coding topology:

- You can modify these properties of an active erasure coding topology:
  - Name
  - Description
  - Distribution method
  - Minimum object size for erasure coding
  - Erasure coding delay
  - Restore period
- You cannot modify a retiring or retired erasure coding topology.
- Changes you make to the configuration of an erasure coding topology apply to existing objects as well as to new objects.
- When you change the distribution method from chunk distribution to full-copy distribution, previously distributed chunks are restored to full copies of object data if the erasure coding delay has not yet expired. The full copies are reduced to chunks again after the erasure coding delay expires.
- When you change the distribution method from full-copy distribution to chunk distribution, previously distributed full copies of object data are reduced to chunks after the erasure coding delay expires.
- When you reduce the minimum object size for erasure coding, for any given object that was previously subject to whole-object protection but is now subject to erasure coding:
  - On a system where the object is not metadata-only, the object data is reduced to a chunk after the erasure coding delay expires

    - On a system where the object is metadata-only:
        - If the erasure coding topology is configured for chunk distribution, the system receives a chunk for the object.
        - If the erasure coding topology is configured for full-copy distribution, the system receives a chunk for the object if the erasure coding delay has already expired. If the erasure coding delay has not yet expired, the system receives a chunk for the object when the delay expires.
- When you increase the minimum object size for erasure coding, for any given object that was previously subject to erasure coding but is now subject to whole-object protection:
    - On a system where the object is not supposed to be metadata-only:
        - If the system has a chunk for the object, the chunk is restored to a full copy of the object data
        - If the system has a full copy of the object, the full copy remains as is
    - On a system where the object should be metadata-only, the chunk for the object or the full copy of the object data, as applicable, is deleted
- When you increase the erasure coding delay for an erasure coding topology configured for full-copy distribution, chunks for existing objects for which the new delay has not yet expired are restored to full copies of the object data.
- When you decrease the restore period, objects that are currently in a restored state and for which the new restore period has already expired are returned to their previous erasure-coded states.
- When you increase the restore period, objects that are currently in a restored state and for which the new restore period has not yet expired are returned to their previous erasure-coded states after the new restore period expires.
- You can modify an erasure coding topology from any system in the topology.
- While a system in an erasure coding topology is being upgraded, you cannot use that system to modify the topology.

Modifying an erasure coding topology

1. In the top-level menu of the HCP System Management Console, select Services > Geo-distributed EC.
2. On the EC Topologies page, click the topology you want to modify.
3. On the erasure coding topology details page, click Settings.
4. In the Settings panel, make the changes you want.
5. Click Update Settings.

Retiring an erasure coding topology

Before retiring an erasure coding topology, be sure you're familiar with the information in Erasure coding topology retirement. You cannot make a retiring or retired topology active again.

1. In the top-level menu of the HCP System Management Console for any system in the topology, select Services > Geo-distributed EC.
2. On the EC Topologies page, click the topology you want to retire.
3. On the erasure coding topology details page, click Management.
4. In the Management panel, click Retire.
5. In response to the confirming message, click Retire.

Considerations for deleting an erasure coding topology

These considerations apply to deleting an erasure coding topology:

- You can delete an erasure coding topology only while either of these is true:
    - At least one system in the topology is available, the total number of erasure-coded objects and erasure-coded parts of multipart objects on each available system is zero, and the state of the topology is retired. These are the normal conditions for deleting a topology.
    - No more than one system in the topology is unavailable, the total number of erasure-coded objects and erasure-coded parts of multipart objects on each available system is zero, and the state of the topology is retiring. In this case, you are prompted to confirm the delete request.
      Important: Deleting an erasure coding topology under these conditions may result in inaccessible data in namespaces on the unavailable system, even if those namespaces are configured to be compliant. You should delete the topology only if that system is no longer needed. If the system is still needed, wait to delete the topology until the topology has finished retiring on all systems.
- You cannot delete an erasure coding topology while either of these is true:
    - The total number of erasure-coded objects and erasure-coded parts of multipart objects on any available system in the topology is greater than zero.

      The Management panel on the EC Topologies page for a retiring or retired topology shows the number of erasure-coded objects and erasure-coded parts of multipart objects on the available systems.

    - More than one system in the topology is unavailable, and the state of the topology is retiring.

Deleting an erasure coding topology

1. In the top-level menu of the HCP System Management Console for any system in the topology, select Services > Geo-distributed EC.
2. On the EC Topologies page, click the topology you want to delete.
3. On the erasure coding topology details page, click Management.
4. In the Management panel, click Delete.

   If deleting the topology could result in inaccessible data in namespaces on an unavailable system, 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. Then click Delete Topology.

Understanding the erasure coding topology list

The EC Topologies page in the HCP System Management Console lists the currently defined erasure coding topologies in which the current system participates. To display this page, in the top-level menu of the System Management Console, select Services > Geo-distributed EC.

For each listed erasure coding topology, the EC Topologies page shows:

Name
: The erasure coding topology name.

State
: The current state of the erasure coding topology: `Active`, `Retiring`, or `Retired`.

Protection Status

The current status of the erasure coding topology with respect to how well-protected erasure-coded objects are: `Healthy`, `Vulnerable`, `Broken`, `Retiring`, `Retired`, or `Unknown`.

Read Status
: The current status of the erasure coding topology with respect to the ability to read erasure-coded objects: `Healthy`, `Vulnerable`, `Broken`, `Retired`, or `Unknown`.

Alerts
: If issues exist with the erasure coding topology, one or both of these icons:

This icon is displayed under these conditions:

- The erasure coding topology protection status is vulnerable.
- The erasure coding topology read status is vulnerable.
- Replication is paused for one or more tenants on one or more replication links in the erasure coding topology. This condition is reported only for active topologies.

This icon is displayed under these conditions:

- The erasure coding topology protection status is broken.
- The erasure coding topology read status is broken.
- One or more tenants added to the 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 the erasure coding topology.

To view text describing the condition that's causing the alert, hover over the alert icon.

Understanding erasure coding topology details

The list of erasure coding topologies on the EC Topologies page shows the current status of each active, retiring, or retired erasure coding topology. To further monitor the status of a topology and to manage the topology, click the name of the topology in the list.

The page that opens shows details about the erasure coding topology in a Status section, HCP Systems section, and Overview panel, each of which is described below. The additional panels you can access on this page are:

Tenants panel
: Shows the tenants that are included in the topology and the tenants that are eligible to be included in the topology.

Settings panel
: Shows the erasure coding topology properties and lets you change those properties.

Management panel
: Lets you retire and delete the erasure coding topology.

Status section

The Status section on the details page for an erasure coding topology shows:

Topology state
: The current state of the topology. The topology state can be `Active`, `Retiring`, or `Retired`.

Protection status
: The current status of the erasure coding topology with respect to how well-protected erasure-coded objects are. The protection status can be:

Healthy
: All of these are true:

- All systems in the topology are available.
- The loss of a link in the topology would not cause any system to become unavailable.
- The suspension of activity on a link in the topology would not prevent any system from receiving data or chunks for newly ingested objects.

Data or chunks for newly ingested objects are being distributed to all systems in the topology. Full copies of object data will be reduced to chunks when the applicable erasure coding delay expires.

Objects that were erasure coded according to the topology are protected.

Vulnerable
: One or both of these are true:

- The loss of a link in the topology would cause a system in the topology to become unavailable.
- The suspension of activity on a link in the topology would prevent a system in the topology from receiving data or chunks for newly ingested objects.

Data or chunks for newly ingested objects are being distributed to all systems in the topology. Full copies of object data will be reduced to chunks when the applicable erasure coding delay expires.

Objects that were erasure coded according to the topology are protected.

Broken
: One or more systems in the topology are unavailable.

Data or chunks for newly ingested objects are being distributed to the systems that are available to the ingest system. However, full copies of object data won't be reduced to chunks until all systems in the topology are available, regardless of the erasure coding delay.

Objects that were erasure coded according to the topology are not protected and may not be available.

Retiring
: Both of these are true:

- The topology is in the process of retiring.
- One or more systems in the topology still have chunks for objects that were erasure coded according to the topology.

Retired
: Both of these are true:

- The topology has finished retiring.
- No systems in the topology have chunks for objects that were erasure coded according to the topology.

Unknown
HCP cannot determine the protection status.

Read status
The current status of the erasure coding topology with respect to the ability to read erasure-coded objects.
Note: For the purpose of determining read status, HCP treats suspended links as broken links. However, if a suspended link is not actually broken, the systems involved in the link can still use the link to read data from each other.
The read status can be:

Healthy
Both of these are true:

- The loss of a link in the topology would not cause the inability to read erasure-coded objects.
- A system in the topology becoming unavailable would not cause the inability to read erasure-coded objects.

The data for objects that were erasure coded according to the topology can be reconstructed or restored as needed.

Vulnerable
All of these are true:

- The data for objects that were erasure coded according to the topology can be reconstructed or restored as needed.
- The loss of a link in the topology would cause the inability to read erasure-coded objects.
- A system in the topology becoming unavailable would cause the inability to read erasure-coded objects.

Broken
Two or more systems in the topology are unavailable. The data for objects that were erasure coded according to the topology cannot be reconstructed or restored unless the unavailability of all or all but one of those systems is due to links with suspended send activity.

Retired
The topology has finished retiring. No systems in the topology have chunks for objects that were erasure coded according to the topology.

Unknown
HCP cannot determine the read status.

Protection level
x+y, where *x* is the number of data chunks and *y* is the number of parity chunks for each object that was erasure coded according to the topology.

Erasure-coded objects and object parts on this system
The number of erasure-coded objects and erasure-coded parts of multipart objects on the current HCP system that were erasure coded according to the topology. An object or part is counted as erasure coded if a chunk for it is stored on the system.
Parts of multipart objects are erasure coded independently of each other.

HCP Systems section

The HCP Systems section on the details page for an erasure coding topology contains a diagram of the topology and a numbered list of the systems in the topology.

The lines between the numbered systems in the topology diagram represent the replication links in the topology. The color of each line indicates the last known status of the applicable link:

- Gray means healthy.
- Orange means not replicating.
- Red means unhealthy.

Overview panel

The Overview panel on the details page for an erasure coding topology contains a list of the replication links in the topology. For each link, the section shows:

Name
The link name.

HCP System, HCP System
The HCP systems involved in the link.

Status
The last known status of the link. This status indicates the general health of the link. If the link is not directly connected to the current HCP system, the link status may be out of date.
The link status can be:

Healthy
The status displayed when the specific status of the link is one of these:

- Synchronizing data
- Scheduled off period

Not replicating
The status displayed when the specific status of the link is one of these:

- Suspended by user
- Remote storage full, link suspended
- Local storage full, link suspended
- Failed over

Unhealthy
The status displayed when the specific status of the link is one of these:

- High error rate
- Stalled link
- Unrecognized link
- Broken link

Unknown
HCP cannot determine the specific status of the link.

Alerts

If issues exist with the link, one or both of these icons:

This icon is displayed while replication is paused for one or more tenants on the link.

