Technical Report

Video Surveillance Solutions with NetApp SANtricity Cloud Connector 3

Backup and Restore

Fayyaz Khan and Frank Poole, NetApp
May 2020 | TR-4703

Abstract

Video surveillance solutions using NetApp® E-Series storage offer the physical security integrator a highly scalable repository for video management systems that support high camera counts, megapixel resolutions, high frame rates, and long retention periods. This solution can be augmented with NetApp SANtricity® Cloud Connector to perform backup and restore jobs to an existing Amazon S3, NetApp StorageGRID®, or NetApp Cloud Backup (formerly AltaVault™) account.

NetApp®

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

NetApp E-Series storage arrays offer performance, efficiency, reliability, and enterprise-class support for large-scale video surveillance deployments.

NetApp SANtricity Cloud Connector is a host-based Linux application that allows users to perform full block and file-based backup and recovery of NetApp E-Series volumes to Amazon Simple Storage Service (S3), NetApp StorageGRID object-based storage, and NetApp Cloud Backup storage.

Together, these solutions can provide video surveillance solution (VSS) users who have not invested in cloud integration software with an integrated software alternative to begin their cloud integration journey.

1.1 Publication Scope

This document contains information for those who need to implement a simple and easy-to-use backup and restore solution of a video surveillance system that uses NetApp E-Series storage.

1.2 Audience

This publication offers guidance to physical security integrators, video surveillance management software engineers, and architects who are responsible for integrating NetApp SANtricity Cloud Connector into existing video surveillance deployments. NetApp expects that these professionals can combine the information in this report with their experience and supporting documents to build a simple and cost-effective backup and restore solution.

2 Overview

The following subsections introduce the terminology used in this document, along with assumptions, sizing and performance considerations, and a detailed solution components diagram for backup and restore to and from various cloud targets.

2.1 Terminology

The following terms are used throughout this document, in the SANtricity GUIs, and in the storage and data management industry.

- **Video surveillance server.** A server with video surveillance management software (VMS) installed and a connection to an E-Series storage array.
- **Live video volume.** The volume that is recording live video stream directly from one or more cameras.
- **Archive video volume.** A dedicated volume used by the VMS to store automatically transferred recordings of the oldest video in another location.
- **SANtricity Cloud Connector host.** The Linux host on which SANtricity Cloud Connector is installed.
- **Volume or base volume.** An E-Series volume that is typically mapped to a host system through LUN mapping.
- **Mount point.** A host term that defines a directory within a currently accessible file system on which an additional file system can be logically attached (mounted).
- **I/O quiescing.** The process of stopping all I/O to a volume.
- **Snapshot image.** A logical point-in-time (created at a specific moment) image of the content of a base volume. A NetApp SANtricity Snapshot™ image is not directly read/write accessible to hosts.
- **Snapshot group.** A collection of Snapshot images of a single base volume.
- **Snapshot volume.** A standard volume that allows the host to access the Snapshot image in a Snapshot group.

- **Backup volume or backup base volume.** The volume or base volume selected for a backup.
- **Backup Snapshot image.** A Snapshot image that has been created for use in a SANtricity Cloud Connector based backup.
- **Backup Snapshot volume.** A standard volume that allows the SANtricity Cloud Connector host to access the backup Snapshot image.
- **Backup target.** The storage destination for the backed-up data. This target is either an S3 bucket or an NFS mount point based on the intended destination.
- **Image-based backup.** An image-based backup reads the raw data blocks from a Snapshot volume and backs them up to a file known as an image. All data blocks on the Snapshot volume are backed up, including empty blocks blocks occupied by deleted files, blocks associated with partitioning, and file system metadata. Image backups have the advantage of storing all information from the Snapshot volume regardless of the partitioning scheme or file systems on it.
- **Restore source.** The S3 bucket or NFS mount point from which data is restored.
- **Restore volume or restore base volume.** The volume or base volume selected to receive the restored data.

2.2 Assumptions

This report assumes the following:

- A video surveillance system using NetApp E-Series storage is already set up with dual LUN configuration (live and archive). For details, refer to TR-4825: NetApp E-Series for Video Surveillance Best Practice Guide.
- Familiarity with NetApp E-Series storage management software, especially with the Snapshot feature as described in the embedded online help documentation.
- The NetApp SANtricity Cloud Connector application is installed on a Linux server, as described in TR-4658i: NetApp SANtricity Cloud Connector.

2.3 Sizing Considerations

Video surveillance solutions that use NetApp E-Series with Cloud Connector backups provide both performance and reliability in a tiered storage environment. Cloud Connector also offers additional flexibility in space utilization based on the end customers' needs or requirements.

Retention periods can be expanded by moving older archived data to the cloud. Alternatively, other camera or surveillance options, such as increased frame rates or resolutions, could be optimized on the local array while maintaining the existing retention period with more frequent cloud backups.

Because of the requirement for quiesced I/O to the source volume while a Snapshot copy is being taken of the data, NetApp recommends a tiered storage solution. In a tiered solution the end user can set periodic archiving of a live recording volume to an archive volume. Because live recording volumes are usually under continuous write utilization, they are not good candidates for immediate backup to the cloud. In contrast, the archive volumes have a predictable I/O schedule for when the volume will be idle and available for backup.

When determining the logical sizing requirements for using Cloud Connector in a surveillance solution, the end customer or consultant must also consider the requirements for using image-based cloud backups and the workload of the surveillance solution. NetApp recommends having a single LUN per volume group for archiving that employs the entire capacity of the volume group or disk pool. However, the Cloud Connector image-based solution requires capacity to be reserved for a Snapshot image for each volume being archived that is equal to the source volume size. This requirement effectively halves the typical capacity used for an archive volume on the array. Also, if a restore of the image is required and if the original archive source volume is valid, then the same capacity that was used for the Snapshot copy can be used to create a restore volume.

