Technical White Paper

Dell EMC Unity: Cloud Tiering Appliance (CTA)

A Detailed Review

Abstract

This white paper describes the Dell EMC Cloud Tiering Appliance (CTA) and how it can be used with Dell EMC Unity systems. CTA allows administrators to move block and file data from a Dell EMC Unity storage system to and from the cloud. CTA also facilitates cloud repository migration, stub aware file migration, and the usage of Dell EMC Unity as a destination repository.

June 2021

Revisions

Date	Description
July 2017	CTA12.0 release
November 2017	CTA12.0 SP1 release
March 2019	CTA12.1 release
June 2020	CTA13.0 release and new template
June 2021	CTA13.1 release

Acknowledgements

Author: Kenneth Avilés Padilla

Table of contents

Executive summary

The Dell EMC Cloud Tiering Appliance (CTA) enables administrators to automatically move data from Dell EMC Unity to and from the cloud based on user-configured policies. This ability optimizes primary storage usage, dramatically improves storage efficiency, shortens the time required to back up data, and reduces overall Total Cost of Ownership (TCO) for primary storage.

Figure 1 shows a graphical representation of CTA actions for the Dell EMC Unity. CTA can be used to tier file data and archive block data to the cloud, as shown by the *Tiering/Archiving* diagram in Figure 1. Likewise, CTA can be used to recall file data and restore block data from cloud, as pictured in the *Retrieval* diagram in Figure 1. Lastly, CTA can be used to migrate repositories between clouds, as shown in the *Repository Migration* diagram in Figure 1. Figure 21 in the File Migration section provides a graphical representation for the File migration feature.

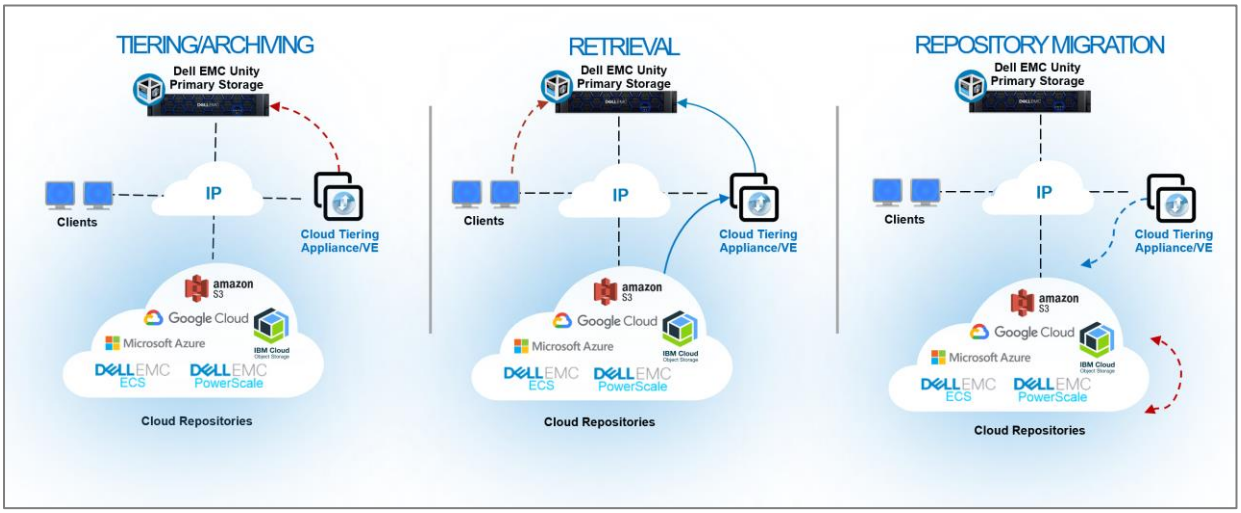

Figure 1 CTA in Action.

Audience

This white paper is intended for Dell EMC customers, partners, and employees who are considering the use of Cloud Tiering Appliance (CTA) for the Dell EMC Unity family of storage systems. It assumes familiarity with Dell EMC Unity, Dell EMC's management software and Cloud Tiering Appliance (CTA).

Scope

This white paper describes the following CTA features for Dell EMC Unity:

- File tiering
- File migration
- Block archiving

For file tiering, CTA acts as a policy engine by interacting with the Dell EMC Unity storage system and identifying files that fit some administrator-defined criteria. For these files, CTA initiates movement to a target cloud repository and places a stub file in the original file location. When a client reads the stub, CTA recalls or passes the IO through the original file located in the cloud. To the user, the file appears to be in its original location on the Dell EMC Unity storage system. The stub utilizes only KBs of space, instead of the full size of the file. This solution makes file tiering seamless for the user who reads the archived file data.

For block archiving, CTA acts as a policy engine by interacting with the Dell EMC Unity storage system and identifying block snapshots that fit some administrator-defined criteria. For these snapshots, CTA initiates a backup to a target cloud repository and leaves the original snapshot untouched. After the snapshots are backed up to the cloud, they can be erased from the source system to free space. The user has the option to restore a snapshot to a new block storage resource located in the source system or in a new storage system. Block archiving is available only for Dell EMC Unity storage systems.

For file tiering and block archiving, the supported target cloud repositories are Dell EMC Elastic Cloud Storage (ECS), Dell EMC PowerScale S3, Microsoft Azure, Google Cloud Platform (GCP), Amazon S3, and IBM Cloud Object Storage (COS). CTA is supported with other storage platforms and has additional functionalities that are not applicable to Dell EMC Unity, for which reason, these functionalities are not discussed in this white paper. For a more in-depth look at CTA's functionalities, refer to the *Cloud Tiering Appliance User Guide* found on Dell Support.

For file migration, CTA acts as a policy engine by interacting with the source VNX storage system and the target Dell EMC Unity storage system. Refer to the latest *CTA Interoperability Matrix* on Dell Support for supported VNX versions. CTA identifies files in the source system that fit some administrator-defined criteria and moves them from the source system to the target system. For source files that had been tiered to a cloud repository, the movement is stub aware, meaning that it maintains the stubs without recalling the files to the target.

Terminology

Amazon S3 – Amazon Simple Storage Service (Amazon S3) is an object storage cloud platform from Amazon.

Block archiving – A primary CTA function that scans the block snapshots that meet administrator-defined criteria and takes a backup of the block resource to the cloud.

DHSM (Distributed Hierarchical Storage Management) – An API on the Dell EMC Unity storage system that enables the file stubbing and recall of archived files.

ECS – Elastic Cloud Storage (ECS) is an object storage platform from Dell EMC.

CTA-HA – Recommended CTA software that is used to configure encryption and ensure recalling of files when the primary CTA is not available.

File tiering – A primary CTA function that scans a file system for files that meet some administrator-defined criteria and moves them to the cloud. CTA replaces the file on the file system with a stub file that points to the full-size file in the cloud repository.

File migration – The movement of files from a source location to a destination target.

FileMover – A service on the Data Mover that provides an API that CTA uses for file tiering and file migration on the VNX.

IBM COS – IBM Cloud Object Storage (COS) is an object storage platform from IBM. It might also be known as Cleversafe.

LUN – A block-based storage resource that a user provision. It represents a SCSI logical unit.

NDMP (Network Data Management Protocol) – An open standard network protocol that is designed for enterprise-wide backup and recovery of heterogeneous network-attached storage.

Orphan file – A file in a repository that does not have a stub file pointing to it. When a file is archived, a stub on the source NAS server points to the archived file. Deleting a stub does not automatically delete the archived file. Instead, the archived file becomes an orphan. To delete orphans, run an orphan delete job on the repository.

Policy – A combination of rule(s) and repositories for tiering and archiving. A policy might contain rules, for example, that would send files that have not been accessed in two years or files older than 3 weeks to a public cloud Amazon S3 repository.

Recall – When a file has been tiered to a repository, and for example, the user clicks the stub file to quickly access the original file.

Repository – The target cloud location for the tiered file data and archived block data.

Restore – A method of transferring archived block data to a new storage resource.

Snapshot – A point-in-time view of a storage resource. When a snapshot is taken, the snapshot is an exact copy of the source storage resource and shares all blocks of data with it. As data changes on the source, new blocks are allocated, and data is written to them.

Storage resource – The top-level object that a user can provision and associated with a specific quantity of storage. All host access and data protection activities are performed at this level. In this document, storage resource refers specifically to those resources that support file tiering (NAS Servers and file systems) and block archiving (LUNs and Consistency Groups).

Stub – A file, that ranges from 8-16KBs, that replaces the original file on the Dell EMC Unity file system. The stub file contains all the metadata associated with the archived file that is required for accessing the archived data on the cloud repository.

Thin Clone – A read/write copy of a thin block storage resource (LUN, Consistency Group, or VMware VMFS Datastore) that shares blocks with the parent resource. Thin Clones can have Snapshot Schedules assigned to them and can be replicated.

Unisphere – A web-based graphical user interface for managing the Dell EMC Unity storage system.

1 Cloud Tiering Appliance Overview

1.1 Introduction

CTA can help customers achieve many benefits, which include reducing capital expenses by reclaiming capacity on primary storage, lowering operating expenses by reducing the number of administrative tasks, and improving performance by reducing backup times. Figure 2 shows that by leveraging CTA to move data to the cloud, there is less data to be back up than without CTA.

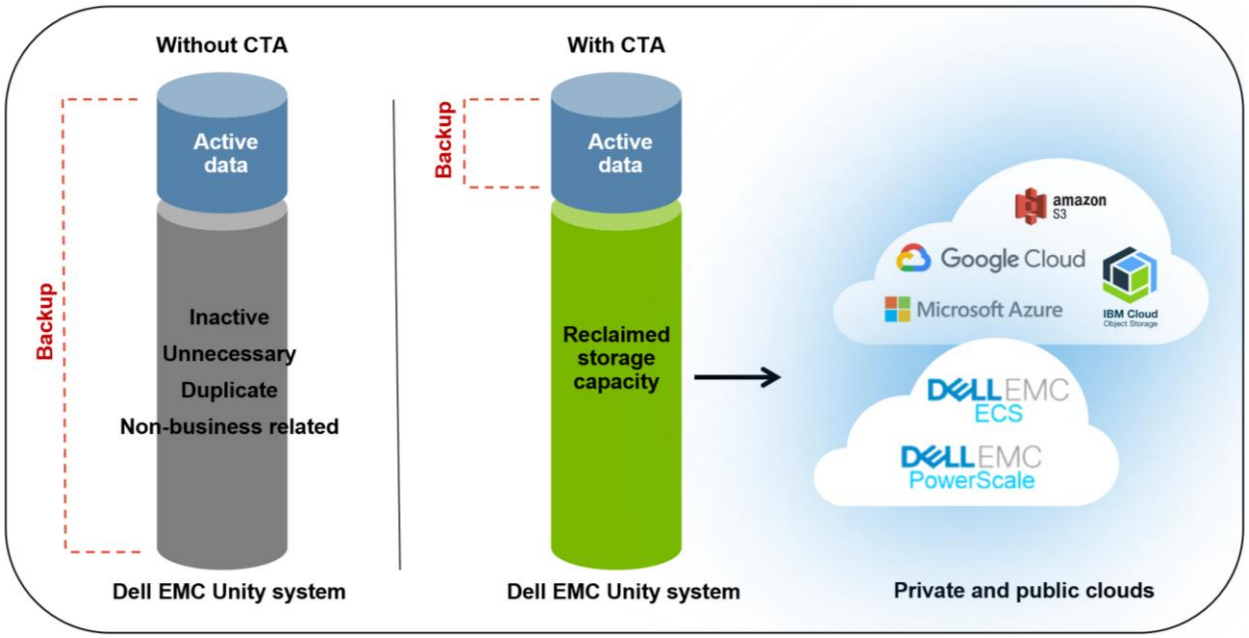

Figure 2 Reduced backup window with CTA.

The three primary CTA functions that we will discuss are file tiering, file migration, and block archiving. File tiering moves file data to the cloud and leaves behind a stub file. In this whitepaper, file tiering describes the functionality of leaving a stub in place of the original file, but in other documentation tiering and archiving might be used interchangeably. In this whitepaper, archiving describes block snapshot archiving, which is the method of taking a backup of block data to the cloud. File migration is the action of moving files from a source array to Dell EMC Unity. This paper also discusses some additional aspects that should be considered to successfully configure CTA with a Dell EMC Unity storage system. In addition to archiving to the cloud, a Dell EMC Unity system can be used as the archiving destination for the VNX and NetApp storage systems. However, Dell EMC Unity does not support tiering to other Dell EMC storage systems or SMB/NFS shares.

The following sections give an overview of some of the CTA functionalities and components that apply to file tiering, file migration, and block archiving.

1.2 Licensing

CTA is supported on all Dell EMC Unity systems and is included at no additional cost. See the *Compatibility* section for the minimum Dell EMC Unity OE requirements. The supported systems include the All Flash models, the Hybrid models, and the Dell EMC UnityVSA Professional Editions.

1.3 CTA configuration

Cloud Tiering Appliance (CTA) is available as a software defined solution with the Cloud Tiering Appliance/Virtual Edition (CTA/VE). CTA/VE is deployed as a Virtual Machine on top of an ESXi host. The *Installing the virtual edition* section in the *Cloud Tiering Appliance User Guide* provides the steps on how to install the CTA/VE on an ESXi host. See the latest *CTA Interoperability Matrix* on Dell Support for the supported ESXi versions and hardware requirements.

To use CTA with Dell EMC Unity, you must complete some configuration steps on the CTA. The *Deploying CTA with Dell EMC Unity* section in the *Cloud Tiering Appliance User Guide*, provides the full procedure to setup the CTA with the Dell EMC Unity storage system.

1.3.1 CTA13.0 Updates

The CTA13.0 version adds support for a new HTML5 based Graphic User Interface (GUI), Figure 3, with support for REST API. Additionally, version CTA 13.0 added support for SMB 3.0.2 along with SMB 2.1 which includes SMB auto-negotiate, signing, Kerberos and NTLM authentication, and performance improvements for large files by optimizing the read/write length to 512KB.

