Configuration and Deployment

Dell EMC Centera to Dell EMC ECS Technology Refresh with Veritas Enterprise Vault

Abstract

This document discusses performing a technology refresh of Dell EMC™ Centera™ and Veritas™ Enterprise Vault™ solutions to use Dell EMC ECS™ storage.

July 2019

Revisions

Date	Description
June 2017	Initial release
July 2019	Content refresh

Acknowledgements

This paper was produced by the Unstructured Technical Marketing Engineering and Solution Architects team.

Author: Paul McKeown

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. [7/9/2019] [Configuration and Deployment] [H15310.2]

Table of contents

Executive summary

This document discusses performing a technology refresh of Dell EMC™ Centera™ and Veritas™ Enterprise Vault™ solutions to use Dell EMC ECS™ storage.

This paper highlights the differences between Centera and ECS systems and discusses the following topics:

- The change in solution architecture
- Transformation and migration options
- How to configure a Vault Store after the technology refresh from Centera to ECS
- How to install and configure the various components

Audience

This document is intended for storage administrators performing a refresh of their Enterprise Vault based Centera assets to ECS storage. This guide assumes a high level of technical knowledge for the devices and technologies described.

Terminology

The abbreviations used in this document are summarized as follows:

CAS: Content Addressable Storage

EV: Veritas Enterprise Vault

PEA File: Process Entry Authorization file, used by application to authenticate to the ECS cluster

EV VAC: Enterprise Vault — Vault Administration Console

1 Solution architecture

Existing Dell EMC Centera systems can be refreshed by implementing a Dell EMC ECS solution and migrating Centera content to ECS storage. Once the content is migrated, the following steps make it accessible (read/delete only) to Veritas Enterprise Vault on the ECS system. All new data (writes) use a new EV partition, using the Dell EMC S3 Streamer driver created for the EV Vault Store.

The following provides an overview of the procedure:

- Create a new ECS Streamer Partition in the Vault Store.
  - This will mark the original Centera Vault Store partition as closed so all new ingest into the Vault Store will go to the new ECS Streamer partition.
  - Change the IP addresses/PEA file of the original Centera Vault Store partition to the ECS node IP addresses / PEA file.
- After a restart of the EV Storage Service this will then read any content in the Vault Store that was archived to the Centera Partition from the ECS

After this is accomplished, access to content in the Vault Store is as shown in Figure 1.

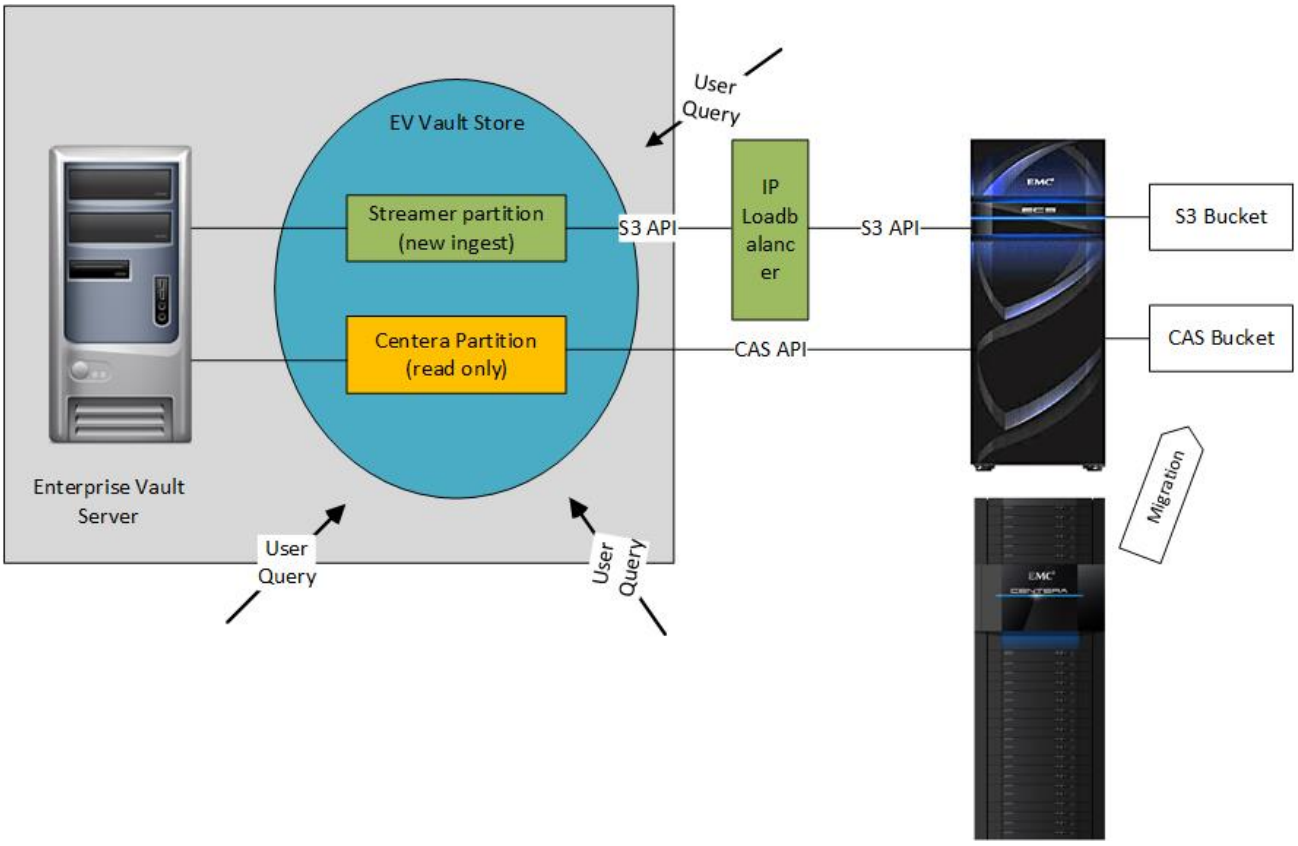


Figure 1 Vault Store access after migration

2 Supported environments

2.1 Veritas Enterprise Vault

Veritas has a detailed support matrix for all Veritas and third-party software and hardware components which is available at the following address:

https://www.veritas.com/support/en_US/article.TECH38537

2.2 Dell EMC ECS

Veritas EV supports ECS CAS access starting with ECS revision 2.2. Refer to the Veritas support matrix linked in section 2.1 to cross reference EV revisions with supported ECS revisions.

2.3 ECS retention support

All the Centera C-Clips that are migrated to an ECS CAS bucket that have retention periods or retention classes will retain their retention period and/or classes.

Dell EMC ECS Streamer driver support is detailed as follows:

- Supports the use of Retention Periods
- Does not support the extension of retention periods
- Does not support the use of ECS Retention Policies (the equivalent of Centera Retention Classes)

2.4 ECS CAS access

Veritas Enterprise Vault supports read and delete access to content migrated from Centera to an ECS CAS Partition. Veritas does not support ingest of new archive content to an ECS CAS Partition.

2.5 Centera Content Addressable Storage (CAS) SDK

Enterprise Vault ships with the revision of the Centera CAS SDK that it has been tested with. Customers should not use a different version of the Centera CAS SDK.

Table 1 Enterprise Vault CAS SDK usage

Enterprise Vault	Centera CAS SDK
10.0,10.0.1, 10.0.2	3.2P5 (3.2.705)
10.0.3, 10.0.4	3.3 (3.3.718)
11.0	3.3 (3.3.718)
12	3.3 (3.3.718)

3 Migration of CAS content

The migration of EV partitions from Centera to ECS will require careful planning with Dell EMC Professional Services. The following discussion is an overview of the process.

3.1 Migration steps

The steps to migrate CAS content from Centera to ECS are represented at a high level in Figure 2.