For more information, refer to TR-4825: NetApp E-Series for Video Surveillance Best Practice Guide.

2.4 Performance Considerations

When considering the performance of a backup or restore, keep the following points in mind.

- **The bandwidth of the network connection to the backup target itself.** A typical business may have 100Mb or 1GbE connections for its internal network. However, connecting to an external backup target (such as Amazon S3) over consumer-grade internet service provides only a fraction of the internal network speed. Depending on cost and customer location, faster internet speeds might not be possible. This situation affects both backup and restore operations.
- **Bandwidth limits imposed by the backup target service.** Services such as Amazon S3 can offer different levels of service based on connection speeds. This situation affects both backup and restore operations.

  Note: SANtricity Cloud Connector uses multiple connections to the backup target to increase the performance of a backup operation. Again, this performance can be limited by bandwidth.

- **SANtricity Cloud Connector uses the underlying E-Series array's Snapshot feature.** NetApp recommends scheduling backup during the storage array's lowest overall I/O processing window to minimize the performance overhead.

2.5 Solution Components

Figure 1 is a high-level configuration diagram using NetApp Cloud Connector with a video surveillance solution. The components include:

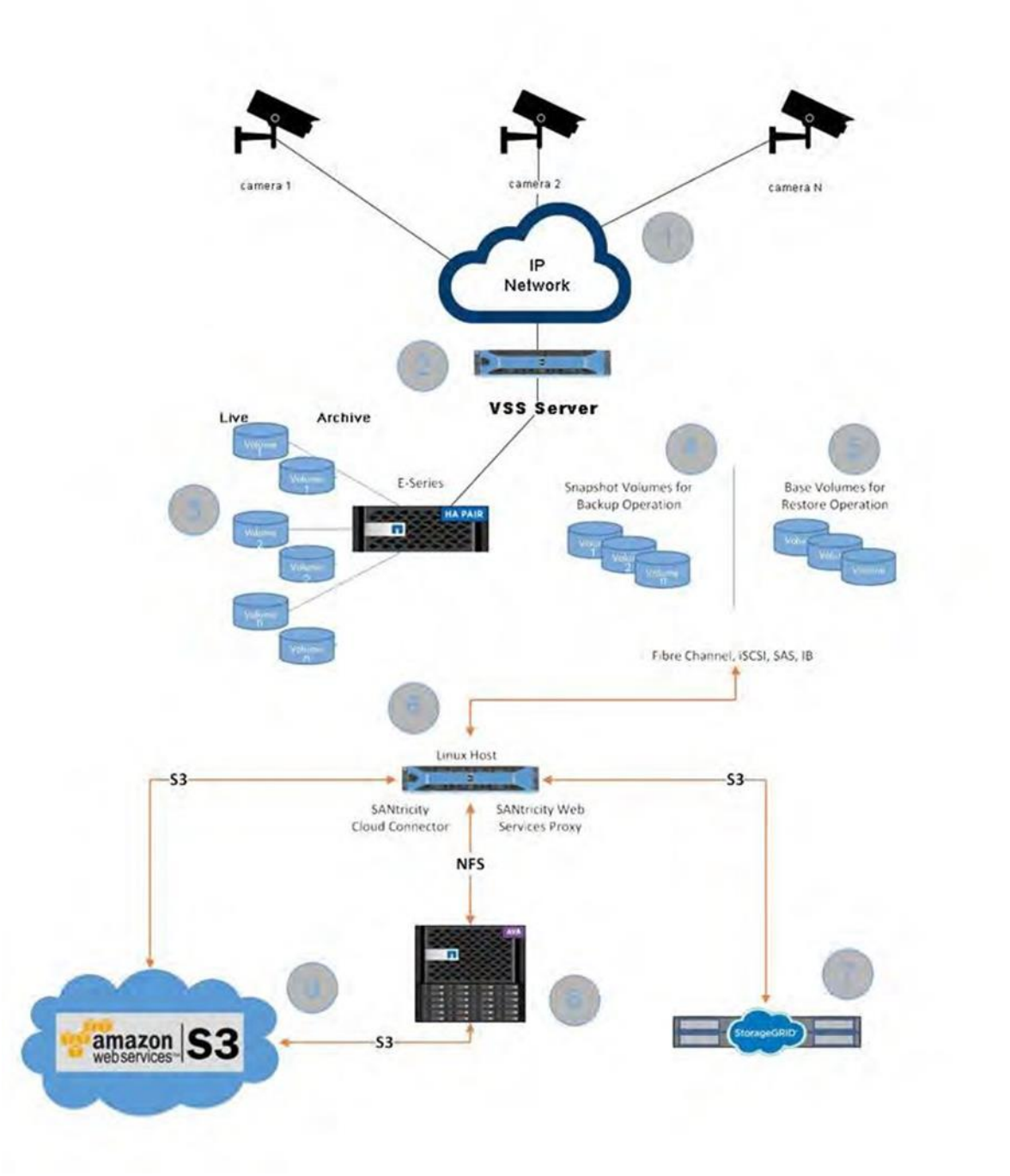
- IP video cameras attached to the VSS server.
- VSS server attached to E-Series storage arrays (commonly via FC, iSCSI).
- Live and archive video volumes on an E-Series array that are used by the VSS server.
- Snapshot volumes for the backup operation. Before Snapshot volumes can be created from the base volumes, any application that uses the base volumes must be quiesced, either manually or scheduled, to ensure data consistency. Snapshot volumes (copy on write) can then be created from the base volumes of the E-Series array and manually mapped to the Cloud Connector server via host interconnect.
- Base volumes for the restore operation. During a restore operation, base volumes are mapped to the Cloud Connector server via host interconnect. The restore data files are read from the restore source to reconstruct the restore volume.
- SANtricity Cloud Connector. A host-based Linux application that is used to back up and restore E-Series volumes. All backup and restore jobs use RESTful API calls to the application. Backup operations consist of reading data from the Snapshot volumes and copying the data to one of the following destinations:
  - Cloud Backup, via NFS mount, which can then be transferred to Amazon Web Services (AWS) via HTTPS and S3 protocols
  - AWS, via HTTPS and S3 protocols
  - StorageGRID, via HTTPS and S3 protocols

