Dell EMC ECS: Data Domain Cloud Tier Architecture and Best Practices

Abstract
This document describes how the Dell EMC™ Data Domain™ Cloud Tier technology integrates with a Dell EMC ECS system to provide a massively scalable architecture.

May 2019
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Initial release</td>
</tr>
<tr>
<td>November 2017</td>
<td>Rev 2</td>
</tr>
<tr>
<td>January 2018</td>
<td>Rev 3</td>
</tr>
<tr>
<td>March 2018</td>
<td>Rev 4</td>
</tr>
<tr>
<td>October 2018</td>
<td>Rev 5</td>
</tr>
<tr>
<td>May 2019</td>
<td>Updated reference to DDOS Admin Guide 6.2; template update</td>
</tr>
</tbody>
</table>

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017–2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [5/7/2019] [Best Practices] [H16169.5]
# Table of contents

Revisions .................................................................................................................. 2

Table of contents ..................................................................................................... 3

Executive summary ................................................................................................. 5

1 Introduction ........................................................................................................... 6
   1.1 Data Domain overview .................................................................................. 6
   1.2 ECS overview .............................................................................................. 6
   1.3 Benefits of a combined solution .................................................................. 6

2 Cloud Tier solution overview ............................................................................... 7
   2.1 ECS and Data Domain code integration ....................................................... 7
   2.1.1 Integration aspects of ECS ..................................................................... 7
   2.1.2 Integration aspects of Data Domain .......................................................... 7
   2.2 Overall data protection workflow ................................................................ 7
   2.3 Data Domain Cloud Tier mechanism ............................................................ 8
   2.3.1 Cloud Units and MTRee organization ....................................................... 8

3 Cloud Tier resiliency ........................................................................................... 10
   3.1 Single-site Cloud Tier resiliency .................................................................. 10
   3.1.1 Scenario 1: controller failure resiliency .................................................. 10
   3.1.2 Scenario 2: disk failure resiliency ........................................................... 11
   3.1.3 Scenario 3: metadata disk shelves resiliency .......................................... 11
   3.1.4 Scenario 4: single-site Cloud Tier site loss ............................................ 12

4 Cloud Tier replication considerations ................................................................. 13
   4.1 Factors of replication .................................................................................. 13
   4.2 Simple replication example ......................................................................... 14

5 General best practices ......................................................................................... 15

6 Deployment and configuration ............................................................................. 17
   6.1 ECS system configuration ........................................................................... 17
   6.1.1 Storage pools ......................................................................................... 17
   6.1.2 Virtual data center .................................................................................. 18
   6.1.3 Replication group ................................................................................... 19
   6.1.4 Namespace ............................................................................................. 20
   6.1.5 Object users ........................................................................................... 21
   6.2 Data Domain system .................................................................................. 23
   6.2.1 License for Cloud Tier ............................................................................ 23
   6.2.2 DNS entries for all components including load balancer ....................... 24
### Table of contents

6.2.3 Create Cloud Tier device ........................................................................................................... 24
6.2.4 Enable Cloud Tier: disable filesystem first ............................................................................... 26
6.2.5 Import SSL cert from load balancer ............................................................................................ 27
6.2.6 Begin logical Cloud Unit on Data Domain .................................................................................. 29
6.2.7 Summary of preparatory elements .............................................................................................. 31
7 Data policies: movement, retention, recall .......................................................................................... 34
  7.1 Data movement policies ............................................................................................................... 34
  7.1.1 Bucket layout on ECS ............................................................................................................... 36
  7.1.2 Objects preserve DD filesystem path with S3 PUT request ...................................................... 37
  7.1.3 Network verification of HTTP PUT from load balancer to ECS of 4MB .................................... 38
  7.1.4 Cloud Tier object size stored/verified on ECS ........................................................................ 38
  7.1.5 Verifying 4MB data write from Data Domain autosupport report ........................................... 39
  7.2 Recall of file data ......................................................................................................................... 39
  7.3 Networker (policy engine for data movement) ............................................................................. 40
A Technical support and resources ....................................................................................................... 41
  A.1 Related resources ......................................................................................................................... 41
Executive summary

Finding reliable long-term storage media in the form of a cost-effective solution for tiered archive storage is a persistent problem. Almost any solution comes up against the constraints of the physical media whether in storage shelf life, or the reality of an ever-growing sprawl of single-purpose storage silos. This means that the more ways a single technology can integrate into a data center, the more workflows can be consolidated onto that platform, making it more valuable due to its ability to address various business needs without creating another silo. The concept of integration into the data center should also include the ability to leverage collaborative technologies to create an overall solution that benefits the business organization.

Dell EMC provides an integrated solution that spans multiple lines of business including traditional Backup/Recovery, protection of virtual environments, Backup to Archive, pure long-term Archive, supplemental disaster recovery, litigation hold, as well as primary storage for modern application development. By combining the technical capabilities of the purpose-built backup appliance Dell EMC™ Data Domain™ with the infinite scalability of the private cloud object store known as Dell EMC ECS, Dell EMC is able to deliver a reliable storage infrastructure which provides all of these business benefits and avoids the confusion and management headaches of an environment arranged in vertical data silos.

The primary value of this architecture is the ability to extend the usable life of the active tier of a Data Domain backup target by moving aged unique data segments on to a secure and private ECS Cloud Tier. This provides a recoverable long term archival content store accessible by the Data Domain which enforces the retention policies of the business.
1 Introduction

Long-term data retention requirements continue to grow throughout all industries. Unstructured data, whether active or archive continues to accumulate at faster rates, and must be kept in readily accessible formats. In order to keep data protection tools from getting overwhelmed by the enormous capacity requirements generated in today’s data centers, technologies which enable data to be tiered from primary backup to secondary LTR/Archive are becoming more attractive.

This white paper is intended for architects and administrators interested in learning how Data Domain Cloud Tier technology integrates with an ECS system (on premises or hosted private cloud) to provide a massively scalable architecture. By leveraging the capabilities of both platforms, IT administrators and architects can continue the path of consolidating critical backup processes, protecting complex environments mixed with unstructured data, database engines, and virtual environments, while at the same time providing the ability to meet long-term retention SLAs as required by the business. All of this is provided while not falling prey to the fallible nature of tape storage, or the risks of moving data offsite.