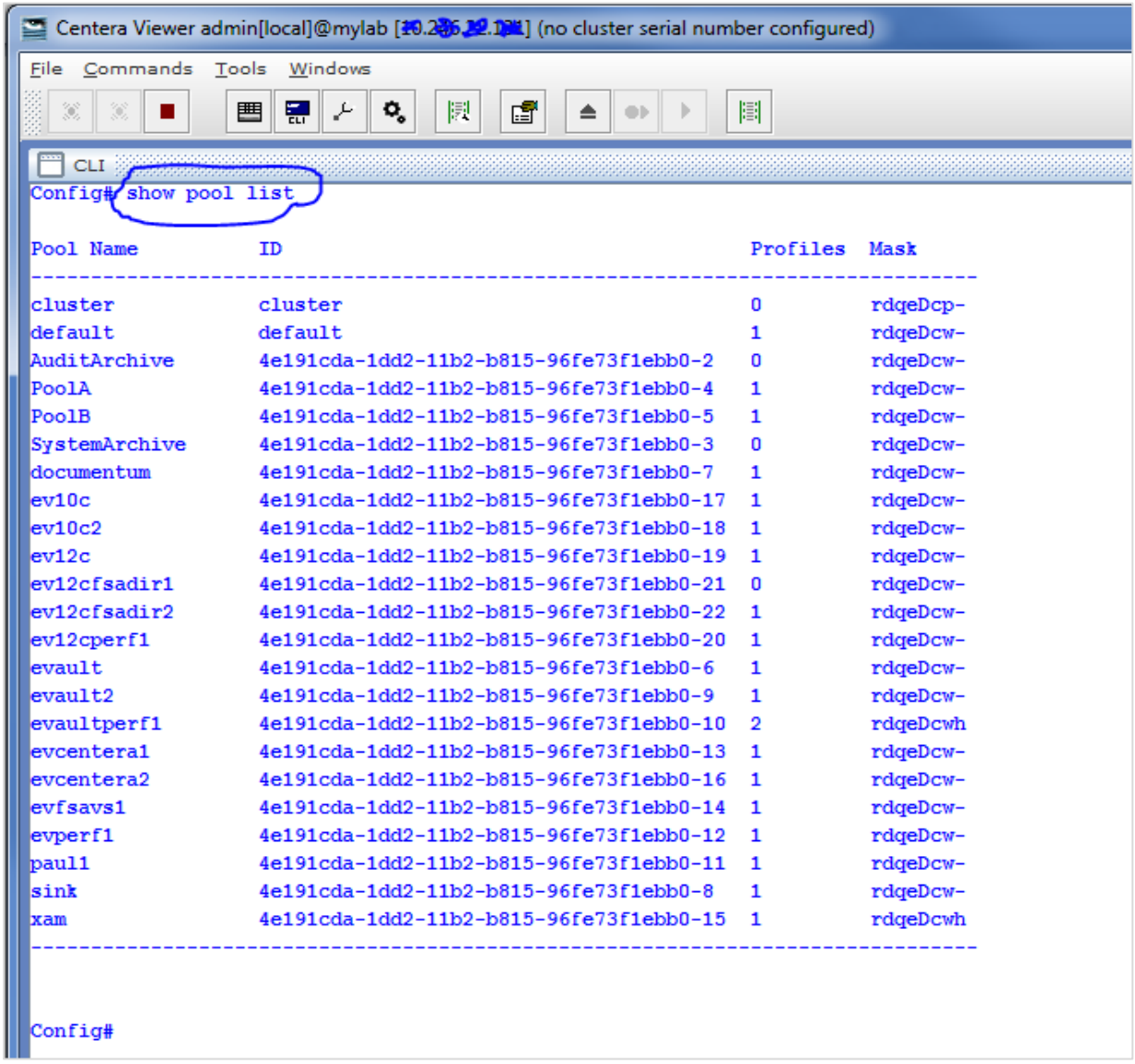
Figure 2 Migration steps

Customers should discuss their migration requirements with their Dell EMC sales team to engage with Dell EMC Professional Services for migration assistance.

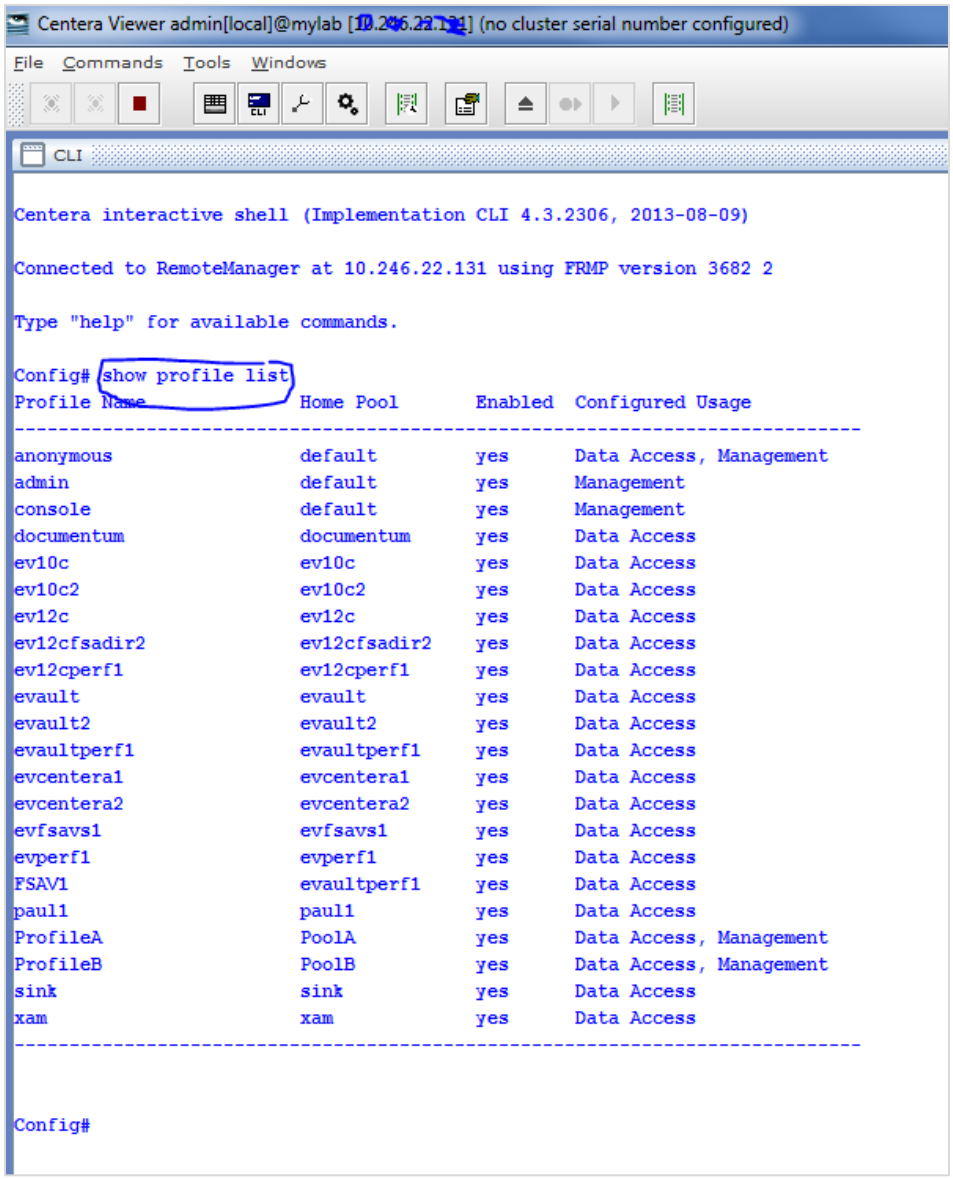
3.2 Identify Centera Application Profiles/Virtual Pools to migrate

Customers can identify which Virtual Pools exist on their Centera system by using the Centera Viewer tool to connect to the Centera cluster and list all Virtual Pools on the cluster.

The **show pool list** shows the Virtual Pools that exist on the Centera cluster.



The **show profile list** command will show all application profiles that are available on the cluster.



The **show profile detail** command can be used to confirm what Virtual Pool an Access Profile is configured to use.

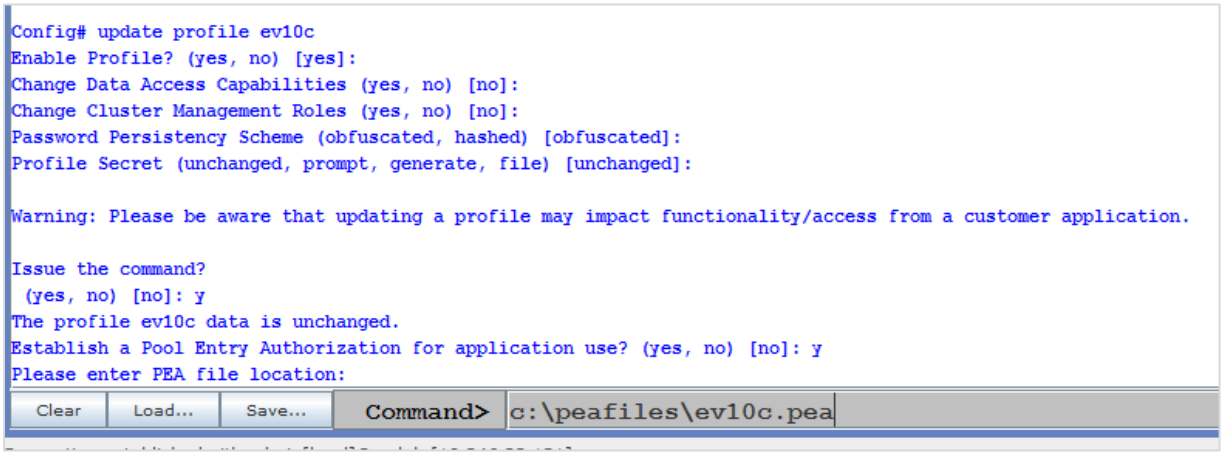
```
Config# show profile detail ev10c
Centera Profile Detail Report
-----------------------------------------------------
Generated on Tuesday, 19 April 2016 12:15:54 BST

Profile Name:                           ev10c
Profile Enabled:                        yes
Profile Secret Persistency Format:      obfuscated
IP Restrictions:                        <no restrictions>

Data Access Capabilities:
    Profile-metadata Capability:        off
    Home Pool:                          ev10c
    Profile Type:                       Access
    Cluster Mask:                       rdqe-cw-Ph

    Granted Rights in Application Pools:
    Pool Name                           Pool Mask   Granted     Effective
    ------------------------------------------------------------------------
    ev10c                               rdqeDcw-    rdqeDcw-    rdqe-cw-
    ------------------------------------------------------------------------

    Scratchpad Pool Mapping:            -
    Active Pool Mapping:                -

Cluster Management Roles:               none

Config#
```

