## Backup and Recovery Procedures for Red Hat Open Shift Cluster

# Backing up etcd data

Prerequisites

* SSH access to a master host.

Procedure

1. Access a master host.
2. If the cluster-wide proxy is enabled, be sure that you have exported the **NO\_PROXY**, **HTTP\_PROXY**, and **HTTPS\_PROXY** environment variables.

|  |  |
| --- | --- |
|  | You can check whether the proxy is enabled by reviewing the output of **oc get proxy cluster -o yaml**. The proxy is enabled if the **httpProxy**, **httpsProxy**, and **noProxy** fields have values set. |

1. Run the **etcd-snapshot-backup.sh** script and pass in the location to save the backup to.

Be sure to pass in the **-E** flag to **sudo** so that environment variables are properly passed to the script.

$ sudo -E /usr/local/bin/etcd-snapshot-backup.sh ./assets/backup

In this example, two files are created in the **./assets/backup/** directory on the master host:

* + **snapshot\_<datetimestamp>.db**: This file is the etcd snapshot.
	+ **static\_kuberesources\_<datetimestamp>.tar.gz**: This file contains the static Kubernetes API server resources. If etcd encryption is enabled, it also contains the encryption keys for the etcd snapshot.

# Replacing a failed master host

## Removing a failed master host from the etcd cluster

Follow these steps to remove a failed master host from the etcd cluster.

Prerequisites

* You have access to the cluster as a user with the cluster-admin role.
* You have SSH access to an active master host.

Procedure

1. View the list of Pods associated with etcd.

In a terminal that has access to the cluster, run the following command:

$ oc get pods -n openshift-etcd

NAME READY STATUS RESTARTS AGE

etcd-member-ip-10-0-128-73.us-east-2.compute.internal 2/2 Running 0 15h

etcd-member-ip-10-0-147-172.us-east-2.compute.internal 2/2 Running 7 122m

etcd-member-ip-10-0-171-108.us-east-2.compute.internal 2/2 Running 0 15h

1. Access an active master host.
2. Run the etcd-member-remove.sh script and pass in the name of the etcd member to remove:
3. [core@ip-10-0-128-73 ~]$ sudo -E /usr/local/bin/etcd-member-remove.sh etcd-member-ip-10-0-147-172.us-east-2.compute.internal
4. Downloading etcdctl binary..
5. etcdctl version: 3.3.10
6. API version: 3.3
7. etcd client certs already backed up and available ./assets/backup/
8. Member 23e4736df4451b32 removed from cluster 6e25bab1bb556673

etcd member etcd-member-ip-10-0-147-172.us-east-2.compute.internal with 23e4736df4451b32 successfully removed..

1. Verify that the etcd member has been successfully removed from the cluster:
	1. Connect to the running etcd container:

[core@ip-10-0-128-73 ~] id=$(sudo crictl ps --name etcd-member | awk 'FNR==2{ print $1}') && sudo crictl exec -it $id /bin/sh

* 1. In the etcd container, export the variables needed for connecting to etcd:

sh-4.3# export ETCDCTL\_API=3 ETCDCTL\_CACERT=/etc/ssl/etcd/ca.crt ETCDCTL\_CERT=$(find /etc/ssl/ -name \*peer\*crt) ETCDCTL\_KEY=$(find /etc/ssl/ -name \*peer\*key)

* 1. In the etcd container, execute etcdctl member list and verify that the removed member is no longer listed:
	2. sh-4.3# etcdctl member list -w table
	3. +------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+
	4. | ID | STATUS | NAME | PEER ADDRS | CLIENT ADDRS |
	5. +------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+
	6. | 29e461db6be4eaaa | started | etcd-member-ip-10-0-128-73.us-east-2.compute.internal | https://etcd-2.clustername.devcluster.openshift.com:2380 | https://10.0.128.73:2379 |
	7. | cbe982c74cbb42f | started | etcd-member-ip-10-0-171-108.us-east-2.compute.internal | https://etcd-1.clustername.devcluster.openshift.com:2380 | https://10.0.171.108:2379 |

+------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+

# Adding the member back to the cluster

After you have removed the member from the etcd cluster, use one of the following procedures to add the member to the cluster:

* If the etcd certificates for the master host are valid, then [add the member back to the etcd cluster](https://docs.openshift.com/container-platform/4.3/backup_and_restore/replacing-failed-master.html#restore-add-master_replacing-failed-master-host).
* If there are no etcd certificates for the master host or they are no longer valid, then [generate etcd certificates and add the member to the etcd cluster](https://docs.openshift.com/container-platform/4.3/backup_and_restore/replacing-failed-master.html#restore-regenerate-etcd-certs_replacing-failed-master-host).

