# Appendix E - Troubleshooting Netmail Store

You can refer to the following information in the event of encountering a problem with Netmail Store. If these troubleshooting tips are not successful in rectifying the problem, you may find it helpful to contact Messaging Architects' Technical Support Team.

**On this page:**

## Restoring Domains and Buckets

This section discusses how to recover domains or buckets after they have been accidentally deleted. When you delete a bucket, for example, the objects it contains are not deleted but they are inaccessible until you recover the bucket.

To recover a deleted domain or bucket, you need the following:

- You must know the name of a child object.

  For example, if a bucket was deleted, you must know the name of an object contained in that bucket.

- The Content Router product.

  You must use the Content Router's metadata enumerator to find the contained object's metadata. The metadata enumerator iterates through all objects in a cluster and returns information about those objects. For example, if a bucket was deleted, the metadata enumerator cannot locate the bucket but it can locate objects contained in the bucket (because the objects were not deleted). Knowing the name of an object, you can find the bucket's UUID, which you use to recover the bucket.

For more information about using the metadata enumerator, see Enumerator API. For information on creating Content Router rules, see Netmail Store Content Router.

- You must upload a realm (that is, user list) for the domain or bucket you recover. There is no way to retrieve the user list after the domain or bucket has been deleted.

### Recovering a Deleted Domain

To recover a domain, you must know the name of a bucket that was contained in the domain. The following procedure shows how to create the domain from the command line using the previous domain's UUID. If you create a domain with the same name in the Admin Console, the new domain has a different UUID. Because all the buckets created in the domain before it was deleted reference the domain's UUID as *Castor-System-CID*, the buckets are inaccessible unless the new domain's UUID is set to the previous value. You must also know the *Castor-Authorization* header corresponding to the domain's protection setting, which is one of the following:

| Protection Setting | Castor-Authorization header |
|---|---|
| All Users. No Authentication required. | Castor-Authorization: domain-name/_administrators, POST= |
| Only users in this domain | Castor-Authorization: domain-name/_administrators, POST=domain-name |
| Only users in domain | Castor-Authorization: domain-name/_administrators, POST=domain-name<br>The difference between this protection setting and the preceding is that in this case, domain-name is the name of a different domain in the cluster. |

To recover the domain:

1. Add a Content Router filter rule to search for streams where the value of the *Castor-System-Name* header is a bucket in the domain.

2. Using the SDK, instantiate a metadata enumerator subscribed to the rule channel you created in the preceding step to obtain the bucket's metadata.

3. In the metadata returned for the object, look for the value of the *Castor-System-CID* header. The *Castor-System-CID* header is the UUID of the

domain in which the bucket was contained.

4. POST the previous domain's UUID using the *recreatecid* query argument to create the new domain, passing in the *Cache-Control*, *Castor-Authorization*, *Castor-Stream-Type*, and lifepoint headers exactly as shown. You can change the *Castor-Authorization* header and upload a user list later.

```
  curl -i -X POST -H "Cache-Control: no-cache-context" -H "Castor- Authorization: protection-setting" -H
"Castor-Stream-Type: admin" -H "lifepoint: [] reps=16" --data-binary '' --post301 --location-trusted
"http://node-ip?domain=domain-name&admin&recreatecid=previous-domain-UUID" --digest -u
"your-username:your-password" [-D log-file-name]
```

> ***Note:*** *The Cache-Control, lifepoint, and Castor-Stream-Type headers must be entered exactly as shown to match the headers used when domains are created by the Admin Console. Cache-Control: no-cache-context does not prevent the domain from being cached. lifepoint: [] reps=16 enables the domain to be replicated as many times as possible. Castor-Stream-Type: admin is recommended for all objects that use a Castor-Authorization header.*