3.3 Collect source PEA files

Typically, the storage administrator will have available the Process Entry Authorization files that will be required for the migration.

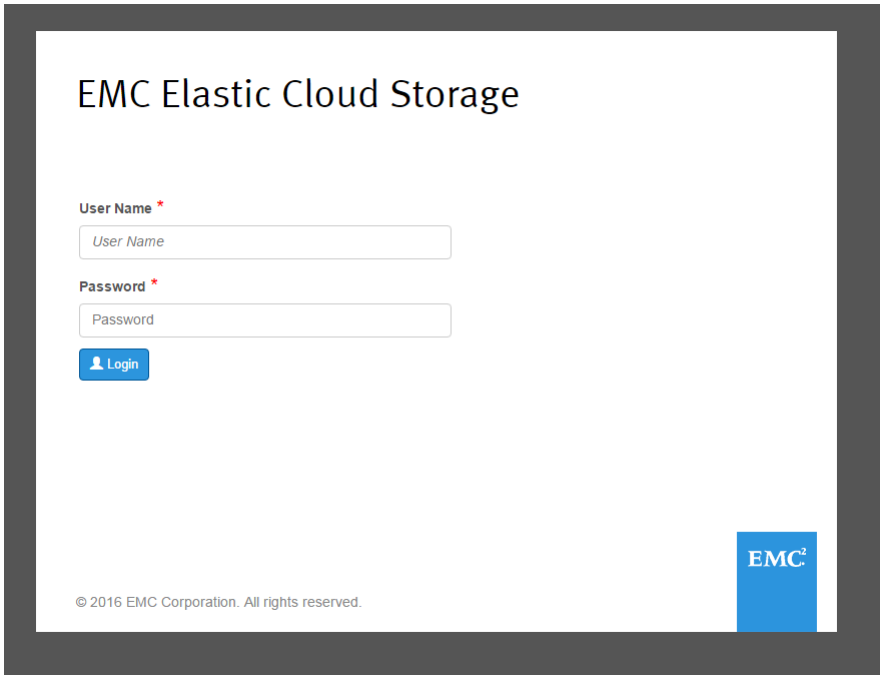
If for some reason these are not available, the Centera Viewer can be used to create them.

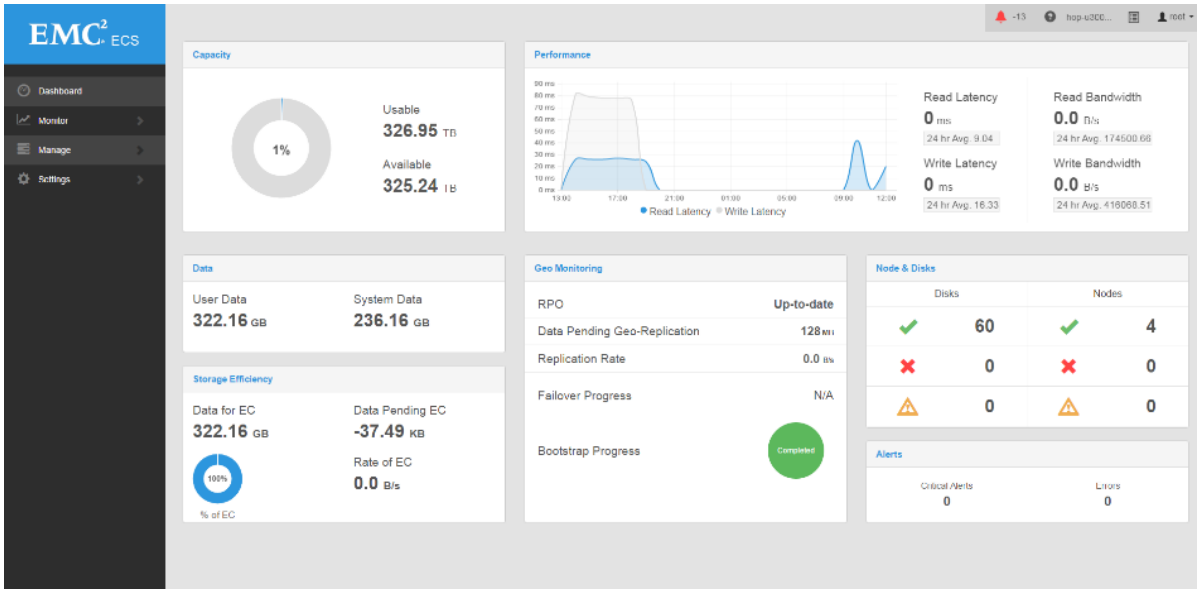
Use the **update profile** command to generate the PEA file. Take care not to alter any existing settings



3.4 Create ECS user(s) and bucket(s)

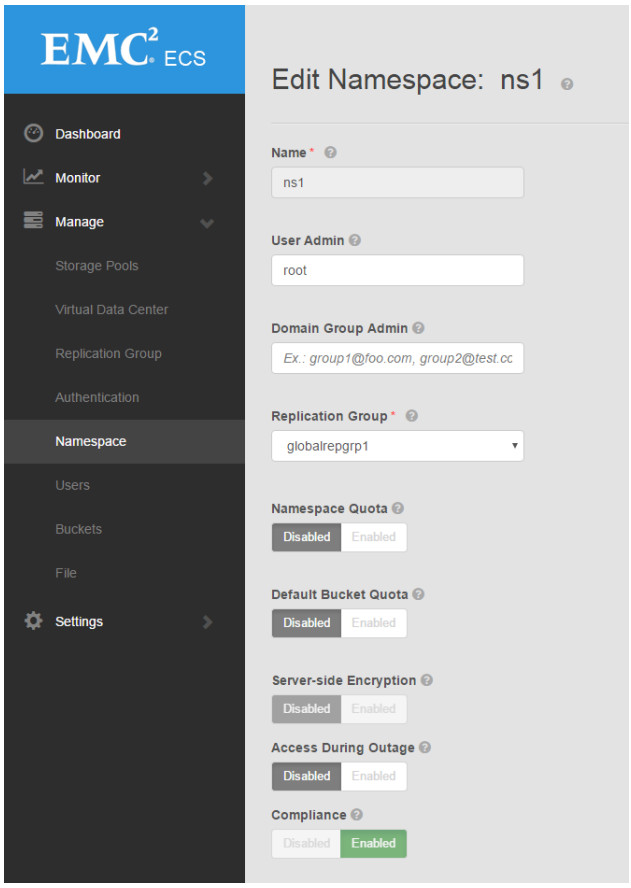
ECS Users can be created using the ECS Management GUI. Log in to the GUI by browsing https://ecsIpaddress as an admin user.





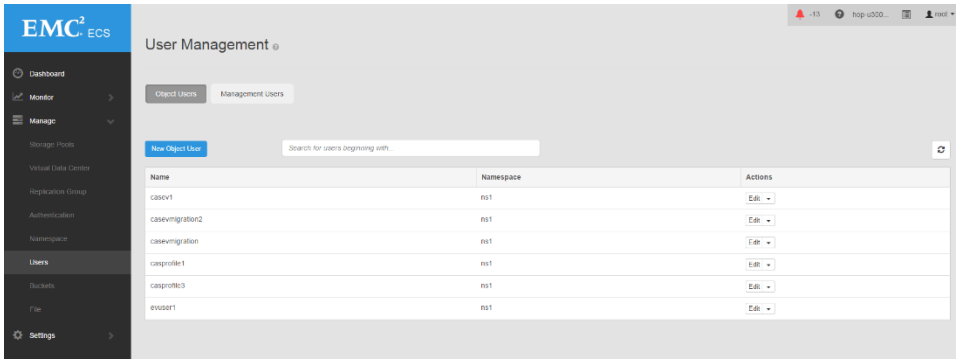
3.4.1 Namespace

If choosing to have compliance enforced, make sure that you use a namespace that has been configured for compliance.

