panzura

Solution Brief

Secure Erase – Eliminating Data from the Cloud

Overview

IT environments subject to strict data security classification and management often require the ability to securely remove all traces of highly sensitive files. Secure Erase makes it possible to delete a file or folder in such a way that the contents cannot be restored, even using the most advanced technology available. In fact, Secure Erase removes all versions of specified files and folders, including the associated objects stored in the cloud.

Snapshots will age out according to the settings defined in User Managed Snapshot settings. Once the snapshots are deleted by the administrator, or aged out, no trace of the file or folder will exist anywhere within the CloudFS.

A log file records the actions that were taken. Upon completion of a Secure Erase operation, a log file can be downloaded from the Web UI, which records the actions that were undertaken. This is provided so administrators can show documentation of the action taken (as per the recommendations of the Guidelines for Media Sanitization: Recommendations of NIST).

Depending on the amount of data to be securely erased, the operation may consume additional CPU and memory for a while. To help limit the effects upon end-user performance, it is possible to schedule Secure Erase operations to take place at a specified day and time, up to seven days in advance.

Key Points

- Secure Erase removes all traces of specified files and folders from the Panzura CloudFS.
  - » Department of Justice was a catalyst for this feature as security status of files may have been reclassified, thereby requiring files to be removed
  - » Mistakenly placed classified data files on shared access that need to be removed
- Secure Erase can be used with any supported cloud provider
- Secure Erase events can be scheduled
  - » Helpful in situations where large quantities of data are being erased
  - » By scheduling Secure Erase events, impact on CPU and memory is limited
- Once operation is complete, a log file can be downloaded indicating what actions, to what files, were taken
- Implementation is modeled after *The National Institute of Standards and Technology (NIST) Special Publication 800-88: Guidelines for Media Sanitization: Recommendations of NIST*
- Panzura uses techniques categorized as a “Purge” by NIST
  - » Highest purge level that can be attained without physically destroying the disk drives
  - » All data is securely erased and replaced with zeroes
- Secure Erase is a licensed feature

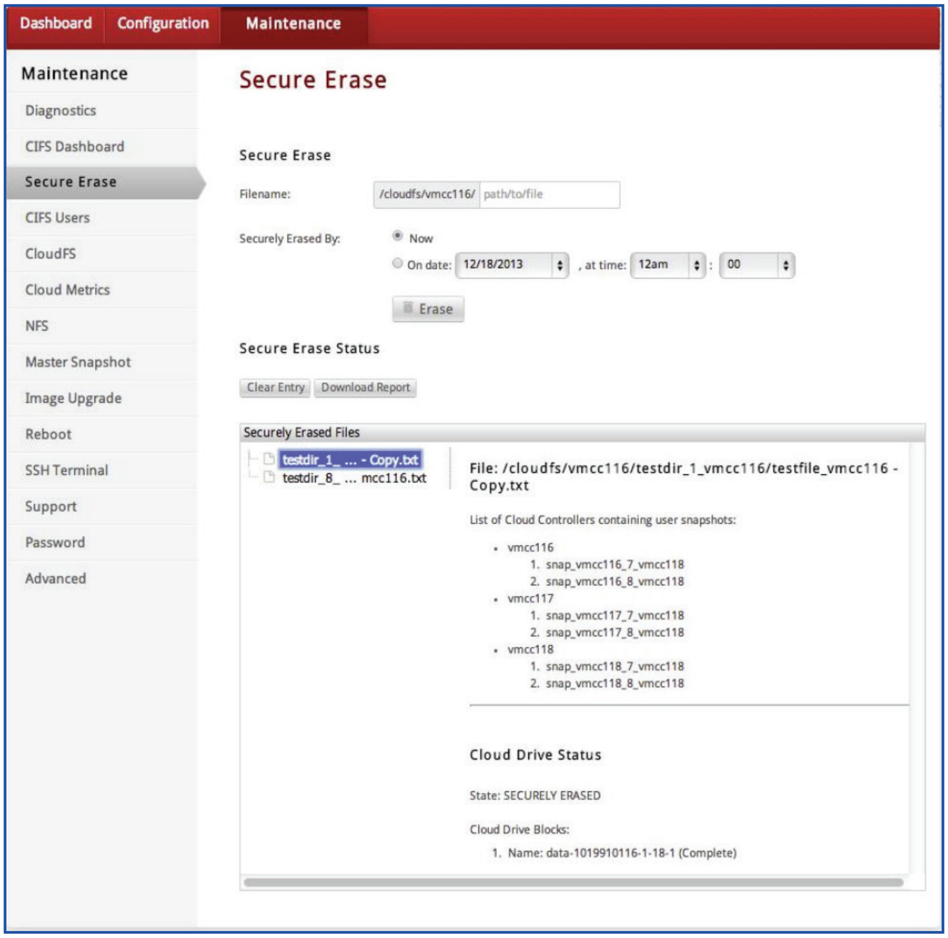
Security

Secure Erase operations conform to the latest recommendations of the *National Institute of Standards and Technology, Computer Security Division, Special Publication 800-88*, dated September, 2012.

Following recommendations put forth by NIST in Publication 800-88 for purging data, Secure Erase is the most complete data erasure method available short of physically destroying the storage media itself. The Secure Erase feature provides a report detailing the exact steps used to remove the data from the cloud.

Total Erasure: Leaving Nothing Behind

The Schedule Files / Directories list shows when scheduled items will be deleted. Cloud Drive Status (see Status page example on next page) lists all files that already have been deleted. By clicking on **Download Report**, a report is generated to show all actions taken by Secure Erase. After the report is downloaded, click on **Clear Entry** to erase all the report contents from the system.



Secure Erase

Secure Erase

Filename: /cloudfs/vmcc116/ path/to/file

Securely Erased By: ● Now
○ On date: 12/18/2013 , at time: 12am : 00

Secure Erase Status

Securely Erased Files

testdir_1_ ... - Copy.txt
testdir_8_ ... mcc116.txt

File: /cloudfs/vmcc116/testdir_1_vmcc116/testfile_vmcc116 - Copy.txt

List of Cloud Controllers containing user snapshots:

- vmcc116
  1. snap_vmcc116_7_vmcc118
  2. snap_vmcc116_8_vmcc118
- vmcc117
  1. snap_vmcc117_7_vmcc118
  2. snap_vmcc117_8_vmcc118
- vmcc118
  1. snap_vmcc118_7_vmcc118
  2. snap_vmcc118_8_vmcc118

Cloud Drive Status

State: SECURELY ERASED

Cloud Drive Blocks:

1. Name: data-1019910116-1-18-1 (Complete)

How to Use: Easy Steps for Secure Erase

- Specify the file or directory name to remove.
- Select a date for deletion, or click **Now** for immediate deletion.
- Click **Erase** to active the delete operation.
- Report generation will show deleted files.

Panzura, Inc. | 695 Campbell Technology Pkwy #225, Campbell, CA, USA | 855-PANZURA | www.panzura.com