This icon is displayed under these conditions:

- One or more tenants added to the erasure coding topology have not been added to the link. HCP does not report this condition for a tenant until ten minutes after the tenant was added to the topology.

  This condition is reported only on the systems involved in the link.

- HCP cannot find the link.

  This condition is reported only on the system where HCP cannot find the link. A link that cannot be found on one of the systems involved in the link is typically reported as broken on the other system involved in the link.

To view text describing the condition that's causing the alert, hover over the alert icon.

Monitoring replication

You can monitor the status of each currently configured replication link, as well as replication and recovery activity on the link, in the HCP System Management Console for either system involved in the link. By periodically reviewing link activity, you can decide whether to change the replication rate in the link configuration to accommodate other loads on system performance. You can also determine whether you need to add more storage capacity to either system.

Under normal circumstances, the Replication service works without any intervention required. System Management Console alerts inform you of conditions, such as network connection problems, that may require action on your part to allow the service to continue processing.

For HCP tenants, you can control whether information about replication activity is displayed in the Tenant Management Console. For the default tenant, this information is always displayed.

This section of the Help describes the information available to you for the links you've created.

To monitor replication, you need the monitor or administrator role.

You can also use the HCP management API to monitor replication links.

Understanding the replication link list

The replication Links page in the HCP System Management Console lists the currently defined replication links in which the current system participates. To display this page, in the top-level menu of the HCP System Management Console, select Services > Replication.

For each listed link, the replication Links page shows:

Name
: The link name.

Type
: The link type. The link type can be Active/Active, Outbound, or Inbound.

  If the link is part of an erasure coding topology, the link type is followed by this icon:

Status
: The link status, represented by an icon and text. The icon indicates the general health of the link. The text specifies the status of the link. The possible icons are:

  The link is healthy. The statuses that can accompany this icon are:

  Synchronizing data
  : On either system for an active/active link, the local system is sending data to the other system involved in the link.

  Sending data
  : On the primary system for an active/passive link during replication, the primary system is sending data to the replica.

  Receiving data
  : On the replica for an active/passive link during replication, the primary system is sending data to the replica.

  The link is healthy, but normal replication is not occurring on the link. The statuses that can accompany this icon are:

  Recovering data
  : On the replica for an active/passive link during the first part of data recovery, the replica is sending data to the primary system.

  Completing recovery
  : On the replica for an active/passive link during final data recovery, the replica is sending data to the primary system.

  Receiving data
  : On the primary system for an active/passive link during data recovery, the replica is sending data to the primary system.

  Scheduled off period
  : No data is being sent on the link because the scheduled performance level for the current time period for the link is Off.

  Suspended by user
  : On both systems for an active/active or active/passive link, activity on the link has been manually suspended. No replication or recovery is occurring.

  The link is unhealthy. The statuses that can accompany this icon are:

  Failed over
  : On both systems for an active/active or active/passive link, the link is currently failed over.

  Remote storage full, link suspended
  : On the local system for an active/active link, on the primary system for an active/passive link during replication, or on the replica for an active/passive link during data recovery, the other system involved in the link does not have enough free space in primary running storage to accept any more data transmissions. In any case, HCP has automatically suspended activity on the link.

  Local storage full, link suspended

On the local system for an active/active link, on the replica for an active/passive link during replication, or on the primary system for an active/passive link during data recovery, the local system does not have enough free space in primary running storage to accept any more data transmissions. In any case, HCP has automatically suspended activity on the link.

High error rate

On both systems for an active/active or active/passive link, errors are occurring at a high rate. If you see this status for:

- An active/active link, check the health of both systems involved in the link
- An active/passive link during replication, check the health of the replica.
- An active/passive link during data recovery, check the health of the primary system

In any case, also check the health of the network connection between the two systems involved in the link.
If you cannot find the problem, contact your authorized HCP service provider for help.

Stalled link

On both systems for an active/active or active/passive link, activity on the link has stopped. Check the network connection between the two systems. If the connection appears to be working properly, contact your authorized HCP service provider for help.

Unrecognized link

On either system for an active/active or active/passive link, the other system involved in the link doesn't recognize the link. Restore the link. Then, if applicable, start data recovery.

Broken link

On both systems for an active/active or active/passive link, the Replication service cannot contact any nodes on the other system involved in the link. If you see this status for:

- An active/active link, check the health of both systems involved in the link
- An active/passive link during replication, check the health of the replica
- An active/passive link during data recovery, check the health of the primary system

In any case, also check the health of the network connection between the two systems involved in the link.
If you cannot find the problem, contact your authorized HCP service provider for help.

If more than one status applies to a link, the page shows the icon and text for only one of the statuses.
For additional information on the status of a link, hover over the status icon.
Note: The System Management Console may not immediately reflect certain changes in link status.

Alerts

If replication or recovery activity is paused for one or more tenants on the link, either of these icons:

Replication or recovery has been manually paused for one or more tenants on the link.

Replication or recovery has been automatically paused for one or more tenants on the link. To view text describing the condition that's causing this alert, hover over the alert icon.

If replication or recovery is paused manually for one or more tenants and automatically for one or more other tenants, the page shows only the icon indicating an automatic pause.

The number of nodes on the other system that can receive replication transmissions from the current system. If the current system can determine the total number of storage nodes on the other system, the page shows that number as well.

General link information

The list of links on the replication Links page shows the current status of each replication link. To further monitor the status of a link and to manage the link, click the name of the link in the list.

The top part of the page that opens shows this information for the link:

- The link name.
- The name of the domain associated with the [hcp_system] network for the local system (the system where you're viewing the link).
- The name of the domain associated with the [hcp_system] network for the other system involved in the link (the remote system for the link).
- A large arrow showing the direction of the link, overlaid with the link status. For an active/active link, this arrow has two arrowheads, one at each end.
- For active/active links, the date and time before which configuration changes and changes to namespace content are guaranteed to be synchronized in both directions between the two systems involved in the link. For active/passive links, the date and time before which configuration changes and changes to namespace content are guaranteed to have been replicated or recovered on the link, as applicable.

Link overview

To monitor the status of and activity on a replication link, you use the link status Overview panel in the HCP System Management Console. To display this panel:

1. In the list of links on the replication Links page, click the link you want to monitor.
2. On the replication link details page, click Status.
3. In the link Status panel, click the Overview tab.

If the replication link is part of one or more active, retiring, or retired erasure coding topologies, the top part of the link status Overview panel lists the topologies that include that link.

The Sending and Receiving sections in the link status Overview panel show the current status of activity on the link:

- For an active/active link, a section labeled Sending shows the status of send activity on the local system. A section labeled Receiving shows the status of send activity on the remote system.
- For an outbound active/passive link during replication and an inbound active/passive link during data recovery, a section labeled Sending shows the status of send activity on the local system.
- For an outbound active/passive link during data recovery and an inbound active/passive link during replication, a section labeled Receiving shows the status of send activity on the remote system.

The Sending and Receiving sections show:

Data pending

The approximate amount of data currently waiting to be sent to the other system, in bytes. This is the sum of the amounts of data waiting to be sent in each HCP namespace being replicated on the link. This value does not include data in the default namespace.

Information about pending data is not available in the Receiving section on a replica during replication or on a primary system during data recovery.

Objects pending

The approximate number of objects and parts of multipart objects currently waiting to be sent to the other system. This is the sum of the numbers of objects and object parts waiting to be sent in each HCP namespace being replicated on the link. This number does not include objects in the default namespace.

The number of objects pending does not include parts of in-progress multipart uploads. Those parts are not replicated until the applicable multipart upload has been completed.

Information about pending objects and object parts is not available in the section on a replica during replication or on a primary system during data recovery.

Up to date as of

The amount of time that is the difference between:

- The date and time before which configuration changes and changes to namespace content are guaranteed to have been sent to the other system
- The current date and time

If the Replication Verification service is running or has ever run, a Verifying section appears below the Receiving section. The Verifying section shows:

Last Pass Completed

The date and time at which the Replication Verification service finished its last run.

Status

The current status of the Replication Verification service. Possible values are:

Enabled

The Replication Verification service is either running or set to run the next time the Replication service runs.

Disabled

The Replication Verification service is not running and is not set to run.

Issues Found

Either `None` or the current total number of nonreplicating objects and object parts in all the namespaces owned by the tenants on the link. If nonreplicating objects or object parts exist, View appears next to Issues Found. To see a list of the tenants with namespaces that contain nonreplicating objects or object parts, click View. The list shows the total number of nonreplicating objects parts for each tenant.

If you have administrative access to a listed tenant, you can click the tenant name in the list to open the Tenant Management Console for that tenant. In the Tenant Management Console, you can see which namespaces have nonreplicating objects and object parts. For each of those namespaces, you can view a list of the nonreplicating objects and object parts in the namespace.

The link status Overview panel also contains:

- A graph showing the history of the rate of data transmissions on the link
- A graph showing the history of the rate of operations on the link
- For active/active links and outbound active/passive links, one or two pie charts showing the amount of used and free storage space on the remote system

The statistics for replication links are updated every ten minutes. To see updated statistics, redisplay the Links page.

Data transmission rate

The Transfer Rate graph in the link status Overview panel for a replication link shows the history of the rate of data transmissions on the link per second. For an active/active link, this is the rate of data transmission from the local system to the remote system. For an active/passive link, this is the rate of data transmission during replication or recovery, whichever is happening at the time. In any case, the data transmission rate is cumulative for all the HCP tenants and default-tenant directories on the link.

If the Transfer Rate graph is not currently visible, click Transfer Rate to display it.

The x-axis in the Transfer Rate graph marks the passage of time. The axis shows 30 days (or fewer if the replication link was created less than 30 days ago). The y-axis marks the data transmission rate in KB, MB, or GB. As the transmission rate varies, the measurement unit for the y-axis grows or shrinks as needed (for example, from KB to MB to GB).

The graph heading displays the current data transmission rate. Factors that affect this rate include the amount of other traffic on the network, the current load on both systems involved in the link, and whether data is being compressed or encrypted. Also, larger objects and object parts have higher rates of throughput.

Operation rate

The Operations per Second graph in the link status Overview panel for a replication link shows the history of the rate of operations on the link per second. An operation is the replication of any of these:

- An object, object part, directory, symbolic link, metadata change, or object deletion
- An HCP tenant or HCP namespace or the modification or deletion of an HCP tenant or HCP namespace
- For HCP tenants only, the creation, modification, or deletion of a user account
- The creation, modification, or deletion of a retention class
- The creation, modification, or deletion of a content class
- A tenant log message

For an active/active link, the Operations per Second graph shows the operation rate for replication from the local system to the remote system. For an active/passive link, the graph shows the operation rate during replication or recovery, whichever is happening at the time. In any case, the operation rate is cumulative for all the tenants being replicated or recovered on the link.

If the Operations per Second graph is not currently visible, click Operations per Second to display it.