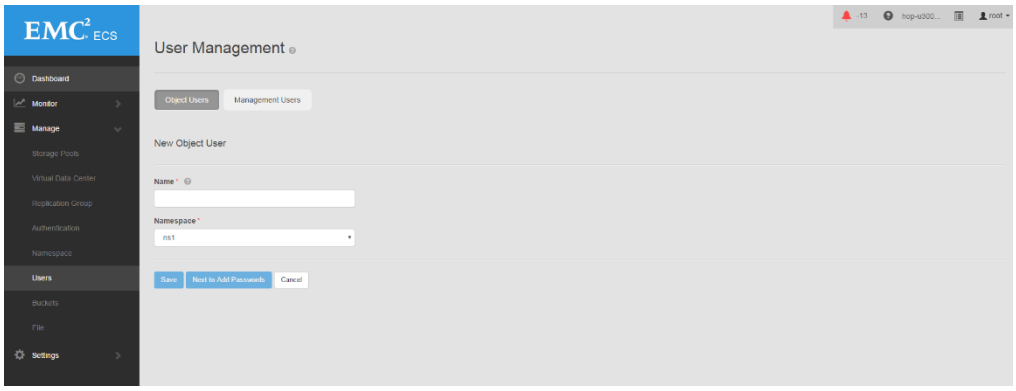


3.4.2 Create the EV user

1. On the left side of the task bar, select **Manage** > **Users**.



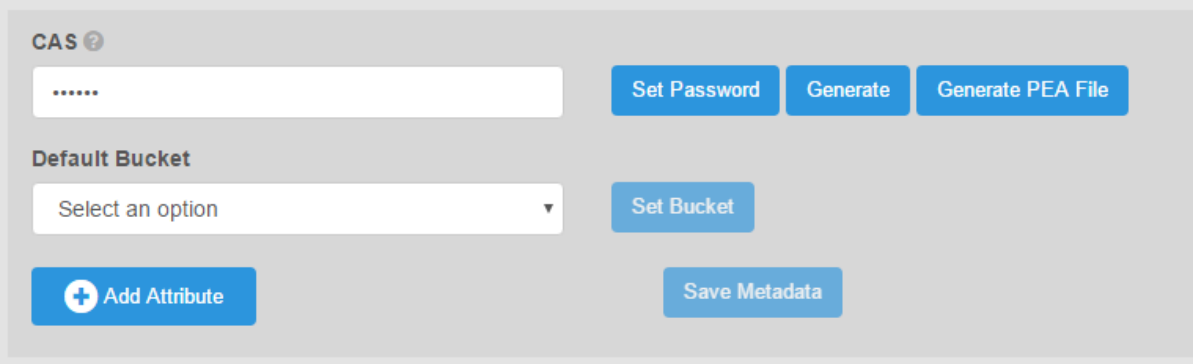
2. To create a user, click the **New Object User** button.



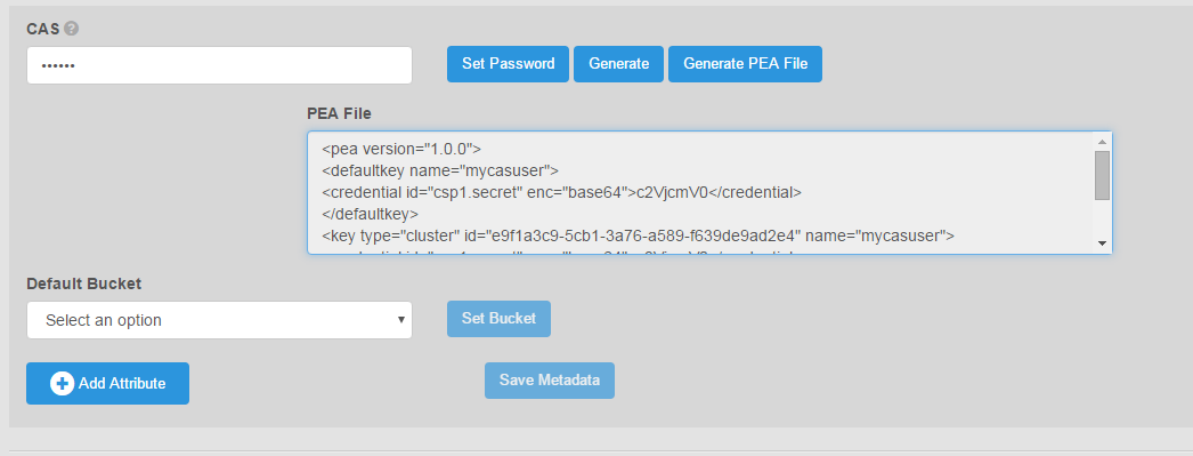
3. Enter the new user name and select the correct Namespace from the drop-down Namespace prompt. Select the **Next to Add Passwords** button.
4. On the next screen, enter a password in the **CAS** prompt.

5. Click the **Set Password** button.

6. Do not enter any details in the S3, Groups, or Swift Password sections.



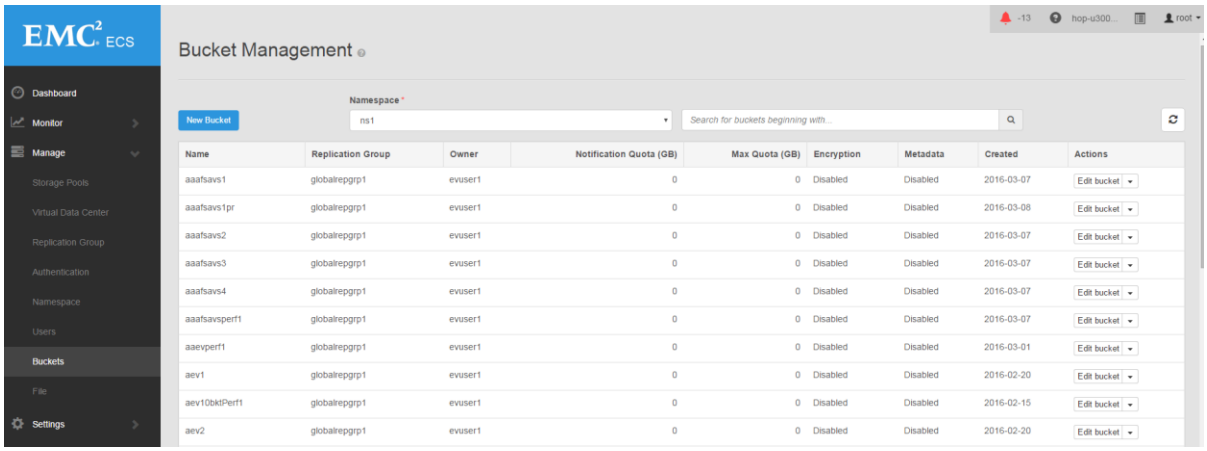
7. Click the **Generate PEA File** button.