  Note: The restore operation consists of reading the data from the restore source and reconstructing the data to the restore volumes.

NetApp SANtricity Web Services Proxy. Used by SANtricity Cloud Connector to communicate with the E-Series array.

- StorageGRID solution.
- Cloud Backup virtual or physical appliance.
- Bucket for AWS cloud account.

Figure 1) Solution components.



3 Backup and Restore Workflow Example

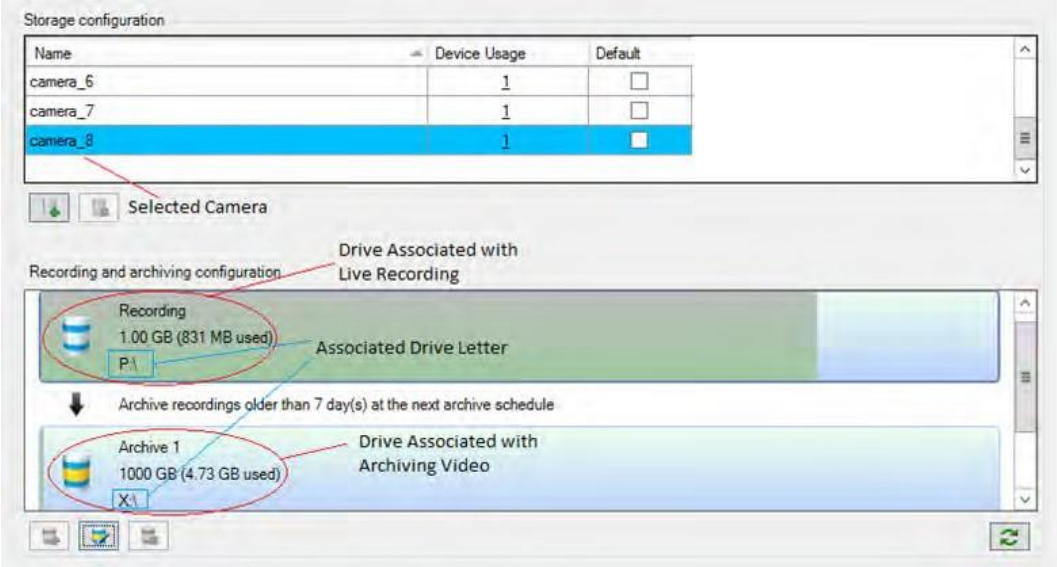
The following example uses Sony SNC Camera Emulator, Milestone XProtect as the video surveillance management software, and NetApp SANtricity Cloud Connector 3 software.

3.1 Backup

The following step-by-step procedure backs up a video archive mount point:

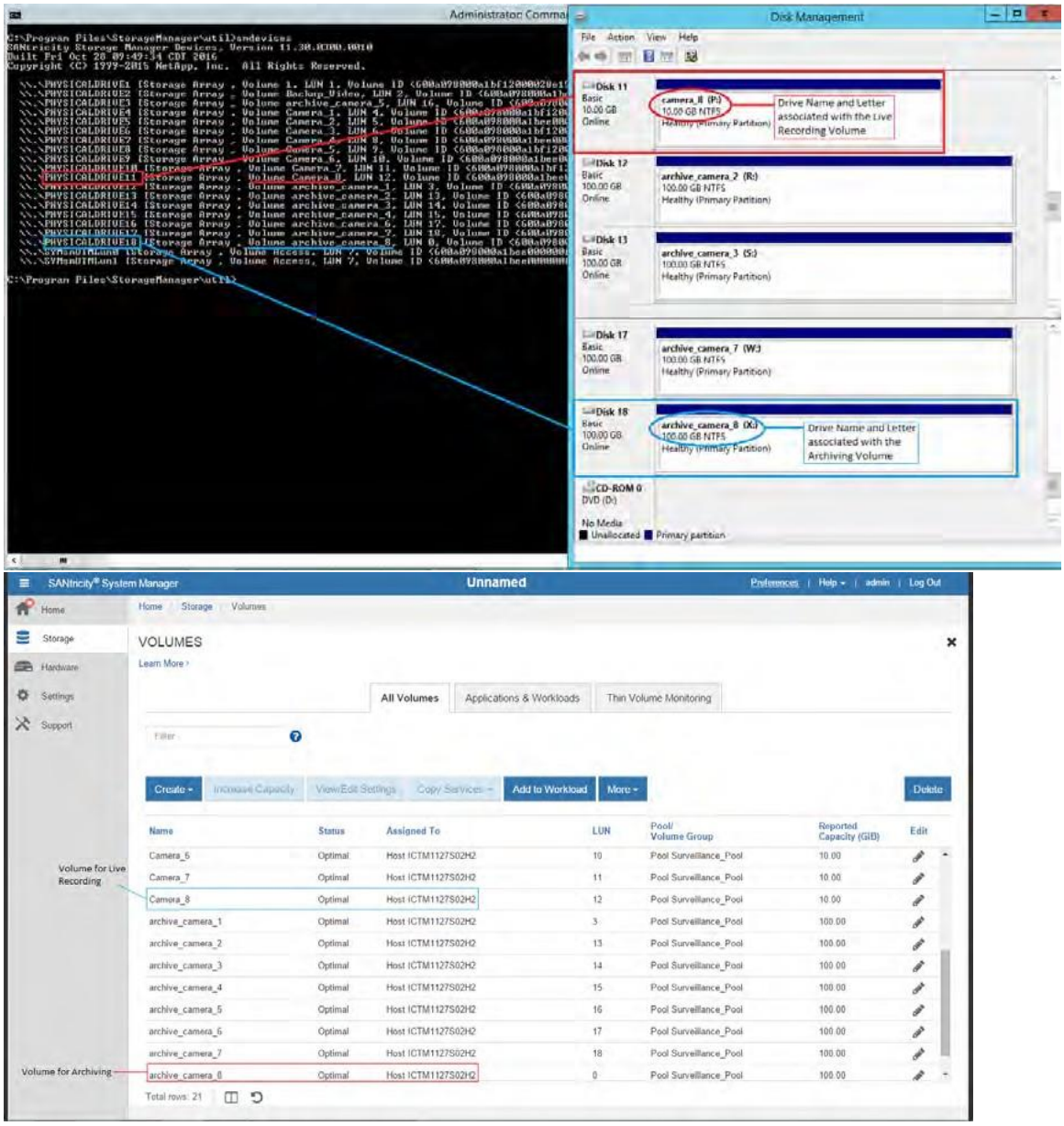
1. In the video surveillance software, locate the associated volume records for the backup by using the archive mount point, as shown in the following screenshot.