1.1 Data Domain overview

Data Domain is a purpose-built backup appliance providing streaming deduplication. Data Domain is able to ingest, at full network speeds, from multiple backup sources while providing proven storage efficiency. As the product has continued to develop, Data Domain has been structured to take advantage of tiered data storage technologies, such as very large multi-terabyte SATA drive trays, or SSD-enabled fast ingest trays. This capability to tier data has been enhanced to utilize cloud archive technologies to enable more efficient long-term archive retention.

1.2 ECS overview

ECS is a true scale-out object storage platform designed around future needs and use cases of an ever expanding cloud enabled data center. The ECS platform is based around the idea of object containers that can be created as an endless pool and scaled out across an expandable pool of storage nodes. Storage nodes take advantage of the industry leading dense storage technologies which enables petabytes of storage for on premise private or hybrid cloud storage. Data is stored as objects and accessed through API calls across multiple protocols including S3, Swift, and NFS among others. Because of its unique architecture, ECS can be utilized not only as a development platform for next generation mobile applications, but as an efficient long-term storage archive.

1.3 Benefits of a combined solution

Combining Data Domain and ECS capabilities provides a way for businesses to leverage private or hybrid cloud technologies in order to control their active backup storage tier costs by extending their long term archive storage system abilities. Businesses who maintain a retention requirement of long term backup storage often find that the sheer volume of data forces them to scale-up their Data Domain backup target units. This has the effect of driving up the costs of performance oriented backup target to meet the needs of long term storage.

At the same time, as the number of data sources increase within a business due to the explosion of new apps and mobile technologies, the need for more active tier backup targets also increases in order to handle the high concurrency of ever-shrinking backup windows. A solution that merges the speed of Data Domain active tier backup space with the near infinite scale-out capability of ECS long term storage meets these business needs.
2 Cloud Tier solution overview

At a high level, Data Domain continues to be the industry leading purpose based deduplication target which is able to receive inbound backup data streams, deduplicate and compress data into unique segments, and store that data efficiently to enable secure and rapid restore of critical operational data. Building on that, Data Domain becomes an S3 client to ECS using built in S3 API tools in the Data Domain UI to actively tier data to ECS for longer term archive retention.

2.1 ECS and Data Domain code integration

Going beyond simple S3 client capability, Data Domain utilizes proprietary S3 extensions to enable a larger 4MB object upload size as well as more granular garbage collection functionality. The larger object upload size increases the overall transaction efficiency for ECS storage. This represents as high as 16X reduction in transactions costs because the overall object count goes down for off-premise ECS compared with the 1MB limit of AWS.

2.1.1 Integration aspects of ECS

ECS brings to the table S3 extensions which provide copy forward capability to Data Domain’s built in garbage cleaning mechanisms. Competing S3 storage targets requires data tagged for deletion to be 100% garbage. In other words, there is no way to clean out data unless there is 100% garbage resident in the object. With a dedupe engine as powerful as Data Domain, a single object can be packed with a large number of independent unique segments which may be linked across many source files. Having to wait until the entire stored object is 100% object can therefore lead to extensive host overhead.

With ECS copy forward, Data Domain can delete out old data from an existing chunk and move the remaining valid object fragments forward into a new storage chunk without having to pull it back over the wire. This leads to far greater storage efficiency and cost control.

2.1.2 Integration aspects of Data Domain

The larger object upload size increases the overall transaction efficiency for ECS storage. This represents as high as 16X reduction in transactions costs because the overall object count goes down for off-premise ECS compared with the 1MB limit of AWS. From an ECS perspective, the larger object size plays to ECS strengths because of the reduced trips to disk and the reduced amount of metadata in relation to active customer data stored.

Best of all, the customer does not have to do anything to gain any of these benefits when using Data Domain OS 6.1.2 and ECS 3.2.1 (with recommended load balancing technology). It all turns on automatically because the two technologies have been actively developed to work in concert.

2.2 Overall data protection workflow

The overall workflow may contain many component technologies depending upon customer choices and preferences. For the purposes of this paper, a hypothetical workflow will be used in order to portray the flow of data from one system to another. This workflow presumes the possibility of multiple sources of data that need to be protected. The overall solution allows for multiple backup technologies which may be working concurrently in a customer environment. For example, one backup system does not preclude another. NetWorker is used in order to take advantage of its policy management interface for the data movement ability of Data Domain.
2.3 Data Domain Cloud Tier mechanism

2.3.1 Cloud Units and MTree organization

Data Domain has a logical extension to its file system and MTree organization which allows a data movement policy to be applied to aging backup content. This data movement policy utilizes a new feature of Data Domain called a Cloud Unit. A cloud unit is a connector to an S3 provider such as Virtustream Storage Cloud, Amazon Web Services S3, or in this case Dell EMC ECS S3.

The result is a Data Domain file system which is represented as an Active Tier and a Cloud tier with a policy engine that moves backup data to the cloud tier when it reaches a minimum data age as stipulated in the policy setup dialogue. Metadata is stored on a physical cloud tier within the Data Domain to facilitate ease of file lookup and recall. Once the logical Cloud Unit is created, Data Domain will place a copy of the meta-data stored on the cloud tier into the ECS Bucket via the Cloud Unit.
Cloud Tier solution overview

![Data Domain System Manager](image)

**Figure 3** Data Domain filesystem display
3 **Cloud Tier resiliency**

Part of the business value of a combined Data Domain and ECS Cloud Tier solution is added levels of system protection and overall system resiliency. There are several potential system failure scenarios where a strongly resilient architecture helps preserve business data availability and provide a clear path to restoring full system functionality.

3.1 **Single-site Cloud Tier resiliency**

A single Data Domain system is resilient against many types of common hardware failures. When the entire system or data center is lost, however, the cloud tier namespace is destroyed along with it. Without the namespace, the data in the cloud tier data is not easily or quickly recoverable. For this reason, the chosen deployment topologies for cloud tier solutions will determine the overall resiliency and recoverability of the data tiered to the cloud. The following section reviews the deployment options and associated recovery capabilities for Data Domain with Cloud Tier.