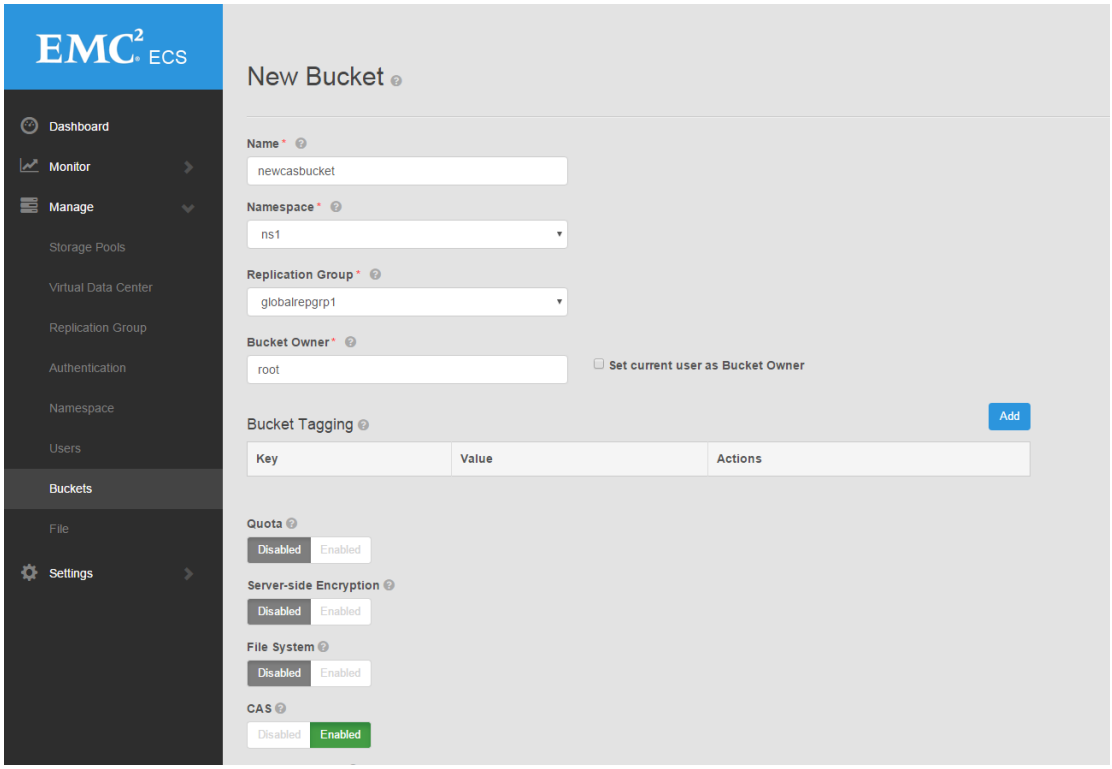
8. Copy the text in the PEA File window, and using a text editor, save this to a file. This is the Process Entry Authorization file used by Enterprise Vault to connect to the CAS Bucket on this ECS.
9. Leave the **Default Bucket** drop-down menu as-is since it has not been created yet.

3.4.3 Create bucket

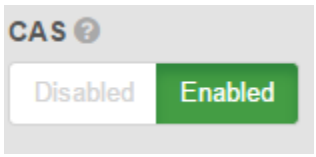
1. In the **Management** window, click the **Bucket** selection on the left.



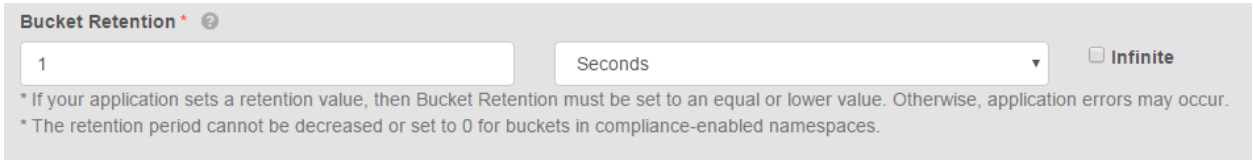
2. Click the **New Bucket** button.
3. Enter the details of the new bucket. Ensure that Bucket Owner is the CAS user created and that CAS is enabled.



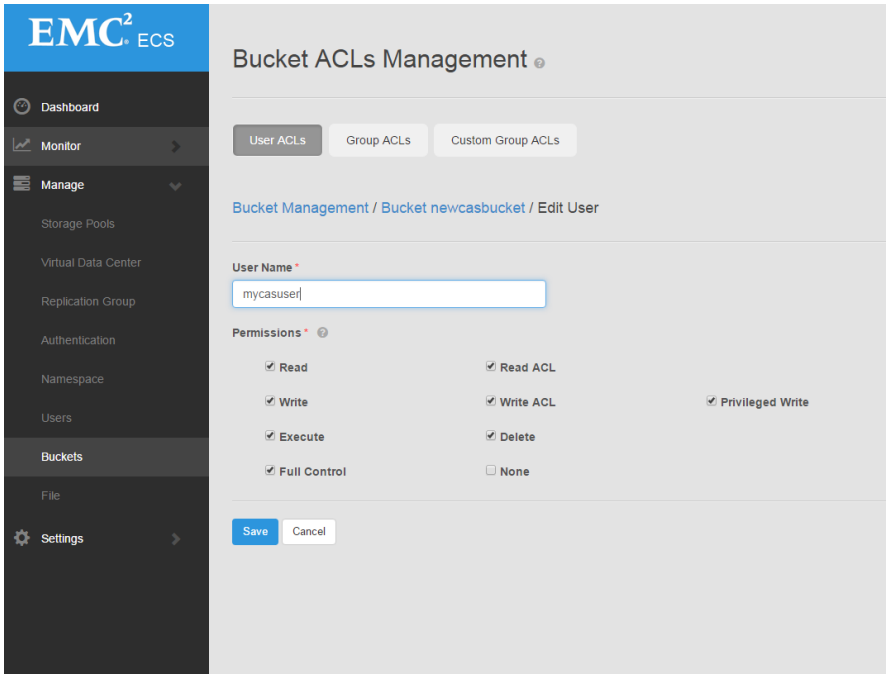
4. Change ownership from root to the new user if it is set to root.



5. If the Namespace you are using is set up for Compliance, ensure that you set a 1 second default retention period for the Bucket.



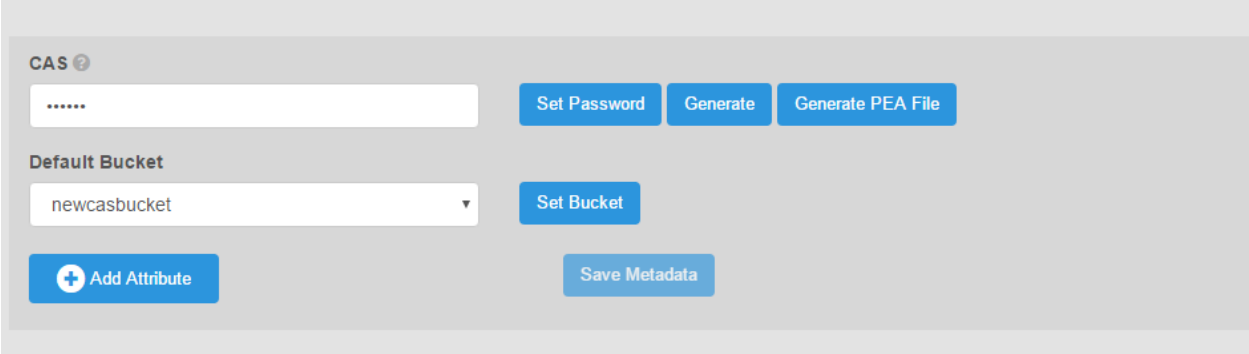
6. Do not set any other retention setting than 1 second.



7. Click **Save**.
8. Return to the CAS user created and add the CAS bucket that you have created as the Default Bucket for the CAS user.

3.4.4 Update the CAS user default bucket

Your new CAS user and CAS bucket has been created and can now be used.



3.5 Migrate content

The procedure used to migrate content from the Centera to ECS system is dependent on the toolset used by the migration service. Possible toolsets include the following:

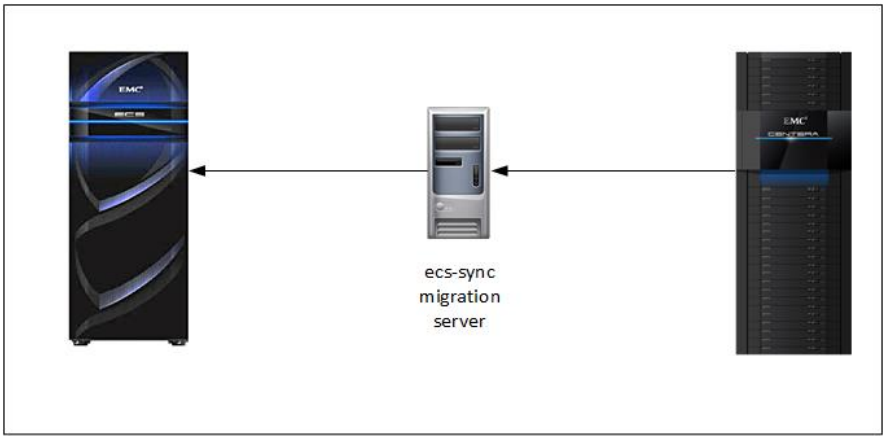
- Dell EMC ecs-sync
- Datadobi Dobiminer
- Interlock Xspedient

All are similar in the sense that they all provide the capability to migrate content from the Centera to ECS system using an external Migration Server which does the actual copying/cloning of the content.

All tools provide a level of audit tracing to confirm what has actually been migrated, highlighting any failures and retries.

3.5.1 ECS-SYNC example

The following diagram shows an example of the ecs-sync migration.