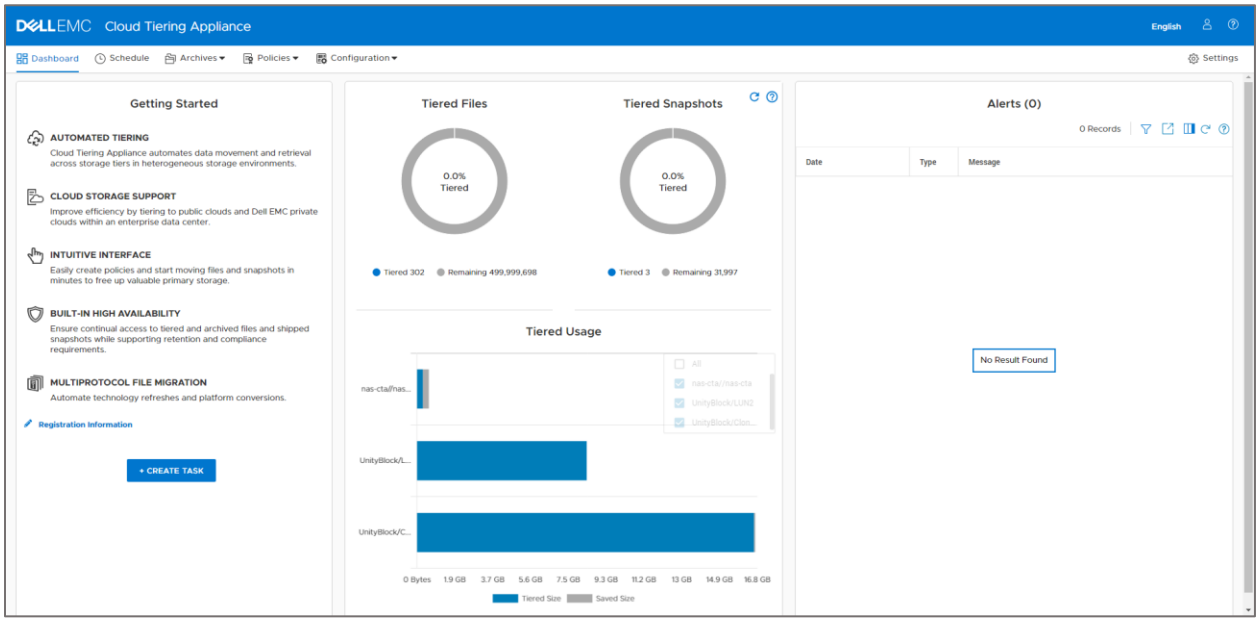

Figure 3 CTA. Dashboard page.

The CTA version software scheme breaks the version number into either four or five separate fields, depending on major version. Fields are separated by a period. In versions up to CTA12.1, there are four fields (ex: 12.0.0.65). From left to right, the first field indicates the major release number, the second indicates the minor release number, the third indicates the service release number, and the fourth field indicates the build number.

In CTA 13.0 and later, the number scheme to track different versions has been changed, making it easier to identify a certain build. The version number is now broken into five fields, each field is defined below, including example build 13.0.0.0.14:

Table 1 Software Version Numbering Schema

Field #	1	2	3	4	5
Value	Major release number	Minor release Number	Service release number	Release type	Build number
Example	13	0	0	0	14

The primary change is the addition of a release type field. The release type will be 0 for any customer deliverable branch, and some value 1 through 5 for internal domain or development builds. The distribution type represents four different distribution possibilities, defined below:

- 0 = General availability
- 1 = Beta
- 2 = Patch
- 3 = Hotfix
- 4 = Internal
- 5 = Debug

1.3.2 CTA13.1 Updates

The CTA13.1 version adds support for public cloud Google Cloud Provider (GCP), private cloud Dell EMC PowerScale S3, and NFSv4 (the user can pick between NFSv3 or NFSv4). It also includes a new GUI tour when first opening the CTA GUI.

1.3.3 CTA/VE for High Availability (CTA/VE-HA)

CTA includes a High Availability (HA) option for file recalling purposes through the deployment of a CTA/VE-HA. CTA/VE-HA will be referenced throughout this whitepaper as CTA-HA for simplicity. CTA-HA is a light-weight Virtual Machine (VM) that is deployed on top of an ESXi host. Figure 4 provides a high-level diagram depicting the differences between the primary CTA and CTA-HA.

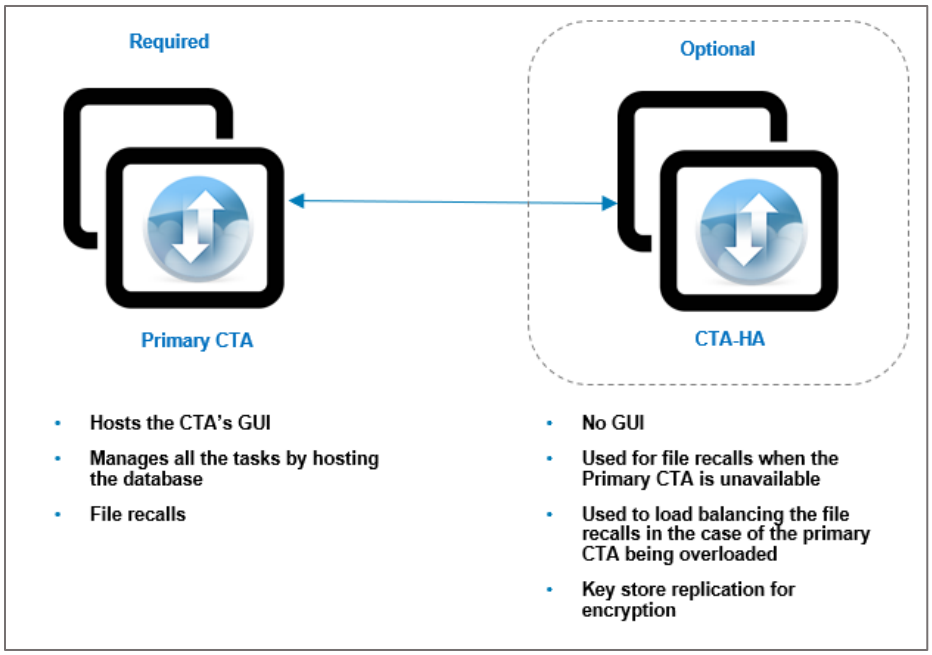

Figure 4 CTA with CTA-HA.

Note that the primary CTA is the component that hosts the GUI and database for all the tasks and management actions. While the CTA-HA does not have any GUI for management or actions by the user. The CTA-HA can be used to provide redundancy to ensure that clients can always access their file data in case the primary appliance fails. For more details regarding file recalls and CTA-HA, see the *Recall using CTA-HA* sub-section under the *CTA for File* section. CTA-HA also performs key store replication for encryption keys, which are required when the encryption feature is enabled during tiering and archiving to cloud platforms. Without CTA-HA, encryption will not work because the key generator cannot generate keys without the key replication daemon.

Refer to the *High availability with VNX or Unity primary storage* and *File Encryption* sections in the *Cloud Tiering Appliance User Guide* for full details to deploy and configure CTA-HA and encryption. The Cloud Tiering Appliance User Guide is available on Dell Support.

1.4 Cloud repositories

The supported target cloud repositories from a Dell EMC Unity array include:

- Public clouds
  - Microsoft Azure
  - Amazon S3
  - IBM Cloud Object Storage (COS)
  - Google Cloud Platform (GCP)
- Private clouds
  - Dell EMC Elastic Cloud Storage (ECS) S3 and CAS
  - Dell EMC PowerScale S3

1.4.1 Cloud Repository Migration

CTA also supports the repository migration of one supported cloud to another supported cloud. The repository can be migrated when the repository is being used for file tiering. Repository migration moves all tiered files

from one repository to another. After repository migration, the original repository can be removed. As part of the repository migration, the stubs on the Dell EMC Unity primary storage system will be updated to point to the archived files on the new repository.

Repository migration with cloud storage retains the same encryption key when moving data. However, if an encrypted data that was tiered without compression is migrated to cloud storage with compression, the destination data will be re-encrypted with the most recent encryption key.

Repository migrations are useful when you need to replace the cloud platform. The cloud target must have enough space to hold the data that is being moved, but the space does not need to be the same size or have the same layout as the source. Refer to the *Cloud Tiering Appliance User Guide* for more details on how to configure CTA for repository migration.

1.5 Scheduler

The CTA's jobs and tasks can be run based on a schedule with the CTA's scheduler. The CTA scheduler sets the task start time. For example, you can schedule an archive task to start at 2 a.m. on Saturday to scan share01 and evaluate the files with a policy for tiering to the cloud. You can also do capacity-based scheduling for file tiering.

Administrators usually schedule a task to run on a regular cadence: weekly, every other week, or monthly. The first archive task often tiers the most data and can require a substantial amount of time. Subsequent jobs move incremental amounts of data, so they will run faster.

1.6 Policy

You can use CTA to define a task to perform a series of actions, for example:

- Move any files that are larger than 10MB and have not been accessed in 30 days to the cloud
- Move any block snapshots that are more than 60 days old to the cloud

A policy is a set of one or more user-created rules. For each rule, you can associate an action, that being an archive, recall, or restore action with the rule. When a policy is applied to a storage resource in CTA, the rules are applied to each share or snapshot under the storage resource. If a file or snapshot falls within the rule, the action is taken. The sections for file tiering and block archiving functions provide more details about rules and actions that apply to each one.

1.7 Simulation

You can schedule a task with a policy, and then run the task as a simulation. As a simulation, CTA scans the source shares, and applies the policy rules against each one, but CTA does not perform any tiering action. Instead, CTA tracks the number of files and amount of data it would have tiered. You can view a report at the end of the simulation by navigating to the History (Simulation) option for a task. It is recommended that before running a task, it should be run as a simulation. Simulation is an efficient way to test the policy's effectiveness and to edit the policy rules before you run a real job.

1.8 Compression and encryption

When tiering and archiving data to a cloud repository, you can use CTA encryption and compression options.

1.8.1 Compression

The compression option is available when you create a policy to tier or archive to cloud repositories. If you select compression, it can be configured as either fast or strong. If you select the fast option, the compression process is fast, but the compressed data is not as small. If you select strong, the compressed data is smaller, but the compression process is slower. Figure 5 shows the **Tiered Usage** chart in the CTA's Dashboard page, noticed that it shows the number of files that are tiered, the logical size, the tiered size, and how much size was saved by tiering the data including the percent saved. Compressed data in Dell EMC Unity will be uncompressed in memory and sent to the cloud repository. It is recommended to leverage the CTA's compression to ensure that the space in the cloud repository is used efficiently. CTA uses the zlib library as its data compression algorithm.

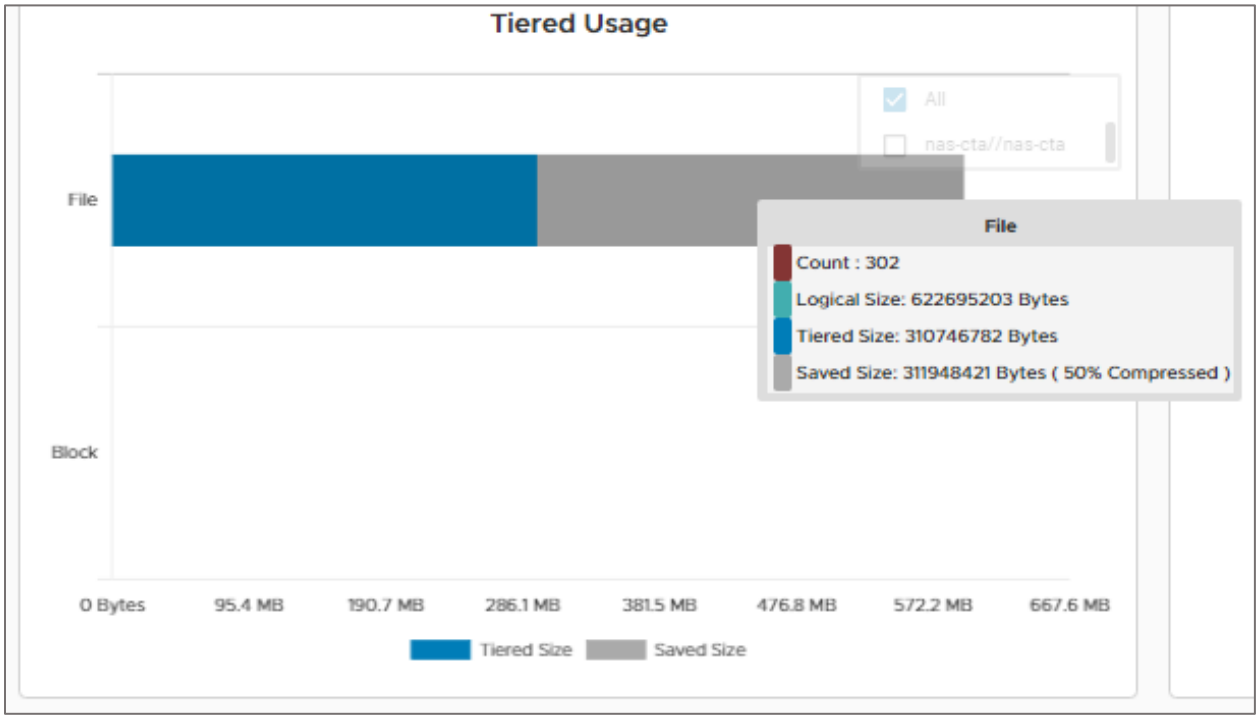

Figure 5 CTA. Dashboard. Tiered Usage.

1.8.2 Encryption

When moving data to a cloud repository, you can also use CTA encryption option. Encryption requires that you deploy and configure the CTA-HA. The encryption option is available when you create a policy to tier or archive to cloud repositories. CTA uses AES 256 in CTR mode as its encryption algorithm.

CTA stores the key in the keystore and replicates it to the CTA-HA. Every task that uses a policy with encryption enabled, uses the key. If a new key is generated, it will be used by any new tasks that use encryption. The old keys will remain in the keystore and continue to apply to the data that was encrypted using the old keys.

Keystore replication can sustain normal outages. However, Dell EMC recommends that you back up the CTA configuration to preserve the keystore after CTA generates a new key. Scheduled CTA backups can be configured as a Backup task from the CTA CLI and GUI. A onetime backup of the CTA configuration is possible from CLI using the `fmbackup` command. For more information about CTA backups, see the *CTA backup and restore* section.

Before you can enable encryption, you must meet the following prerequisites:

1. Generate an encryption key using the CTA GUI.
2. Install CTA-HA and run `krdsetup` to enable the encryption key and to start the keystore replication.

CTA13.0 adds support for Linux based CEMA Encryption Services to accommodate augmentation of CEMA robustness and hardening for better memory and system resources handling.

1.9 Compatibility

Table 2 below shows the Dell EMC Unity OE and CTA versions required per feature. See the latest *CTA Interoperability Matrix* on Dell Support for more details.

Table 2 Supported versioning per feature.

Feature	Dell EMC Unity OE	CTA	Source Storage System
File tiering	OE 4.1 or later	Version 11 or later	N/A
File migration	OE 4.2 or later	Version 12 or later	VNX: OE 7.0 or later
Block archiving	OE 4.2 or later	Version 12 or later	N/A

1.10 Common API Settings

The Management and DHSM Credentials for the Dell EMC Unity are configured on CTA's **Configuration** > **Common API Settings** page, as seen in Figure 6. Before starting the daemon to move data to the cloud, you need to populate the Management and DHSM credentials when configuring CTA with Dell EMC Unity. CTA will use the Management credentials when making any REST API calls to Dell EMC Unity. The DHSM credentials are used for stub management.