For example, if the domain name is cluster.example.com with the protection setting **Only users in this domain**, and the old domain alias was c0d0fa42bccac73cd3f2324bb53e40a5, enter the following command:

```
curl -i -X POST -H "Cache-Control: no-cache-context" -H "Castor-Authorization:
cluster.example.com/_administrators, POST=cluster.example.com" -H "Castor-Stream-Type: admin" -H
"lifepoint: [] reps=16" --data-binary '' --post301 --location-trusted "http://172.16.0.35?
domain=cluster.example.com&admin&recreatecid=c0d0fa42bccac73cd3f2324bb53e40a5" --digest -u
"admin:ourpwdofchoicehere"
```

5.  Create the *_administrators* bucket for the domain.

```
  curl -i -X POST -H "Cache-Control: no-cache-context" -H "Castor-Authorization:
domain-name/_administrators" -H "Castor-Stream-Type: admin" -H "lifepoint: [] reps=16" --data-binary ''
--post301 -- location-trusted "http://node-ip/_administrators?domain=domainname&admin" --digest -u
"your-username:your-password" [-D log-filename]
```

> ***Note:*** *The following error indicates you omitted --post301 from the command: CAStor Error Content-Length header is required*

For example, to create the cluster.example.com/_administrators bucket:

```
  curl -i -X POST -H "Cache-Control: no-cache-context" -H "Castor-Authorization:
cluster.example.com/_administrators" -H "Castor-Stream-Type: admin" -H "lifepoint: [] reps=16" --databinary
'' --post301 --location-trusted "http://172.16.0.35/ _administrators?domain=cluster.example.com&admin"
--digest -u "admin:ourpwdofchoicehere"
```

6. To verify that the procedure worked, connect to the Netmail Store Admin Console.

7. In the Storage Console window, click **Settings**.

8. In the Cluster Tenants section, make sure the domain name and protection setting display correctly.

9. Click **Edit** next to the name of the domain you just restored.

10. Click **Add Domain Manager**.

11. Follow the prompts on your screen to create a domain manager.

If you added a domain manager successfully, the procedure completed successfully. There is likely an alert in the Admin Console due to not having an _administrators bucket for the domain. You can optionally clear the error from the Admin Console as discussed in the next step.

12. *Optional*. Return to the Cluster Settings page and click the IP address of any node for which there is a red Alert message. Look for an alert message similar to the following:

```
 Error reading admin bucket 'cluster.example.com/

 _administrators' ([Errno 2] Bucket not found)
```

13. Click **Clear Errors**. You are required to confirm the action.

## Recovering a Deleted Bucket

In the procedure that follows, assume that an application developer notifies you that the following objects are not accessible:

```
 photo1.jpg, photo2.jpg, photo3.jpg
```

You do not know the name of the bucket in which the objects were contained. To recover the bucket:

1. Add a Content Router filter rule to search for streams where the value of the *Castor-System-Name* header is *photo1.jpg*, *photo2.jpg*, or *photo3.jpg*.

2. Using the SDK, instantiate a metadata enumerator subscribed to the rule channel you created in the preceding step to obtain the object's metadata.

3. In the metadata returned for the object, look for the value of the *Castor-System-CID* header. The *Castor-System-CID* header is the UUID of the bucket in which the object was contained.

4. After you find the bucket's UUID, use the following command to recover it:

```
 curl -i -X POST --post301 --digest -u "cluster-administrator-username:password" --data-binary @realm
--location-trusted "http://node-ip/bucket-name?domain=domain=name&admin&recreatecid=alias-uuid"
```

You must provide the domain name or IP address as the Host in the request. For example, to recover a bucket named mybucket with an alias UUID of 75edd708dc250137849bbf590458d401 in the domain named *cluster.example.com*, enter:

```
 curl -i --post301 --anyauth -u "admin:ourpwdofchoicehere" -X POST --data-binary
@cluster_example_com_mybucket --location-trusted
"http://172.16.0.35/mybucket?domain=cluster.example.com&admin
&recreatecid=75edd708dc250137849bbf590458d401"
```

5. In the example above, *cluster_example_com_mybucket* is the name of the user list to upload to *mybucket*.

## Resolving Duplicate Domain Names in a Mirrored or Disaster Recovery (DR) Cluster

This section discusses how to resolve duplicate domain names in a mirrored or disaster recovery (DR) cluster. These optional configurations with Content Router work as follows:

- A DR cluster enables you to copy one or more clusters and their contents in another physical location.
- A mirrored configuration copies the contents of cluster 1 to cluster 2, and copies the contents of cluster 2 to cluster 1.