### Adding a master host back to the etcd cluster

Follow these steps to add a master host back to the etcd cluster. This procedure assumes that you previously removed the master host from the cluster and that its etcd dependencies, such as TLS certificates and DNS, are valid.

Prerequisites

* You have access to the cluster as a user with the cluster-admin role.
* You have SSH access to the master host to add to the etcd cluster.
* You have the IP address of an existing active etcd member.

Procedure

1. Access the master host to add to the etcd cluster.

|  |  |
| --- | --- |
|  | You must run this procedure on the master host that is being added to the etcd cluster. |

1. Run the etcd-member-add.sh script and pass in two parameters:
	* the IP address of an existing etcd member
	* the name of the etcd member to add
2. [core@ip-10-0-147-172 ~]$ sudo -E /usr/local/bin/etcd-member-add.sh \
3. 10.0.128.73 \ **(1)**
4. etcd-member-ip-10-0-147-172.us-east-2.compute.internal **(2)**
5. Downloading etcdctl binary..
6. etcdctl version: 3.3.10
7. API version: 3.3
8. etcd-member.yaml found in ./assets/backup/
9. etcd.conf backup upready exists ./assets/backup/etcd.conf
10. Stopping etcd..
11. Waiting for etcd-member to stop
12. etcd data-dir backup found ./assets/backup/etcd..
13. Updating etcd membership..
14. Removing etcd data\_dir /var/lib/etcd..
15. ETCD\_NAME="etcd-member-ip-10-0-147-172.us-east-2.compute.internal"
16. ETCD\_INITIAL\_CLUSTER="etcd-member-ip-10-0-147-172.us-east-2.compute.internal=https://etcd-1.clustername.devcluster.openshift.com:2380,etcd-member-ip-10-0-171-108.us-east-2.compute.internal=https://etcd-2.clustername.devcluster.openshift.com:2380,etcd-member-ip-10-0-128-73.us-east-2.compute.internal=https://etcd-0.clustername.devcluster.openshift.com:2380"
17. ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS="https://etcd-1.clustername.devcluster.openshift.com:2380"
18. ETCD\_INITIAL\_CLUSTER\_STATE="existing"'
19. Member 1e42c7070decd39 added to cluster 6e25bab1bb556673

Starting etcd..

|  |  |
| --- | --- |
| **1** | The IP address of an active etcd member. This is not the IP address of the member that you are adding. |
| **2** | The name of the etcd member to add. |

1. Verify that the etcd member has been successfully added to the etcd cluster:
	* Connect to the running etcd container:

[core@ip-10-0-147-172 ~] id=$(sudo crictl ps --name etcd-member | awk 'FNR==2{ print $1}') && sudo crictl exec -it $id /bin/sh

* + In the etcd container, export the variables needed for connecting to etcd:

sh-4.3# export ETCDCTL\_API=3 ETCDCTL\_CACERT=/etc/ssl/etcd/ca.crt ETCDCTL\_CERT=$(find /etc/ssl/ -name \*peer\*crt) ETCDCTL\_KEY=$(find /etc/ssl/ -name \*peer\*key)

* + In the etcd container, execute etcdctl member list and verify that the new member is listed:
	+ sh-4.3# etcdctl member list -w table
	+ +------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+
	+ | ID | STATUS | NAME | PEER ADDRS | CLIENT ADDRS |
	+ +------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+
	+ | 29e461db6be4eaaa | started | etcd-member-ip-10-0-128-73.us-east-2.compute.internal | https://etcd-2.clustername.devcluster.openshift.com:2380 | https://10.0.128.73:2379 |
	+ | cbe982c74cbb42f | started | etcd-member-ip-10-0-147-172.us-east-2.compute.internal | https://etcd-0.clustername.devcluster.openshift.com:2380 | https://10.0.147.172:2379 |
	+ | a752f80bcb0da3e8 | started | etcd-member-ip-10-0-171-108.us-east-2.compute.internal | https://etcd-1.clustername.devcluster.openshift.com:2380 | https://10.0.171.108:2379 |

+------------------+---------+------------------------------------------+------------------------------------------------------------------+---------------------------+

It may take up to 10 minutes for the new member to start.