   Note: Do not use a live recording mount point for backup



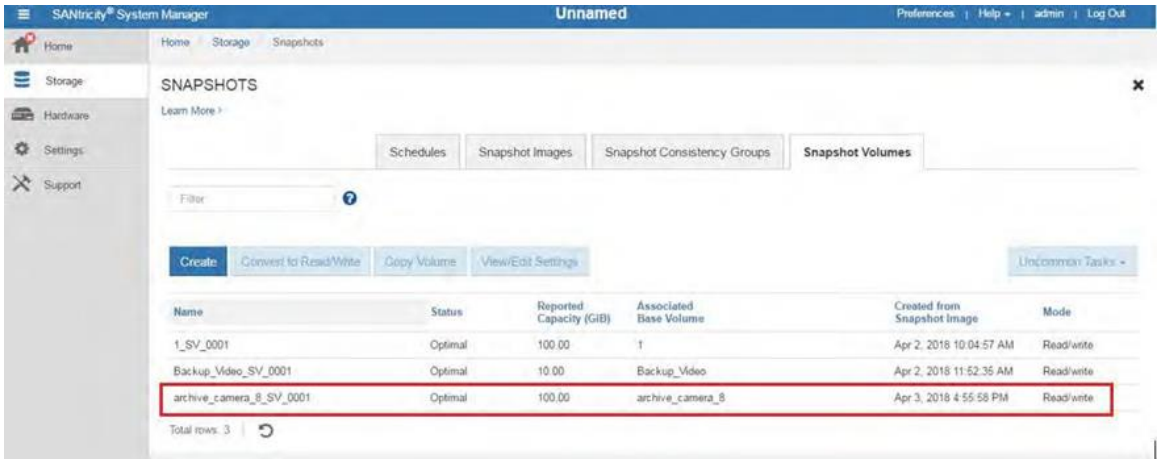
.

2. Locate the LUN associated with the video archive mount point under the disk manager, as well as the Storage Array Manager software, as shown in the following screenshots.

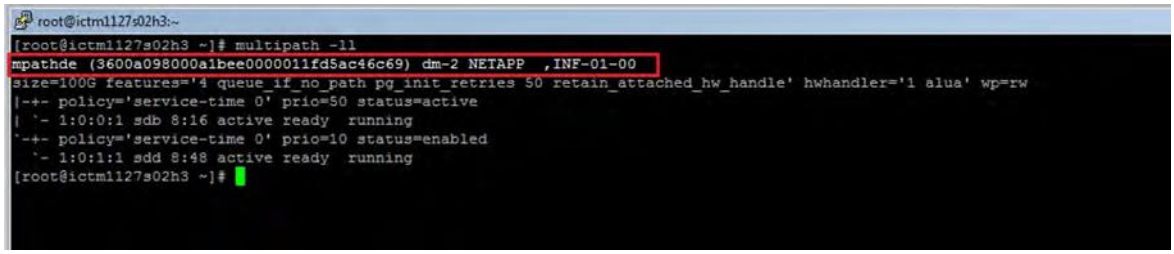


Note: Before proceeding to the next steps, make sure that all I/O to the archive volume are quiesced.

