Shredding service

Shredding, also called *secure deletion*, is the process of overwriting the places where all the copies of the data, secondary metadata, and custom metadata for an object were stored in such a way that the object cannot be reconstructed.

The Shredding service shreds deleted objects that are marked for shredding. If the object is a multipart object, the Shredding service shreds each part of the object. The Shredding service also shreds unused parts of multipart uploads that were initiated in namespaces where the default shred setting is true.

The primary metadata for a shredded object is deleted from HCP after all of these events have happened:

*   The object is removed from the metadata query engine index, if applicable.
*   The object deletion is replicated, if applicable.
*   For old versions of objects, the version is pruned or purged.
*   The deletion record for the object is deleted from the transaction log. If the Garbage Collection service is configured never to delete deletion records from the transaction log, the primary metadata for the object remains in the system indefinitely.

The shredding policy for each object determines whether that object is shredded.
NoteThe Shredding service does not shred object data if:

*   The data is stored in a namespace that uses a service plan that has HCP S Series storage set as the ingest tier.
*   The data is stored on extended storage.

Shredding service processing

By default, the Shredding service uses three passes to overwrite the areas where the object data, secondary metadata, and custom metadata were stored. The three passes are applied to the entire object, repeating for each 128-KB block. Each pass has this pattern:

*   Set to a specified value (write the 0xAA pattern to the file)
*   Set to the complement of that value (write the 0x55 (~0xAA) pattern to the file)
*   Set to a random value (write a random value to every byte of the entire file)
*   Verify the value by reading it back

To use a different shredding algorithm, contact your authorized HCP service provider.

Sending shredding messages to syslog servers

HCP gives you the option of sending a log message for each shredded object or part to the syslog servers specified in the syslog logging configuration. This option takes effect only while syslog logging is enabled and the syslog logging level is set to `Notice`. The log message for a shredded object or part is sent to the syslog servers only after the primary metadata for the object is deleted.

Object shredding is a namespace-level event. Therefore, messages about shredded objects and parts are sent to the syslog servers only if syslog logging is enabled at the tenant level.

Log messages about shredded objects and parts do not appear in the System Management Console or Tenant Management Console regardless of whether those messages are sent to the syslog servers.
NoteHCP never sends messages about shredded objects and parts to the system log or SNMP managers.

Understanding shredding statistics

The Shredding page in the HCP System Management Console lets you monitor the amount of data waiting to be shredded. It also lets you control various aspects of shredding activity.
NoteTo view the Shredding page, you need the monitor or administrator role. To change shredding settings, you need the administrator role.

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

The Shredding page shows:

• Objects and object parts waiting to be shredded

   The total number of these items waiting to be shredded: objects, parts of multipart objects, replaced parts of multipart uploads, parts of aborted multipart uploads, unused parts of completed multipart uploads, and transient parts created during the processing of certain multipart upload operations

• Total bytes to be shredded

   The total number of bytes of object and part data and metadata waiting to be shredded

These statistics include all objects and parts marked for shredding for which the primary metadata has not yet been deleted.

The panel also shows the current shredding settings.

Changing shredding settings

Depending on the system load, the HCP system can develop a backlog of objects and parts to be shredded. If the system load from other activities is light, you can increase the rate at which shredding occurs. If the load is heavy, you can lower the shredding rate.

To change the settings for the Shredding service:

1. On the Shredding page in the System Management Console, set the options you want:
   - To change the shredding rate, in the Shredding Rate field, select Low, Medium, or High. The higher the shredding rate, the greater the load on the HCP system.
   - To enable or disable sending log messages about shredded objects and parts to syslog servers, select or deselect, respectively, Log shredded objects and object parts to syslog.
2. Click Submit.

Duplicate elimination and shredding

Objects merged by the Duplicate Elimination service do not necessarily have the same shred settings.

When merged objects with different shred settings are deleted:

- If the last object deleted is not marked for shredding, the merged data is not shredded.
- If the last object deleted is marked for shredding, the merged data is shredded.

Erasure coding and shredding

For an object that's subject to both erasure coding and shredding:

- Each time a full copy of the data for the object is reduced to a chunk, the full copy must be shredded
- Each time a chunk for the object is restored to a full copy of the object data, the chunk must be shredded

As a result, shredding objects that are subject to erasure coding can put a significant load on all the systems in the replication topology across which the objects are erasure coded.

To minimize the load that the combination of erasure coding and shredding can put on an HCP system, take one of these actions:

- At the system level, do not enable erasure coding as an option for implementing replicaton.
- If you enable erasure coding as the replication method for all cloud-optimized namespaces, tell tenant administrators not to set shredding as the default for deleted objects in cloud-optimized namespaces that are selected for replication.
- If you allow tenant administrators to select erasure coding for their namespaces, tell the administrators not to do both of these for any given namespace:
  - Set shredding as the default for deleted objects
  - Allow erasure coding

Shredding service trigger

The Shredding service is event driven only, not scheduled. It is triggered by the deletion of an object that's marked for shredding. The delete operation can be invoked by a user or application or by the Garbage Collection service.