* + In the etcd container, execute etcdctl endpoint health and verify that the new member is healthy:
	+ sh-4.3# etcdctl endpoint health --cluster
	+ https://10.0.128.73:2379 is healthy: successfully committed proposal: took = 4.5576ms
	+ https://10.0.147.172:2379 is healthy: successfully committed proposal: took = 5.1521ms

https://10.0.171.108:2379 is healthy: successfully committed proposal: took = 4.2631ms

1. Verify that the new member is in the list of Pods associated with etcd and that its status is Running.

In a terminal that has access to the cluster, run the following command:

$ oc get pods -n openshift-etcd

NAME READY STATUS RESTARTS AGE

etcd-member-ip-10-0-128-73.us-east-2.compute.internal 2/2 Running 0 15h

etcd-member-ip-10-0-147-172.us-east-2.compute.internal 2/2 Running 7 122m

etcd-member-ip-10-0-171-108.us-east-2.compute.internal 2/2 Running 0 15h

## Generating etcd certificates and adding the member to the cluster

If the node is new or the etcd certificates on the node are no longer valid, you must generate the etcd certificates before you can add the member to the etcd cluster.

Prerequisites

* You have access to the cluster as a user with the cluster-admin role.
* You have SSH access to the new master host to add to the etcd cluster.
* You have SSH access to the one of the healthy master hosts.
* You have the IP address of one of the healthy master hosts.

Procedure

1. Set up a temporary etcd certificate signer service on one of the healthy master nodes.
	1. Access one of the healthy master nodes and log in to your cluster as a cluster-admin user using the following command.
	2. [core@ip-10-0-143-125 ~]$ sudo oc login https://localhost:6443
	3. Authentication required for https://localhost:6443 (openshift)
	4. Username: kubeadmin
	5. Password:

Login successful.

* 1. Obtain the pull specification for the kube-etcd-signer-server image.

[core@ip-10-0-143-125 ~]$ export KUBE\_ETCD\_SIGNER\_SERVER=$(sudo oc adm release info --image-for kube-etcd-signer-server --registry-config=/var/lib/kubelet/config.json)

* 1. Run the tokenize-signer.sh script.

Be sure to pass in the -E flag to sudo so that environment variables are properly passed to the script.

[core@ip-10-0-143-125 ~]$ sudo -E /usr/local/bin/tokenize-signer.sh ip-10-0-143-125 **(1)**

Populating template /usr/local/share/openshift-recovery/template/kube-etcd-cert-signer.yaml.template

Populating template ./assets/tmp/kube-etcd-cert-signer.yaml.stage1

Tokenized template now ready: ./assets/manifests/kube-etcd-cert-signer.yaml

|  |  |
| --- | --- |
| **1** | The host name of the healthy master, where the signer should be deployed. |

* 1. Create the signer Pod using the file that was generated.
	2. [core@ip-10-0-143-125 ~]$ sudo oc create -f assets/manifests/kube-etcd-cert-signer.yaml

pod/etcd-signer created

* 1. Verify that the signer is listening on this master node.
	2. [core@ip-10-0-143-125 ~]$ ss -ltn | grep 9943

LISTEN 0 128 \*:9943 \*:\*

1. Add the new master host to the etcd cluster.
	1. Access the new master host to be added to the cluster, and log in to your cluster as a cluster-admin user using the following command.
	2. [core@ip-10-0-156-255 ~]$ sudo oc login https://localhost:6443
	3. Authentication required for https://localhost:6443 (openshift)
	4. Username: kubeadmin
	5. Password:

Login successful.

* 1. Export two environment variables that are required by the etcd-member-recover.sh script.