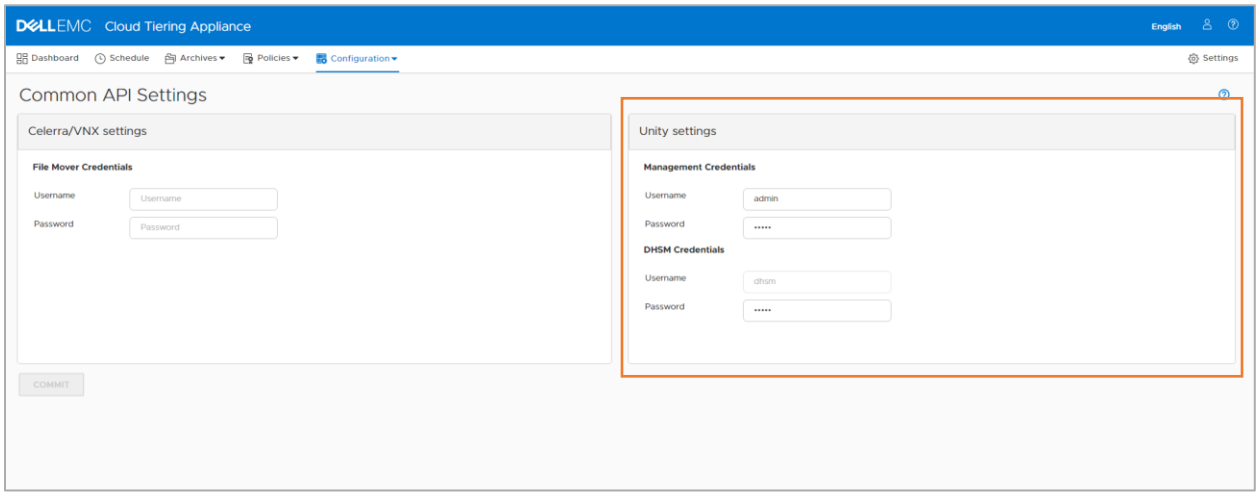

Figure 6 CTA. Configuration. Common API Settings. Unity Settings

Once the credentials are added, we can start the *acdsetup* daemon from the CTA's console (Common Line Interface), as shown below:

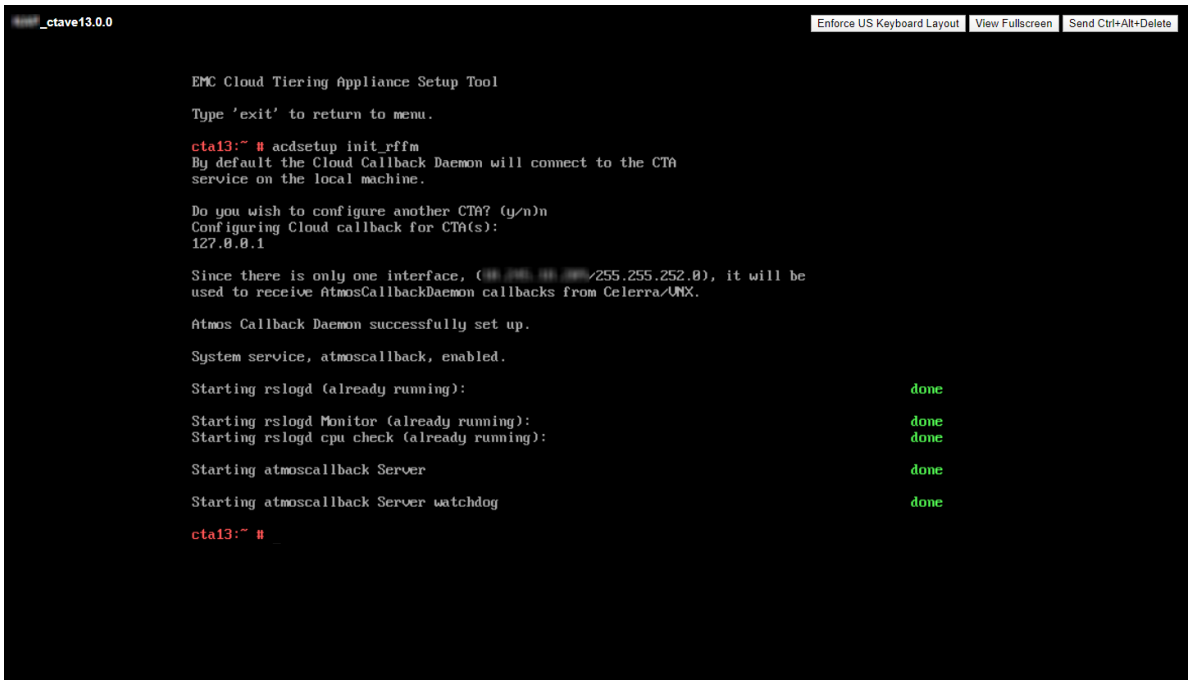

Figure 7 vSphere Web Console. Common Line Interface. ACD Setup.

Note that the DHSM option will be automatically enabled as part of a running the first file archive task, but it can still be enabled manually on the NAS Server. DHSM is enabled per NAS Server, as seen in Figure 8. The **Enforce HTTP Secure** setting is not supported with CTA.

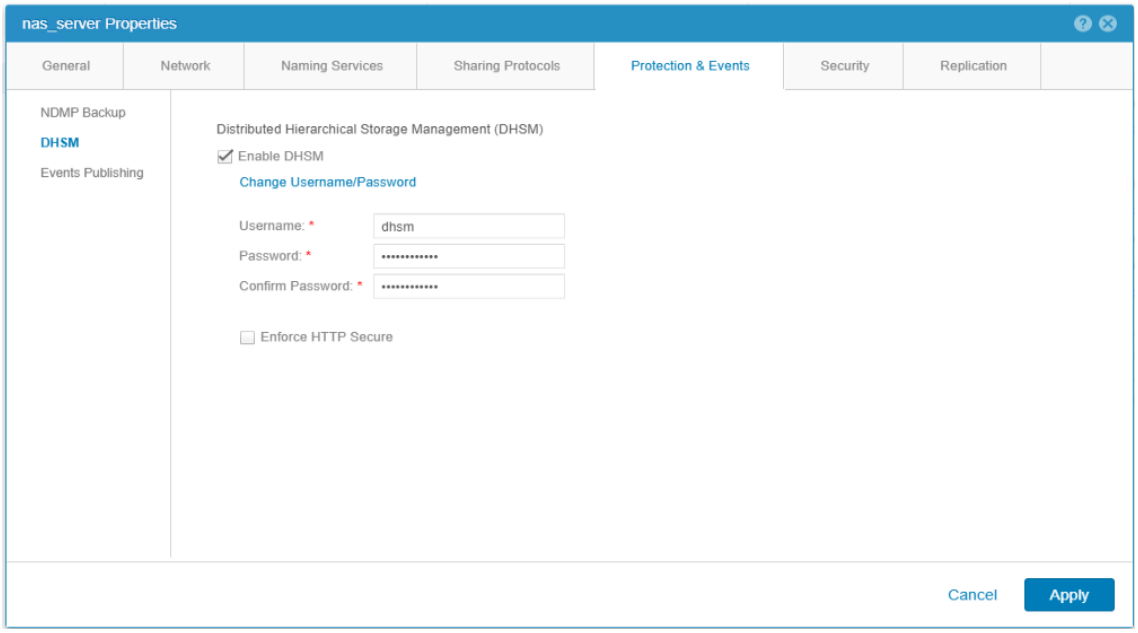

Figure 8 Unisphere. NAS Server properties. Protection & Events. DHSM.

1.11 CTA backup and restore

1.11.1 Backup

To take a backup of the CTA configuration and database, follow the following steps:

1. Add a NAS destination, from the **Configuration** > **Servers** page, to which the backup will be saved to.
2. Add a NAS repository, from the **Configuration** > **NAS Repository** page.
3. Set up the location of the backups in the **Backup and Recovery** page under **Configuration**, as shown Figure 9.
4. Then, schedule the **Backup** task, as shown in Figure 10.

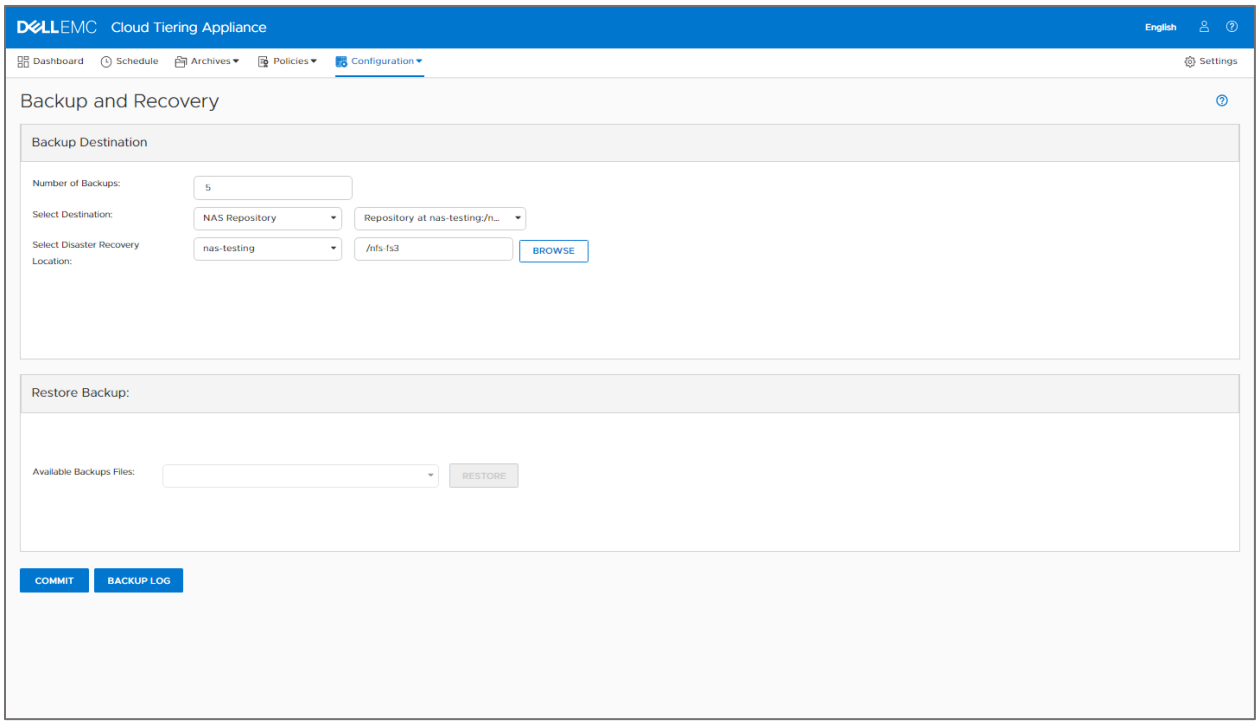

Figure 9 CTA. Configuration. Backup and Recovery.

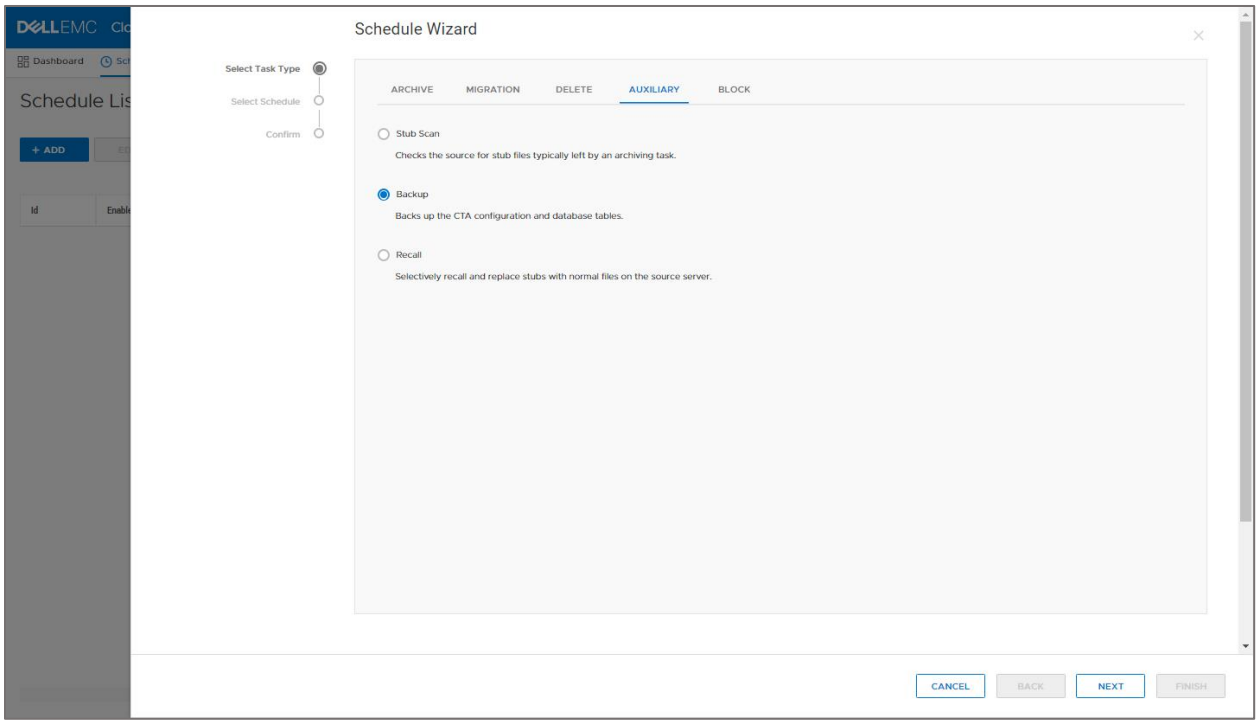

Figure 10 CTA. Schedule Wizard. Backup task.

1.11.2 Restore

To restore from backup, navigate to the **Backup and Recovery** page under **Configuration**, as shown in Figure 9. Select a file in the **Available Backup Files** list under **Restore Backup** and click **Restore**.

See the *Backing up the configuration* section in *the Cloud Tiering Appliance User Guide* for more details on backing up and restoring the CTA configuration.

2 CTA for file

The file tiering feature found on CTA allows the movement of file data to the cloud. The following sections of this paper will discuss:

- The benefits of file tiering
- How the file tiering works
- The general tasks that can be applied to file data

2.1 Benefits

Leveraging CTA file tiering you can use your Dell EMC Unity file shares more cost effectively and efficiently. For example, you can free up capacity on a Dell EMC Unity storage system by transferring your file data to the cloud and leaving a stub in place of the files. File tiering can also decrease the time required to backup file data, because it eliminates the need to back up the full-size original files.