The x-axis in the Operations per Second graph marks the passage of time. The axis shows 30 days (or fewer if the replication link was created less than 30 days ago). The y-axis marks the operation rate in tens, hundreds, or thousands. As the operation rate varies, the measurement unit on the y-axis grows or shrinks as needed (for example, from tens to hundreds to thousands).

The graph heading displays the current rate of replication operations. Factors that affect the operation rate are the same as those that affect the data transmission rate.

Remote storage space

The Remote Total Primary Storage pie chart in the link status Overview panel for an active/active link or an outbound active/passive link during replication shows the amounts of free and used space in primary storage for the other system involved in the link. Each amount is also shown as a number of bytes.

In a HCP with SAN-attached storage system with spindown storage, the storage being measured in this chart includes both primary running storage and primary spindown storage. In this case, a second pie chart to the right, labeled Remote Primary Running Storage, shows the amounts of free and used space in only primary running storage.

The two systems involved in a replication link do not necessarily have the same storage capacity or storage tiering strategies. If a system receiving replicated data starts to run low on free space in primary running storage, you need to evaluate whether to take action on that system to address the issue (for example, by increasing the primary running storage capacity or by tiering more data to other types of storage).

When primary running storage in the remote system for a replication link is almost full, the Overview page in the HCP System Management Console for the local system displays an alert. When the storage is full, the Console displays a different alert, and HCP automatically suspends replication on the link.

Tenants view

To monitor the status of replication or recovery activity for the individual tenants on a given replication link, you use the link status Tenants panel in the HCP System Management Console.

Display the Tenants panel

1. In the list of links on the replication Links page, click the name of the link you want.
2. On the replication link details page, click Status.
3. In the link Status panel, click the Tenants tab.

Understanding the tenant list

The link status Tenants panel lists the tenants on a replication link, including the default tenant if the link includes any default-namespace directories. For each tenant, the list shows:

Name
: The tenant name.

Sent as Of
: For an active/active link, an outbound active/passive link during replication, or an inbound active/passive link during data recovery, the average of the sent-as-of times for the tenant's namespaces. The sent-as-of time for a namespace is the amount of time that is the difference between:

  - The date and time before which the namespace content is guaranteed to have been sent from the local system to the remote system
  - The current date and time

  For the default tenant, this is the average sent-as-of time among the directories on the link.
  Tip:

  - If some tenants are significantly less up to date than others, set the replication priority for the link to Oldest Object First to reduce the gap.
  - If the sent-as-of time is consistently increasing for one or more tenants, even with the replication performance level set to High, you may need to add more processing power (for example, additional nodes) to your system or increase the bandwidth between the two systems involved in the link.

Received as Of
: For an active/active link, an outbound active/passive link during data recovery, or an inbound active/passive link during replication, the average of the received-as-of times for the tenant's namespaces. The received-as-of time for a namespace is the amount of time that is the difference between:

  - The date and time before which the namespace content is guaranteed to have been sent from the remote system to the local system
  - The current date and time

  For the default tenant, this is the average received-as-of time among the directories on the link.

Status
: The current status of replication or recovery activity for the tenant, represented by one or more of these icons, as applicable:

  If the icon is animated, replication or recovery of the tenant is proceeding normally. If the icon is static, no replication or recovery is occurring on the replication link.

  A user paused replication or recovery of the tenant.

  The Replication service automatically paused replication or recovery of the tenant. To view text describing the condition that’s causing this status, hover over the status icon.

  The tenant is on a link that’s chained into the link you’re viewing.

Managing the tenant list

By default, the tenant list in the Tenants panel includes all tenants in the link. 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 panel 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 in the Tenants panel. 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 jump to a specific page in the tenant list:

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

Sorting

You can sort the tenants in the tenant list by tenant name, outbound or inbound synchronization time, or status. To sort the list:

- By name, click the Name column heading. Each time you click the column heading, the sort order switches between ascending and descending.
- By outbound or inbound synchronization time, click the Sent as Of or Received as Of column heading, as applicable. The first time you click the column heading, the tenants are sorted in ascending order by the applicable synchronization time. Each time you click the column heading after that, the sort order switches between ascending and descending.

- By status, click the Status column heading. The first time you click the column heading, tenants for which replication has been automatically paused are listed first, followed by tenants for which replication has been manually paused, followed by the remaining tenants. Each time you click the column heading after that, the order reverses from what it currently is.

Filtering

You can filter the tenant list by tenant name or tag. The filtered list includes only those tenants with a name or tag, as applicable, that begins with or is the same as a specified text string.

1. In the field above the Name column, select Name to filter by name or Tag to filter by tag.
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 ( ).

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

Tenant replication details

To see more details about the replication of a tenant, hover over the row for the tenant in the list of tenants in the link status Tenants panel. The information shown is:

Most up-to-date namespace

- For an active/active link, an outbound active/passive link during replication, or an inbound active/passive link during data recovery, the smallest sent-as-of time among the tenant's namespaces
- For an outbound active/passive link during data recovery or an inbound active/passive link during replication, the smallest received-as-of time among the tenant's namespaces

For the default tenant, this is the smallest sent-as-of time or received-as-of time, as applicable, among the directories on the replication link.

Average up-to-date time

- For an active/active link, an outbound active/passive link during replication, or an inbound active/passive link during data recovery, the average of the sent-as-of times for the tenant's namespaces
- For an outbound active/passive link during data recovery or an inbound active/passive link during replication, the average of the received-as-of times for the tenant's namespaces

For the default tenant, this is the average of the sent-as-of times or received-as-of times, as applicable, for the directories on the replication link.

Objects pending

For an active/active link, an outbound active/passive link during replication, or an inbound active/passive link during data recovery, the approximate number of objects and parts of multipart objects currently waiting to be sent to the remote system in the tenant's namespaces.

The number of objects pending does not include parts of in-progress multipart uploads. Those parts are not replicated until the applicable multipart upload has been completed.

Information about pending objects and object parts is not available for an outbound link during data recovery or for an inbound link during replication. This information is also not available for the default tenant.

Data pending

For an active/active link, an outbound active/passive link during replication, or an inbound active/passive link during data recovery, the approximate amount of data currently waiting to be sent to the remote system in the tenant's namespaces.

Information about pending data is not available for an outbound link during data recovery or for an inbound link during replication. This information is also not available for the default tenant.

Controlling the Tenant Management Console replication display

For HCP tenants that are on at least one replication link, you control whether the Tenant Management Console displays information about the status of replication of the tenant and its namespaces. The Tenant Management Console for the default tenant always displays this information.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, take either of these actions:
   - To have the Tenant Management Console display replication status information for all HCP tenants, select Allow tenants to monitor replication of their namespaces.
   - To have the Tenant Management Console hide replication status information for all HCP tenants, deselect Allow tenants to monitor replication of their namespaces.
4. Click Update Settings.

System Management Console alerts

The Overview page in the HCP System Management Console has a section in which it displays alerts about abnormal conditions. Each alert consists of an icon and accompanying text that identifies the problem. Each alert also has text that’s displayed when you hover over the icon.

The list below describes the alerts that relate to replication. The alerts are listed alphabetically by their hover text.

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.

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.

Front-end connection error

All front-end connections to one or more nodes in the local system are unavailable. If the system is currently a source for replication, some objects and object parts will not be replicated. If the system is a replication target, replication performance is degraded.

Nonreplicating objects

One or more nonreplicating objects or object parts have been detected. These objects and object parts cannot be replicated until they are repaired. If the objects and object parts cannot be repaired, they are never replicated. If the system has nonreplicating objects or object parts that are irreparable, contact your authorized service provider for help.

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 assign IP addresses in those networks to all nodes, or select a different network for replication.

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, 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, 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.

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.

Managing replication

To help manage the load on an HCP system and the replication network, you can control the performance level for send activity on each replication link in which the system participates. You can use a schedule to change the performance level for a link automatically at specific times on a weekly basis. Alternatively, you can choose a single performance level for the entire week.

Occasionally, you may need to temporarily stop all send activity on an individual link. Or, you may want to temporarily stop send activity only for particular tenants.

Rarely, you may need to stop all activity on all links in which the HCP system participates. This action stops not only replication and recovery but also read and repair from remote systems. It also prevents you from changing which items are included on the links.

If the HCP system uses virtual networking, you can select the network to use for communications through any replication link. You typically do this only once.

You can control whether the HCP system allows DNS failover to other systems in the replication topology. Disallowing DNS failover prevents the system from servicing requests redirected from remote systems regardless of whether this is allowed by the targeted namespace.

You can configure an HCP system to automatically share its domains and SSL server certificates with other systems with which it participates in replication links. This ensures that SSL works for access to replicated namespaces on those systems.

You can manage the load the Replication Verification service puts on the system by disabling the service, setting the service to run once, or allowing the service to run continuously.

This section of the Help explains how to perform the tasks outlined above.

To view replication link schedules and global replication settings, you need the monitor role. To modify replication link schedules, manage replication at the link, tenant, and system levels, and set global replication options, you need the administrator role.

Note: You can also use the HCP management API to manage replication.

Scheduling activity on a replication link

The amount of send activity that can occur on a replication link at any given time is controlled by the performance level that applies to the sending system. An active/active link has two performance levels at any given time, one for each system involved in the link. An active/passive link has only one performance level at any given time. That level applies to the primary system during replication and to the replica during data recovery.

The performance levels for different replication links are independent of each other, as are the performance levels for the two systems involved in an active/active link. In each case, the performance level can be low, medium, high, custom, or off. Off means that no send activity is occurring for the applicable link on the applicable system.

For each system involved in an active/active link and for an active/passive link, you can schedule the performance level to change automatically over the course of a week. At any time, if you don't want to use the schedule, you can override it by selecting a single performance level to apply until you cancel the override.

Overriding a replication schedule lets you change the performance level without changing the configured schedule. You might do this, for example, on a holiday when the load on the applicable HCP system is expected to be light.

Note: When data recovery begins on an active/passive link, a schedule override with a performance level of high takes effect. When data recovery is complete, the performance level automatically returns to the currently scheduled level if the schedule was in effect when data recovery began or to the override level that was in effect when data recovery began, as applicable.

The performance level for a sending system determines the amount of load replication or recovery processing puts on that system and on the network connecting that system to the other system involved in the applicable replication link. If a system is sending data on multiple links, the total load on the system is determined by the performance levels for all of those links together. To minimize the load, you should schedule the links to be active at different times.

Tip: If the system load from other activities is light, consider raising the performance level for one or more links to reduce any replication backlog. If the system load is heavy, consider lowering the performance level for one or more links to free resources for other system activity.

About replication schedules

You use the Schedule panel on the Replication page in the HCP System Management Console to set the schedule for replication activity on a replication link. For an active/active link, this panel has two tabs on each system involved in the link — one labeled Local for the local system and one labeled Remote for the remote system.

For an active/passive link, you set the schedule only for the primary system. Therefore, on the primary system the Schedule panel has a tab labeled Local. On the replica, the Schedule panel has a tab labeled Remote.