3.5.1.1 Generate a C-Clip List

First generate a list of all C-Clips to be migrated from Centera to ECS. This can be done in a number of ways. For this example, we will use jcasscript to get a list of all Content Addresses of C-Clips in a Centera Virtual Pool written to a file on the ecs-sync server being used.

```
paul@etdh205:~/cas
[paul@etdh205 cas]$ java -jar jcasscript.jar


CASScript>poolopen 10.246.22.131?evcentera1.pea

Attempting to connect to: 10.246.22.131?evcentera1.pea

Connected to: 10.246.22.131?evcentera1.pea

CASPool Properties:
        Connection String:              10.246.22.131?evcentera1.pea
        Cluster Time:                   2016.03.09 03:18:29 GMT
        Buffer Size:                    16384
        Prefetch Buffer Size:           32768
        Connection Timeout:             120000
        Multi-Cluster Failover Enabled: True
        Collision Avoidance Enabled:    False

CASScript>querytofile evcliplist.txt
```

This will generate a filename named evcliplist.txt with a list of all the Content Addresses of all C-Clips in the Virtual Pool on Centera with the IP address of 10.246.22.131, as accessed by the Application Profile indicated by the PEA file evcentera1.pea

3.5.1.2 Migrate C-Clips from Centera to ECS

On the ecs-sync migration server, run the following command:

```
java -jar ecs-sync-2.1.jar --source cas://10.246.22.131?evcentera1.pea --source-clip-list evcliplist.txt --target cas://10.246.22.151?name=casevmigration,secret=secret
```

This will migrate all the C-Clips referenced in the file evcliplist.txt from the source Centera to the target ECS system.

The following commands can control the execution of ecs-sync:

Command	Description
`ecs-sync-cli-2.1.jar --list-jobs`	This will show all ecs-jobs running e.g. 1
`ecs-sync-cli-2.1.jar --status 1`	Will show the status of job #1
`ecs-sync-ctl-2.1.jar --set-threads 1 --sync-threads 24`	Sets the number of sync threads in job 1 to 24

3.5.1.3 Audit/confirm migration

At this stage, the migration user should confirm that all of the clips that were on the source Centera system are now on the target ECS cluster.

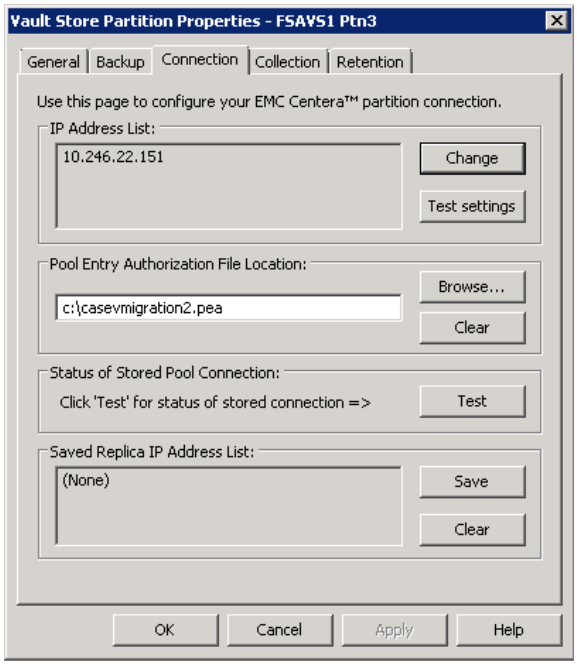
The simplest way to do this would be to generate a list of C-Clips using the jcasscript utility as shown above but this time from the target ECS. Then use a difference tool (such as Linux® diff) to compare the two files. If there are any differences, then these can be investigated.

Note: The order of the C-Clip Content Addresses may be different, sort the files into alphabetical order before using diff to compare them.

Other toolsets may have a more sophisticated methodology for auditing the migration.

3.5.1.4 Change Centera EV partition IPs

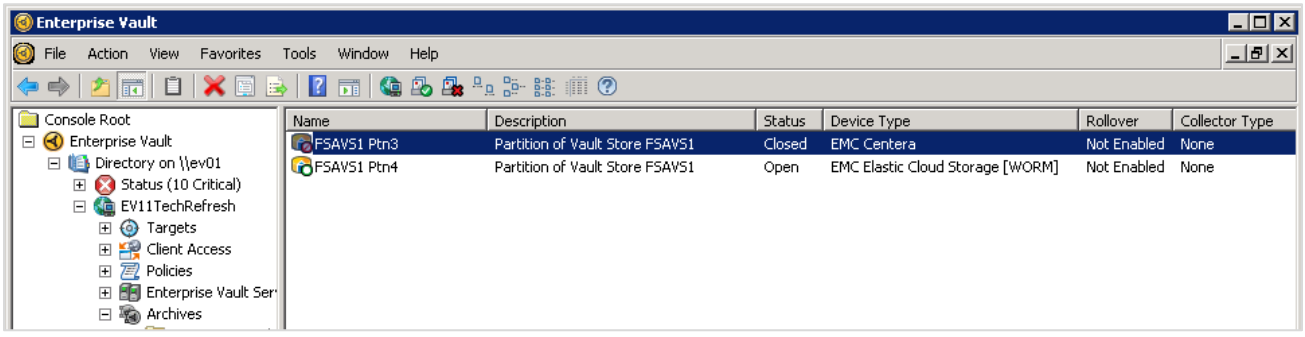
In the Enterprise Vault VAC, change the IPs of the Centera partition to be those of the ECS CAS cluster.

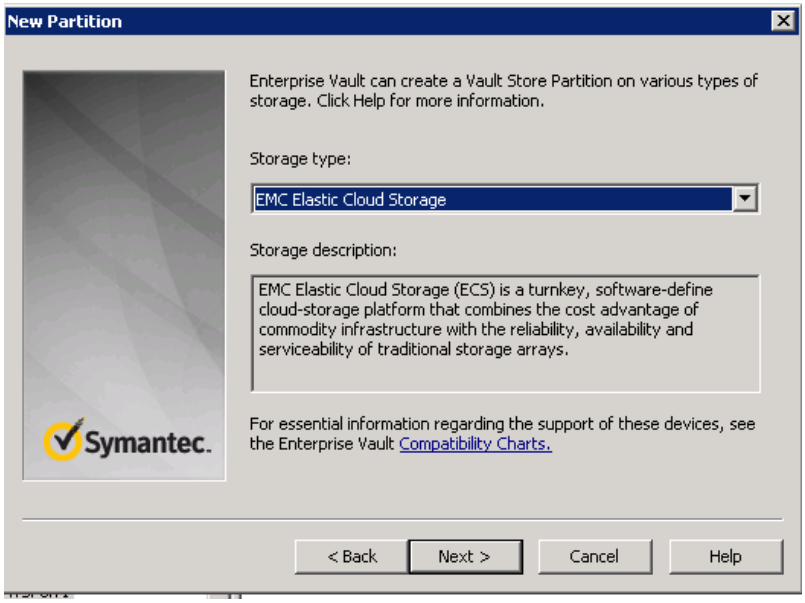


In this example, the IP address and the PEA file pertain to the new ECS CAS user/bucket.

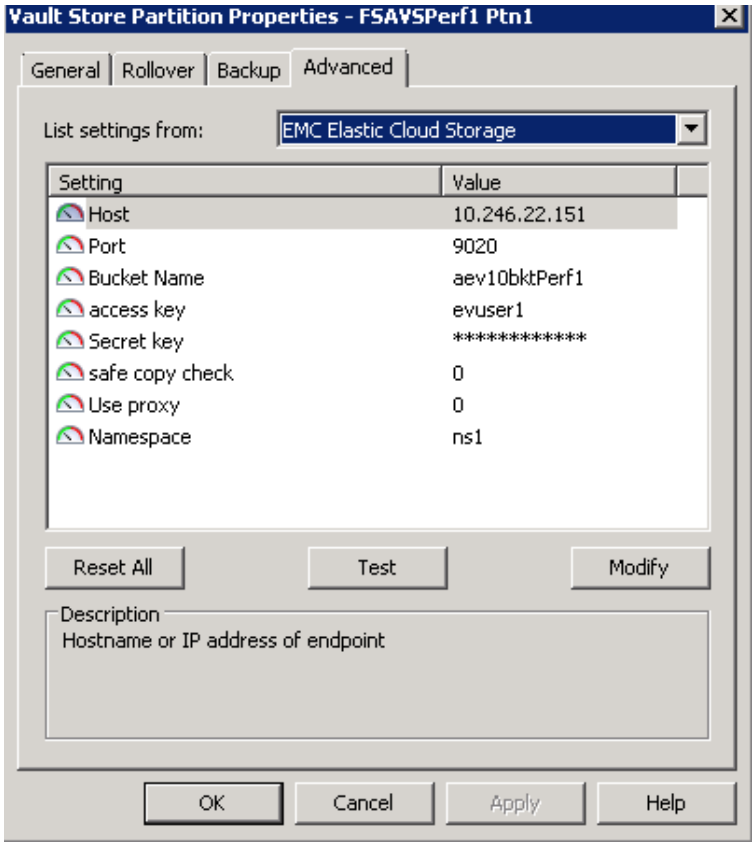
3.5.1.5 Create new ECS Streamer partition

In this final step, a new ECS Streamer type partition is created for the Vault Store. The creation of the new partition will close the Centera partition meaning all new ingest into the Vault Store will be to the new ECS partition but content will still be able to be read from the Centera partition.