2.2 Distributed Hierarchical Storage Management (DHSM)

The Dell EMC Unity storage system has a native DHSM API, which can move a file from the storage system to the cloud. Moving the file leaves behind a small stub pointer in the file's original location. This process of stubbing and relocating file data describes file tiering.

After the stub files are in place, CTA's stub scanner constantly monitors them. At a basic level, DHSM intercepts client access to data and takes an action before the client accesses the data. When a client tries to read or write to the file, DHSM intercepts that access request and takes an action on the archived data using the stub's information. See the *Recall policy* section for more details about the available recall actions.

2.3 Requirements for the source NAS Server

DHSM achieves the file tiering services. To identify stub files, DHSM reads the offline bit on the stubs. The SMB protocol supports offline bits, but NFS does not so Dell EMC Unity handles offline bits internally for NFS-only archival. CTA communicates with Dell EMC Unity using the DHSM API. Before archiving data from a storage array, the CTA must be configured with the details of the source array. CTA automatically creates the DHSM connections when they are needed by sending a REST API call to Dell EMC Unity. Users can also create the DHSM connection manually using Unisphere CLI (UEMCLI) on Dell EMC Unity.

Deleting the DHSM connection on a Dell EMC Unity using the UEMCLI can optionally trigger a recall of all stubbed data from the repository that is linked to the Dell EMC Unity file system that uses that connection. Before triggering a recall, ensure that enough space is available on the system for all the recalled data. For more details on the UEMCLI, refer to the *Unisphere Command Line Interface Guide* found on Dell EMC Unity Info Hub.

When tiering from SMB shares, the source server must belong to a domain and the CTA configuration settings require a username and password from that domain. The username should be part of the SMB servers' local Administrators group. By default, all members of the Active Directory Domain Admins group are members of the local Administrators group on the Dell EMC Unity SMB Server. The fully qualified domain name (FQDN) and IP address of the Domain Controller should be configured, in the CTA's Fully Qualified Domain page, for Kerberos authentication. If the source includes NFS shares, these shares must have root and read/write permission for CTA and CTA-HA IP addresses.

With the CTA12.1 version, all the communication between CTA and the SMB shares is achieved using SMB version 2. In prior versions of CTA, the communication was through SMB version 1. This entails that if the environment only supports SMB version 1, the communication between the SMB shares and CTA will be interrupted until SMB version 2 is enabled. SMB version 2 adds security enhancements including support for SMB signing.

With the CTA13.0 version, all the communication between CTA and SMB shares is done using SMB 3.0.2 along with SMB 2.1 by SMB auto-negotiation with signing, Kerberos and NTLM authentication, and performance improvements for large files by optimizing the read/write length to 512KB.

2.4 File policies

The following table, Table 3, provides the available tasks for file data:

Table 3 Available CTA tasks for file data.

Task	Description
Archive	Checks files on a source against policy rules and tiers the files to a repository
Multi Tier	Identifies and acts on files that match the multi-tier archive policy
Multi Tier Stub	Updates stubs files and relocates archived data per the multi-tier stub archive policy
Delete Orphans	Identifies orphans and deletes the ones that fit the delete orphan policy
Delete Stubs	Used to delete stubs
Stub Scan	Verifies the source for stub files
Recall	Used to recall and replace stubs with normal files on the source

2.4.1 Archive policy

A CTA policy for tiering consists of one or more rules and destinations. For example, a simple policy might read:

> If this file has not been accessed in 6 months, send it to the ECS, and replace it with a stub.

The one-rule, one-destination policy is common, and many CTA users use this type of policy on their data. However, CTA rules are flexible. CTA supports the creation of more complex rules that archive data to multiple tiers. For example, a policy consisting of multiple rules might look like this:

> If any file has not been accessed in more than 1 year and is larger than 1 MB in size, send it to ECS and leave a stub. However, if the file is a PDF, do not archive it at all. Then, when these PDF files have not been accessed for two years, move them to Amazon S3, and update the stub file to point to the new location.

Policy rules are based on attributes such as access time, modify time, change time, file size, file name, or directory name. The archive policy action is either “archive” or “don’t archive.” A single expression or a combination of expressions defines the archive policy. See Figure 11 for the example of the attributes in the CTA GUI.

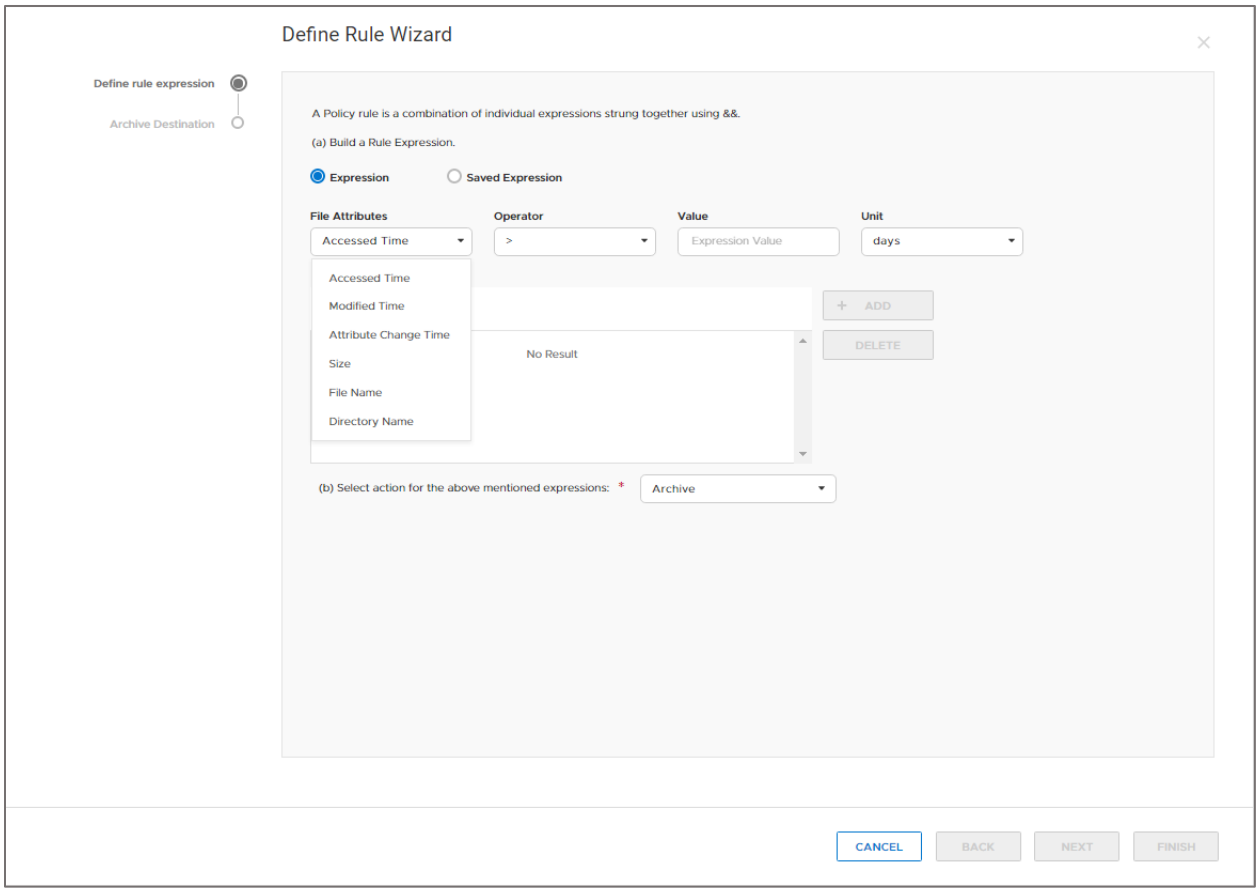

Figure 11 CTA. Define Rule Wizard.

A policy is not associated to a share name hence a single policy can be used by multiple tasks to evaluate different shares. An Archive policy could move files to different cloud repositories by having multiple rules that point to different cloud repositories.

2.4.2 Multi-tiered archive policy

CTA supports multi-tiered archiving, a feature used to specify how files of different ages, for example, can be stored to different types of repositories. A Multi-Tiered Archive policy applies to normal files as well as to files which are already stubbed.

Consider the following example of a multi-tiered archive:

> Find files that have not been accessed in 1 year, and tier them to the Amazon public cloud storage. Find files that have not been accessed in 6 months and send them to ECS private cloud.

By creating a multi-tiered policy type with several rules, each with a different repository, you can design data movement schemes to fit your needs. For the previous example, the multi-tiered archiving policy could have the following rules:

1. If access time > 1 year, archive to Amazon public cloud
2. If access time > 6 months, archive to ECS private cloud

When files that were tiered to ECS are not accessed for 1 year, then they qualify for the first rule. Consequently, the files will be migrated from ECS to Amazon with the stubs being updated accordingly.

Figure 12 provides an example of the multi-tiered policy in CTA.

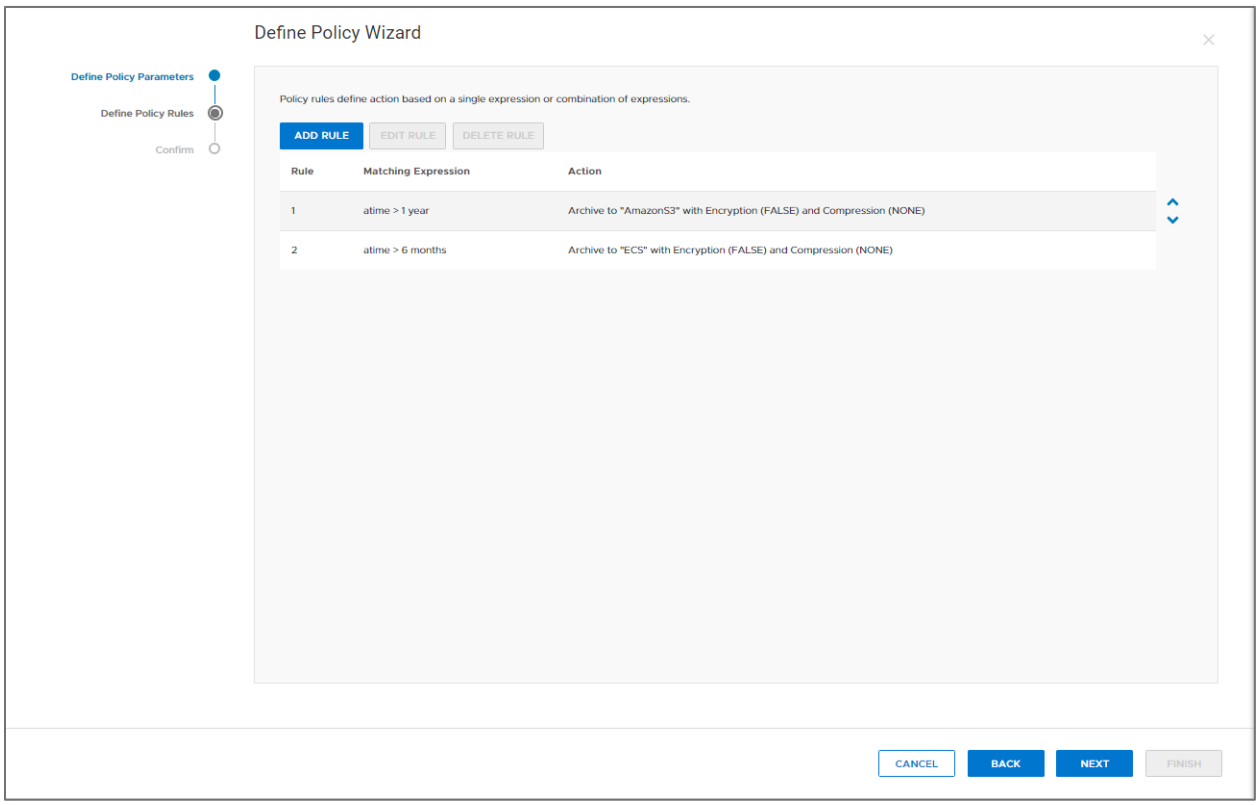

Figure 12 CTA. Define Policy Wizard.

The order of the rules is important because they are applied sequentially. When the first rule evaluates as true, CTA takes the action this rule specifies, either “archive” or “do not archive.” CTA does not apply the subsequent rules, and the policy moves on to the next file.

In the example shown in Figure 12, reversing the order of Rule 1 and Rule 2 would produce an unintended result. The 6-month old rule would be applied first, and the 1-year old rule would never be applied because any file older than 1 year is also older than 6 months. All data older than 6 months would be archived to the private ECS cloud, and no files would be archived to the Amazon. If there are multiple rules in the policy, CTA continues to apply the rules until a rule evaluates to “true.” It then takes the action associated with the rule (such as “archive” or “do not archive”) and moves on to the next file.

2.5 Providing file data to CTA

File tiering is supported on the following storage resources: SMB, NFS, and Multiprotocol Shares on Dell EMC Unity NAS Servers. Administrators usually direct a CTA archive policy to evaluate an SMB or NFS share. CTA scans the files and applies the policy rules to each file, one rule at a time.

A CTA policy can also be directed at specific files. Instead of directing CTA to scan an entire SMB or NFS share, you might instead import a list of filenames; then CTA will scan and apply the archive policy only to the files in that list. The *Cloud Tiering Appliance User Guide* describes the file ingest feature and is available from Dell Support.

2.5.1 Delayed stubbing

When you use one of the following policy types: Archive, Multi Tier, or Multi Tier Stub, you can set a delayed stubbing option. Figure 13 shows the Define Policy Wizard > Define Policy Parameters when creating a multi-tier policy. As the figure shows, you can set the Delay Period property, for which you can provide the number of days when the files should be stubbed on the source. By default, the setting is set to 0 days, so there is no delayed stubbing.