![Cloud Tier resiliency diagram]

Data Domain offers the following recovery capabilities for single data domain system:

3.1.1 **Scenario 1: controller failure resiliency**

Data Domain controller failures do not lead to the loss of cloud tier data.

![CT Controller failure resiliency diagram]
Cloud Tier resiliency

If a Data Domain controller fails or needs to be replaced, a new controller can be added to the system using the “Head Swap” operation. All Active and cloud tier operations can be resumed after the “Head Swap” operation and reconfiguration occurs.

For some Data Domain models, resiliency against controller loss can be added via the High Availability option. With HA, the Data Domain system can withstand the loss of a controller with minimal operational disruption.

3.1.2 Scenario 2: disk failure resiliency
Data Domain single and dual drive failures do not lead to the loss of cloud tier data.

![CT Disk failure resiliency](image)

Figure 6  CT Disk failure resiliency
Each disk shelf on the DD device is protected by RAID 6 and can respectively lose 2 disk drives at a time and maintain all functions and operations.

3.1.3 Scenario 3: metadata disk shelves resiliency
Data Domain cloud tier metadata disk and shelf loss does not lead to the loss of cloud tier data.

![CT Metadata disk shelves resiliency](image)

Figure 7  CT Metadata disk shelves resiliency
In the event of a loss to one or more disk shelves containing cloud tier metadata, the disk shelf replacement process (performed by Dell EMC support services) can also recover metadata back from the cloud storage provider to replacement disks. The original Data Domain appliance is then able to resume cloud tier operations without loss of cloud tier data or the associated metadata.
3.1.4 Scenario 4: single-site Cloud Tier site loss

In the extremely rare circumstance a Data Domain unit is destroyed (i.e. due to flood, fire, natural disaster), the corresponding cloud tier namespace is also destroyed. As of DDOS release 6.0.1, the Namespace information is copied out to the ECS/Cloud target. In the event of a total site failure of a Data Domain unit, such as flood, fire, natural disaster, it is still possible to recover the entire cloud tier once a replacement Data Domain unit has been procured and provisioned. Cloud tier data must be recovered first before the restoration of Active Tier data.
4 Cloud Tier replication considerations

An ECS and Data Domain Cloud Tier solution supports a variety of replication architectures which may be employed to meet various customer business objectives. Each platform has been designed as a standalone solution for specific use cases and therefore has built-in replication capabilities that meet those specific use case needs. Data Domain features MTree replication and also support managed file replication (MFR). ECS provides Active/Active geo-disbursed multisite replication across up to 8 sites. In addition, both technologies have been actively developed to work together efficiently to provide a multi-tiered purpose built backup target and archive platform.

However, with such a significant selection of replication features and choices, care must be taken to architect the best choice of features in order to meet customer driven restore/recovery SLAs and business needs. For instance, there is the ability to provide not only failover from site to site, but also split site redirection of Data Domain from one site to another. The value in this is highly flexible replication reconfiguration, done very rapidly, but results in a storage cost of 4X copies of data on ECS and 2 more copies on Data Domain. Speed and availability of data always come at a cost of greater hardware/disk space consumption, and more moderate resource consumption always comes with less aggressive restore/recovery goals. The business must be the driving factor in determining the best mix of features and costs for their individual situations.

4.1 Factors of replication

The first consideration of replication is whether MFR (Data Domain managed file replication) is being used, or if Data Domain MTree replication will be the primary method. In each case, it is important to leverage Data Domain snapshot technology to limit growth on the primary Data Domain. It is also critical to obtain the customer definition of active tier (sometimes known as operational data), and what is deemed to be long term retention data. Having these data sets defined will help establish what types of replication to employ and what the tier policies will used to move data between Data Domain and ECS.

Depending on the customer’s failover needs, it may or may not be advisable to employ ECS replication. In older versions of DDOS and ECS, replication between ECS was not recommended. However, with more recent releases, replication between sites can occur both at the Data Domain to Data Domain level as well as ECS to ECS level.

In general, the workload is divided into Operational Data (active tier), and long term retention (archive tier). Operational data is always present on Data Domain to allow for immediate restore of the previous backup. Long term retention data is tiered to any combination of single or replicated ECS, or even a subscribed ECS service such as ECS Dedicated Cloud. Additionally, there can be many Data Domain units which tier data to any of these ECS solutions.

A summary list of primary replication factors to consider would then include (but not be limited to)

- MFR (managed file replication)
- MTree replication
- Data Domain snapshots/scripted snapshots
- Definition of Active Tier and long-term-retention tier data
- Data Domain Cloud Tier data movement policy engine
- Type of ECS replication group
4.2 Simple replication example

Here is a basic replication example that is reminiscent of the older industry tape-out methodology wherein two Data Domains replicate 45–90 days of operational backup copies. Either one of the Data Domains can be assigned the job of archiving out long-term retention data. Since backup software is involved, the example here represents the MFR approach to managed backup replication, snapshots, and long term retention.

Figure 8 Data Domain MFR replication with single LTR archival path to ECS
General best practices

Always check with the latest Systems Administration Guide to verify the latest support platforms for a Cloud Tier deployment. The current release is: Data Domain Operating System 6.0 Administration Guide.

- For ECS 3.0 and Data Domain 6.0.x code levels, Data Domain Cloud Tier interacts with a standalone ECS VDC Namespace for each physical location. Multi-site replication groups are not recommended. Do not use a geo-replicated bucket unless absolutely necessary (i.e., use a local replication group with one VDC) Use a local, standalone replication group and associated namespace to create the target buckets for Data Domain Cloud Tier. It is recommended to utilize Data Domain replication to achieve multi-site data redundancy.

- For ECS 3.1 and Data Domain 6.0.x code levels, geo-replicated ECS namespaces may be used to replicate the LTR tier of archive data. Data Domain replication is still required, at the same time, to provide redundancy for active tier operational data. Utilizing ECS federation in this way provides recoverability in the case of full site failure, as well as failure of either Data Domain or ECS independently for the same site. This will result in a total of 4 copies of the same data being housed in ECS. It will also produce an accordingly similar increase in network traffic to accommodate the data replication. This deployment model is supported, but it is not a recommended best practice and should only be used when the customer SLAs required this level of failover recoverability and have a full understanding of the associated storage and network costs.