Each Local and Remote schedule panel contains a grid in which the weekdays from Sunday through Saturday are each broken out into 24 hours. To set a schedule, you assign performance levels to time periods in the grid. The Console makes it easy for you to do this for the whole week, individual days, individual hours, or ranges of hours within a day.

In the schedule grid, the top of each time period with a given performance level displays the start and end times for that period (for example, 8 am to 6 pm). These times are in the time zone of the primary system.

The top of each time period also displays the performance level for that period. Additionally, each time period is color coded in the schedule grid to indicate the performance level so you can easily see which levels are assigned to which periods:

- Low: (light green)
- Medium: (green)
- High: (dark green)
- Custom: (blue)
- Off: (gray)

While a schedule is overridden, the words `Schedule Overridden` appear on the schedule grid.

You cannot set a schedule to off for the entire week. Instead, to disable activity on a replication link for an extended period of time, suspend activity on the link.

Modifying a replication schedule

By default, the schedules for an active/active link and the schedule for an active/passive link specify a performance level of medium for the entire week.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the link with the schdule you want to modify.
3. On the replication link details page, click Schedule.
4. In the link Schedule panel, click the Local or Remote tab, as applicable.
5. In the Local or Remote panel, as applicable, take any of these actions as many times as needed to set the schedule you want:
   - To set the performance level for the entire week:
     a. Hover over All to display the list of performance levels.
     b. Click the performance level you want.
   - To set the performance level for an individual day:
     a. Hover over the name of the day to display the list of performance levels.
     b. Click the performance level you want.
   - To set the performance level for a single hour or a range of hours:
     a. Either click an hour, or click and drag from one hour to another in the same day.

        The Set Performance Level window opens.

     b. (Optional) Select different start and end times in the Start time and End time fields, respectively.
     c. In the Level field, select the performance level you want.
     d. Click Submit.
6. Click Update Schedule.

Overriding a replication schedule

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the link with the schedule you want to override.
3. On the replication link details page, click Schedule .
4. In the Schedule panel, click the Local or Remote tab, as applicable.
5. In the Local or Remote panel, as applicable, click Schedule Override.
6. In the Schedule Override section:
   a. Select Override schedule.
   b. Under Performance Level, select the performance level you want.
7. Click Update Schedule.

Suspending and resuming activity on an individual link

You can suspend and resume replication or recovery activity on individual replication links. When you suspend activity on a link, HCP stops all send activity on the link. You might suspend activity on a link, for example, before making changes to system hardware or to the network over which the two systems involved in the link communicate with each other.

While send activity is suspended on a link, the applicable HCP tenants and namespaces and default-namespace directories on each system remain read-write or read-only, as applicable. Additionally, the link continues to support other functions such as read from remote and repair from remote.

Resuming activity on a link restarts all send activity on the link. After suspending activity on a link, you need to resume activity manually.

Suspending activity on a link in an erasure coding topology prevents each system involved in the link from sending full copies of object data and chunks for objects to the other system over that link. Link suspensions, therefore, may prevent newly ingested objects from being protected. Suspending a link does not prevent full copies of object data from being reduced to chunks on the systems involved in the link.

The Replication service periodically checkpoints its progress. When you suspend activity on a link, no special checkpoint occurs. When you resume link activity, therefore, processing starts from the last checkpoint before the suspension.

1. In the top-level menu of the System Management Console for either system involved in the link, select Services > Replication.
2. On the replication Links page, click the link on which you want you want to suspend or resume activity.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Management tab.
5. In the link Management panel, click Suspend or Resume, as applicable.

Pausing and resuming replication or recovery of a tenant

You can pause and resume replication or recovery of an individual tenant on a replication link. Pausing replication or recovery of a tenant on a link causes the Replication service on the sending system to stop all send activity for the tenant on that link. With an active/active link, the Replication service on both systems involved in the link stops all send activity for the tenant on the link.

Resuming replication or recovery of a tenant on a link restarts all send activity for that tenant on that link. After pausing replication or recovery of a tenant on a link, you need to resume replication or recovery manually.

You might pause replication of some tenants on a link, for example, to give more processing time to other tenants with greater replication backlogs. While replication or recovery of a tenant is paused on a link, the two systems involved in the link can still use the link to read from each other the objects in the tenant's replicated namespaces.

Replication or recovery of a tenant can also be paused automatically due to certain events. After replication or recovery of a tenant is paused automatically, you need to resume replication or recovery manually. However, you cannot do this until the issue that caused replication or recovery to be paused is resolved.

Pausing replication or recovery of a tenant on a link in an erasure coding topology prevents each system involved in the link from sending full copies of object data and chunks for objects in the tenant's namespaces to the other system over that link. Pausing replication or recovery of a tenant, therefore, may prevent newly ingested objects in those namespaces from being protected.

Pausing replication or recovery of a tenant on a link does not prevent full copies of object data in the tenant's namespaces from being reduced to chunks on the systems involved in that link.

The Replication service periodically checkpoints its progress. When you pause replication or recovery of a tenant, no special checkpoint occurs. When you resume processing, therefore, processing starts from the last checkpoint before the pause.

Pausing and resuming tenant replication or recovery

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the replication Links page, click the link for which you want to pause or resume replication or recovery.

3. On the replication link details page, click Status.
4. In the link Status panel, click the Tenants tab.
5. In the list of tenants, click the pause control ( ) or resume control ( ), as applicable, for the tenant for which you want to pause or resume activity.

Automatically paused tenant replication or recovery

Certain events can cause the Replication service to automatically pause replication or recovery of a tenant on a replication link. The following sections describe these events.

Tip: To avoid situations that can cause the Replication service to automatically pause replication of a tenant, do not try to create the same tenants, namespaces, content classes, user accounts, and group accounts on both of the systems that are replicating to each other on an active/active link. Instead, allow the items you create on each system to replicate to the other system.

Tenant name collisions

A tenant name collision occurs when the Replication service tries to replicate an HCP tenant from one HCP system to another HCP system that already has a different tenant with the same name.

To recover from a tenant name collision, take one of these actions:

- Rename the tenant on one of the systems involved in the link.
- Delete the tenant on the receiving system.

Here are two scenarios that show how a tenant name collision can cause the Replication service to pause replication of a tenant.

Scenario 1

In this scenario:

- System A replicates to system B on link AB. Link AB can be either active/active or active/passive.
- System A has a tenant named T1 that is not on link AB.

These events occur in the order shown:

1. On system A, you add T1 to link AB.
2. Before T1 is replicated to system B, you create a tenant named T1 on system B.
3. The Replication service tries to replicate T1 to system B. The replication is unsuccessful because a different tenant named T1 already exists on system B. As a result, the service automatically pauses replication of T1 on link AB.

Scenario 2

In this scenario:

- System A replicates to system B on link AB, which replicates to system C on link BC, where link AB is chained into link BC. Link AB can be either active/active or active/passive. Link BC is active/passive.
- System A and system C each have a tenant named T1, where T1 was created independently on each system.

These events occur in the order shown:

1. On system A, you add T1 to link AB.
2. T1 is replicated to system B.
3. Because link BC includes link AB, the Replication service tries to replicate T1 to system C. The replication is unsuccessful because a different tenant named T1 already exists on system C. As a result, the service automatically pauses replication of T1 on link BC.

Namespace name collisions

Each HCP namespace you create in an HCP system has an internal ID that uniquely identifies that namespace. As a result, two namespaces created on different systems are different from each other, even if they have the same name and are owned by the same tenant.

A namespace name collision occurs when the Replication service tries to replicate a namespace from one system to another system that already has a different namespace with the same name, where both namespaces are owned by the same tenant.

To recover from a namespace name collision, take one of these actions:

- Rename the namespace on one of the systems involved in the link.
- Deselect the namespace from replication.
- Delete the namespace on the receiving system.

Here's a scenario that shows how a namespace name collision can cause the Replication service to pause replication of a tenant. In this scenario:

- System A and system B replicate to each other over active/active link AB.
- Link AB includes tenant T1, so T1 exists on both systems.
- On system A, T1 owns namespace NS1, which is not selected for replication.

These events occur in the order shown:

1. On system A, you select NS1 for replication.
2. Before NS1 is replicated to system B, you create a namespace named NS1 for T1 on system B.
3. The Replication service tries to replicate NS1 to system B. The replication is unsuccessful because a different namespace named NS1 already exists on system B. As a result, the service automatically pauses replication of T1 on link AB.

Namespace compliance issues

Different HCP systems can have different definitions for service plans with the same name. When an HCP tenant or namespace is replicated, the name of its associated service plan, not the service plan itself, is replicated with it. As a result, the service plan that applies to a namespace can differ on the two HCP systems involved in a link on which the namespace is being replicated.

Service plans can be compliant or noncompliant. However, the service plan that applies to a namespace in compliance mode must be compliant. A namespace compliance issue occurs when replication of a namespace in compliance mode would cause a noncompliant service plan to apply to the namespace on the receiving system.

To recover from namespace compliance issue, take one of these actions:

- Redefine the noncompliant service plan on the receiving system to be compliant.
- If the service plan is assigned to the tenant that owns the namespace, assign a different service plan to the tenant on the sending system, where that service plan is complaint on both systems involved in the link.
- If the service plan is assigned to the namespace, have the tenant administrator assign a different service plan to the namespace on the sending system, where that service plan is complaint on both systems involved in the link.
- Deselect the namespace from replication.

Here are two scenarios that show how a namespace compliance issue can cause the Replication service to pause replication of a tenant.

Scenario 1

In this scenario:

- System A replicates to system B on link AB. Link AB can be either active/active or active/passive.
- Link AB includes tenant T1, so T1 exists on both systems.
- On system A, T1 owns namespace NS1, which is in compliance mode. NS1 not selected for replication.
- The service plan that applies to NS1 is named SP1. SP1 is compliant on system A and noncompliant on system B.

These events occur in the order shown:

1. On system A, you select NS1 for replication.
2. The Replication service tries to replicate NS1 to system B. The replication is unsuccessful because it would cause NS1, which is in compliance mode, to have a noncompliant service plan on system B. As a result, the service automatically pauses replication of T1 on link AB.

Scenario 2

In this scenario:

- System A replicates to system B on link AB. Link AB can be either active/active or active/passive.
- Link AB includes namespace NS1, which is owned by tenant T1, so NS1 exists on both systems.
- NS1 is in enterprise mode, not compliance mode.
- The service plan that applies to NS1 is named SP1. SP1 is compliant on system A and noncompliant on system B.

These events occur in the order shown:

1. On system A, you change NS1 to be in compliance mode.
2. The Replication service tries to replicate the change to system B. The replication is unsuccessful because it would cause NS1 to be in compliance mode with a noncompliant service plan on system B. As a result, the service automatically pauses replication of T1 on link AB.

Content class collisions

Each content class you create in an HCP system has an internal ID that uniquely identifies that content class. As a result, two content classes created on different HCP systems are different from each other, even if they have the same name and are defined for the same tenant.