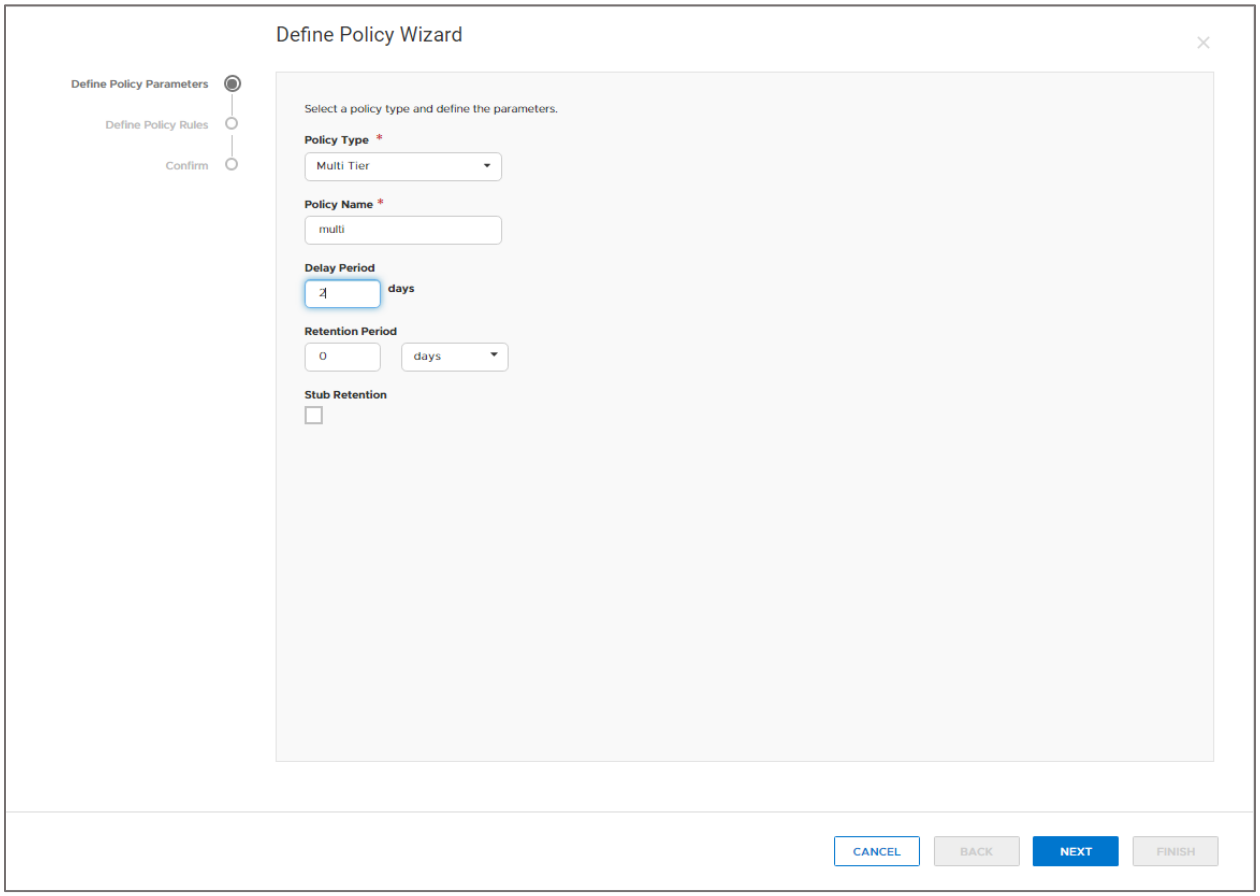

Figure 13 CTA. Define Policy Wizard. Delay period.

2.5.2 Retention

Starting with Dell EMC Unity OE 5.1 and CTA13.0, the retention parameters Retention Period and Stub Retention are supported when tiering data to Dell EMC ECS CAS repositories from Dell EMC Unity.

Dell EMC Unity OE 4.5 and newer, adds File-Level Retention (FLR) support. Archiving an FLR-enabled file system to the cloud is not supported. It is not possible to use a file system with FLR enabled as primary source in CTA. However, Unity's FLR-enabled file systems can be used as a destination repository when tiering from Celerra, VNX, or NetApp systems. Refer to the latest *CTA Interoperability Matrix* on Dell Support for more details.

2.6 Recall policy

When a file has been tiered to a cloud repository and replaced with a stub on the source share, the stub should look and behave like the original file. When a file has been tiered, as seen in Figure 14, it will have an

X icon and the size on disk attribute for the file will be KBs in size. File recall is the process by which the user clicks the stub file and quickly accesses the original file.

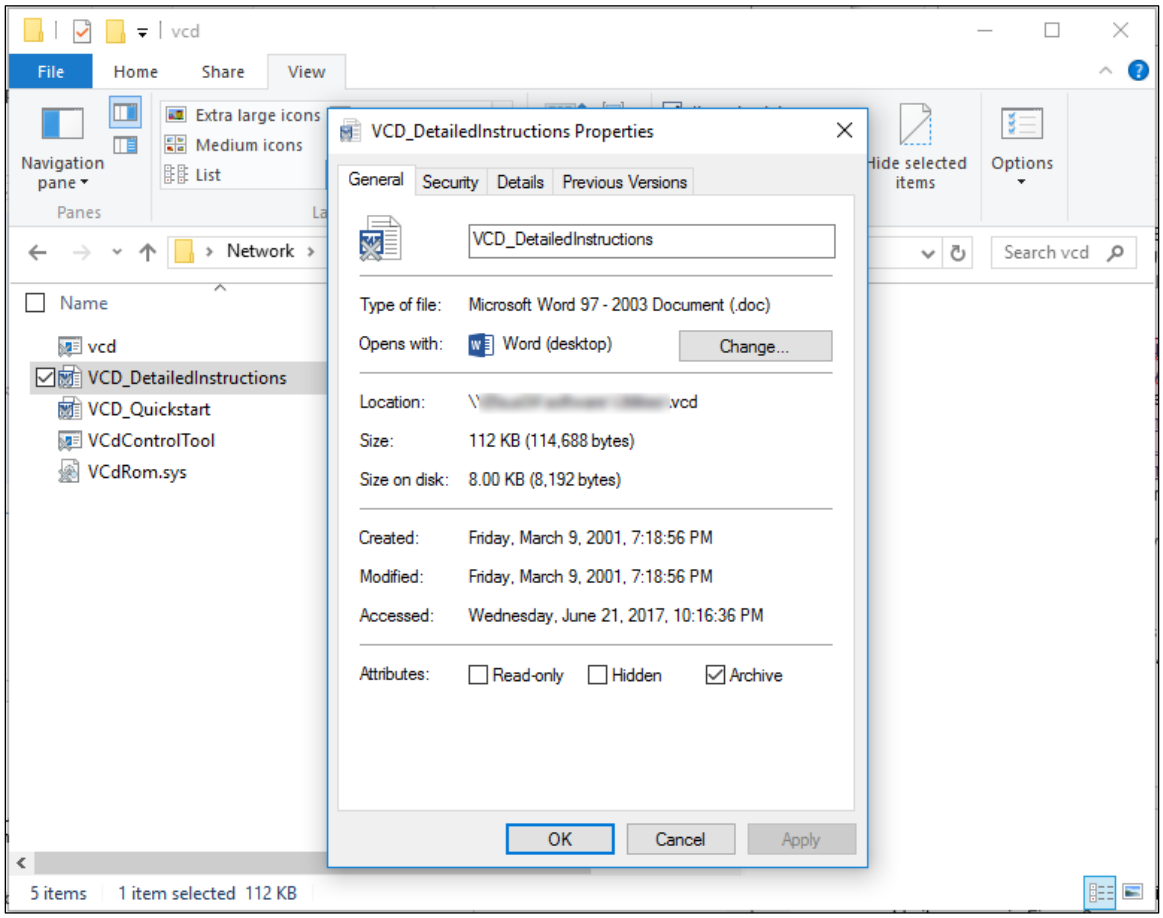

Figure 14 Example of a stub.

The stub file contains information needed to find the actual file. The Dell EMC Unity sets the offline bit on the stub when the file is archived. When a user attempts to read a stub file, the Dell EMC Unity sends the recall request to CTA, which then executes the recall and passes the file to the Dell EMC Unity system.

When recalling the file, Dell EMC Unity performs one of the actions given in Table 4:

Table 4 Available recall options.

Action	Description
Passthrough recall (default)	Retrieves the data without recalling the data to NAS Server. The stubs stay in place.
Partial recall	Recalls only as much of the file's contents as it needs to satisfy the client read request and saves the partial file on Dell EMC Unity.
Full recall	Writes the file back to its original location and deletes the stub.
None	Specifies no override of the method that is specified in the stub file.

In Dell EMC Unity, you can use the Unisphere CLI to set the recall style, which can be configured on each file system. The usage of the optional `readPolicy` flag that is available for the `/net/nas/dhsmconn create` and `modify` commands follows.

```
uemcli -d x.x.x.x -u username -p password /net/nas/dhsmconn -help

Manage DHSM connections between the specified primary file system of Unity
and a secondary file system of CTA.
Actions:

[Create/Modify]
...
[Optional] -readPolicy { none | full | passthrough | partial }
Specify the migration method option used by the NAS Server in the
connection level to override the migration method specified in the stub
file.
```

2.7 Recall using CTA-HA

If an archive task job fails, no data is lost. Simply correct the problem and then rerun the job. For this reason, the complexity of a High Availability (HA) configuration for moving data to the cloud is not required. However, recalls are mission-critical because they affect clients' ability to access their data. Therefore, configurations where CTA is in the recall path require a CTA-HA to be configured.

CTA-HA is a recall-only version of CTA. The HA configuration pairs the CTA/VE-HA virtual appliance with one or more CTA/VE systems. If the primary CTA cannot perform the recall, its associated CTA-HA partner can. There is no set limit for CTA-HA systems that can be configured with a primary CTA.

By creating a DNS hostname that maps to the IP addresses of both the CTA and CTA-HA appliances and is configured in the ACD DNS Name property for the Dell EMC Unity Fileserver in CTA, as shown in Figure 15 and Figure 16, either CTA or CTA-HA could be used when performing recalls for that Dell EMC Unity Fileserver in a round-robin fashion. This setup balances the recall load. If recalls fail with one of the appliances, the other appliance can perform recalls until the failed appliance returns to service. This configuration also allows maintenance of one appliance while the other continues to perform recalls.

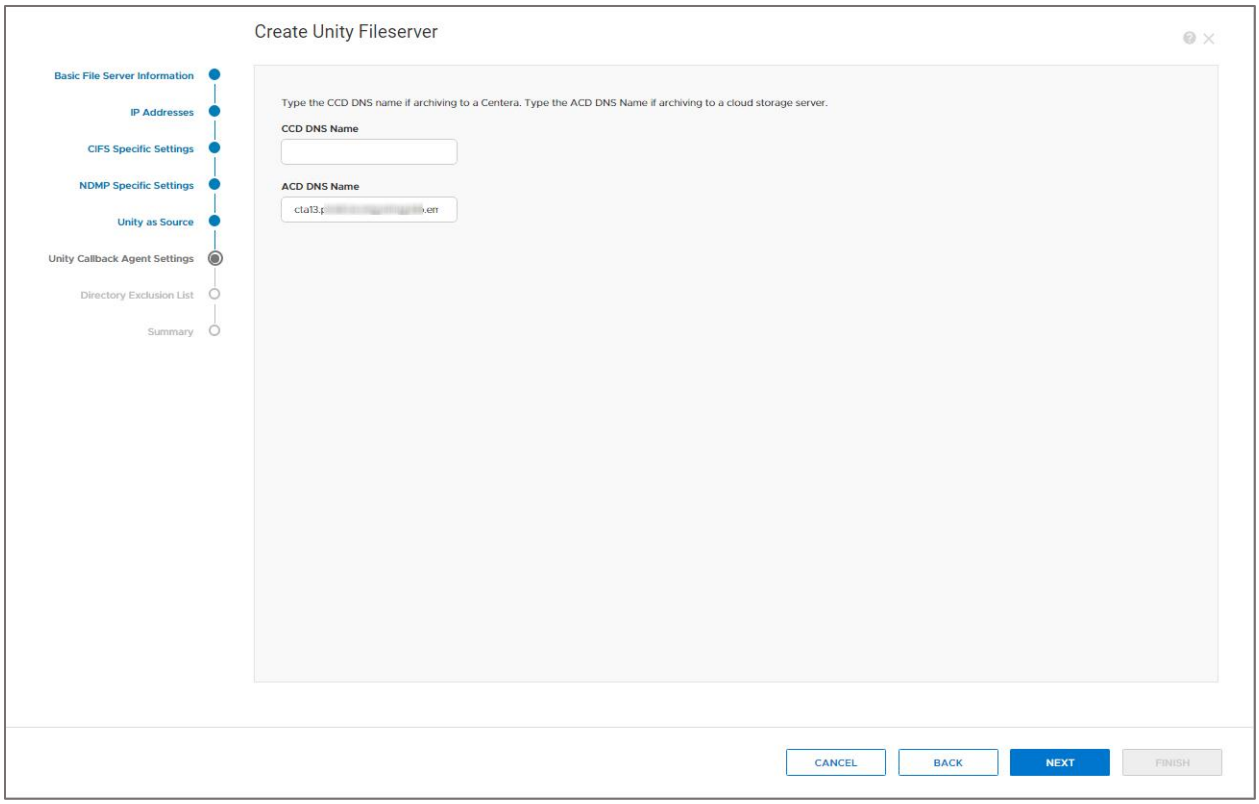

Figure 15 ACD DNS Name when adding a Unity Fileserver to CTA.

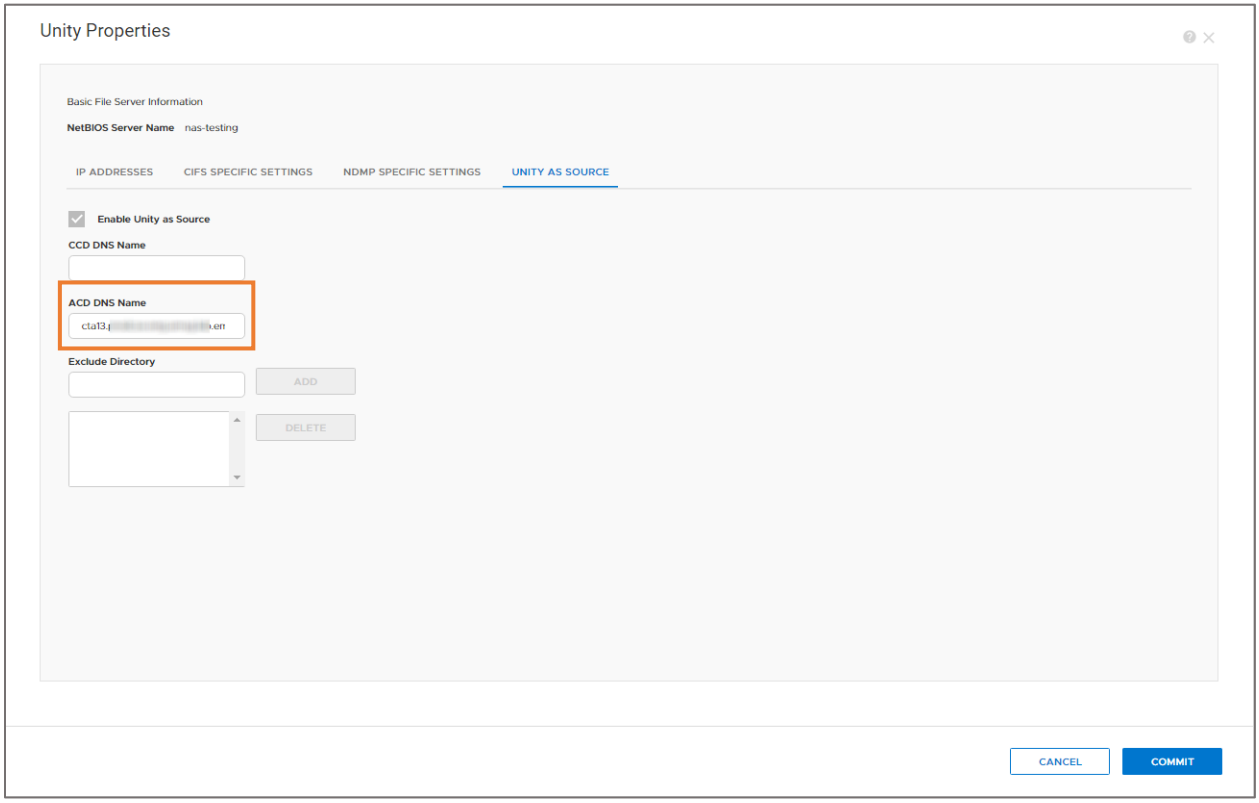

Figure 16 ACD DNS Name when editing a Unity File Server.