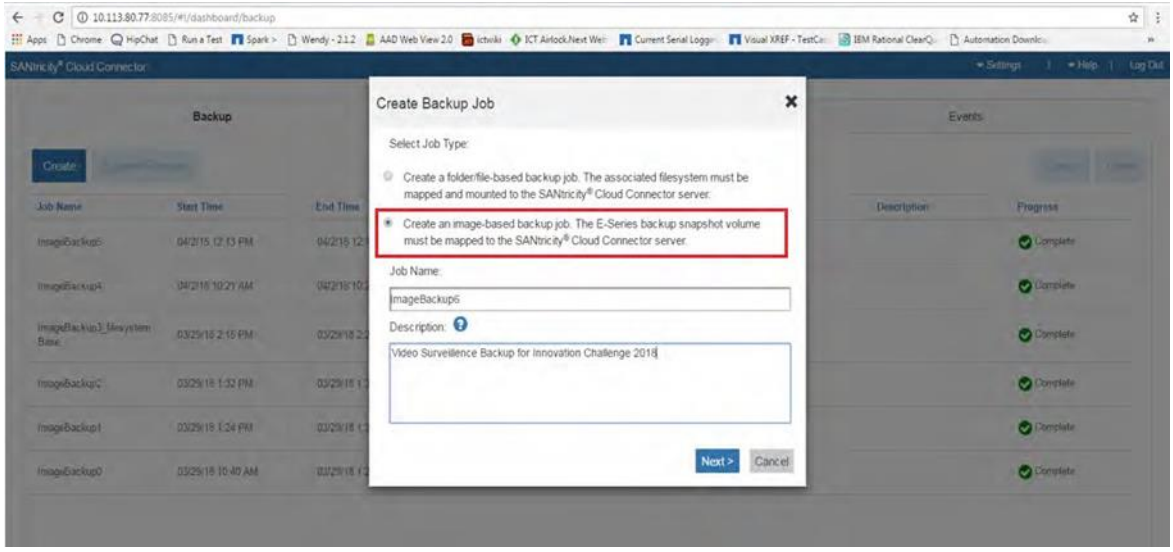
3. In the SANtricity System Manager, create a Snapshot volume of the archive volume by first creating the Snapshot image and the Snapshot volume. The following screenshot shows the resulting Snapshot volume archive_camera_8_SV_0001.

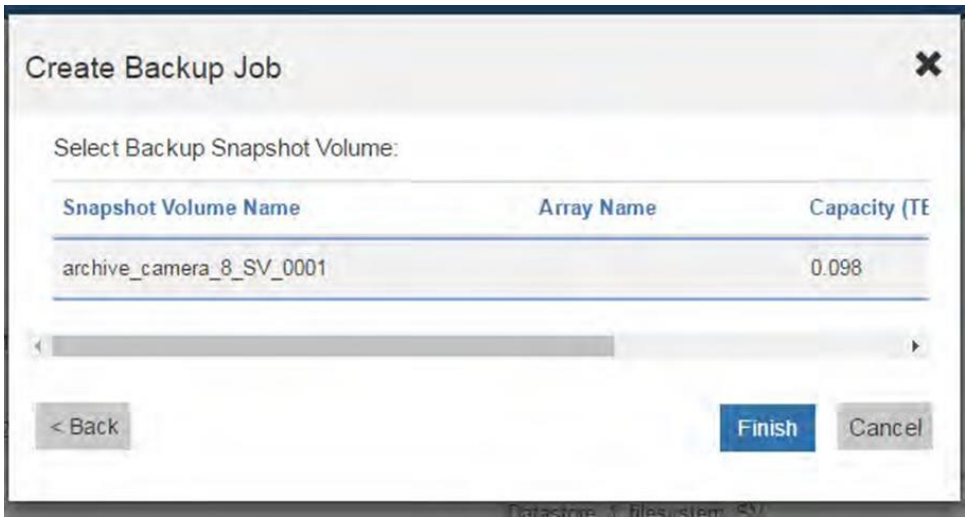


4. Map the Snapshot volume to the Cloud Connector server and verify that the server can see the mapped volume, as shown in the following screenshots.

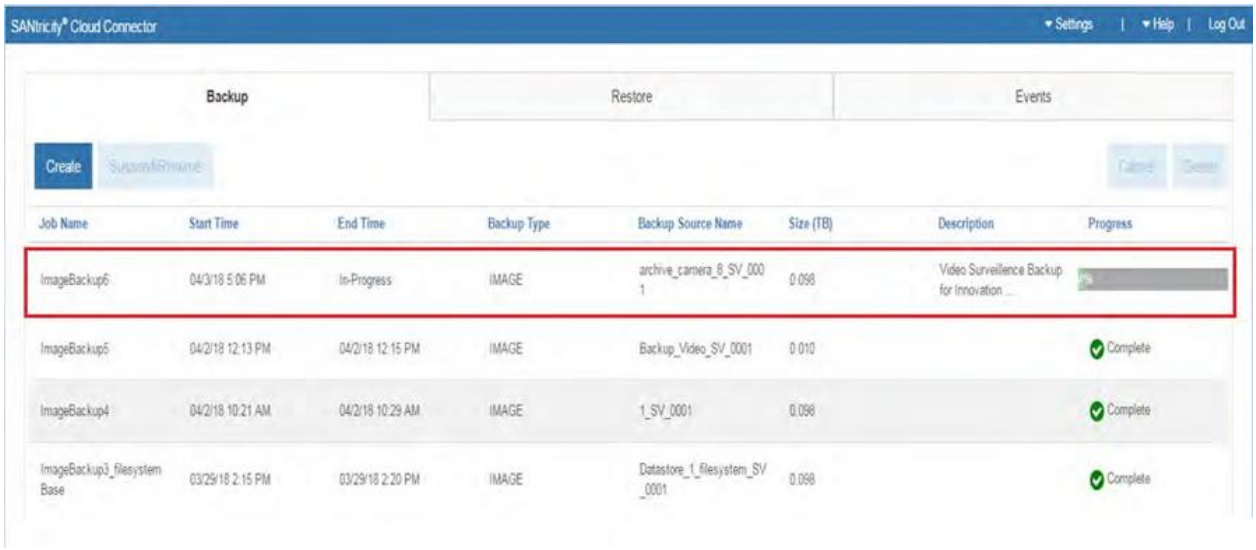


5. From the Cloud Connector management software, initiate an image-based backup job for the Snapshot volume to upload data to the cloud, as shown in the following screenshots.