The ECS partition is created per the following screen.



Refer to the document, Dell EMC ECS: Using Veritas Enterprise Vault, for details on the settings in the partition definition GUI.

3.5.1.6 Confirm ECS CAS partition content accessible

After the Centera content has been successfully migrated to ECS and the EV Partition has been configured to access ECS and not Centera, check that content can be successfully accessed as before.

A number of tests can be performed to confirm this:

Run EVSVR.EXE before and after the migration – Count Files

The EV tool EVSVR.EXE should be run on the Centera before the migration to count all objects in all Vault Stores/Partitions.

This can be run after the migration to ECS to produce the same report for a before and after comparison.

Run EVSVR.EXE – Verify Archive Objects

The EV tool EVSVR.EXE can be run to check the consistency of Archive Objects in EV Partitions. The log file output can be checked for any errors.

Run EVSVR.EXE – Verify Database References

The EV tool EVSVR.EXE can be run to check the EV Database is consistent with what is actually on the EV Partitions. The log file output can be checked for any errors.

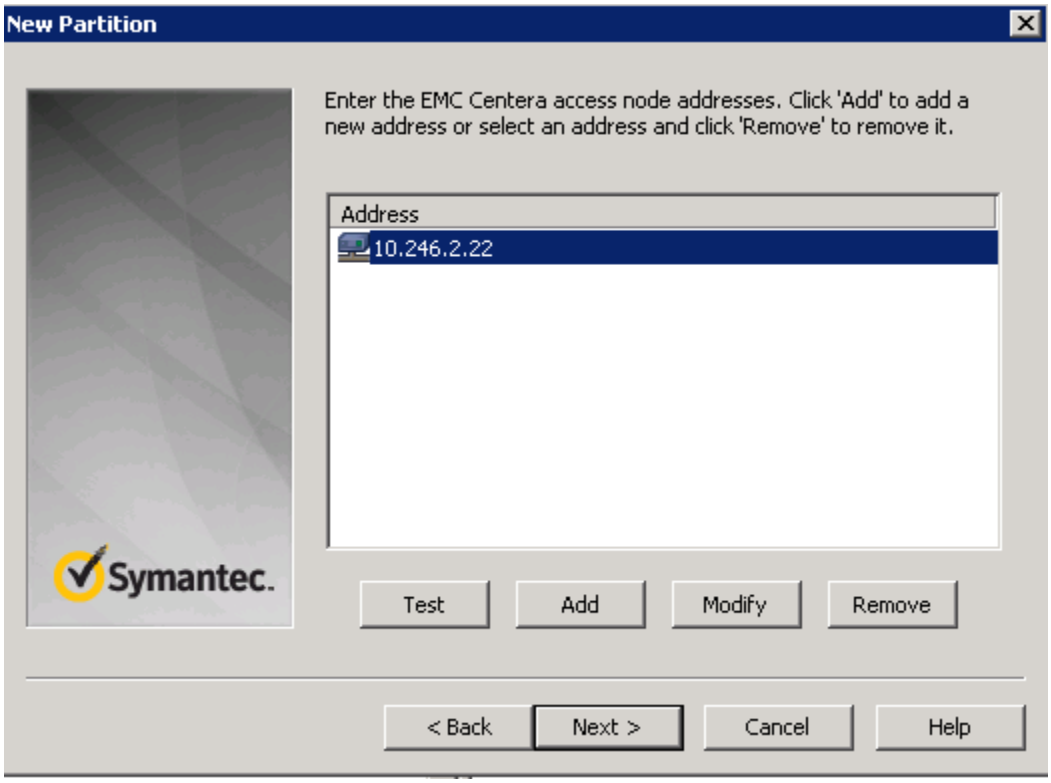
4 Configuration issues

4.1 Configuring the ECS CAS partition in the EV VAC

The ECS CAS partition is configured in the EV VAC the same way that Centera partitions are configured. However, the differing behavior between Centera and ECS CAS on handling connections using the Anonymous Profile will cause different results during configuration.

Both the ECS CAS and the Centera partitions are initially configured during the creation of a new Vault Store or when a new partition is added to an existing Vault Store.

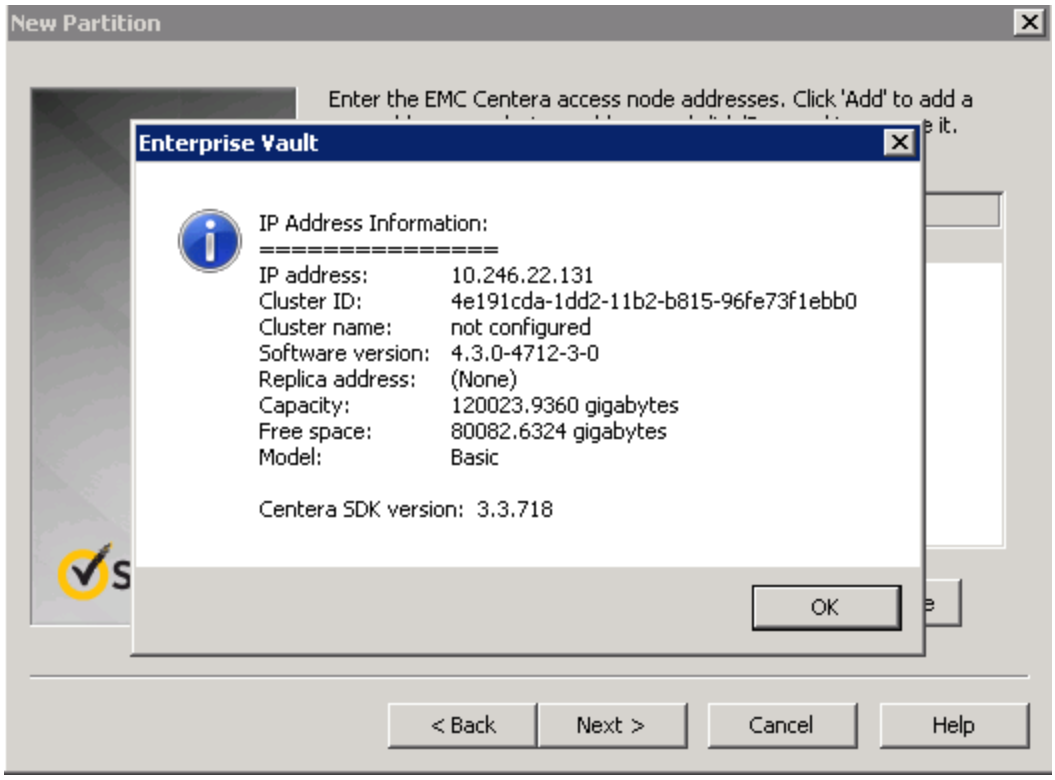
The administrator will be presented with this GUI to input the IP connectivity for the partition



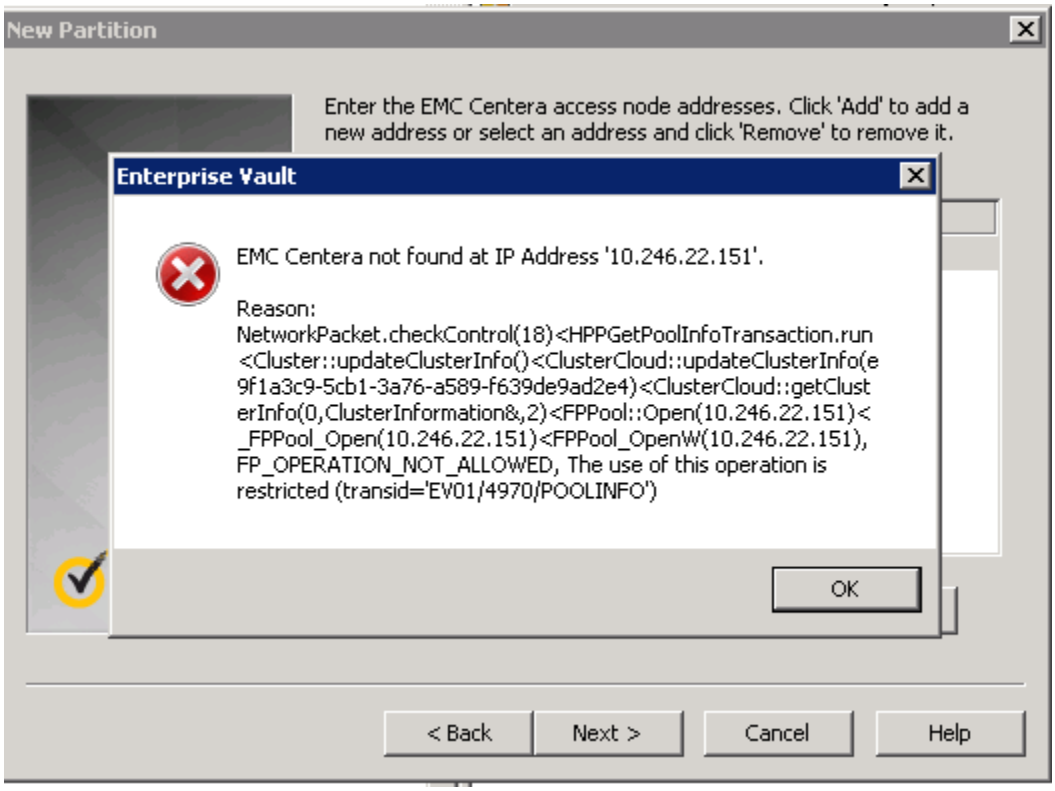
At this point, the administrator should test the connection by clicking the **Test** button.