2.8 CTA database with file data

When a file is archived to a cloud repository, the stub in the source NAS Server points to the file location in the cloud repository. However, the file in the cloud repository has no pointer back to the source, which means that repository files have no connection to the source. Archived files are not named the same way on the cloud repository as they are on the source.

The CTA database solves this problem. Each time a file is archived, an entry in the CTA database records the file's original location on the source and the file's location in the repository. The database includes entries for every archived file. CTA does not use the database for recalls because the stub on the source includes the information required to locate the file in the repository.

2.9 Stub scanner jobs

For every scheduled archive job, CTA automatically schedules a monthly Stub Scanner task. Stub Scanner is a utility that reads the stubs in a share and compares them to the entries in the CTA database. If stubs move to different locations or if orphans appear, Stub Scanner ensures that the CTA database is kept current.

Because a stub on the source has the information necessary to recall a file from the repository, CTA does not need to query for stub and repository file locations in the CTA database. However, CTA can more efficiently manage the repository storage if information in the database is synchronized with the system. You can run the Stub Scanner task more frequently than the default 30 days but doing so generally is not necessary.

2.10 Orphans

Orphans are created when stub files are deleted from the source, as the actual files in the repository are not automatically deleted and become orphans. The files are not deleted automatically to prevent unwanted deletion of a file being used by a service or application. If CTA had deleted the archived files when the stubs were deleted, restoring the backup would restore stubs that point to nothing.

To delete orphan files and recover space on the repository, run the Delete Orphans task. Do not delete orphans until you are certain that you will not restore stubs that point to orphans. For example, if backups are kept for six months, define the orphan deletion job to delete files that have been orphans for at least that long.

The CTA database and the Stub Scanner jobs play important roles in managing orphan files. Every time the Stub Scanner sees a stub, CTA records a "last seen" time in its database. If the stub is deleted, the stub scanner identifies the file in the repository that was linked to the stub as an orphan. Because it records the "last seen" time in its database, CTA can calculate how long the file has been an orphan. CTA uses the orphan age to determine which orphans to delete. You can set a policy to delete stubs that fit a criterion that you set. For example, delete any orphans larger than 2 MBs or older than 4 months.

2.11 File general workflow

2.11.1 Configure file tiering

1. In CTA:
    a. Configure the Common API settings in CTA, as seen in Figure 6. CTA will use the management credentials to automatically enable DHSM on the NAS Server.
    b. From the console of the CTA, run the following command: `acdsetup init_rffm`

2. In Unisphere:

    a. Make sure that DHSM is enabled for the NAS Server for which file data will be tiered from. If not enabled, manually enable it, as seen in Figure 8.

3. In CTA:

    a. Add the cloud repository that will be used as a Cloud Server.

Note: To use ECS S3, PowerScale S3, and IBM COS as a destination repository, the S3 option can be used. See Figure 17 for an example of it in the CTA GUI. Refer to the *Deploying CTA with Amazon S3* section in the CTA User Guide for the full details.

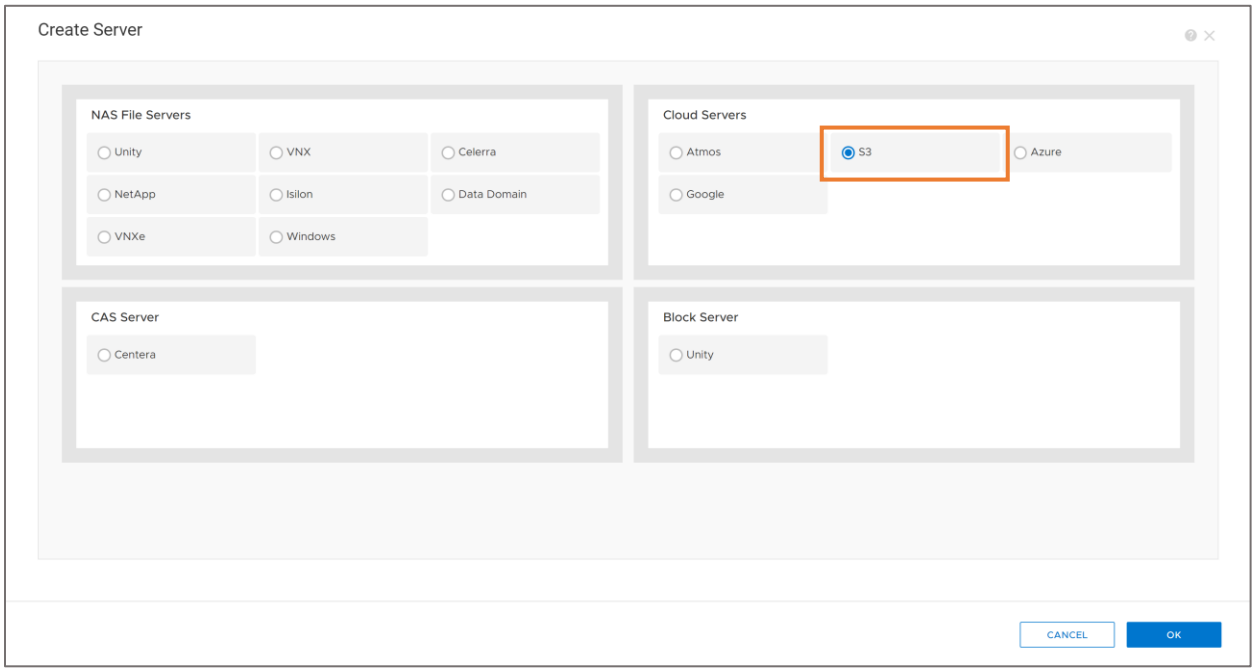

Figure 17 CTA. Create Server. Cloud Servers.

    b. Configure Dell EMC Unity as a NAS File Server.
    c. Create an Archive Policy Scheduled task.

        i. Select the share path from which files will be tiered from.
        ii. Select or add a policy for the files that will fit a predefined criteria, for example, any files greater than 2MB in size.
        iii. Select the schedule for the task.

    d. Run the Archive task.
    e. View Archived File List.

The *Deploying CTA with Unity* section in the *Cloud Tiering Appliance User Guide* provides more details to configure file tiering.

2.12 Reporting

CTA includes a robust reporting interface that provides valuable insight into the efficacy of file tiering policies. CTA generates reports on the files it tiers only. For tiered files, the reports display the size, number of files tiered, and breakdown by file types, but CTA does not give a detailed profile of the data in the file system. Figure 18 shows an example of a report for a share that had a variety of files, including PPT, XLS, PDF, and other files.

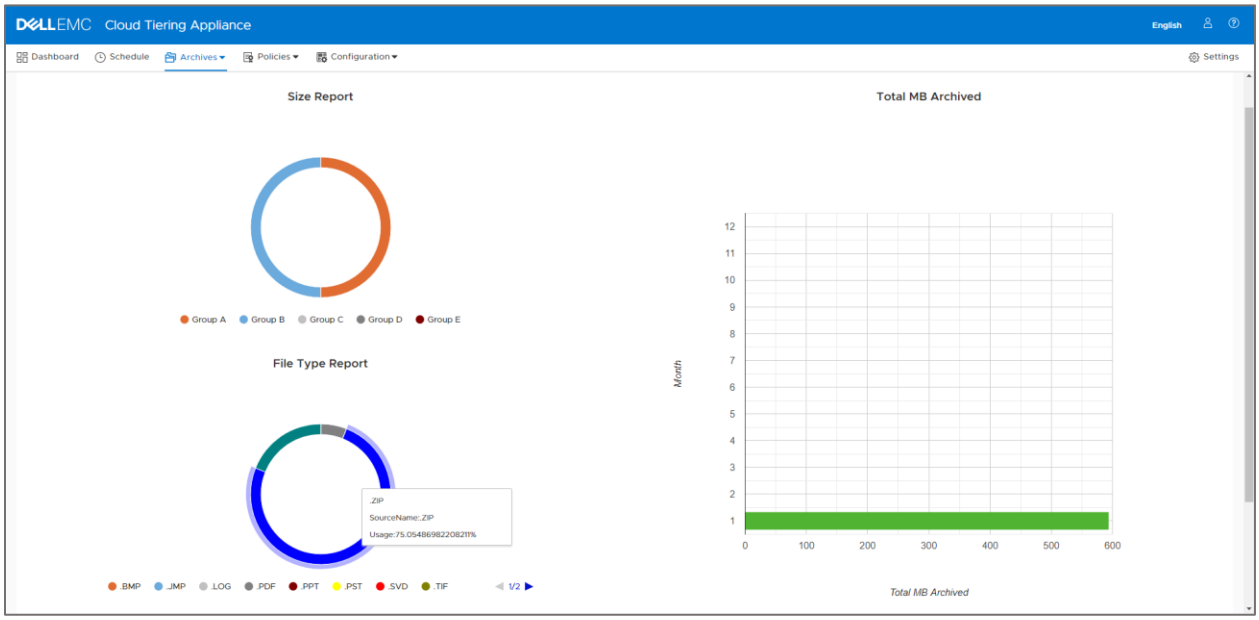

Figure 18 CTA. Archives. View Reports. Sample report

3 CTA for block

3.1.1 Overview

The CTA block archiving feature allows you to move block data to the cloud. The following sections of this paper will discuss:

The benefits of block archiving

- How block archiving works
- The general tasks that apply to block data

3.1.2 Benefits

By leveraging CTA and its block archiving feature, you can more efficiently use your storage system. For example, you can free up space on the storage system by deleting source snapshots after they are backed up to the cloud. Block archiving can also fulfill any compliance need that you might have for your data, for example, when a requirement exists to keep snapshots for a longer period.

3.2 Providing block data to CTA

Block archiving is supported on the following storage resources:

- LUNs
- Consistency Groups
- Thin Clones

3.3 Block archiving

CTA leverages the native Dell EMC Unity's snapshot differentials API to efficiently take backups of the block data to the cloud. Users can archive a full copy of a LUN, Consistency Group or Thin Clone to the cloud as well as all subsequent snapshots. By default, every 30th archived snapshot is a full-copy baseline snapshot. This can be customize using the *Common Base Frequency* attribute in the CTA management GUI. By setting this attribute to a custom value, CTA can establish a baseline for the restore operation that depends upon the set value.

Block snapshots that have been archived to the cloud are independent of the base resource on the source and are not altered by the archiving. Instead, they share blocks with the baseline snapshot established by CTA. After the snapshot is archived, the LUN and/or snapshot can be deleted in the source array to free space.

CTA12.1 adds support for the Block Archive Resume operation. In the case of a Block Archive failure, for example if the CTA was in the process of archiving block data and there was a network outage and the task was interrupted, the user now has the option to resume the operation and continue from the point of time in which the task was interrupted, as shown in Figure 19.

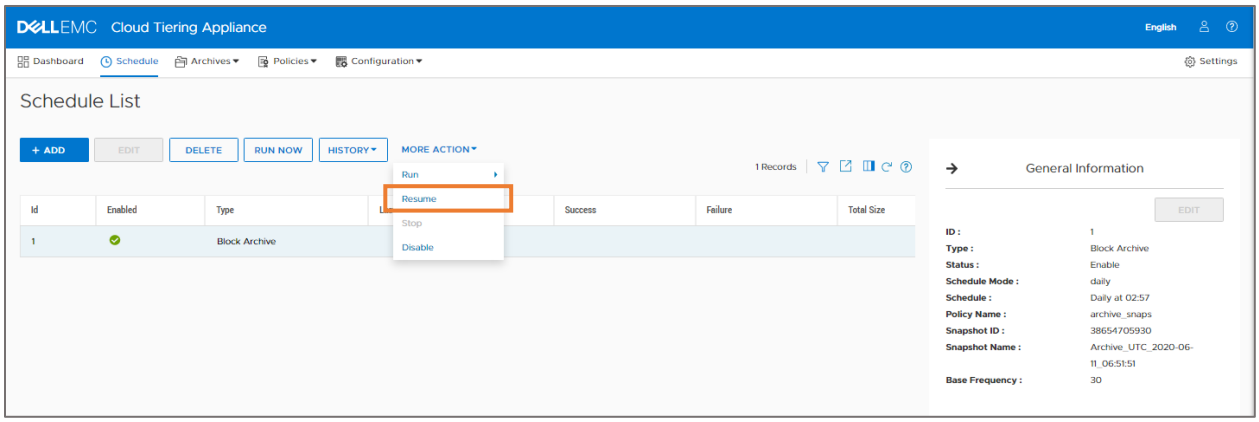

Figure 19 CTA. Block Archive Resume action.

3.3.1 Block archive policy

You can use a Block Archive policy to analyze a Dell EMC Unity storage system for the block snapshots and archive them to the cloud. Figure 20 shows the snapshot attributes that are used by CTA to evaluate the snapshots. CTA scans the snapshots and applies the policy rules to each snapshot, one rule at a time. If there are multiple rules in the policy, CTA continues to apply the rules until a rule evaluates to “true.” It then takes the action associated with the rule (such as “archive” or “don’t archive”) and moves to the next snapshot. A policy is not associated to a block resource (LUN or CG). Hence a single policy can be used by multiple tasks to evaluate different block resources.