- A Data Domain cloud unit cannot be temporarily redirected to the secondary ECS during a TSO if the ECS VDCs share a replication group. This is not supported. The best practice would be to disable the cloud unit at the primary site data domain until the TSO can be resolved. Then the primary site Data Domain can re-enable its cloud unit again.

- For ECS 3.1-current version and Data Domain 6.1.X, both full site disaster (Both ECS and Data Domain are removed) and ECS PSO with Data Domain redirect to the secondary ECS is supported. However, there is a significant cost in terms of consumed ECS storage because a total of 4 copies of the same data will reside on ECS. There will also be an associated network cost required to facilitate the increase of replicated data copies.

- Data Domain target bucket names are assigned by the Data Domain during the Cloud Tier configuration steps. These cannot be changed. Use Dell customer service engineering to assist with migration to multisite replication groups on supported code levels or migrations to other Data Domain replacement targets.

- ADO (Access During Outage) refers to eventual consistency of data. For example, if the primary site fails (bucket owned site) and the data is replicated (w/ADO enabled) to the secondary site, the data at the secondary site will be accessible, however, it may not be the latest, most up to date copy. When a replicated bucket does not have ADO enabled, this implies a strong consistency model whereby the data will not be accessible at the secondary site because it cannot guarantee that the local copy of data is the latest, most up to date copy. The only way to get ECS data access at the surviving site in a strong consistency model is to either wait for the primary (bucket owning site) to come back up, or execute a PSO event.

- ADO also provides control over the balance between performance SLAs and general data availability during an outage of an entire site in a multi-site configuration. If using 3.0 ECS code level and standalone local replication group target, disable the ‘Access During Outage’ option.

- An ECS namespace user must be created via the ECS management UI and assigned to the Data Domain Cloud Tier configuration meaning that user will be assigned to the ECS namespace to be used by the Data Domain. Data Domain will log into the ECS namespace with this user, so this user name will be used during the Data Domain Cloud Tier configuration. It is recommended that this user be dedicated to cloud tier access and not used to access other data written to the namespace by other means.
General best practices

- For Data Domain Cloud Tier to ECS, a load balancer is required. Either hardware or software load balancing technology may be used. In other general usages, use of a load balancer is highly recommended for access to ECS Nodes. DNS round robin is not an acceptable load balancing method for Data Domain/ECS Cloud Tier.

- Data Domain Cloud Tier should resolve to the load balancer. The load balancer should be capable of completing an SSL connection request from the Data Domain Cloud Tier instance, thereby providing a termination point for the SSL encryption. Both proprietary and opensource solutions such as HAProxy work very well and have been documented in the ECS TME document archive.

- DNS entries should resolve to the recommended load balancer appliance in order to assist proper configuration with SSL encrypted traffic and the installation of CA certificates, private or otherwise. Data Domain should be configured to use a domain host name rather than a hardcoded IP address in the cloud tier cloud unit.

- For DDOS6.0.x code level, Data Domain rapidly writes large amounts of small objects to ECS. In order to improve the efficiency of data tiering activity, and to help the target ECS unit complete its commit to disk and indexing as quickly as possible, it is recommended to tune ECS 3.0 memory size. Professional services can disable CAS-related data migration services (Dell EMC Centera™ software) which may likely not be necessary in a Data Domain/ECS environment. The freed memory can then be assigned to the blob services module of ECS. Professional services can then modify the MOTD (message of the day) for all nodes in the cluster to make note that a modification in memory assignment has been applied. Message of the day modification is recommended in order to provide visibility of the transformation services being disabled which may generate a 'DTs unready' warning message.

- Both ECS 3.0 and 3.1 code levels should have storage patch 19440 applied by professional services to ensure Data Domain file system stability when reading ECS index information. Starting with ECS code level 3.1.0.3, this patch is included and will be included in ECS 3.2 as well. The patch helps insure that no stale data is returned to Data Domain.
6 Deployment and configuration

Before beginning the process of setting up the actual components of a Cloud Tier solution on Data Domain, it is necessary to have a functioning ECS target tier that is configured to receive data moved by Data Domain. Once the ECS components are ready, and a load balancer is in place, the Data Domain can be configured with a new cloud tier layer.

6.1 ECS system configuration

ECS setup for Data Domain Cloud Tier is fairly straightforward and consistent with other S3 application requirements for archive on ECS. ECS requires a storage pool, virtual data center, replication group, namespace and an object user with a S3 password. If these are not already created, follow these instructions to create them.

Log in the ECS user interface (UI) to begin necessary configurations.

6.1.1 Storage pools

Storage pools are used to group nodes and their associated disks within a single site. If physical separation is required for different data or business units, multiple storage pools can be created within the same site. Data will be distributed across nodes within a storage pool. As an example, if you had 16 nodes and you wanted to physically isolate sales data from engineering data, providing more space for engineering data, you would setup two storage pools. You could assign nodes 1 – 4 to the sales storage pool and nodes 5 – 16 to the engineering storage pool.

If a storage pool containing the nodes you want to have the cloud tier data written to is not already created, select New Storage Pool.

![Create a New Storage Pool](image)

Figure 9  Create a New Storage Pool

Give the storage pool a name and from the available nodes, click on the + icon next to the nodes you would like to be used to store the cloud tier data. Storage pools require a minimum of four nodes. Optionally you can enable cold storage which uses an erasure coding with higher efficiency and requires a minimum of six nodes. See the ECS Systems Administration Guide for more details on cold storage and erasure coding schemes.
6.1.2 Virtual data center

A virtual data centers (VDC) is a logical construct that contains a collection of ECS nodes that are managed as a single unit; typically a VDC contains all ECS nodes within a single site.

If a VDC containing the IP addresses for the nodes you want to have the cloud tier data written to is not already created, select New Virtual Data Center.