In either type of configuration, if two source clusters contain two domains with the same name, Content Router duplicates the domain names in the DR or mirrored cluster. This results in indeterminate access to objects in the duplicated domains; in other words, sometimes a request to a particular object in one of the duplicate domains succeeds, but other times it fails.

When Content Router detects a duplicate domain, it logs a Critical error to its Netmail Store Admin Console. If you are alerted to such an error, the following resolutions are suggested:

- For a DR cluster conflict, it is recommended that you rename either domain in its source cluster. This method is recommended because it solves the issue and prevents it from happening in the future. You can perform this task using the source cluster's Admin Console.

> ***Note:*** *This method does not work in a mirrored configuration because both clusters have duplicates. Instead, use the procedure discussed in the next bullet.*

- Rename either conflicting domain. For a DR cluster conflict, this method is not as desirable because the next time the same domain is replicated to the DR cluster, the domain name duplicate still exists. While this is the only method you can use in a mirrored cluster conflict, it solves the issue and prevents it from reoccurring.

### Renaming a Domain in its Source Cluster (DR Cluster Conflict Only)

This section discusses how to rename a domain in its source cluster, where the name of the domain is assumed to be unique. After you rename the domain, it replicates without errors to the DR cluster. To resolve a conflict in a mirrored configuration, refer to Renaming a Domain in a Mirrored or DR Cluster.

To rename a domain in the source cluster of a DR cluster, use the Admin Console as follows:

1. Connect to the Admin Console.

2. Click **Settings**.

3. On the Cluster Settings page, click **Edit** next to the name of the domain to rename.

4. In the Add Cluster Tenant section, enter a new name in the **Domain Name** field.

5. Click **Save**.

6. If prompted, enter an administrator user name and password.

## Renaming a Domain in a Mirrored or DR Cluster

To rename a domain in a mirrored or DR cluster, use an SCSP COPY command with the following query arguments, and authenticate as a cluster administrator:

| Query argument | Meaning |
|---|---|
| `admin` | Also referred to as administrative override, enables you to ignore Allow headers and bypass the *Castor-Authorization* header; requires your cluster administrator credentials. |
| `newname=new-domain-name` | New name for the domain. |
| `aliasuuid=domain-UUID` | The UUID of the domain to rename. You can find the UUID using a HEAD on the domain in its source cluster, as discussed in the example following the table. |

## Boot Errors

Refer to the following table for help with boot errors.

| Symptom | Resolution |
|---|---|
| 1. When booting, the node gives an error saying that no boot device is available. | Verify that the node is capable of booting from a USB device and that the USB memory device is configured as the primary boot device. To verify that your hardware setup is correct, see Hardware Setup. |
| 2. The node boots into an operating system other than Netmail Store. | |
| 3. The node boots from the USB device but Netmail Store fails to start. | This is likely a hardware compatibility issue with the hardware. Contact Messaging Architects' Technical Support Team with the details of your hardware setup. |
| 4. The node begins to boot but reports a "kernel panic" error and stops. | |

To rename a domain in a mirrored or DR cluster:

1. HEAD the alias UUID of the domain to rename. Use SCSP INFO command as follows:

```
 INFO /?domain=domain-name&admin

 Host: domain-name-or-ip
```

You must authenticate as a cluster administrator (that is, a user in the CAStor administrator realm). The value of the Castor-System-Alias header is the domain's UUID. You must also get the value of the Castor-Authorization header from the HEAD request and pass it in using the new cluster name with the rename command as shown in the next step.