6. Monitor the progress of the backup job to completion.



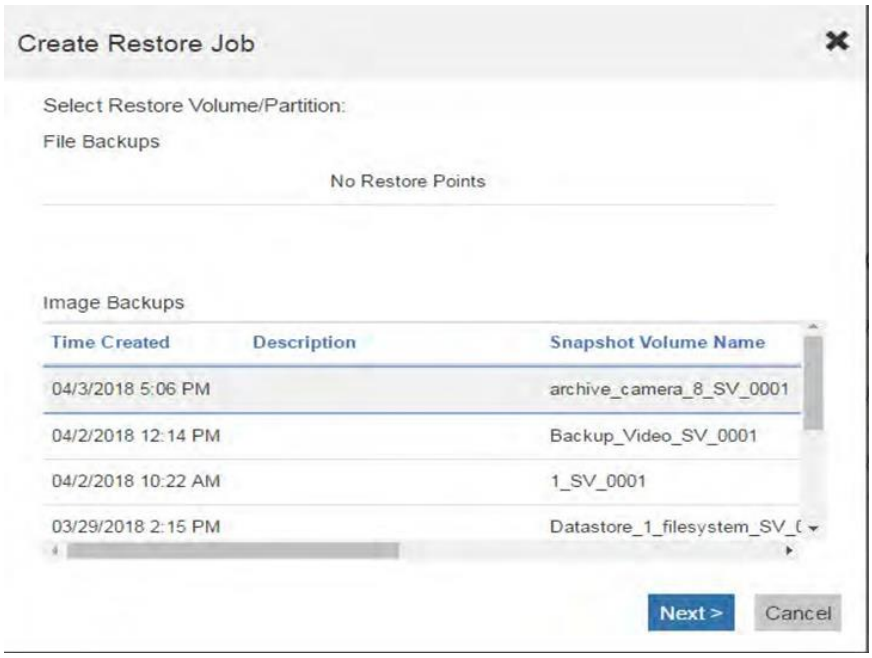
Note: Steps 3 through 6 can be repeated to accomplish incremental backups.

3.2 Restore

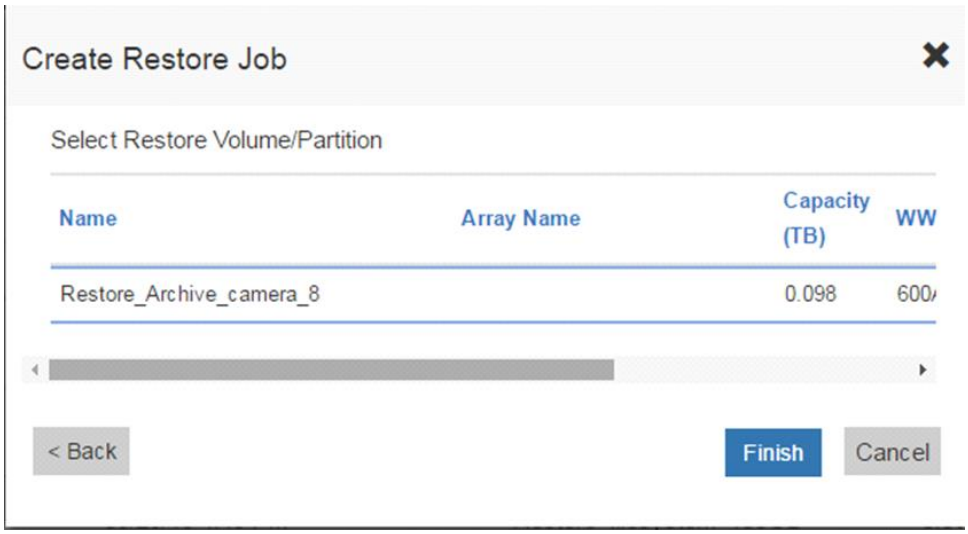
The following step-by-step procedure restores and reviews a video archive backup:

Note: Make sure that a volume has been created on the storage array to receive the data from the restore process. This volume must be equal to or greater than the size of the archive volume. In the following steps, it is labeled Restore_Archive_camera8.

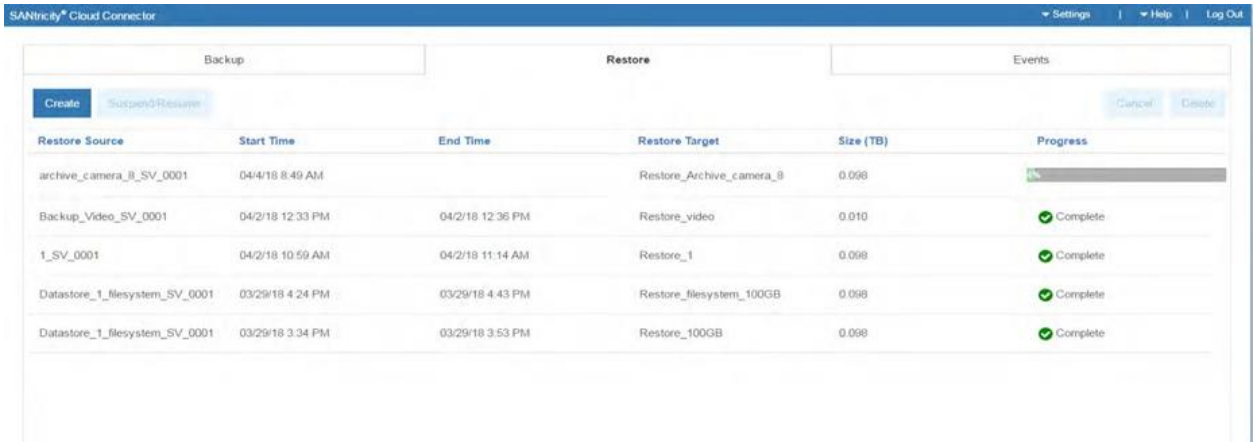
1. From the Cloud Connector management software, create a restore job from a specified backup; in this case, the volume archive_camera_8_SV_0001.