Provide the following:

- A name for the virtual data center.
- Replication and management endpoints. The endpoints should contain a comma separated listing of each node’s IP address. This can either be the node’s public IP address or if a separate replication or management network is configured this will be that IP addresses for each node. If network separation is not configured, both replication and management endpoints will be the same.
- Select to generate a key.

If you wish to set up multiple sites, refer to the ECS Systems Administration Guide for details on adding additional VDCs to a federation. As a caution, Data Domain Cloud Tier supports only standalone VDCs for cloud unit storage on ECS 3.0 code level. More recent combinations of Data Domain and ECS code levels
support replication at the ECS level. From this same UI, it is possible to add other ECS VDCs to this ECS, creating a federation.

![New Virtual Data Center](image1)

**Figure 12  Configure New Virtual Data Center**

### 6.1.3 Replication group

A replication group is a logical construct that defines if data within a storage pool is only written locally or if it can be replicated to other sites or virtual data centers.

If a replication group is not configured, select **New Replication Group**.

![Replication Group Management](image2)

**Figure 13  Select New Replication Group**
Perform the following:

1. Give the replication group a name.
2. Add the appropriate local virtual data centers and storage pools.

See the [ECS Systems Administration Guide](#) for more details on replication groups.

![Configure replication group](image)

**Figure 14  Configure replication group**

### 6.1.4 Namespace

A namespace is a logical construct that provides tenant isolation. Users from one namespace can only access objects within their own namespace, they cannot access objects that reside in another namespace. It is recommended to create a namespace that is dedicated to cloud tier usage.

If a namespace is not configured for the cloud tier data, select **New Namespace**.

![Select New Namespace](image)

**Figure 15  Select New Namespace**

At a minimum, you will have to provide a name for the namespace and a replication group. The replication group will determine if the cloud tier data sent to this namespace will be replicated to other ECS sites or not.
6.1.5 Object users

Object users are end-users of the ECS object store. Objects users are defined by a username and a secret key (like a password) that they use to gain read write access to the ECS namespace. You will need to create an object user that will be used by the cloud tier to read and write data to the ECS object store. It is recommended that this user be dedicated to cloud tier access and not used to access other data written to the namespace by other means.

If an object user with S3 password is not configured for the namespace the cloud tier data will be written to, select New Object User.
Perform the following:

1. Give the object user a name.
2. Provide it a namespace that it will be given permission to use (a dropdown list will be provided in the field)
3. Select Next to Add Passwords
4. Select Generate & Add S3 Password
5. Keep a copy of the user name and the S3 password that is generated, you will need this to configure Cloud Unit on the Data Domain system.
6.2 Data Domain system

For a new Data Domain, it is necessary to create the overall file system as shown below.

```
sysadmin@ecstmeddve# filesystem status
The filesystem doesn't exist.
sysadmin@ecstmeddve# filesystem create
A filesystem of approximate size 447.20 GiB will be created.
   Do you want to continue? (yes/no) [yes]: yes
Ok, continuing.

This will take 5 - 10 minutes.

Provisioning storage...
#####################################################################[100%]

Initializing filesystem...
#####################################################################[100%]
```

Figure 19  DD create file system CLI

Upon completion of the filesystem creation, a notice is given that the newly initialed system needs to be enabled. This can be done either through the command line or through the web-based UI. These steps are common to all Data Domain systems.

```
You now have a freshly initialized filesystem.
Enable the filesystem using ‘filesystem enable’.

sysadmin@ecstmeddve#
sysadmin@ecstmeddve# filesystem enable
```

Figure 20  DD enabling file system after create
Alternately, perform this procedure from the UI.

![EMC Data Domain System Manager](image)

**Figure 21** DD enable filesystem UI

### 6.2.1 License for Cloud Tier


### 6.2.2 DNS entries for all components including load balancer

While all systems represented in this workflow can be configured via direct hardcoded IP addresses, it is advisable that all components have appropriate A level and C level DNS entries for use in the configuration dialogues. DNS entries should include the recommended load balancer appliance, in this case HAProxy, in order to assist proper configuration with SSL encrypted traffic and the installation of CA certificates, private or otherwise. Refer to the HAProxy guide [http://www.emc.com/collateral/white-paper/h15785-ecs-haproxy-load-balancer-deploy-ref.pdf](http://www.emc.com/collateral/white-paper/h15785-ecs-haproxy-load-balancer-deploy-ref.pdf) for detail on load balancer configurations. Use of a load balancer is a requirement for Data Domain access to ECS Nodes.

### 6.2.3 Create Cloud Tier device

Before creating the Data Domain cloud unit (the logical S3 policy container), it is necessary to add dedicated storage as a tier to the Data Domain to be used for managing the metadata associated with each object moved to cloud storage. For data integrity purposes, this metadata is also mirrored to the target cloud storage. Adding the cloud tier storage will disable the filesystem, meaning no other read/write activity may occur while this process is running.

#### 6.2.3.1 View disk devices available

It may be helpful to review which disk devices are available and verify that the Data Domain is able to see the devices which may be used. At the command line run the ‘disk show hardware’ command to get a listing of devices. In this example, all the disk devices are presented to a virtual edition Data Domain. However, we can still see the Capacity and corresponding Disk name for the devices we can use to build the cloud tier.
6.2.3.2 Building the hardware layer of Cloud Tier

Begin building the hardware layer Cloud Tier from the Data Domain **Hardware > Storage** management section.

The Addable Storage wizard appears which allows for the selection of storage devices to be selected for use in the cloud tier. Based on whether a physical or virtual Data Domain appliance is being used as the backup target, the storage device refers to either physically configured disk groups or as mapped virtual drives. By checking the box next to a device, it is now possible to click the ‘Add to Tier’ button and designate that device for use in the cloud tier.
Deployment and configuration

6.2.4 Enable Cloud Tier: disable filesystem first

Once the physical Cloud Tier device has been added to the system, the Data Domain unit must be told that it may use the available resources by enabling the cloud capability. This can be done via command line as shown here, or by using the UI under the Data Management > Filesystem management screen by clicking the Enable Cloud Tier link.

```
sysadmin@ecstmeddve# cloud status
Cloud feature is disabled.
sysadmin@ecstmeddve# cloud enable
    Do you want to enable encryption? (yes|no) [yes]: yes
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
sysadmin@ecstmeddve#
```

Figure 24  DDCT add storage to tier

Figure 25  CLI enable and encryption on Cloud Tier
Enable Cloud Tier UI

6.2.5 Import SSL cert from load balancer

Setting up the Data Domain to access ECS over SSL requires a valid CA certificate to be imported into Data Domain. This is a critical step where mistakes often occur that prevent completion of Cloud Tier set up.