A content class collision occurs when the Replication service tries to replicate a content class from one system to another system that already has a different content class with the same name, where both content classes are defined for the same tenant.

To recover from a content class collision, take one of these actions:

- Rename the content class on either of the systems involved in the link.
- Delete the content class on either of the systems involved in the link.

Here's a scenario that shows how a content class collision can cause the Replication service to pause replication of a tenant. In this scenario:

- System A and system B replicate to each other over active/active link AB.
- Link AB includes tenant T1, so T1 exists on both systems.

These events occur in the order shown:

1. On system A, you create a content class named CC1 for T1.
2. Before CC1 is replicated to system B, you create a content class named CC1 for T1 on system B.
3. The Replication service tries to replicate CC1 to system B. The replication is unsuccessful because a different content class named CC1 already exists on system B. As a result, the service automatically pauses replication of T1 on link AB.

User account collisions

Each user account you create in an HCP system has an internal ID that uniquely identifies that user account. As a result, two user accounts created on different systems are different from each other, even if they have the same username and are defined for the same HCP tenant.

A user account collision occurs when the Replication service tries to replicate a user account from one system to another system that already has a different user account with the same username, where both user accounts are defined for the same tenant.

To recover from a user account collision, take one of these actions:

- Change the username for the user account on either of the systems involved in the link.
- Delete the user account on either of the systems involved in the link.

Here's a scenario that shows how a user account collision can cause the Replication service to pause replication of a tenant. In this scenario:

- System A and system B replicate to each other over active/active link AB.
- Link AB includes tenant T1, so T1 exists on both systems.

These events occur in the order shown:

1. On system A, you create a user account with username U1 for T1.
2. Before U1 is replicated to system B, you create a user account with username U1 for T1 on system B.
3. The Replication service tries to replicate U1 to system B. The replication is unsuccessful because a different user account with username U1 already exists on system B. As a result, the service automatically pauses replication of T1 on link AB.

Group account collisions

Each HCP group account you create in an HCP system has an internal ID that uniquely identifies that group account. As a result, two group accounts created on different systems are different from each other, even if they are created from the same Active Directory group and are defined for the same HCP tenant. (An HCP group account always has the same name as the AD group it's created from, so group accounts created from the same AD group on two different systems have the same name as each other.)

A group account collision occurs when the Replication service tries to replicate a group account from one system to another system that already has a different group account created from the same AD group, where both group accounts are defined for the same tenant.

To recover from a group account collision, delete the group account on either of the systems involved in the link.

Here's a scenario that shows how a group account collision can cause the Replication service to pause replication of a tenant. In this scenario:

- System A and system B replicate to each other over active/active link AB.
- Link AB includes tenant T1, so T1 exists on both systems.

These events occur in the order shown:

1. On system A, you create an HCP group account for T1 from the AD group named AD1. The name of the group account you create is AD1.
2. Before AD1 is replicated to system B, you create an HCP group account for T1 from the AD group named AD1 on system B. The name of the group account you create is AD1.
3. The Replication service tries to replicate the HCP group account named AD1 to system B. The replication is unsuccessful because a different group account named AD1 already exists on system B. As a result, the service automatically pauses replication of T1 on link AB.

Tenant conflicts

A tenant conflict occurs when you add a tenant to an erasure coding topology and that tenant is on one or more replication links where:

- The link is not in the topology
- One or both of the systems involved in the link are in the topology

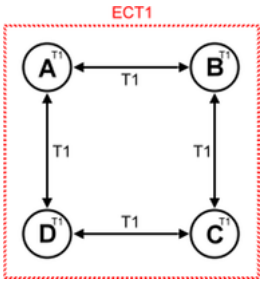
When a tenant conflict occurs, the Replication service automatically pauses replication or recovery of the tenant on each link that meets the criteria listed above.

To recover from a tenant conflict, take one of these actions:

- Remove the tenant from the links on which replication or recovery of the tenant is paused.
- Remove the tenant from the erasure coding topology. Then resume replication or recovery of the tenant on the applicable links.

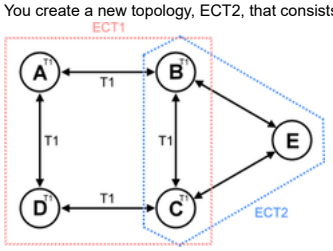
Here's a scenario that shows how a tenant conflict can cause the Replication service to pause replication of a tenant. In this scenario:

- Erase coding topology ECT1 is a ring topology that consists of:
  - Systems A, B, C, and D
  - Active/active link AB between systems A and B
  - Active/active link BC between systems B and C
  - Active/active link CD between systems C and D
  - Active/active link DA between systems D and A
- ECT1 is the active erasure coding topology.
- Tenant T1 is included in topology ECT1. Therefore, T1 is included on links AB, BC, CD, and DA and exists on systems A, B, C, and D.

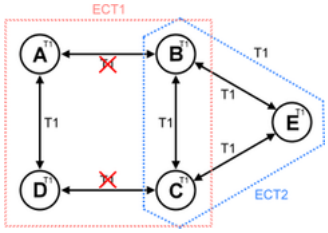


These events occur in the order shown:

1. You deploy system E.
2. You retire topology ECT1.
3. You create active/active link BE between systems B and E.
4. You create active/active link CE between systems C and E.
5. You create a new topology, ECT2, that consists of systems B, C, and E and links BC, BE, and CE.



6. You add tenant T1 to topology ECT2.
7. All of these occur:
   - T1 is added to links BE and CE and is replicated to system E.
   - The Replication service on system B pauses replication or recovery of T1 on link AB because system B is in topology ECT2 and system A is not
   - The Replication service on system C pauses replication or recovery of T1 on link CD because system C is in topology ECT2 and system D is not



Labeled holds in a replication topology

In a replication topology, when one or more labeled retention holds are placed on an object, there is a small time period when the hold settings will not be synchronized across all clusters. In a healthy replication environment, this time period should be minimal.

Before labeled hold settings are synchronized, the object is not protected from deletion. The object should not be considered on labeled retention hold until all clusters in the replication topology are synchronized.

There are several ways to verify the labeled hold status of an object in a replication topology, including:

- Use the REST API HTTP HEAD request with the `X-HCP-Get-Replicated:true` parameter on the same cluster where you added the labeled hold. In the resulting response header, check that `X-HCP-Replicated:true`.
- Use the HTTP HEAD request against the object on each cluster in the replicated topology. In the resulting response header, check that `X-HCP-LabelRetentionHold:true`.
- View the object in the NameSpace Browser on each cluster in the replication topology. Look in the Metadata column associated with object to verify that the lock icon, indicating that retention hold is enabled, is displayed.

Replication in an environment with mixed HCP versions

Starting in HCP 9.1, the labeled retention hold feature is supported. In a replication topology with mixed HCP versions, if you attempt to replicate objects that contain a labeled retention hold to a pre-version 9.1 cluster, the affected tenant on the replication link will be paused, while other tenants on the replication link will continue to replicate.

Therefore, before using the labeled retention hold feature, it is a best practice to upgrade all clusters in the replication topology to HCP 9.1 or later.

Shutting down and reestablishing all replication links

Shutting down replication links on an HCP system stops all activity on all links in which the system participates. You cannot shut down an individual link.

While links are shut down:

- No replication or recovery activity occurs on the links.
- The system where the links are shut down cannot read or repair objects from other HCP systems.
- Other HCP systems cannot read or repair objects from the system where the links are shut down.
- The system where the links are shut down can still service requests that are redirected from other HCP systems in the replication topology.
- Objects ingested on the system where the links are shut down are not protected from system failure.
- The system where the links are shut down is isolated in all erasure coding topologies that include the system. As a result:
  - Erasure-coded objects cannot be read from that system.
  - For a system in the active erasure coding topology, other systems in that topology cannot send full copies of object data or chunks for objects to that system. As a result, the topology protection status is broken on all systems in the topology.
- You cannot change which HCP tenants and namespaces, default-namespace directories, and inbound links are included in the links in which the system participates.
- An alert indicating that all links are shut down appears on the Overview page in the System Management Console for the system where the links are shut down.
- A message indicating that all links are shut down appears at the top of the Replication page in the System Management Console for the system where the links are shut down.

You may want to shut down replication links, for example, if you need to temporarily dedicate as much network bandwidth as possible to applications that are unrelated to HCP. Additionally, your authorized HCP service provider may ask you to shut down all links for certain system upgrade scenarios.

When you shut down all replication links, you are required to specify a reason for the action.

To restart activity on replication links after you’ve shut them down, you need to reestablish the links. Reestablishing the links returns each link to the state it was in before you shut down the links. If a link was active when you shut down all links, it becomes active again when you reestablish the links. If a link was suspended when you shut down all links, it remains suspended when you reestablish the links.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, take either of these actions:
   - To shut down all replication links:
     a. Click Shut Down All Links.

        The Shut Down All Replication Links window appears.

     b. In the Reason field, type the reason why you’re shutting down all links. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
     c. Click Shut Down All Links.
   - To reestablish all replication links, click Reestablish All Links.

Selecting the network for replication

In an HCP system that uses virtual networking, you can define multiple networks and then select the networks to use for various purposes, including replication. The network you select for replication on a given system is used for both incoming and outgoing replication traffic.

Networking infrastructure

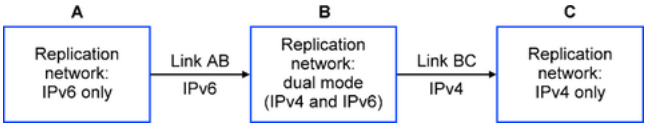
Different HCP systems can use different networks for the purpose of replication. When you select a replication network for a given system, you need to ensure that your networking infrastructure is configured to allow communications to be routed between that system and all other systems with which that system participates in a replication link.

IP mode

The two systems involved in a replication link must be able to use the same IP mode to communicate with each other. That is, either both networks must be configured with IPv4 addresses, or both networks must be configured with IPv6 addresses.

One or both of the networks involved can have both IPv4 and IPv6 addresses. If the replication networks for the two systems involved in a replication link have both types of addresses, HCP uses the IP addresses for the first mode in which it can establish communication between the two systems, with preference given to IPv6.

Within a replication topology, different pairs of systems can use different IP modes for communication. The figure below shows a replication chain in which different IP modes are used for communication over each link.



In the topology shown above:

- System A replicates to system B on link AB.
- System B replicates to system C on link BC.
- The replication network for system A has only IPv6 IP addresses.
- The replication network for system B has both IPv4 IP address and IPv6 addresses.
- The replication network for system C has only IPv4 IP addresses.
- System A and system B use IPv6 addresses to communicate with each other.
- System B and system C use IPv4 addresses to communicate with each other.

Loss of connectivity

You can select a different network for replication at any time. Selecting a different replication network on any given system can result in loss of connectivity to other systems with which that system is directly involved in replication.

When connectivity is lost between the two systems that participate in a replication link, the Replication service automatically suspends activity on that link. After restoring connectivity, you need to manually resume activity on the link.