2. Select the volume on the array to receive the data from the cloud.

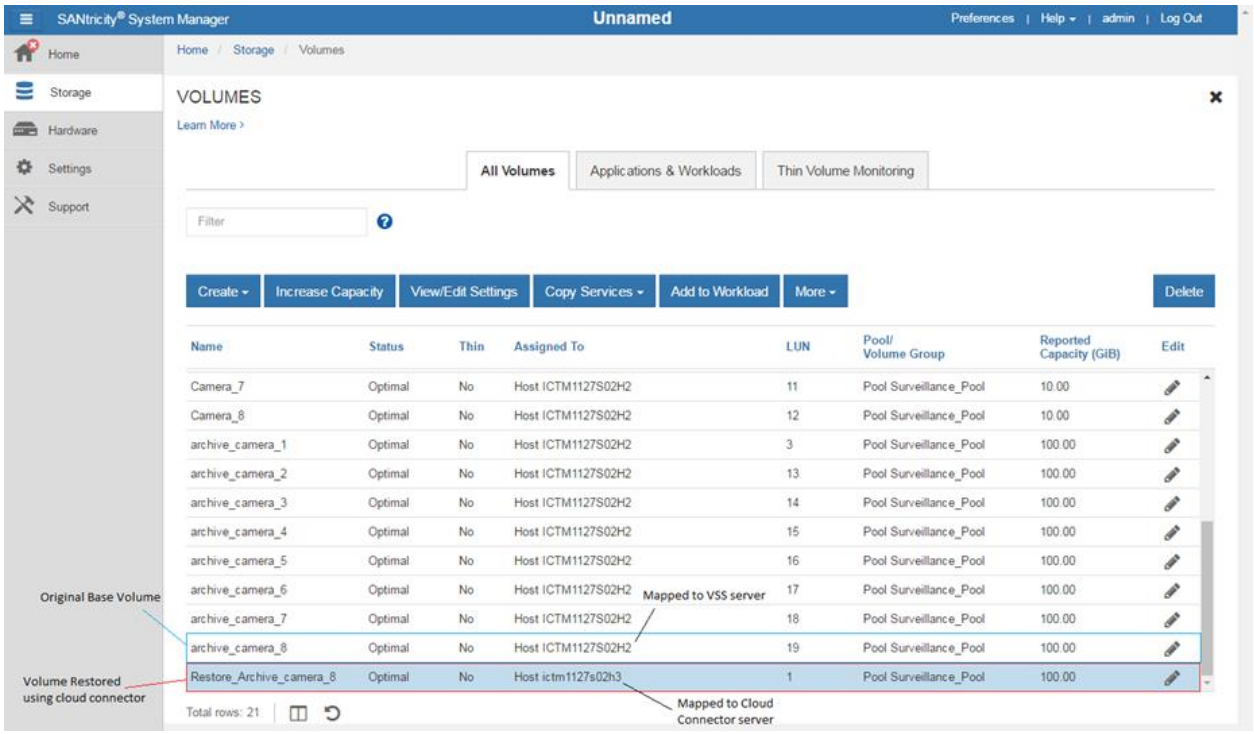


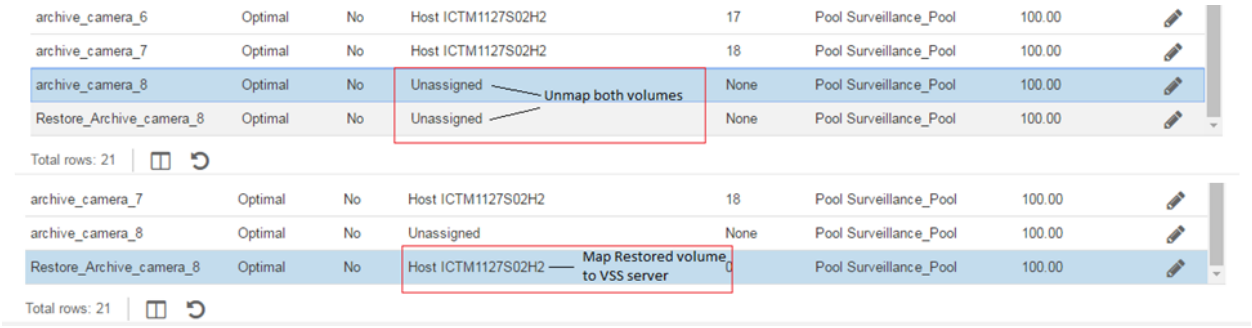
3. Monitor the progress of the restore job to completion.