If your organization is not using a public Certificate Authority service, it may be necessary to internally generate a CA certificate in order to enable an SSL connection from the Data Domain unit to the load balancer which handles traffic for the ECS. In most cases where an internal CA is being used, it is important to install the *root* CA, not the server certificate installed on the LB. Even if using a public CA, it is still likely that installing the root CA is the best way to go. For purely private networks, such as offsite DR or test locations which may be isolated from public DNS and CA servers, it is possible to create a self-signed certificate which can be imported into the Data Domain for use in building the SSL tunnel.

A utility is provided to help extract the correct root CA which can be used for Data Domain / ECS Cloud Tier setup. The authors of this tool explain:

“When dealing with SSL servers inside enterprises, you will see a lot of self-signed certificates and internal CAs. Sometimes it's difficult for users to understand what certificate is required to properly trust the server. This utility will connect to the server and analyze the certificate chain presented and identify the root certificate needed to trust the server. The root certificate (if found) will then be stored in a file for later use. If the root certificate cannot be found, the DN (Distinguished Name) of the certificate will be printed so the user can locate the correct root certificate elsewhere (usually an enterprise CA).

The application will also analyze the chain presented from the server and identify any issues it finds in the chain, e.g. the chain's certificates are not in the correct order.

Finally, there is also an option to supply a root certificate to validate the chain for situations where Java does not have the root CA certificate installed by default.”

The CA certificate utility can be found at this URL: [https://github.com/EMCECS/ssl-certificate-extractor](https://github.com/EMCECS/ssl-certificate-extractor)
For Data Domain Cloud Tier implementations, it is recommended to terminate the SSL connection at the load balancer for improved performance as well as some other benefits. There is a specific concern connected with Data Domain cloud units that makes having a local load balancer a good idea. During creation of the cloud unit on Data Domain, DDOS sets up an SSL tunnel to the specified end point and authenticates with a CA certificate. If the end point is a single node on the ECS cluster, all is well until that node crashes and must be replaced. Suddenly, the cloud unit, with its hard coded IP address and CA certificate, must be destroyed and created from scratch manually to the next node in the cluster. When you create a new cloud unit, because the old one has been destroyed, 3 new empty buckets will be created and the DD box starts from the beginning of time repopulating the Cloud Tier from its own local cache of unique segments tagged for archive. Additionally, there is nothing to tell the ECS unit to discard the original three buckets with all those data objects within. This results in duplicate data on the ECS. There currently is no easy way to delete all those objects in the original 3 buckets so that you can remove them without creating a custom S3 app which queries each object and issues an object delete command. Following that step, there is the time waiting for garbage collection to kick in and clean up everything deleted in order to recapture that capacity.

Once a self-signed CA certificate file has been generated in PEM (x509 with Subject Alternative Name entries) format, it can be imported into Data Domain as shown here.

![Manage Certificates for Cloud](image)

Figure 27  Manually add trusted certificate of authority

Now that the physical layer of Cloud Tier storage has been added to the Data Domain, and SSL encryption to the ECS target has been addressed, it is time to create the logical Cloud Unit which will provide a means for Data Domain to move marked files from the active tier to the ECS for long term storage. It should be noted here that Data Domain does not move entire files to any tier, either physical or cloud. The nature of Data Domain deduplication breaks file backup data down into unique (deduplicated) and compressed segments. It is these segments which get stored and moved from tier to tier. Only unique segments get moved up to cloud storage which may or may not comprise complete files. The net result is the gaining of greater storage efficiency from both the active tier and the Cloud Tier while providing a means for recalling or recovering the complete file upon demand.
6.2.6  **Begin logical Cloud Unit on Data Domain**

From the **Data Management > File System** interface, choose the **Cloud Units** tab on the right side of the UI.

![Filesystem Cloud Unit Tab](image)

Since no cloud units exist, click on the Add (green “plus” icon) to begin creation of a new cloud unit. The following dialogue appears.

![Create Cloud Unit UI with IP](image)

The first field requests an arbitrary name to be assigned to this cloud unit. This does not correlate to anything in DNS or to what may be configured on the ECS. It is only a logical name for the new unit that Data Domain will use for management purposes, or to announce to backup management software such as Networker.

Since this paper is focused on a Data Domain/ECS solution, it shows ECS in the dialogue as the choice of target.

The next fields are very important. They instruct the Data Domain as to how to access storage on the ECS unit. The ‘Access key’ is the object user as defined on the ECS management interface. Creation of the object user (‘access key’) and the S3 password (‘Secret Key’) on the target ECS system are necessary prior to beginning this step.
The endpoint field is the actual network connection point. This most likely will be the DNS resolvable URL of the load balancer. If connecting directly to an ECS cluster, it is possible to use the actual IP address of an ECS storage Node as an endpoint IP address. The endpoint must contain an indication of the port in standard form such as http://x.x.x.x:9020. Use port 9020 for regular S3 and port 9021 for encrypted traffic. It is highly recommended to use a registered DNS URL as the target for the cloud unit rather than an IP address. Additionally, it is also recommended that the DNS URL point to a load balancer configured in front of an ECS cluster.

![Edit Cloud Unit](image)

**Figure 30** Recommended Cloud Unit configuration with DNS URL pointing to load balancer

Also note that the HTTP Proxy Server field is not used when configuring a Cloud Unit to use the recommended Load Balancer as in this case with HAProxy. The load balancer is just an endpoint.

Viewing this configuration from the command line CLI on the Data Domain you can list the status of the cloud unit, and the detail of the cloud profile which confirms the Provider and Endpoint.