For any given replication link, connectivity is lost between the two systems involved when you select a different network on one of the systems and either of these apply:

- The networking infrastructure is not configured to route communications between the new network and the network selected for replication on the other system.
- The new network is associated with a different domain from the previously selected network. In this case, the SSL server certificate used for replication changes, and you need to share the new certificate with the other system involved in the link.

  Additionally, in this case, if the system where you selected the new network is identified by domain name in the link configuration, you need to update the domain name in the link configuration.

In any case, if you select a different network on one system and the link identifies that system by IP addresses, you need to update those IP addresses in the link configuration.

If you need to both share new SSL server certificates and update the identification of one of the systems in the link configuration, you should share the certificates first. If you update the link first and then share the certificates, the link status changes to broken. To recover from this situation, you need to click again on Update Link in the Settings panel for the link.

Shared domain name

When you create a replication link, if both of the following are true, you need to use the replication.admin.*hcp-domain-name* format to identify the other system involved in the link:

- You are identifying the other system by domain name.
- The domain associated with the network selected for replication on the other system is also associated with another network.

In the configuration of an existing replication link, the domain name used to identify a system can have a format other than replication.admin.*hcp-domain-name*. In this case, you need to update the system identification to use the replication.admin.hcp-domain-name format if any of these happens on that system:

- You change the domain associated with the replication network to a domain that's also associated with another network.
- You select a new replication network, and the new network is associated with a domain that's also associated with another network.
- You change the domain associated with another network to the domain that's associated with the replication network.

Selecting the replication network

By default, HCP uses the [hcp_system] network for replication.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, in the Replication Network field, select the network you want to use for replication traffic.
   The dropdown list of networks does not include empty, degraded, or partial networks.
   The Replication Network field is present only while virtual network management is enabled for the HCP system.
4. Click Update Settings.

Displaying the zone definition for the replication network domain

Each network in HCP is associated with a domain. Multiple networks can be associated with the same domain. If you're using DNS for domain name resolution, the DNS needs to include a zone definition for each combination of network and domain.

If an HCP system is involved in replication, the zone definition for the replication network domain for that system needs to be added to the upstream DNS servers for the other system on the replication link. An *upstream DNS server* is a DNS server to which HCP routes the outbound communications HCP initiates (for example, for sending log messages to syslog servers or for communicating with Active Directory).

If the domain for the replication network is shared with other networks, the domain name in the zone definition you add for the replication network domain must be:

`replication.admin.`*`replicaton-network-domain-name`*

From the Replication page, you can display the zone definition for the replication network domain, formatted for Unix DNS servers. You can then copy that definition to the upstream DNS servers.

Note: You can display the zone definition only while virtual network management is enabled for the HCP system and only if at least one user-defined network exists.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, click Zone Definition.

The Zone Definition section opens. This section shows the zone definition for the network (with a type of slave or stub, as applicable), formatted as shown in this example:

```
# net1 Special-purpose HCP system network
zone "replication.admin.system_1.example.com" IN {
       type slave;
       file "/var/named/slave/replication.admin.system_1.example.com";
       masters {
             172.25.147.11;
             172.25.147.12;
             172.25.147.13;
             172.25.147.14;
       };
};
```

Managing DNS failover

HCP replication helps ensure continuous namespace availability. If a system in a replication topology fails, client requests for access to a replicated namespace can be serviced by other systems in the topology.

You can use the HCP DNS failover feature to automate the process of redirecting client requests from a failed system to a healthy one. For active/active links, this process can be automated in other ways as well. Automating redirection means that applications do not need to be modified to explicitly direct requests to another system when the normally targeted system fails.

The DNS failover feature requires that the HCP systems involved use a shared DNS for system addressing. If the systems don't use a shared DNS, DNS failover is not an option for automating redirection of client requests.

An HCP system can service automatically redirected requests only if the target namespace is configured to support service by remote systems. If the namespace is not configured this way, requests to access the namespace on a failed system fail.

About DNS failover

DNS failover is an HCP system configuration option that, when enabled on the one system involved in a replication link, forces requests to that system to be automatically redirected to the other system involved in the link while the link is failed over to the other system. This redirection occurs only when the request identifies the target system by domain name, not by IP address.

In effect, DNS failover causes the domain name for the failed-over system to be associated with the IP addresses for the nodes in the other system. Therefore, all types of requests that specify that domain name are redirected to the other system. This includes not only requests for namespace access but also requests for access to HCP interfaces such as the Tenant Management Console and HCP management API.

An HCP system can service redirected requests only if they come in through a namespace access protocol. This means that requests for access to the failed-over system that are made through other interfaces fail.

With an active/active link, failover can occur in either direction between the two systems involved in the link. Therefore, if you are using DNS failover for automatic redirection of client requests, you should enable it on both systems.

With an active/passive link, failover can occur only from the primary system to the replica. In this case, therefore, you need to enable DNS failover only on the primary system. However, if the replica is also the primary system for another link, you need to enable DNS failover on the replica as well.

For DNS failover to work for the system where it's enabled, the HCP domains for that system in the DNS must be configured to support service by remote systems. If DNS failover is not enabled, the HCP domains should not be configured that way.

DNS failover is intended to address cases of catastrophic failure of the HCP system where DNS failover is enabled. However, DNS failover also applies if you fail over a link while the system is healthy. In this case, the method used to access unreplicated items on that system depends on the data access network for the tenant that owns the target namespace.

For example, suppose:

- Tenants ten1 and ten2 both use the network named net1 for data access.
- Tenant ten1 and its namespace ns1 are in a replication link that is failed over from system A to system B.
- Tenant ten2 and its namespace ns2 are not in the failed-over replication link.

Client requests for access to ns1 on system A, where the request URL specifies the name of the domain associated with net1, are redirected to system B. Because they come in on the same network, client requests for access to ns2 on system A, where the request URL specifies the domain name, are also redirected to the system B and, therefore, fail. For those requests to succeed, they need to access system A by using an IP address assigned to a node in net1 on that system instead of by using the domain name.

The same consideration applies to access to other HCP interfaces. For example, if the data access network for a tenant in a link that's failed over from system A to system B is [hcp_system], you need to use an IP address to access the HCP System Management Console on system A.

DNS failover also affects replication between the failed-over system and any other system with which that system participates in a replication link. If the other system identifies the failed-over system by domain name, all replication activity on the link between the two systems stops.

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.

Enabling or disabling DNS failover

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, take either of these actions:
   - To enable DNS failover, select Enable DNS failover to other systems in the replication topology.
   - To disable DNS failover, deselect Enable DNS failover to other systems in the replication topology.
4. Click Update Settings.

Alternatives to DNS failover

DNS failover is an HCP-specific method for automatically managing service by remote systems. With active/active replication, other options exist:

- In an environment in which load balancers are used to spread client requests among multiple HCP systems, if one of the systems fails, the load balancers can ensure that the requests go to other systems.
- In a cloud storage environment, the networking and DNS infrastructure can be configured to support multiple HCP systems that use the same domain names. In this configuration, client requests are normally handled by the local DNS, but if an HCP system fails, the request can be passed on to another DNS that's local to another HCP system.

Managing the Replication Verification service

You can set the Replication Verification service to run once or to run continuously, or you can disable the service so that it doesn't run at all.

1. In the top-level menu of the HCP System Management Console, select Services > Replication.
2. On the left side of the Replication page, click Settings.
3. On the replication Settings page, take one of these actions:
   - To run the Replication Verification service once, select Run Replication Verification service. Then select Run once.
   - To run the Replication Verification service continuously, select Run Replication Verification service. Then select Run continuously.
   - To disable the Replication Verification service, deselect Run Replication Verification service.
4. Click Update Settings.

Changing link connectivity failure reporting

In the HCP System Management Console, you can set how long you want the HCP system to wait after a failed replication link connection before reporting the link connectivity failure.

1. In the top-level menu of the HCP System Management Console, select Services > Replication
2. On the left side of the Replication page, click Settings..
3. On the replication Settings page, locate the option to Report link connectivity failure after n seconds.
4. In the field represented by *n* in the above step, type the number of seconds you want HCP to wait before reporting a replication link connectivity failure.
   Valid values are integers greater than or equal to zero. On new installations of HCP, *n* is set to 0.
5. Click Update Settings.

Managing failover and failback

When one system involved in an active/active link fails or when the primary system for an active/passive link fails, you can fail over the link to the other system involved in the link. Failing over the link stops replication on the link and, if DNS failover is enabled, allows client requests that target the failed system to be redirected to the healthy system.

If a system failure results in a replication link being broken (for example, due to the system being rebuilt after a catastrophic failure), you need to restore the link before replication can restart or data recovery can occur on that link. This applies regardless of the link type and, for an active/passive link, regardless of whether the failed system is the primary system or the replica.

To restart replication after failing over a link, you need to fail back the link. Failing back the link restarts replication on the link and returns the HCP systems involved to normal operation. For an active/passive link, failing back includes recovering data from the replica to the primary system.

Failover can be automated for both active/active and active/passive links. Failback can be partially automated for active/passive links.

This section of the Help provides instructions and considerations for managing failover and failback manually.

To fail over a replication link, restore a link, or recover replicated data, you need the administrator role.

Note: You can also use the HCP management API to manage failover and failback of replication links.

Failover and failback workflows

Three failover and failback scenarios are possible, depending on which of these HCP systems fails:

- One of the systems involved in an active/active link
- The primary system for an active/passive link
- The replica for an active/passive link

This section of the Help describes the basic workflows for these scenarios.

System failure workflow with an active/active link

The table below outlines what happens when one of the systems involved in an active/active link fails, where the system that fails is system A and the system that remains healthy is system B.

Step	What you do	What happens
System A fails		
1	On system B, fail over the link	If DNS failover is enabled, system B broadcasts new DNS configuration
2	If DNS failover is disabled, direct clients to write only to system B	

Step	What you do	What happens
System A comes back online		
3	If system A has been rebuilt: • On system A, upload the replication SSL server certificate from system B • On system B, upload the replication SSL server certificate from system A	
4	On system B, update the link configuration as needed	
5	If the link is broken, on system B, send a request to restore the link	Replication link is recreated
6	On system B, fail back the link	System A and system B broadcast original DNS configurations; replication restarts in both directions on the link

Primary system failure workflow

The table below outlines what happens when the primary system for an active/passive link fails.