2. Rename the domain.

```
 curl -X COPY -H "Castor-Authorization: renamed-value-from-HEAD" - H "Cache-Control: no-cache-context" -H
"lifepoint: [] reps=16" - H "Castor-Stream-Type: admin" --anyauth -u
"cluster-administrator-username:password" --location-trusted
"http://node-ip?domain=domainname&admin&aliasuuid=uuid&newname=new-domain-name"
```

For example, to rename *cluster.example.com* to *archive.example.com* by sending commands to a node whose IP address is 172.16.0.35:

1. HEAD the domain to get its alias UUID:

```
    curl -I --anyauth -u "admin:ourpwdofchoicehere" --location-trusted

    "http://172.16.0.35?domain=cluster.example.com&admin"

    Sample output follows:

    HTTP/1.1 200 OK

    Cache-Control: no-cache-context

    Castor-Authorization: cluster.example.com/_administrators,

    POST=cluster.example.com

    Castor-Stream-Type: admin
    Castor-System-Alias: bbc2365b3283c23c47595abcfd09034a

    Castor-System-CID: ffffffffffffffffffffffffffffffff

    Castor-System-Cluster: cluster.example.com

    Castor-System-Created: Wed, 17 Nov 2010 15:59:13 GMT

    Castor-System-Name: cluster.example.com

    Castor-System-Owner: admin@CAStor administrator

    Castor-System-Version: 1290009553.775

    Content-Length: 0

    Last-Modified: Wed, 17 Nov 2010 15:59:13 GMT

    lifepoint: [] reps=16

    Etag: "099e2bc25eb8346ed5d94a598fa73bfa"

    Date: Wed, 17 Nov 2010 16:02:07 GMT

     Server: CAStor Cluster/5.0.0
```

The information you need to rename the domain is:

```
    Castor-Authorization: cluster.example.com/_administrators,

    POST=cluster.example.com
```

You must change this header to: Castor-Authorization: archive.example.com/

```
    _administrators, POST=archive.example.com

   Castor-System-Alias: bbc2365b3283c23c47595abcfd09034a
```

You must also add the following headers exactly as shown:

```
    -H "Castor-Stream-Type: admin"

    -H "Cache-Control: no-cache-context"

    -H "lifepoint: [] reps=16"
```

> ***Note:*** *The Cache-Control, lifepoint, and Castor-Stream-Type headers must be entered exactly as shown to match the headers used when domains are created by the Admin Console. Cache-Control: no-cache-context does not prevent the domain from being cached. lifepoint: [] reps=16 enables the domain to be replicated as many times as possible. Castor-Stream-Type: admin is recommended for all objects that use a Castor-Authorization header.*

2. Rename the domain.

```
      curl -i -X COPY -H "Castor-Authorization: archive.example.com/ _administrators,
POST=archive.example.com" -H "Castor-Stream-Type: admin" -H "Cache-Control: no-cachecontext" -H "lifepoint:
[] reps=16" --anyauth -u "admin:ourpwdofchoicehere" --location-trusted "http://172.16.0.35?
domain=cluster.example.com&admin&aliasuuid=bbc2365b3283c23c47595abcfd09034a&newname=archive.example.com" -D
rename-domain.log
```

3. Verify the new domain name through the Admin Console.

## Using Content Router to List Buckets and Objects

To optionally use Netmail Store Content Router to list the buckets in a domain or objects in a bucket:

1. Find the value of the *Castor-System-CID* for the child of an object to list. For example, to list all buckets in a domain, INFO an object in the bucket to find the value of the object's *Castor-System-CID* header. (The *Castor-System-CID* of the object is the *Castor-System-Alias* of its parent, the bucket.)

2. Add a Content Router filter rule to search for streams where the value of the *Castor-System-CID* header matches the value in step 1 and the value of *Castor-System-Alias* is not null. (The *Castor-System-Alias* of a named object is null.)

3. Using the SDK, instantiate a metadata enumerator subscribed to the rule channel you created in the preceding step to obtain the stream's

metadata.