[core@ip-10-0-156-255 ~]$ export SETUP\_ETCD\_ENVIRONMENT=$(sudo oc adm release info --image-for machine-config-operator --registry-config=/var/lib/kubelet/config.json)

[core@ip-10-0-156-255 ~]$ export KUBE\_CLIENT\_AGENT=$(sudo oc adm release info --image-for kube-client-agent --registry-config=/var/lib/kubelet/config.json)

* 1. Run the etcd-member-recover.sh script.

Be sure to pass in the -E flag to sudo so that environment variables are properly passed to the script.

[core@ip-10-0-156-255 ~]$ sudo -E /usr/local/bin/etcd-member-recover.sh 10.0.143.125 etcd-member-ip-10-0-156-255.ec2.internal **(1)**

Downloading etcdctl binary..

etcdctl version: 3.3.10

API version: 3.3

etcd-member.yaml found in ./assets/backup/

etcd.conf backup upready exists ./assets/backup/etcd.conf

Trying to backup etcd client certs..

etcd client certs already backed up and available ./assets/backup/

Stopping etcd..

Waiting for etcd-member to stop

etcd data-dir backup found ./assets/backup/etcd..

etcd TLS certificate backups found in ./assets/backup..

Removing etcd certs..

Populating template /usr/local/share/openshift-recovery/template/etcd-generate-certs.yaml.template

Populating template ./assets/tmp/etcd-generate-certs.stage1

Populating template ./assets/tmp/etcd-generate-certs.stage2

Starting etcd client cert recovery agent..

Waiting for certs to generate..

Waiting for certs to generate..

Waiting for certs to generate..

Waiting for certs to generate..

Stopping cert recover..

Waiting for generate-certs to stop

Patching etcd-member manifest..

Updating etcd membership..

Member 249a4b9a790b3719 added to cluster 807ae3bffc8d69ca

ETCD\_NAME="etcd-member-ip-10-0-156-255.ec2.internal"

ETCD\_INITIAL\_CLUSTER="etcd-member-ip-10-0-143-125.ec2.internal=https://etcd-0.clustername.devcluster.openshift.com:2380,etcd-member-ip-10-0-156-255.ec2.internal=https://etcd-1.clustername.devcluster.openshift.com:2380"

ETCD\_INITIAL\_ADVERTISE\_PEER\_URLS="https://etcd-1.clustername.devcluster.openshift.com:2380"

ETCD\_INITIAL\_CLUSTER\_STATE="existing"

Starting etcd..

|  |  |
| --- | --- |
| **1** | Specify both the IP address of the healthy master where the signer server is running, and the etcd name of the new member. |

* 1. Verify that the new master host has been added to the etcd member list.
		1. Access the healthy master and connect to the running etcd container.

[core@ip-10-0-143-125 ~] id=$(sudo crictl ps --name etcd-member | awk 'FNR==2{ print $1}') && sudo crictl exec -it $id /bin/sh

* + 1. In the etcd container, export variables needed for connecting to etcd.

sh-4.3# export ETCDCTL\_API=3 ETCDCTL\_CACERT=/etc/ssl/etcd/ca.crt ETCDCTL\_CERT=$(find /etc/ssl/ -name \*peer\*crt) ETCDCTL\_KEY=$(find /etc/ssl/ -name \*peer\*key)

* + 1. In the etcd container, execute etcdctl member list and verify that the new member is listed.
		2. sh-4.3# etcdctl member list -w table
		3. +------------------+---------+------------------------------------------+----------------------------------------------------------------+---------------------------+
		4. | ID | STATUS | NAME | PEER ADDRS | CLIENT ADDRS |
		5. +------------------+---------+------------------------------------------+----------------------------------------------------------------+---------------------------+
		6. | cbe982c74cbb42f | started | etcd-member-ip-10-0-156-255.ec2.internal | https://etcd-0.clustername.devcluster.openshift.com:2380 | https://10.0.156.255:2379 |
		7. | 249a4b9a790b3719 | started | etcd-member-ip-10-0-143-125.ec2.internal | https://etcd-1.clustername.devcluster.openshift.com:2380 | https://10.0.143.125:2379 |

+------------------+---------+------------------------------------------+----------------------------------------------------------------+---------------------------+

It may take up to 20 minutes for the new member to start.

1. After the new member is added, remove the signer Pod because it is no longer needed.

In a terminal that has access to the cluster, run the following command:

$ oc delete pod -n openshift-config etcd-signer