Step	What you do	What happens
Primary system fails		
1	On the replica, fail over the link	Applicable tenants and directories on the replica become read-write; applicable tenants and directories on the primary system either remain read-write or become read-only depending on whether the two systems can communicate with each other; if DNS failover is enabled, the replica broadcasts new DNS configuration
2	If DNS failover is disabled, direct clients to write only to the replica	
Primary system comes back online		
3	If the primary system has been rebuilt: • On the primary system, upload the replication SSL server certificate from the replica • On the replica, upload the replication SSL server certificate from the primary system	
4	On the replica, update the link configuration as needed	
5	If the link is broken, on the replica, send a request to restore the link	Replication link is recreated
6	On the replica, begin data recovery	Applicable tenants and directories on the replica remain read-write; applicable tenants and directories on the primary system remain or become read-only; data recovery from the replica to the primary system begins
7	Wait for data recovery to come close to being up to date	
8	On the replica, complete data recovery	Applicable tenants and directories on the replica become read-only; applicable tenants and directories on the primary system remain read-only; data recovery from the replica to the primary system continues to completion
Data recovery finishes		
9	Nothing	Applicable tenants and directories on the replica remain read-only; applicable tenants and directories on the primary system become read-write; the primary system and the replica broadcast original DNS configurations; replication from the primary system to the replica restarts
10	If DNS failover is disabled, after you see this message in the system log, direct clients to write only to the primary system: *Replication data recovery completed*	

Replica failure workflow

The table below outlines what happens when the replica for an active/passive link fails.

Step	What you do	What happens
Replica fails		
1	On the primary system, suspend activity on the link	
Replica comes back online		
2	If the replica has been rebuilt: • On the replica, upload the replication SSL server certificate from the primary system • On the primary system, upload the replication SSL server certificate from the replica	
3	On the primary system, update the link configuration as needed	

Step	What you do	What happens
4	If the link is broken, on the primary system, send a request to restore the link	Replication link is recreated; applicable tenants and directories on the primary system remain read-write; applicable tenants and directories on the replica are read-only
5	On the primary system or the replica, resume activity on the link	Replication from the primary system to the replica restarts from the beginning

Failing over

1. In the top-level menu of the HCP System Management Console for the system you want to fail over to, select Services > Replication.
2. On the replication Links page, click the link you want to fail over.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Failover tab.
5. In the link Failover panel, click Fail Over.
   A confirming message appears.
6. In the window with the confirming message, select I understand to confirm that you understand the consequences of your action. Then click Fail Over Link.
7. For an active/passive link, if DNS failover is disabled, tell the applicable tenant administrators to direct all client access requests to the replica.

Recovering from a failure

During a catastrophic failure, an HCP system can lose all configuration information. In this case, if the system participates in a replication link, you need to restore the link configuration after the system is rebuilt. If the failure did not cause the system to lose the link configuration, you don't need to restore the link.

Once the link configuration exists on both systems involved in the link:

- For an active/active link, you need to perform the failback procedure.
- For an active/passive link:
  - If the primary system failed, you need to recover namespace content and other applicable information from the replica.
    Note: After you fail over an active/passive link, the only way to return to normal replication is by going through the data recovery procedure. You need to perform this procedure even if you don't need to restore the link and even if no changes have been made to the configuration or content of the replicated items. Even when nothing has change, the data recovery process can take more than five minutes.
  - If the replica failed, replication automatically restarts, beginning again with the objects with the oldest metadata changes either across all namespaces or within each namespace, depending on the link configuration.

Restoring a link

You do not need to restore a replication link if both systems involved in the link have the correct link configuration. In this scenario, you can skip this portion of the recovery procedure even though the Restore Link button is enabled.

Note: Clicking Restore Link will cause the pending recovery to attempt to replicate all object data over the restored link. If the failover and recovery procedures are part of a failover and recover test, clicking this button might cause the recovery procedure to take a lot more time than necessary.
Before you can restore a replication link, both systems involved in the link must have the required SSL certificates installed.

1. In the top-level menu of the HCP System Management Console for the system where the link configuration still exists, select Services > Replication.
2. On the replication Links page, click the link you want to restore.
3. On the Replication Link Details page, click Link.
4. If necessary, update the link configuration.
   You must complete this step only if the domain name or IP addresses of the other system has changed. If the domain name of the other system has not changed, do not replace the displayed IP addresses with the domain name.
   Note: After a system failure that is part of an erasure coding topology, if the replacement system has a different domain name or different IP addresses from the failed system, you need to reconfigure all the replication links that connect other systems in the topology to the failed system. When reconfiguring the links, ensure that they all connect to the same replacement or rebuilt system; otherwise, the erasure coding topology will no longer function.
5. In the replication Link panel, click the Failover tab.
6. In the Failover pane, click Restore Link.
   Note: If you do not see the Restore Link button, wait a few minutes and then refresh the Replication page. Before displaying this button, HCP must recognize that the other system is available, has the necessary SSL certificates installed, and is unaware of the existing link.

After you restore a link, the Restore Link button remains active. This state enables you to repeat the restore procedure if the system that failed needs to be rebuilt again before you fail back or begin recovery on the link. Although the button is still active, you can proceed to the next part of the recovery procedure.

Failing back an active/active link

1. In the top-level menu of the HCP System Management Console for the system you failed over to, select Services > Replication.
2. On the replication Links page, click the link you want to fail back.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Failover tab.
5. In the link Failover panel, click Fail Back.

Recovering the data after a primary system failure

1. In the top-level menu of the HCP System Management Console for the replica, select Services > Replication.
2. On the replication Links page, click the link on which you want to recover data.
3. On the replication link details page, click Link.
4. In the replication Link panel, click the Failover tab.
5. In the link Failover panel, click Begin Recovery.
   Note: After uploading new trusted replication server certificates, you may need to wait more than ten minutes for the Begin Recovery button to become active.

   The applicable HCP tenants and default-namespace directories become read-only on the primary system, and the Replication service starts copying the applicable objects and configuration information from the replica to the primary system. As with replication from the primary system to the replica, the service starts with the objects with the oldest metadata changes either across all namespaces or within each namespace, depending on the link configuration.

Note: If the primary system cannot communicate with Active Directory and either of these is true for a tenant, recovery of that tenant is automatically paused:
- The tenant to be recovered supports AD authentication.
- A namespace owned by the tenant supports AD single sign-on.

When communication between the primary system and AD is restored, you can resume recovery of the tenant.

6. Monitor the recovery process by periodically reviewing the information in the status Overview and status Tenants panels for the link.
7. When data recovery is almost synchronized with current tenant and namespace activities on the replica, return to the Failover panel for the link.
   Synchronization is nearing completion when the up-to-date-as-of time for the link is close to zero.
   Note: As long as clients continue writing to the replica, synchronization won't reach one hundred percent. Synchronization doesn't need to be completely up to date for you to start the complete recovery phase.
8. In the link Failover panel, click Complete Recovery.
   The applicable tenants and directories on the replica immediately become read-only. The tenants and directories on both systems then remain read-only until the Replication service finishes the data recovery. The amount of time this takes depends on how much data is left to recover.

   When recovery is complete, the tenants and directories on the primary system become read-write, those on the replica remain read-only, and the Replication service on the primary system starts copying objects to the replica again.

   Tip:
   - You can schedule completion of the data recovery process for a time when client usage of the repository is low.
   - If, before final recovery is complete, you need to allow clients to write to the applicable tenants and directories on the replica again, click Cancel Final Recovery in the link Failover panel. The recovery process continues, but the applicable tenants and directories become read-write on the replica and remain read-only on the primary system until you click Complete Recovery again.
9. If DNS failover is disabled:
   a. Wait for this message to appear in the system log:

      ```
      Replication data recovery completed
      ```

   b. Tell the applicable tenant administrators to redirect all client access requests to the primary system.

Failover and failback considerations

These basic rules apply to replication, failover, and failback on replication links, regardless of the replication topology:

- Multiple failed-over active/active links in a replication topology can be failed back in any order.
- With failback of multiple failed-over active/passive links in a replication topology, order matters.
- If a topology includes both failed-over active/active links and failed-over active/passive links, order matters for failing back the active/passive links, but the active/active links can be failed back in any order and at any time.
- With active/passive links, failover occurs from the primary system to the replica for the same link. Failover cannot occur from the primary system for one link to the replica for a different link.
- With active/passive links, failback occurs from the replica to the primary system for the same link. Failback cannot occur from the replica for one link to the primary system for another link.
- With an active/passive link, when a link fails over to the replica, only the HCP tenants and namespaces and default-namespace directories that were read-write on the primary system become read-write on the replica.
- In a complex replication topology that includes only active/passive links in many-to-one and/or chained relationships, the HCP tenants and namespaces and default-namespace directories being replicated in the topology are read-write on at most one HCP system at a time. This is true regardless of the type of activity on the links.

Additional considerations apply to failover and failback in replication topologies that include multiple links.

Failover and failback in an active/passive many-to-one topology

In an active/passive many-to-one replication topology, multiple HCP systems replicate to a single other HCP system.

To recover from a single primary system failure in an active/passive many-to-one replication topology, you follow the normal pattern:

1. Fail over the link between the failed primary system and the replica.
2. When the primary system becomes available again, restore the link from the replica.
3. Begin and complete data recovery from the replica to the primary system.

If more than one primary system fails in an active/passive many-to-one topology, you need to fail the link from each failed system over to the replica. Multiple inbound links on the replica can be in the failed-over state at the same time.

When the failed systems become available again, you can restore the links at any time. However, you can perform data recovery on only one link at a time. (You don't need to wait for all the failed systems to become available before recovering data to the first one.)

For example, suppose systems A, B, and C all replicate to system D. If both A and B fail, you can return to normal replication with these steps after the failed systems become available again:

1. On system D, restore the link from A to D.
2. On system D, begin and complete data recovery from D to A.
3. On system D, restore the link from B to D.
4. After the recovery of data from D to A is complete and replication from A to D has restarted, on system D, begin and complete data recovery from D to B.

Failover and failback in an active/passive chained topology

In an active/passive chained replication topology, one HCP system replicates to a second HCP system, which replicates to a third HCP system.

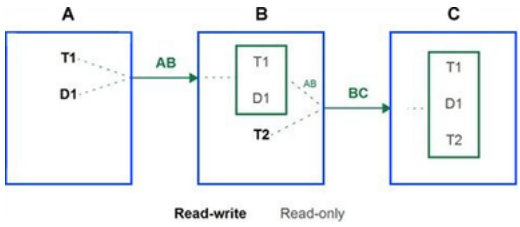
The way you manage failover and failback in an active/passive chained replication topology depends on which system or systems have failed. The links from the first system in the chain to the second system and from the second system to the third system function independently of each other, but order matters when you fail them over or restore and perform data recovery on them.

This section of the Help outlines the steps you need to take to return an active/passive replication chain to normal operation after the failure of any one or two of the systems in the chain. These sections assume a replication topology in which, when all three systems are healthy:

- System A replicates to system B on link AB.
- Link AB includes HCP tenant T1 and default-namespace directory D1, both of which were originally created on system A.
- System B replicates to system C on link BC.

- Link BC includes link AB and HCP tenant T2, which was originally created on system B.
- T1 and D1 are read-write on system A and read-only on systems B and C.
- T2 is read-write on system B and read-only on system C.

The figure below shows this topology.



Scenario: System A fails

To return to normal operation after system A fails:

1. On system B, fail link AB over to B.
   T1 and D1 become read-write on B.
2. When system A becomes available again, on system B, restore link AB.
3. On system A, accept the restored link.
4. On system B, begin and complete data recovery on link AB.