With Data Domain 6.1.2, Dell EMC has added a useful verification feature in the Edit Cloud Unit window. The reality of uploading critical long-term retention data to off-premise targets means there are occasional network outages, DNS issues, etc. Data Domain allows the admin to run a Verify Cloud Target routine which calls for user credentials and returns the status of the cloud account’s accessibility.
Cloud Verification

Figure 31 Verification of Cloud Vendor: Edit Cloud Unit

```bash
sysadmin@ecstmeddve# cloud unit list ddcloud
Name       Profile        Status
----------  -------------  -------
ddcloud    ddcloud_profile Active
```

```bash
sysadmin@ecstmeddve# cloud profile show all
Profile name: ddcloud_profile
  Provider: ECS
  Endpoint: http://os.ecstme.org
  Proxy host:
  Proxy port: 0
  Proxy user name:
```

Figure 32 CLI cloud unit configuration review

6.2.7 Summary of preparatory elements

Here are preparatory elements that were completed prior to this name based configuration:

- A-Level and C-Level DNS records created for the Load Balancer listening IP address. In this example the DNS records specifically reference an HAProxy load balancer as os.domain.org
- In most cases a root-CA certificate should be imported into Data Domain. In this case, a private self-signed CA certificate generated with Subject Alternative Names that included os.domain.org was generated and imported into Data Domain in order to enable usage of an SSL connection.
- Load balancer configuration that includes all of the ECS nodes as an available pool of storage resources
- An ECS Storage Pool and Replication group
- An ECS dedicated Namespace
- An ECS S3 object user and S3 secret key
During the Cloud Unit creation process, the Data Domain logs into the ECS cluster as the indicated ‘access key’ user and creates the buckets in the ECS Namespace in which it will place its cloud tiered data. There is no need for the system administrator to create the buckets in advance on the ECS. The image below shows the standalone Namespace, the buckets which were created (highlighted in yellow), and the user/owner which has been granted access. This Owner is the Data Domain ‘Access Key’ field that was specified in the Data Domain configuration dialogue.

![Bucket Management](image)

Figure 33  ECS view of buckets created by the Data Domain when configuring a Cloud Unit

The final result is displayed on the Data Domain UI in the **Data Management > Filesystem > Cloud Units** summary as shown here:

![Data Domain Cloud Unit summary](image)

Figure 34  Data Domain Cloud Unit summary after configuration
If the connection between Data Domain and its cloud target such as ECS is dropped for an extended time, the Cloud Unit may be marked as 'Disabled'. In order to reestablish connectivity to the target, it is necessary to work at the command line level over an SSH connection. Issue a 'filesys disable command' to bring the file system to a quiescent state. Once the filesystem is down, enter a 'cloud unit enable <cloud unit name>'. This will bring the cloud unit connection back online. Once the cloud unit is marked as Enabled, it is safe to re-enable the filesystem by entering 'filesys enable'.
Data policies: movement, retention, recall

This example includes some basic examples utilizing Networker as the backup application which also controls clone jobs through a policy engine that guide Data Movement policies on Data Domain. However, Data Movement can be controlled directly by Data Domain policy user interface in order to provide compatibility with other backup software tools.

7.1 Data movement policies

The frequency for running the Data Domain Cloud Tier policy can be controlled in terms of Daily, Weekly, or Monthly and at specific time of day. There is also the option of throttle control for how much resources this process will be able to consume. This is an important consideration as resources used for data movement to cloud will lessen resources available for primary backup data ingest operations. So, if your long term retention is defined as keeping (1) monthly backup for long term retention, then it is not necessary to run the data movement policy engine on a daily basis.

Under the Data Management > File System Summary screen, click the Settings icon in the upper right-hand corner to access the Data Movement UI.

Along with scheduling the frequency, the actual data movement policy must be created. The policy sets a minimum amount of time for which a file exists on the active tier before it ages enough to be moved to the cloud tier. The policy also determines how long the file may be kept out on the cloud tier.

All of this policy configuration is done at the MTree level. In this example below, the appropriate MTree has been selected from the Data Management section. Click add to add a Data Movement policy to the MTree.
the data movement policy is applied to the previously configured Cloud Unit by name. This can be selected in the cloud unit drop down box. If an external application, such as Networker is controlling the policy for the MTree, then it is not possible to modify the policy from the Data Domain via this UI.
The minimum “Older than” value that can be applied is 14 days. This is a built-in system parameter. Values greater than 14 days can be applied, but 14 days is the minimum. Once the minimum data age has been recognized, the Data Domain system will begin moving data onto the actual cloud tier.

Data Domain provides a CLI way to manually start up the data movement process and monitor it real-time. It uses the ‘data-movement start’ and ‘data-movement watch’ commands, once the user is logged into a Data Domain CLI via an SSH session. This view compares overall process time from a Data Domain perspective compared with actual over the wire network time.

Using the S3 browser, it is possible to see the buckets which Data Domain creates on ECS when it establishes its cloud account during configuration of the Cloud Unit. Three overall buckets are created which contain both the actual archive data content, as well as cloud tier restore information and Data Domain metadata which is helpful for enforcing retention policies, garbage cleaning, etc.
Data policies: movement, retention, recall