4. In the metadata returned for the object, look for the value of the Castor-System-Name header.

## Configuration Problems

Refer to the following table for help with configuration problems.

| Symptom | Resolution |
|---|---|
| 1. After the system has booted, there is a message on the screen saying that the *node.cfg* file is missing.<br>2. The node boots, but there is no storage available on it.<br>3. There is hard disk in a node that does not appear in the available storage.<br>4. After adding a new drive to a node, some of the volumes will not mount.<br>5. After moving a volume from one node to another, some volumes in the new node will not mount. | Every node needs to have a *node.cfg* file on the USB stick and all the volumes within the node need to be specified in the *vols* option. For detailed instructions on configuring a node, see Node Configuration.<br>If the *vols* specification is correct, this may be an issue with the amount of RAM in the node. For hardware recommendations, see Hardware Requirements and Recommendations. |
| 6. The node boots from the USB device, but Netmail Store fails to start.<br>7. The node begins to boot but reports a “kernel panic” error and stops. | This is likely a hardware compatibility issue with the hardware. Contact Messaging Architects’ Technical Support Team with the details of your hardware setup. |
| 8. Some changes to the *node.cfg* file disappear after editing. | If a USB stick is removed from a computer without unmounting, some changes can be lost. Use the proper method for your OS to stop and unmount the USB media before removing it. |
| 9. *Local clock is out of sync with node ip-address* alert displays in the Admin Console. The following indicator displays for each node on which the error occurs:<br>🕒❗ | There is an issue with synchronization of clocks between nodes in the cluster. The node on which the indicator displays has failed to synchronize its clock with other nodes. Make sure your Network Time Protocol (NTP) settings are correct, as discussed in Time Synchronization . |
| 10. A node hangs during boot while initializing ACPI services. | Some hardware presents issues with the ACPI interface. The solution is to add the argument **acpi=off** to the *syslinux.cfg* file on the USB flash drive for local booting or to the PXE configuration file for network booting. |
| 11. The Netmail Store node boots as having an unregistered license. | The license file is not in the Caringo directory on the USB drive, or the licenseFileURL option in the *node.cfg* file has not been properly set. |

## Operational Problems

Refer to the following table for help with configuration problems.

| Symptom | Resolution |
|---|---|
| 1. A volume device has failed. | The node can either be allowed to continue to run in a degraded state (lowered storage), or the node may be gracefully shutdown in order to replace the failed device. The node must be returned to service within 14 days. |
| 2. A node has failed. | If a node fails but the volume storage devices are still good, you may repair the hardware and return it to service within 14 days. If it has been more than 14 days, see Volume Management, for information on volume handling. |
| 3. You have read-only access to the Admin Console even though you are a member of the Netmail Store realm, or cannot view the Admin Console. | You added an operator (that is, a read-only user) to the Netmail Store operators realm but did not add your administrator user name and password to the Netmail Store operators realm. Failure to do so prevents you, an administrator, from properly accessing the Admin Console. To resolve this issue, add all of your administrator users to the operators parameter in the node or cluster configuration file. |

| | |
|---|---|
| 4. A node has become unresponsive to network requests. | Ensure that your client network settings are correct and that the node has really become unresponsive before taking the next steps. This can be done by pinging the node and trying to display the web console (i.e., http://192.168.3.200:90).<br>If you have a keyboard that can be attached to the system, you may hit **CTRL+ALT+DEL** in order to attempt a graceful shutdown. Otherwise, hit the hardware reset button or power cycle the node. |
| 5. Network never becomes connected on a node with multiple network interface ports. | Check that the network cable is plugged into the correct NIC. Depending on the bus order and the order in which kernel drivers are loaded, the network ports may not match their external labeling. |
| 6. A node is rebooting itself. | If the electrical power is constant and the hardware is functioning properly, this may indicate a software problem. The Netmail Store system has a built-in failsafe and will reboot itself if something goes wrong. You should contact the Messaging Architects Technical Support Team. |