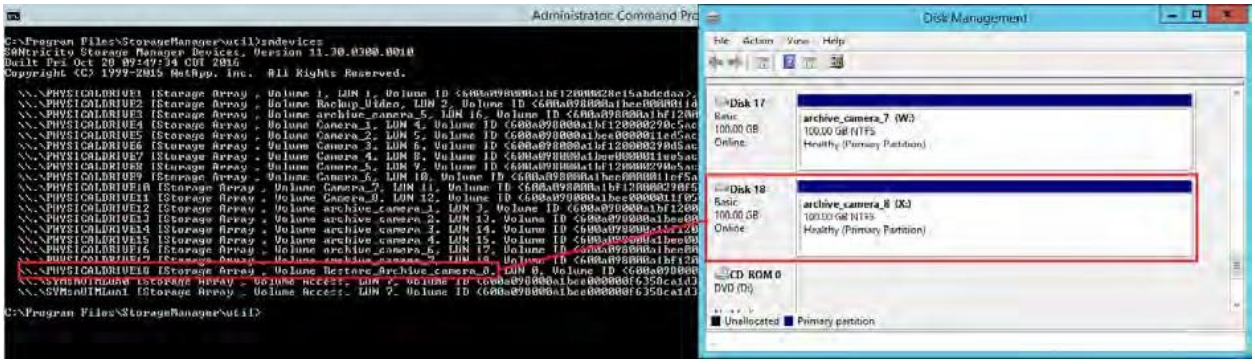
4. Change the host mapping of the restore volume from the Cloud Connector host to the VSS server, as shown in the following screenshots.

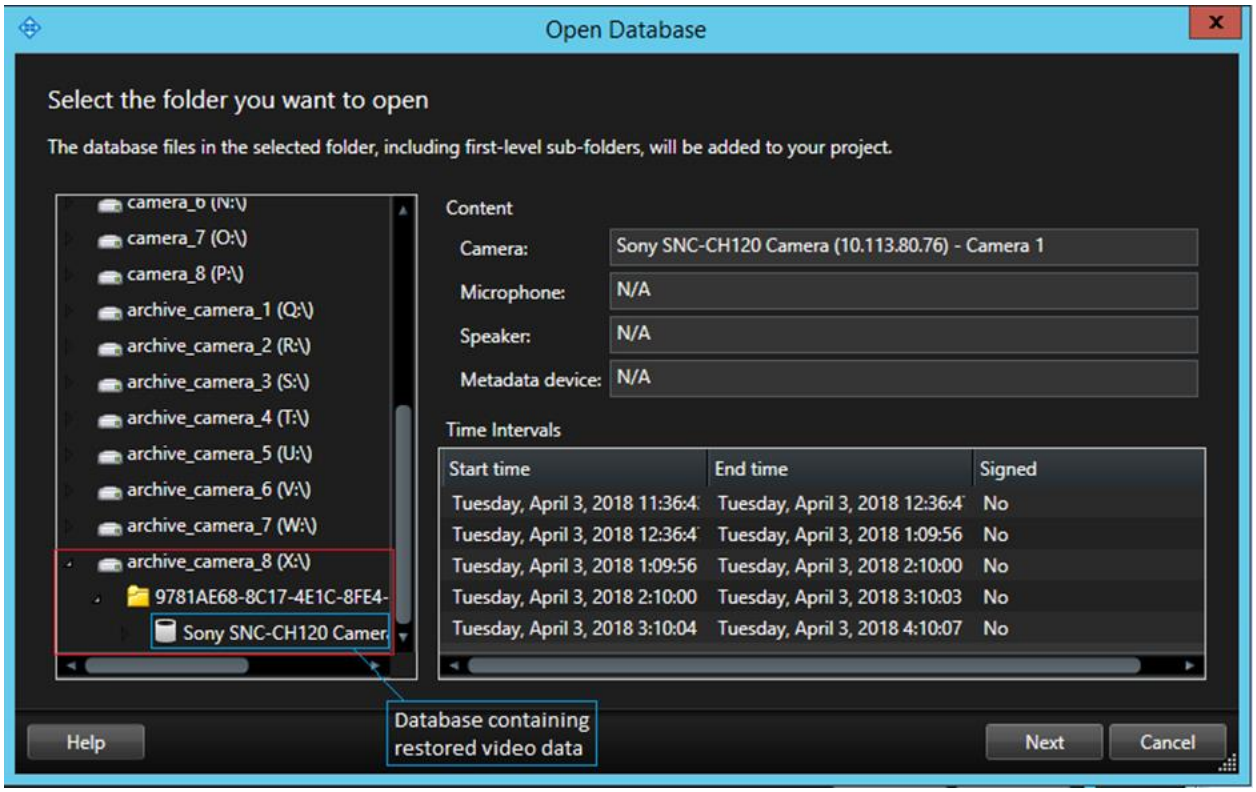
   Note: If the source archive volume is still operational, to avoid disk conflicts it may be necessary to discontinue archiving and remove the mapping from the video server before bringing the restored data online. This is because the volume image restore process creates an exact block-by-block copy of the volume.





5. Add the restore volume to the video surveillance software and return it to archiving.





4 Summary

NetApp SANtricity Cloud Connector offers a simple and cost-effective option to perform backup and restore jobs to an existing Amazon S3, StorageGRID, or Cloud Backupaccount for video surveillance solution customers.

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- TR-4825: NetApp E-Series for Video Surveillance Best Practice Guide
  https://www.netapp.com/us/media/tr-4825.pdf
- TR-4658: NetApp SANtricity Cloud Connector
  https://www.netapp.com/us/media/tr-4658.pdf

Version History

Version	Date	Document Version History
Version 1.0	June 2018	Draft
Version 1.1	April 2020	Added references to NetApp E-Series for Video Surveillance Best Practice Guide throughout the document.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

TR-4703-0520