Figure 39  ECS view of Cloud Tier bucket assignments

7.1.2 Objects preserve DD filesystem path with S3 PUT request

A capture of an actual PUT statement from Data Domain provides some interesting detail. Here the full PATH is used as part of the object name. This reveals that this 4MB object is being put into the –d0 bucket with a location subvalue of ‘cset’. So ECS preserves the filesystem hierarchy present on Data Domain by containing that information in the object metadata as it is received from Data Domain. The conversation (Http PUT) ends with an ETag unique identifier being returned to the Data Domain so that a recall of the data (Http GET) can be issued if needed.

```
PUT /43c0ebf13fb81236-687c139ea30adlf-d0/cset/cont/00000000000000c0c/000000003c780000 HTTP/1.1
Host: 10.246.150.141
Accept: */*
User-Agent: APN/1.0 DellEMC/1.0 Data Domain/6.1
Date:Tue, 25 Sep 2018 22:00:48 GMT
Content-Range:4718592
x-emc-index-granularity:131072
Authorization: AWS dduser:OebDXUYdtPtyvRwqR4P4Fx4FxfI=
X-Client: 10.246.150.140

%...x<..............................%...y................@....G...2..5..n..wb.
.....2..5..n..wb....................%..."..........................x<.................U4..c6."...

<snip snip snip>

HTTP/1.1 200 OK
Date: Tue, 25 Sep 2018 22:00:48 GMT
Server: ViPR/1.0
x-amz-request-id: 0af696b5:165a692583f:10090:1116
x-amz-id-2: 59c334c96e61d876a8d91aa2951605ca3ac4ca8b49783d33b58efe43b2d1f6
ETag: "0a5c9319232bb0a1155238ff80b2a51d"
Last-Modified: Tue, 25 Sep 2018 22:00:48 GMT
```
Note: The original source data file names are not visible from the original backup source in the workflow. Specifically, this applies to client data names that Data Domain has already performed its deduplication process for, identified unique segments, compressed and encrypted those segments, and sent them to ECS.

7.1.3  Network verification of HTTP PUT from load balancer to ECS of 4MB

The ‘Content-Length’ field shows the data content of the entire conversation which may be comprised of hundreds of network packets. A Wireshark conversation summary provides a breakdown that confirms an overall send of 4MB object content. Here a packet capture summary from a load balancer to port 9020 an ECS node is 4091kB or roughly 4MB.

![Wireshark HTTP PUT conversation summary from Load Balancer to ECS node 182 port 9020](image)

7.1.4  Cloud Tier object size stored/verified on ECS

A diagnostic query of ECS object table for a Cloud Tier object provides detail and insight about the archive data stored on ECS by Data Domain. Highlighted in the example below, they system metadata for the object shows a size value of 4MB. Additionally, the entire source path name is captured in the ‘object-name’ key-pair. The system also identifies this object as being a member of the ‘dd-cloudtier’ namespace. This example is only a partial pull of the key-value pairs associated with this object, but illustrates how the data is represented at rest on ECS.

```plaintext
schemaType OBJECT_TABLE_KEY objectId 09a04b987e9c210bb48f084afdc714412a26c6c479a4b57edde759f4b1c7a12 type UPDATE
sequence 0
segment {
    segmentUMR {
        sysMd {
            key: "mtime"
            value: "1537908773434"
        }
        sysMd {
            key: "size"
            value: "4108288"
        }
        sysMd {
            key: "data-range"
            value: "CAAQgOD6AQ=="
        }
    }
}
```
Data policies: movement, retention, recall

```json
sysMd {
  key: "object-name"
  value: "/crstore/cont/0000000000000874/0000000000000000"
}
sysMd {
  key: "keypoolname"
  value: "43c0ebf13fb81236-687c139eaa30ad1f-d0"
}
sysMd {
  key: "namespace"
  value: "dd-cloudtier"
}
```

7.1.5 Verifying 4MB data write from Data Domain autosupport report

The Data Domain autosupport report, which can be generated at any time manually, or set up to be run automatically, captures a histogram of reads and writes. One of those categories give insight about the set of objects moved during the last data-movement sequence. In this example, a count of 2932 objects measured as greater than 4MB size were sent to ECS. Since previous generations of DDOS sent objects strictly at the 64KB size, the 4MB increased object size is proved out which yields much better write efficiency.

<table>
<thead>
<tr>
<th>CAL size histograms for context: /crstore.ddcloud UUID: 43c0ebf13fb81236-687c139eaa30ad1f</th>
<th>mean</th>
<th>std-dev</th>
<th>&lt;64KB</th>
<th>&lt;128KB</th>
<th>&lt;1MB</th>
<th>&lt;4MB</th>
<th>&lt;5MB</th>
<th>&gt;5MB</th>
<th>total</th>
<th>max</th>
<th>min</th>
</tr>
</thead>
<tbody>
<tr>
<td>W_size</td>
<td>3994.161KB</td>
<td>152.315KB</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2932</td>
<td>0</td>
<td>0</td>
<td>2936</td>
<td>4061.500</td>
<td>0.500</td>
</tr>
</tbody>
</table>

Figure 41  Data Domain autosupport with 4MB objects

7.2 Recall of file data

Data can be recalled from the cloud tier as needed either through the Backup Software interface such as Networker provides, or directly via the Data Domain UI as indicated below. This prevents the necessity of requiring Backup Administrators to perform these actions via the command line utilities.

![UI Data recall option](image-url)

Figure 42  UI Data recall option
The Cloud Unit may be used by multiple MTrees. Individual data movement policies are set for each MTree moving data to the Cloud Unit.

Recalling data requires a filename to be passed to the Data Domain unit either through the command line CLI or via the UI. The ‘Recall’ function specifically reconstructs the entire file from the cloud tier placing it in the active tier. At that point, the file may be selected for RESTORE by the original backup software or by manual restore.

Depending on which backup software is being used by the organization, the method of determining file path vary.

### 7.3 Networker (policy engine for data movement)

In this example, Networker was used as the primary backup engine as well as the management point for the cloud tier in order to illustrate the backup workflow shown here. Networker is not a necessary component as this same architecture will work with many backup engines.

![Networker data flow illustration](image)

**Figure 43** Networker data flow illustration

This example workflow begins with a group labeled ‘TestBackup’ that has a basic filesystem policy of ServerBackup. The backup data is directed to the Data Domain deduplication target named ecstemddve.ecstme.org. From that point, a clone job is defined which is responsible for copying unique data segments to the cloud tier device. In this dialogue it is possible to see that the source savset data on the active tier can be deleted once the clone is completed to the cloud tier thus providing the space savings on the active tier which is the primary value of leveraging cloud technology.

![Specify clone job to the DD Cloud Tier](image)

**Figure 44** Specify clone job to the DD Cloud Tier
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.

A.1 Related resources

- NetWorker_9.1_Data_Domain_Boost_Integration_Guide_.pdf
- Combined Data Domain ECS Release Notes
- Data Domain Operating System 6.1.x Administration Guide
- ECS with HAProxy Load Balancer Deployment Reference Guide
- ECS Overview and Architecture
- ECS 3.2.x Administrator’s Guide