When data recovery is complete, T1 and D1 become read-write on A and read-only on B, and replication resumes on link AB.

Scenario: System B fails

To return to normal operation after system B fails:

1. On system C, fail link BC over to C.
   T1 and D1 remain read-write on A and read-only on C. T2 becomes read-write on C.
2. When system B becomes available again, on system A, restore link AB.
3. On system B, accept the restored link.
   T1 and D1 are read-write on A and read-only on B and C, and replication restarts on link AB.
4. On system C, restore link BC.
5. On system B, accept the restored link.
6. On system C, begin and complete data recovery on link BC.

When data recovery is complete, T1 and D1 are read-only on B and C. T2 becomes read-write on B and read-only on C, and replication resumes on link BC.

Scenario: System C fails

To return to normal operation after system C fails:

1. When system C becomes available again, on system B, restore link BC.
2. On system C, accept the restored link.

T1 and D1 remain read-only on B and C. T2 remains read-write on B and read-only on C, and replication restarts on link BC.

Scenario: Systems A and B fail

To return to normal operation after systems A and B fail:

1. On system C, fail link BC over to C.
   T1 and D1 remain read-only on C. T2 becomes read-write on C.
2. When system B becomes available again, on system C, restore link BC.
3. On system B, accept the restored link.
4. On system C, begin and complete data recovery on link BC.
   When data recovery is complete, T1 and D1 are read-only on B and C. T2 becomes read-write on B and read-only on C, and replication resumes on link BC.

   System B automatically recreates link AB without the primary system IP addresses or hostname from the inbound link AB in link BC.

5. When system A becomes available again, take either of these actions:
   - If link AB still exists on A:
     a. On system A, restore link AB.
     b. On system B, accept the restored link.
     c. On system B, begin and complete data recovery on link AB.

     When data recovery is complete, T1 and D1 become read-write on A and remain read-only on B, and replication resumes on link AB.

   - If link AB no longer exists on A, follow the steps for option one or option two below.

     Option one:

     a. On system B, update the configuration of the automatically recreated link AB to include the IP addresses or hostname for system A.
     b. On system B, restore link AB.
     c. On system A, accept the restored link.
     d. On system B, begin and complete data recovery on link AB.

     When data recovery is complete, T1 and D1 are read-write on A and read-only on B and C, and replication restarts on link AB.

     Option two:

     a. On system B, suspend and then delete link AB.

T1 and D1 become directly included on link BC, which still includes T2, and become read-write on B.

b. Optionally, create a new replication chain B > C > A:
   i. Reinstall HCP on A.
   ii. On system C, create outbound link CA, including link BC as an inbound link.
   iii. On system A, accept the new link.

c. T1, D1, and T2 are read-write on B and read-only on C and A, and replication starts on link CA.

Scenario: Systems A and C fail

To return to normal operation after systems A and C fail:

1. On system B, fail link AB over to B.
   T1 and D1 become read-write on B. T2 remains read-write on B.
2. When system C becomes available again, on system B, restore link BC.
3. On system C, accept the restored link.
   T1, D1, and T2 are read-write on B and read-only on C, and replication restarts on link BC.
4. When system A becomes available again, on system B, restore link AB.
5. On system A, accept the restored link.
6. On system B, begin and complete data recovery on link AB.

When data recovery is complete, T1 and D1 become read-write on A and read-only on B, and replication resumes on link AB.

Scenario: Systems B and C fail

To return to normal operation after systems B and C fail:

1. When system B becomes available again, on system A, restore link AB.
2. On system B, accept the restored link.
   T1 and D1 are read-write on A and read-only on B, and replication restarts.
3. When system C becomes available again, if T1 and D1 still exist on system C, delete them.
   This requires that all objects in the namespaces owned by T1 and in D1 be deleted first.
   Note: If T2 still exists on systems B and C, delete it from C. If T2 still exists on system C and not on system B, you can recover it to B by creating a link from C to B. However, you cannot then replicate T2 from B to C unless you first delete it from C.
4. On system B, create outbound link BC, including link AB as an inbound link. If T2 still exists on B, also include T2 in the link.
5. On system C, accept the new link.

T1 and D1 are read-only on B and C. If T2 is on link BC, T2 is read-write on B and read-only on C. Replication restarts on link BC.

Failover and failback in an active/passive one-to-many topology

In an active/passive one-to many replication topology, one HCP system replicates to two or more other systems.

If one of the replicas fails, you follow the normal pattern for recovering from a replica failure. If more than one replica fails, you follow the normal recovery pattern for each replication link individually. The order in which you perform the recovery procedures doesn't matter.

Throughout these failure scenarios, the HCP tenants and namespaces and default-namespace directories on each link remain read-write on the primary system and read-only on the replicas. Therefore, even if the links include the same items, no conflicts can occur.

However, if two or more links include the same HCP tenants and namespaces and default-namespace directories and the primary system fails, these items can be read-write on multiple systems at the same time. This can lead to conflicts during data recovery.

For example, assume a replication topology in which, when all three systems are healthy:

- System A replicates to system B on link AB. Link AB includes HCP tenant T1.
- System A replicates to system C on link AC. Link AC also includes HCP tenant T1.

1. On system B, fail link AB over to B.
   T1 becomes read-write on B and read-only on A and remains read-only on C.
2. On system C, fail link AC over to C.
   T1 becomes read-write on C and remains read-only on A and read-write on B. T1 is now read-write on two systems.
   Tip: To prevent recovery conflicts, ensure that clients write to only system B or only system C while both systems are read-write.
3. When system A becomes available again, on system B, restore link AB.
   You could restore link AC first. The order in which you restore the links doesn't matter.
4. On system A, accept the restored link.
5. On system B, begin and complete data recovery on link AB.
   When data recovery is complete, T1 remains read-only on A because link AC is stilled failed over to C. It becomes read-only on B and remains read-write on C. Replication resumes on link AB.
6. When data recovery on link AB is complete, on system C, restore link AC.
7. On system A, accept the restored link.
8. On system C, begin and complete data recovery on link AC.

T1 becomes read-write on A and read-only on C and remains read-only on B. Replication resumes on link AC.

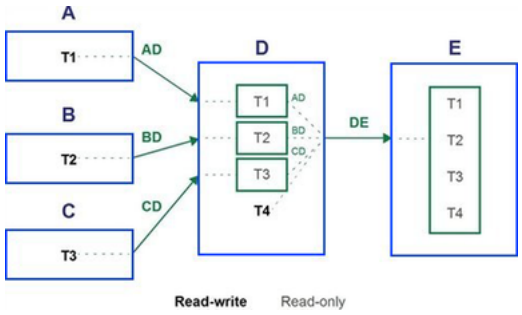
Failover and failback in an active/passive many-to-one topology with disaster recovery support

When HCP systems fail in an active/passive many-to-one topology with disaster recovery support, you need to combine the failback patterns for the many-to-one and chained topologies.

For example, assume a replication topology in which, when all five systems are healthy:

- System A replicates to system D on link AD. Link AD includes HCP tenant T1, which was originally created on system A.
- System B replicates to system D on link BD. Link BD includes HCP tenant T2, which was originally created on system B.
- System C replicates to system D on link CD. Link CD includes HCP tenant T3, which was originally created on system C.
- System D replicates to system E on link DE. Link DE includes links AD, BD, and CD and tenant T4, which was originally created on system D.
- T1, T2, and T3 are read-write on systems A, B, and C, respectively, and read-only on systems D and E.
- T4 is read-write on system D and read-only on system E.

The figure below shows this topology.



To return to normal operation after systems A, B, and D fail:

1. On system E, fail link DE over to E.
   T1, T2, and T3 are read-only on E. T4 becomes read-write on E. T3 remains read-write on C.
2. When system D becomes available again, on system E, restore link DE.
3. On system D, accept the restored link.
4. On system E, begin and complete data recovery on link DE.
   When data recovery is complete, T1, T2, and T3 are read-only on D and E. T4 becomes read-write on D and read-only on E, and replication resumes on link DE.
5. On system C, restore link CD.
6. On system D, accept the restored link.
   T3 is read-write on C and read-only on D, and replication restarts on link CD.
7. When system A becomes available again, on system D, update the configuration of the automatically recreated link AD.
8. On system D, restore link AD.
9. On system A, accept the restored link.
10. On system D, begin and complete data recovery on link AD.
    When data recovery is complete, T1 becomes read-write on A and remains read-only on D. Replication resumes on link AD.
11. When system B becomes available again and data recovery on link AD is complete, on system D, update the configuration of the automatically recreated link BD.
12. On system D, restore link BD.
13. On system B, accept the restored link.
14. On system D, begin and complete data recovery on link BD.

When data recovery is complete, T2 becomes read-write on B and remains read-only on D. Replication resumes on link BD.

Reenabling user accounts disabled on the replica

For HCP tenants on an active/passive link, tenant-level user accounts are replicated and are available for use on the replica. If an account becomes disabled on the replica due to consecutive failed login attempts, it cannot be reenabled on the replica because the tenant is read-only.

1. In the top-level menu of the Tenant Management Console for the applicable HCP tenant on the primary system, select Security > Users.
2. In the list of user accounts on the Users page, click the user account you want to modify.
3. Click Update Settings.
4. Wait for the updated account to be replicated.

When the account is replicated, it becomes enabled on the replica.

Setting advanced replication options

To perform the activities listed, you need the service role.

Changing the custom performance level

At any given time, a sending system on a replication link has a performance level that's set in accordance with a schedule or a schedule override. The performance level controls the number of replication threads that can run on each node in the system for that link. For the low, medium, and high performance levels, the numbers of threads are one, five, and ten, respectively. For the custom performance level, the default number of threads is 25, but you can change this number.

The performance level is a maximum. On any given node, fewer threads can be running than the number indicated by the performance level.

If a system is sending data on more than one link, the maximum number of threads per node on that system is the total allowed by all those links.

The number of threads for the custom performance level is a systemwide setting that applies to all links in which the system participates.

- To perform the activities in this procedure, you need the service role.
- If a sending system is already using the custom performance level when you change the number of threads, you need to suspend and resume the link for the change to take effect.

1. In the top-level menu of the HCP System Management Console, select Configuration > Miscellaneous.
2. In the Replication Threads for Custom Performance Level field, type the new number of threads for the custom performance level.
   Valid values are integers in the range one through 25.
3. Click Update Settings.

Changing the broken-link reporting interval

HCP supports the use of SNMP for reporting certain events and conditions. When this capability is enabled, HCP reports broken links on a periodic basis. That is, while a link is broken, HCP sends an SNMP notification about the broken link every n minutes. By default, n equals 60. You can change this value.

1. In the top-level menu of the HCP System Management Console, select Configuration > Miscellaneous.
2. In the SNMP Broken-link Reporting Interval field, type the number of minutes you want HCP to wait between SNMP notifications about broken links.

Valid values are integers greater than or equal to one.

3. Click Update Settings.