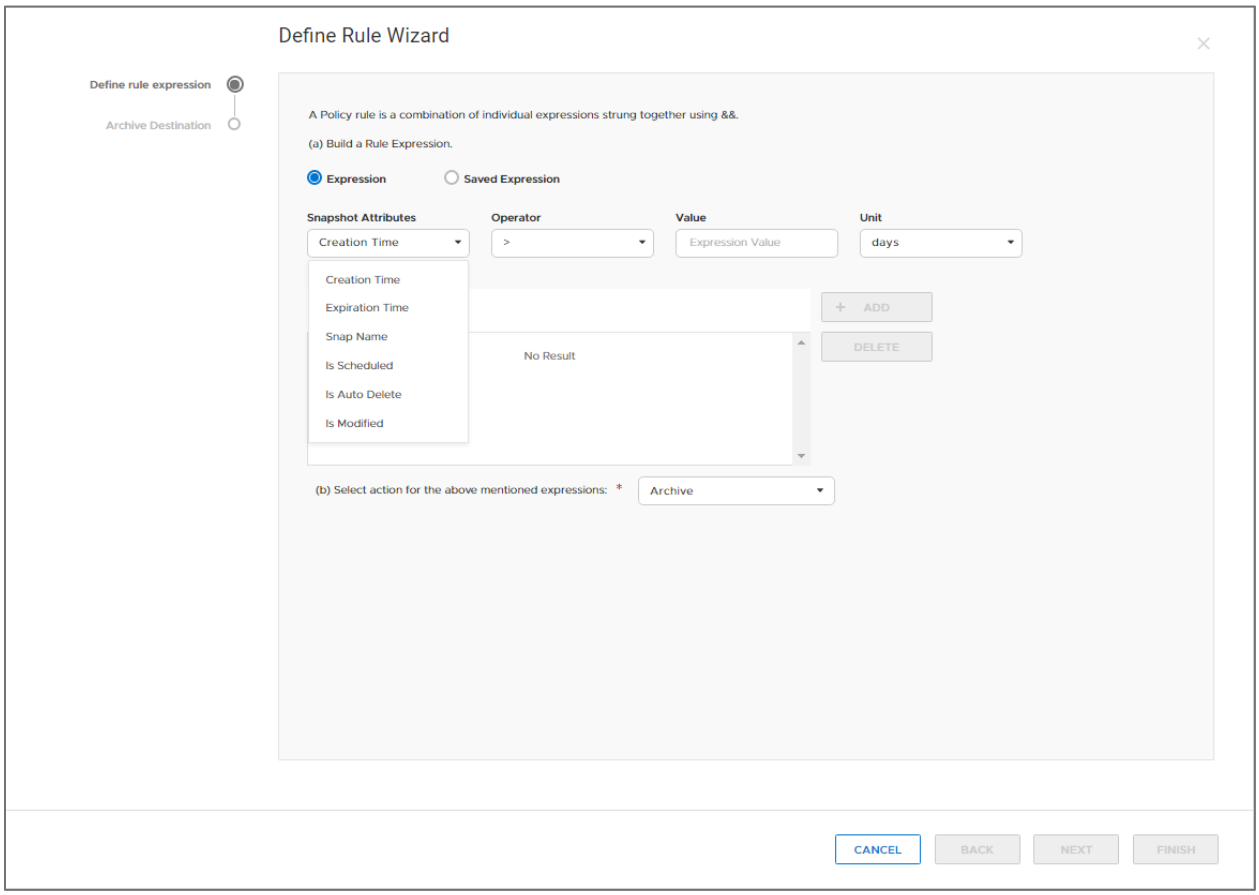

Figure 20 CTA. Matching expression for snapshots.

3.4 Block restore policy

After block resource and its snapshots have been archived to the cloud, they can be restored back to the storage array. The Block Restore policy can be used to restore snapshots to a new block resource. The new block resource can reside in the same Dell EMC Unity storage systems from which it was archived or in a new Dell EMC Unity system.

3.4.1 Prerequisites

- In Unisphere:
  - Ensure that you have iSCSI Interfaces already created in the system. For physical systems, it is recommended that you have at least one iSCSI Interface per Storage Processor (SP) to ensure that multiple paths are available.
- CTA12.1 adds support for multipath iSCSI for Unity. This entails that CTA will login to multiple iSCSI targets and perform IO operations on all available targets. If any iSCSI target goes down, IO operation will happen over the other alive targets and the load will be shared. IO operation will continue while a single target is alive.
- Ensure that the CTA has host access to the destination LUN or CG.

3.5 Block general workflow

3.5.1 Configure block archive

1. In Unisphere

   a. Make sure that the resource from which the data wants to be archived from already has a snapshot schedule assigned or manual snapshots created.

2. In CTA:

   a. From the console, configure the ISCSI IQN target
   b. From the GUI, add the cloud repository that will be used as a Cloud Server.

Note: To use ECS S3, PowerScale S3, and IBM COS as a destination repository, the S3 option can be used. See Figure 17 for an example of it in the CTA GUI. Refer to the *Deploying CTA with Amazon S3* section in the CTA User Guide for the full details.

---

   c. Configure Dell EMC Unity as a Block Server
   d. Create a Block Archive Policy Scheduled task

      i. Create a Snapshot Attribute Expression. This determines the snapshots that will be archived with the task, for example, manually user-created snapshots and/or snapshots created by a snapshot schedule
      ii. Create a Block Archive Scheduled Task
         1. Select the block LUN or CG that snapshots will be archived from
         2. Select the Common base Snapshot. This will be snapshot that be the full copy of the block resource.
         3. Select the Block Archive Policy that you previously created

   e. Run the Block Archive task
   f. View Archived Snapshot List

3.5.2 Configure block restore

1. In Unisphere, if not already created, create a LUN or CG in which CTA will restore the archived snapshot(s)
2. In CTA:

    a. Create a Block Restore Scheduled Task

        i. Select the source block LUN or CG that was already archived
        ii. Select the snapshot to restore from the cloud
        iii. Select a destination LUN or CG. The destination resource can be in a different Dell EMC Unity system.

    b. Run the Block Restore Task

The *Deploying CTA with Unity* section in the Cloud Tiering Appliance User Guide provides more details to configure block archiving.

4 File migration

4.1 Overview

With CTA version 12 SP1, the CTA file migration feature is supported with Dell EMC Unity systems. File migration moves files from one location to another while preserving stubs and without needing to rehydrate the data.

File migration is a task in CTA to move data from a source File System to a target File System. The target File System needs to be large enough to hold the data being moved, but it does not need to be of the same size as the source File System. Administrators can use CTA to move data from a legacy array to Dell EMC Unity with minimal disruption to the clients. CTA can perform multi-protocol, incremental, stub-aware, cross-vendor migrations that can greatly reduce the effort and complexity when replacing legacy arrays and implementing their NAS environment on a Dell EMC Unity.

CTA supports SMB (CIFS), NFS, and multi-protocol source File Systems. When having a Dell EMC Unity as a target, the supported source platform is VNX2. Refer to the latest *CTA Interoperability Matrix* on Dell Support for supported VNX2 versions. Figure 21 provides a graphical representation for file migration. File Migration requires both source and destination file systems to be shared as well as exported. Hence when migrating to Dell EMC Unity, the NAS Server on which the destination file system will reside in needs to be Multiprotocol Enabled.

For source SMB (CIFS) servers, CTA needs access permissions of a domain user that is part of the Backup Operators and the Local Administrators group on the source and target File Systems. For NFS servers, the NFS exports need to have root and read/write permissions for the CTA IPs.

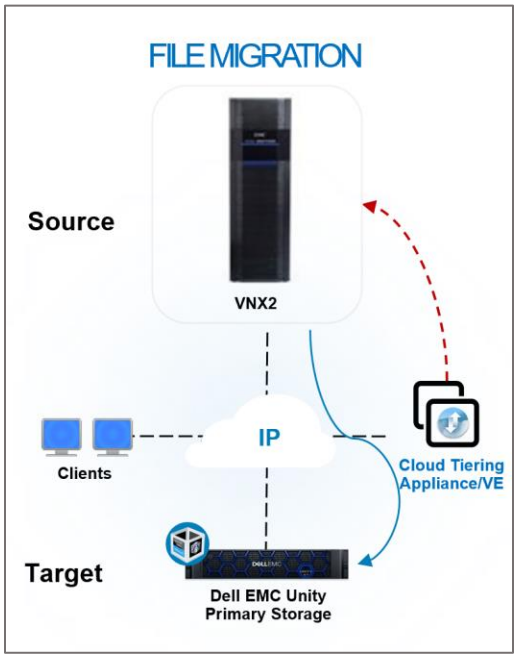

Figure 21 CTA File Migration with Dell EMC Unity.

4.2 Migration source

CTA Migration is policy-based and uses NDMP as its file transfer engine when migrating from VNX. Figure 22 shows an example for a rule used to migrate all PDF files excluding files older than 3 years. CTA uses the FileMover to create snapshots and migrate files from VNX using NDMPCOPY. CTA creates snapshots on the source File System by making API calls. Snapshots enable users to continue to access and write to the source share while the migration is taking place. Note: The CTA-HA is not used for CTA Migration.

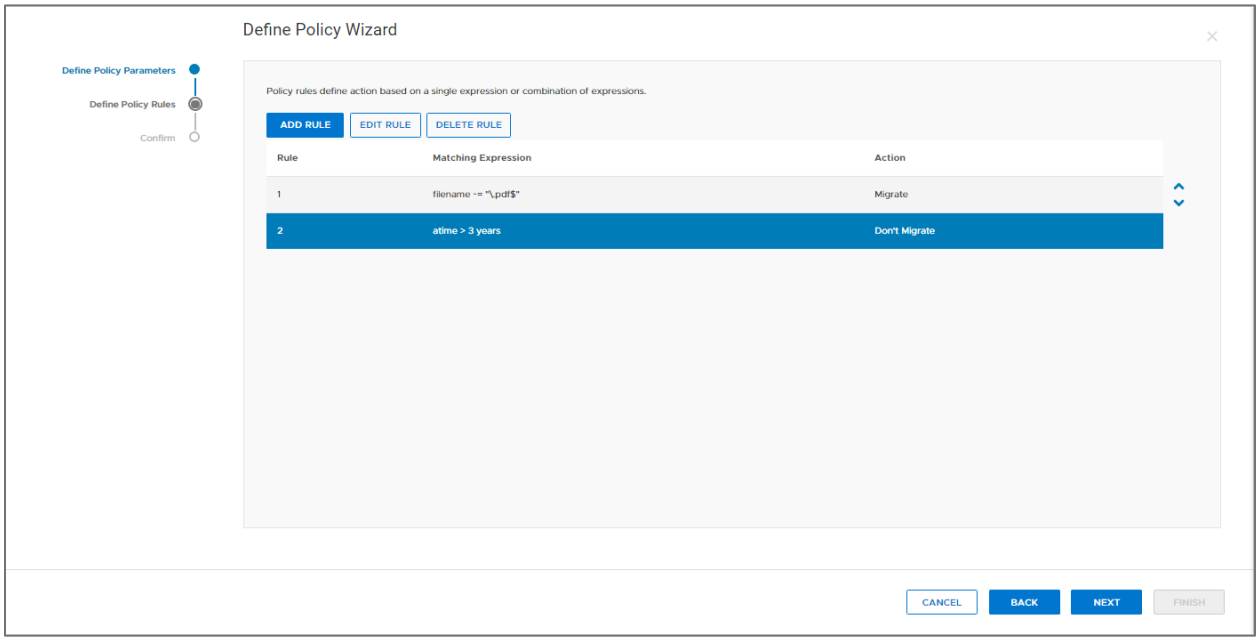

Figure 22 CTA. Creating a rule.

To migrate all the data without filtering any files, requires a simple policy with a rule like the following:

1. If size >= 0 bytes, then Migrate

4.2.1 Migration targets

Before starting a migration task, the target File System in the Dell EMC Unity must exist. CTA does not create the target File System automatically. Migrating files to the root level requires that the directories to be empty, except for system directories such as *lost+found*. However, files can be migrated to any empty directory in a share.

The protocol of the target Dell EMC Unity File System must be multi-protocol. Requiring that the target NAS Server must be multiprotocol. For more information on how to configure a multi-protocol NAS Server on a Dell EMC Unity system, review the *Configuring Multiprotocol File Sharing* guide on Dell Support.

For NDMP-style migrations, NDMP must be enabled on the Dell EMC Unity target NAS Server from Unisphere, as seen in Figure 23. By default, the *ndmp* username is used. The server configuration for the target server on CTA requires the same NDMP password as the one set in Unisphere for the *ndmp* username. For the source server, the NDMP username in the server configuration could be different.

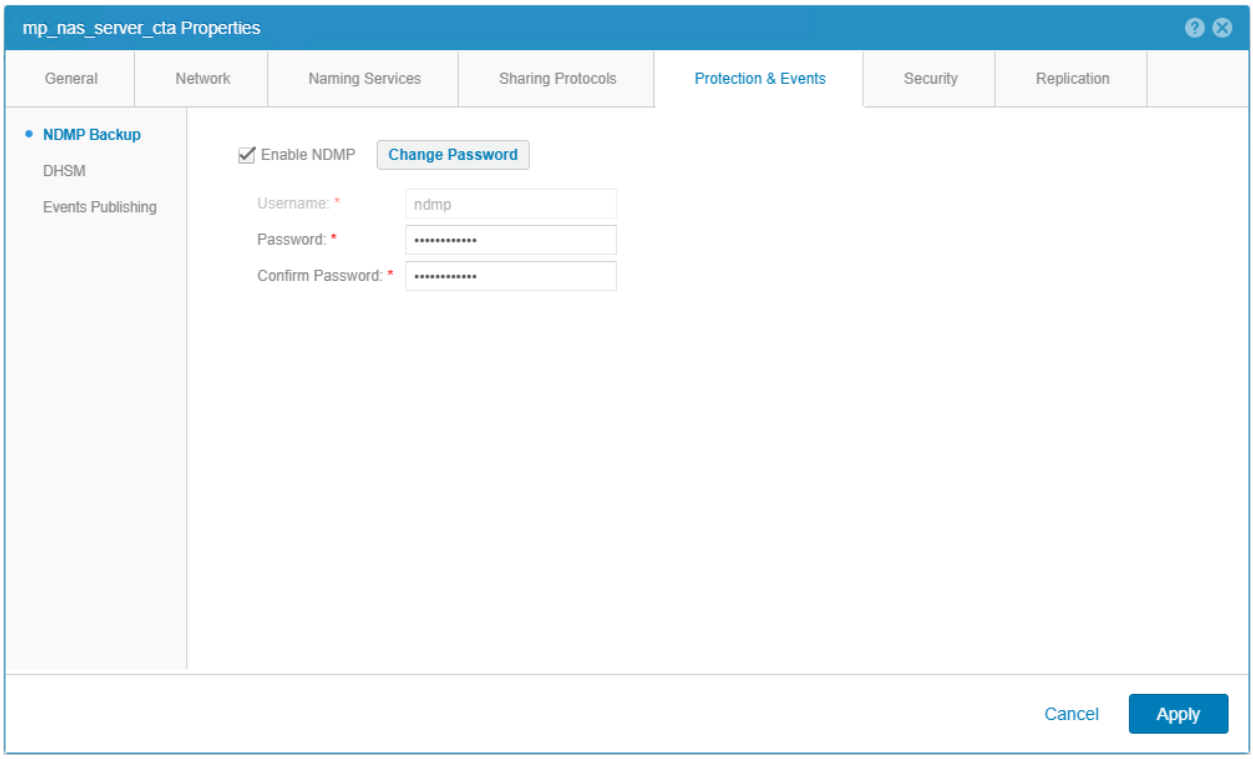

Figure 23 Unisphere. NAS Server Properties. Protection & Events. NDMP Backup.