Readers may notice that there is no PEA file detailed in this GUI so far. When you click the Test button, the EV VAC is connecting to the Centera/ECS using the Anonymous Profile.

This is just a network connectivity test which normally will result in the following response from a Centera cluster.

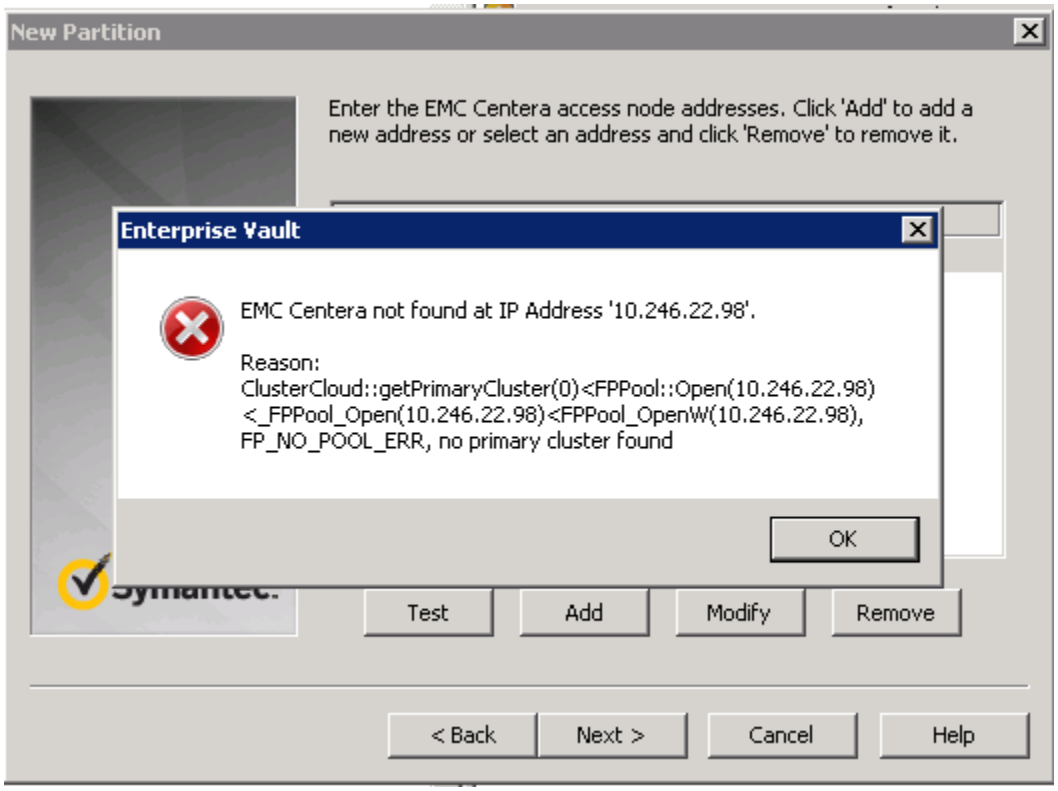


With ECS, access with the anonymous profile is not allowed and will result in an error.



This is occurring because at this point, the EV VAC is not using a PEA file to authenticate with the EV Access Profile (ECS User) and the ECS displays that the VAC managed to connect to the ECS system with the IPs specified, but is returning “FP_OPERATION_NOT_ALLOWED” because anonymous access is disabled.

The EV VAC is interpreting this error as “EMC Centera not found at IP address…” which is not correct. If the ECS was not accessible at all, the EV VAC would get the following error from the CAS SDK.

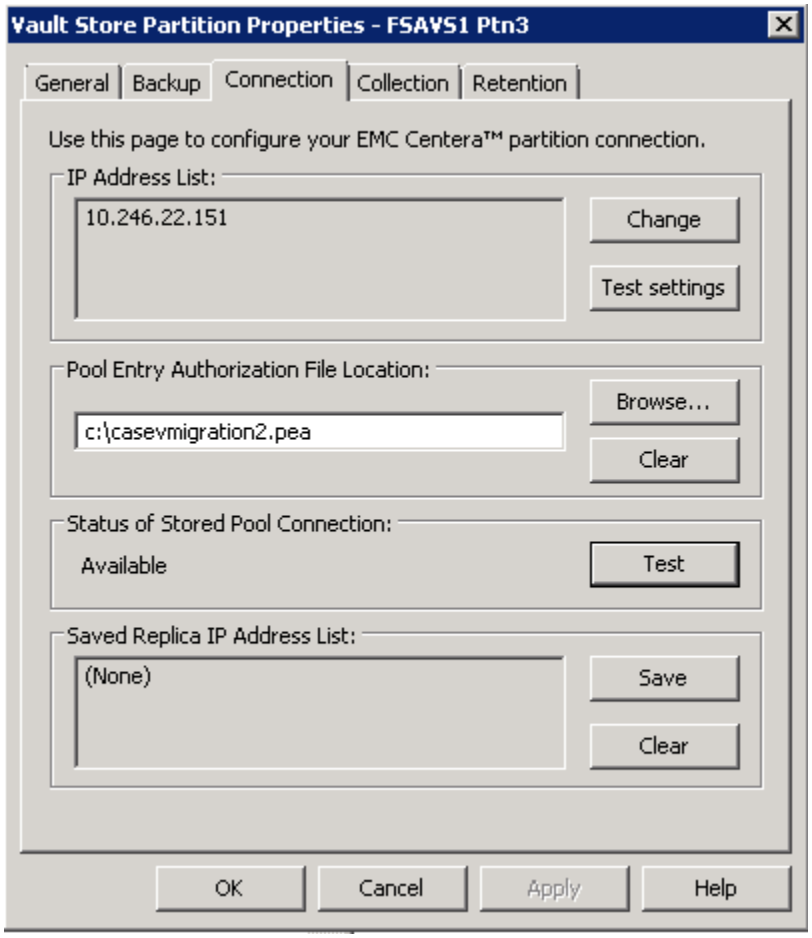


The FP_NO_POOL_ERR means that the IP connectivity details are wrong, and the CAS SDK timed out on the connection attempt.

4.2 Configuring the ECS CAS partition PEA file in the EV VAC

When configuring a Centera or ECS CAS partition, edit the partition to include the Process Entry Authentication file so that the Vault Store Partition can authenticate to the Centera or ECS cluster.

The VAC GUI for this is shown in the following screen:



Like the connectivity test above, you will get an “FP_OPERATION_NOT_ALLOWED” error when you click the Test button if the IP details are correct and you will get “FP_NO_POOL_ERR” if they are not.

Note: The Test button is not testing the validity of the PEA file for either the Centera or ECS system. At present, there is no way to test this except to restart the EV Storage Service and see if it logs an error in the Windows Event log.

4.3 Single instancing

Unlike the Centera system, ECS does not single-instance duplicate objects that are stored on it. ECS uses inline compression to reduce the storage consumed when storing objects.

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

Title	Link
ECS documentation site	https://community.emc.com/docs/DOC-73931
ECS Administration Guide	https://support.emc.com/docu92968_ECS-3.3-Administration-Guide.pdf?language=en_US
Dell EMC ECS: Using Veritas Enterprise Vault	https://www.dellemc.com/resources/en-us/asset/white-papers/products/storage-2/h15309-vertias-vault-emc-elastic-cloud-storage.pdf
Veritas Enterprise Vault Compatibility Charts	https://www.veritas.com/support/en_US/doc/128058600-128865835-0/index