4.2.2 Migration process

Migrations run as scheduled batch jobs. Schedule the migration task on the CTA Schedule page or through the CLI, where you specify the following information:

- A source share
- A policy
- An empty target share or directory

When the job begins, CTA creates a snapshot on the source. The CTA copies the data that matches the policy to the target. The migration can begin anywhere in the source share (for example, at the top level or in a subdirectory), and can move files to any empty share or directory on the target.

After the first pass completes, the target has a copy of the data from the snapshot on the source. However, if users have continued updating the source during migration, the source share will probably have changed from the snapshot. You can run a second pass to pick up those incremental changes. CTA will create another snapshot, compare the second to the first, and only transfer the changes between the two snapshots such as new files, deleted files, metadata changes, and so forth.

You can continue running passes as needed to pick up changes. Prior to running the final pass, put the source in offline or in read-only mode to ensure that the target is identical to the source. To complete the migration, transfer the client mounts to the target. The target has copied of all CIFS and/or NFS ACLs or permissions. After transferring the clients, delete the source share and recover its storage space on the source NAS system.

CTA can run migration tasks in a continuous mode. The migration task has the option of running incremental migrations until reaching a files-moved threshold. The threshold can be set when creating a File Migration task, by selecting *Automatic Recursive File Migration* and setting a *File Threshold Limit* in the Schedule step,

as shown in Figure 24. For example, you might want to continue running incremental migrations until fewer than 1000 files are moved in one run. At that point, you would want the system to stop and notify you. Administrators typically perform incremental runs during scheduled off-hour periods over the course of several evenings, with the final locked cutover also performed during off hours.

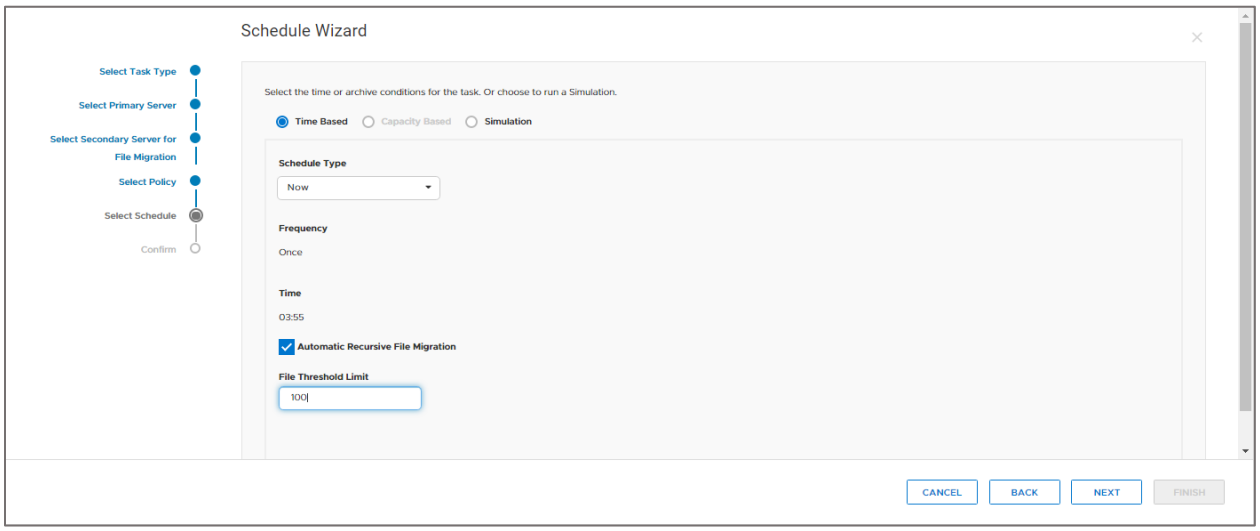

Figure 24 CTA. File Migrate Task. Schedule Step.

If you wish to throttle CTA migration tasks, you can specify a maximum bandwidth rate when creating the task schedule. This way, the migration does not consume all the network bandwidth. You can also use the CTA SID translation tool to create a SID mapping of local to domain SIDs. CTA applies the mapping at migration time to ensure that the SIDs on the target will be correct. This guards against having permissions issues after the migration is complete. For more information about the SID translation tool see the SID translator section in the *Cloud Tiering Appliance User Guide* on Dell Support.

In addition, CTA can migrate stub files. For a stub aware File Migration from VNX to Dell EMC Unity, source file should be archived to a cloud repository. If the source and target both support CTA stubs and are properly configured, CTA migrates stubs without recalling the archived data and the stubs continue to function after migration. To confirm that the servers are configured properly, run a Verify from the Server page for the source and target servers.

4.3 File migration workflow

The same workflow and procedures apply to both CTA and CTA/VE deployments.

4.3.1 Configure file migration

1. In CTA:
    a. Under the Common API Settings page, configure the Dell EMC Unity Management and DHSM Credentials. For Dell EMC Unity, CTA will use the management credentials to automatically enable DHSM on the NAS Server. If migrating from a VNX source system also configure the VNX Management credentials, reference Figure 6.
2. In Unisphere:
    a. Create a new multiprotocol target NAS Server.

b. Enable NDMP on the target NAS Server and set a password for the *ndmp* username. As shown in Figure 23.
c. Create a multiprotocol File System and create a share on it.

3. In CTA:

a. Add the source VNX2 system as a NAS File Server. Making sure to select *Yes* in the *Server as Source* step.
b. Add the Dell EMC Unity target NAS Server as a NAS File Server. In the Dell EMC *Unity as Source* step, select *No* since the Dell EMC Unity is a target.
c. Create a Scheduled task for a File Migration Policy.

i. Select the Primary Server from which files will be migrated from. Figure 25 shows an example of the Primary Server step when creating a File Migration task.

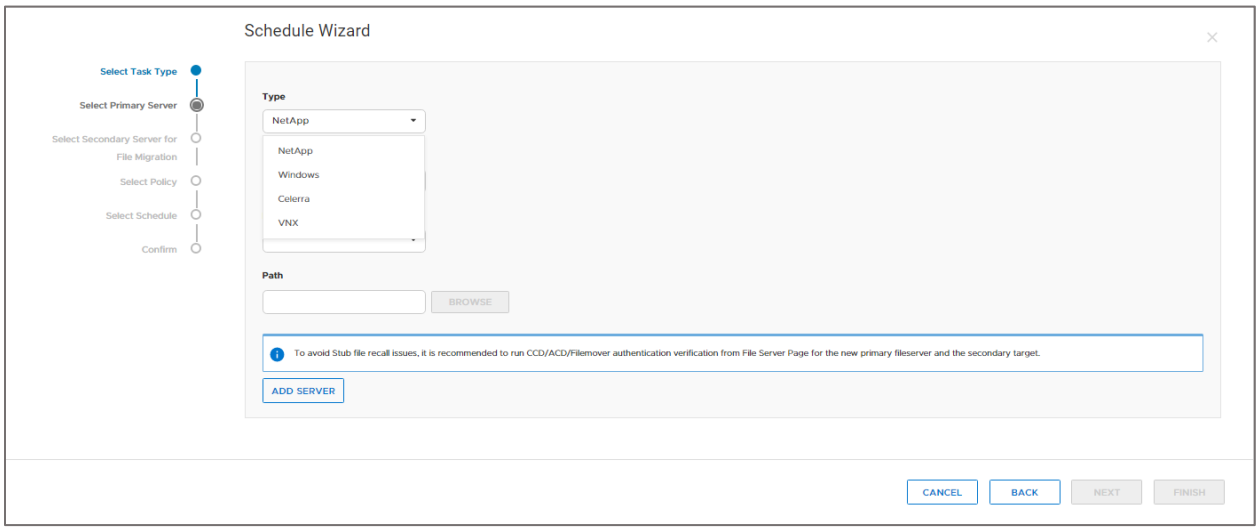

Figure 25 CTA. File Migration. Primary Server.

ii. Select the Secondary Server to which files will be migrated to.
iii. Select or add a policy for the files that will fit a predefined criteria, for example, any files greater than 2MB in size.
iv. Select the schedule for the task.

d. Run the File Migration task.
e. The files that fit the predefined criteria are migrated to the target Dell EMC Unity system. To migrate all the data without filtering any files, the policy configured needs to have a rule set to size >= 0 bytes, then Migrate.

4.4 Stub migration

As an alternative to the CTA file migration feature, you can migrate stubs in a VNX system to a Dell EMC Unity system without recalling the files, by using EMCopy. The EMCopy tool can be downloaded from Dell EMC Online Support. Table 5 provides the supported version for the Dell EMC Unity, VNX, and EMCopy.

Table 5 Stub migration supported versions.

System/Tool	Supported version
Dell EMC Unity	OE 4.1.2 or later
VNX	OE 7.0 or later
EMCopy	4.17 or later

4.4.1 Migrate stubs

1. In VNX, after the file data has been tiered, change the DHSM settings per file system to set the recall style to offline.

   a. Below is the usage of *backup* switch available for the VNX *fs_dhsm modify* command:

```
[nasadmin@dr-vnx-cs0 ~]$ fs_dhsm
    -list
  | -info [<fs_name>|id=<fs_id>]
  | -modify {<fs_name>|id=<fs_id>} [-state {enabled|disabled}]
      [-popup_timeout <sec>] [-backup {offline|passthrough}]
```

   b. From an SSH session to the VNX:

      i. Get a list of all file systems with DHSM enabled by typing the following command: `fs_dhsm -list`

Example:

```
[nasadmin@dr-vnx-cs0 ~]$ fs_dhsm -list
 id      name
 220     cta_fs
 36      Test_FS1
 171     ctamigvnx
```

      ii. Type the following command: fs_dhsm -modify <file system name> -backup offline.

Example:

```
 [nasadmin@dr-vnx-cs0 ~]$ fs_dhsm -modify Test_FS1 -backup offline
Test_FS1:
state                = enabled
offline attr         = on
popup timeout        = 0
backup               = offline
```

   Ensure that the backup method is changed to offline for all the file systems for which stubs will be migrated.

2. In Dell EMC Unity, create the destination NAS Server with file systems that have enough space for the migration of the data.
3. In CTA, ensure that the target Dell EMC Unity NAS Server has been added as a NAS File Server.
4. For each file system that has stubs that need to be migrated, map the source and target shares in the host,

5. Open a command window in the folder where the EMCopy tool is located. Run the following EMCopy command for each share:

   ```
   emcopy.exe [source] [destination]
   ```

   Example:

   ```
   C:\Users\Administrator\Desktop\emcopy042002>emcopy.exe U:\source Y:\dest
   ```

The stubs from the VNX source file system will be migrated to the target Dell EMC Unity file system without rehydrating the data. The files can be opened and recalled from the Dell EMC Unity system. Reference the documentation on Dell Support for EMCopy to see additional flags and options available.

5 Miscellaneous

5.1 Dell EMC Unity as a destination

Dell EMC Unity can be used as the archiving destination for the VNX and NetApp storage systems. For more details, see the latest *CTA and CTA/VE Interoperability Matrix* and the *Cloud Tiering Appliance User Guide* on Dell Support.

5.2 Troubleshooting

When facing any issues configuring CTA with any of the features, review the *Cloud Tiering Appliance User Guide* and search for *CTA* on the on Dell Support site to find Knowledgebase articles.

The following list provides some suggestions for configuring CTA with a Dell EMC Unity system.

- Ensure that the time between the ESXi server, the Dell EMC Unity storage system, and CTA are synchronized. It is recommended to use the same NTP Server for all the components. Also, ensure that the CTA has the correct time zone configured.
- When setting the Networking for the CTA, ensure that the **Speed** value for the Physical Interface is set to **Auto**.
- Ensure that your CTA instance has been added as a host to your environment's DNS server. Ensure that the FQDN for the CTA does not have any dashes in it.
- Ensure that your DNS server has been added as a **Fully Qualified Domain Name** under the **Configuration** > **Fully Qualified Domain** page on CTA.
- Ensure that the **File Management Daemon** and **Atmos Callback Daemon** services are running. The *Deploying CTA with Unity* section in the *Cloud Tiering Appliance User Guide*, provides more details to configure Dell EMC Unity on CTA.
- To verify if you can authenticate with the current configuration given for a file server use: `rffm authServer file_system_name`, for example, `rffm authServer MIG-SMB`
- When using ECS, the **Use with Namespace** setting for the Base URL needs to be set to **No**. Reference KB512667 on Dell Support for more details.

5.3 CTA ports

The following provides a list of the ports that are used by CTA when used with Dell EMC Unity:

- SSH Access: port 22
- To archive data from a VNX and Dell EMC Unity - Common API: TCP port 5080
- To archive SMB/CIFS data, the CTA needs SMB over NetBIOS: TCP port 139
- To create the connection for a cloud storage server: port 9000
- Amazon S3:
  - port 443 (XML API access)
  - port 80 (Management GUI over HTTP)
- ECS uses Port 9020 (for HTTP) and 9021 (for HTTPS))
- Portmap v2 RPC service: TCP port 111
- Configuring SNMP alerts: UDP port (typically SNMP uses UDP port 161 for general SNMP messages and UDP port 162 for SNMP trap messages)

6 Conclusion

In this paper, we discussed the various features provided by the Cloud Tiering Appliance (CTA) that apply for the Dell EMC Unity. Configuring file tiering and block archiving dramatically improves storage usage efficiency. CTA seamlessly automates policy-based file tiering and block archiving with easy management and zero impact on the user's data. CTA allows storage administrators to create scheduled policies that move inactive file and block data off the Dell EMC Unity system to public clouds Microsoft Azure, Google Cloud Platform (GCP), Amazon S3, and IBM COS, or to a Dell EMC ECS and PowerScale S3 private clouds.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

The Dell EMC Unity Info Hub provides detailed documentation on how to install, configure, and manage Dell EMC Unity systems.

A.1 Related resources

The following resources can be found on Dell Support:

- Cloud Tiering Appliance User Guide
- CTA and CTA/VE 13.1 Interoperability Matrix
- Configuring Multiprotocol File Sharing