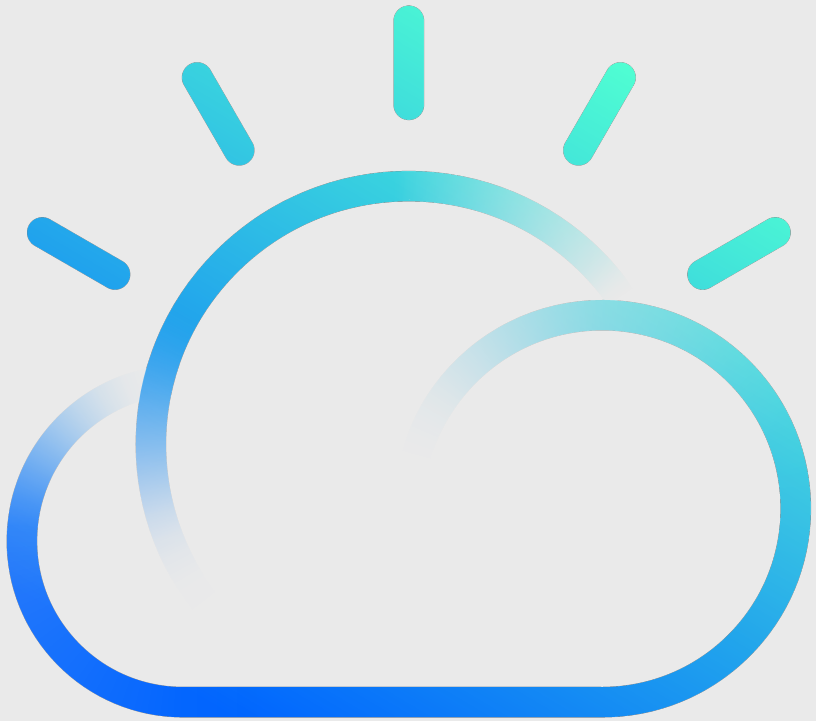
IBM Cloud Private
Backup and Restore Strategy



IBM Cloud

Overview

Consider the backup and recovery schema to meet your resilience requirements.

Each implementation will have its own specific procedure

Scenarios should be rehearsed in your non-production environment to validate

Your enterprise is relied upon for specific procedures to manage backups of the cluster nodes, their filesystems and persistent storage solution

Consider the following possible node failures: Boot, Worker, Proxy, Management Master in single Master topology, Master in multi-Master topology

Consider failure of your shared storage / persistent storage solution

Consider catastrophic failures such as multiple Masters and the entire cluster potentially including a DR declaration

Key Guidelines for ICP Backup Routine

Critical considerations

Post installation you must establish a clean archived fallback point via a full backup of idle infrastructure.

Special consideration exist for ICP components

Process Summary

- Install ICP
- Disable etcd on all Master nodes
- Disable all other pods
- Shutdown all Infrastructure
- Take Initial Backup of Infrastructure
- Start ICP Infrastructure
- Re-enable etcd
- Re-enable all other pods

Note: After establishing your initial baseline enact regular storage and component backups

Stopping and Starting ICP Nodes

Stop Master Nodes first then proceed with the rest of the cluster
Start rest of cluster first and finish with Masters

Stop kubelet first! Kubelet will attempt to start Docker otherwise.
`sudo systemctl stop kubelet`

Next stop Docker: **`sudo systemctl stop docker`**

Confirm that all processes are shutdown (be patient): **`top`**
And that all related network ports are no longer in use: **`netstat –antp`**

To restart the cluster reboot the nodes (Masters Last). If this is not possible:
start Docker and then the kubelet:
`sudo start docker`
`sudo start kubelet`

You can follow the logs for the kubelet: **`sudo journalctl -e -u kubelet`**

Backup/Restore Infrastructure

Infrastructure backups are only valid when all systems are stopped
Disable etcd and other pods before snapshot

Use preferred tool (e.g.) (VMware snapshot or equivalent, VEEAM,IBM Spectrum Protect)

Restore all infrastructure from consistent backup

If regular backups are taken while ICP is running then these backups should not be used to restore running Master nodes

Note: Care should be taken to ensure that the Initial backup is not deleted

Management Node Failure

To back up the Management Node, use traditional VM backup mechanisms.

For baremetal environment use equivalent tooling.

The frequency of the back up will determine the RPO.

Balance the procedural overhead with your requirement for management data / configuration currency.

Guidance

- Take frequent / constant node snapshots
- Redeploy from backup

Note: In most environments this data is not critical enough to require restores versus create-new and replace.

Note on Master Node Backup

The key component in the ICP Kubernetes cluster master node is etcd

- Special considerations are required for backing up etcd
- Use the etcd tool to create and restore snapshots
- Step-by-step instructions on how to back up and restore etcd: https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/etcd.md

Additionally, we need to provide a way to recreate a master node

- After you deploy an ICP environment, take a VM (or equivalent) backup for every master node, using the available solution (VMware snapshots, Spectrum Protect, etc)
- Continue with taking regular VM backups, but the initial backup will be sufficient for restoration

Take constant snapshots of the ICP components, as described at https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/components.md

Note: Backup the components from only one of the master nodes

Additional Guidelines on etcd

ICP / Kubernetes and Calico rely heavily on etcd to store configurations

Avoid restarting an etcd member with a data directory from an out-of-date backup
Using an out-of-date data directory can lead to inconsistency

If an etcd member suffers any sort of data corruption or loss, it must be removed from the cluster

Once removed the member can be re-added with an empty data directory

Note: Currently there is no method to add new Master nodes to a cluster

Single Master Failure
(single master topology)

In the case of a disaster, recover the master's VM using the snapshot and follow by recovering the state of the ICP components running on the master.

Since this is your only master, you need the etcd snapshot. Follow this procedure https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/etcd.md#etcd-restore-on-multi-master-icp-configuration to restore the etcd to the latest backup.

Recovery Restore from Backup

- Restore the node from initial backup
- Restore current certificates (if boot/master) from in-host backup
- Restore MongoDB from backup
- Restore Docker registry from backup
- Restore etcd from backup

Multi Master Failure
(multi-master topology)

Recover the masters' VMs using the snapshot and follow by recovering the state of the ICP components.

As long as a single master node is available in a multi-master environment, then you can simply restore the VMs from a snapshot, and the *etcd* master, running in another master node will update the restored node.

Recovery Restore from Backup

- Restore the node from initial backup
- Restore current certificates (if boot/master) from in-host backup
- The Docker registry is on shared storage and requires no restoration

Boot Node Failure

Recovering from a boot node failure can be accomplished very easily providing you have access to the initial post installation infrastructure backup.

Recovery Plan

- Restore from system / VM backup
- Reload ICP certificates

Worker Node Failure

Worker Nodes can be created on demand in ICP, so they should not be backed up and restored.

If a certain worker node fails, you should simply create another one.

Kubernetes will manage the redeployment and distribution of workload.

Guidance

- Do not backup worker nodes
- Deploy replacement worker node

Proxy Node Failure

Starting with ICP 2.1.0.2, it’s possible to create Proxy Nodes as needed.

As with Worker Nodes, you should not back up or restore a Proxy Node you will simply remove the failed node and add a new one.

Guidance

- Do not backup proxy nodes
- Deploy replacement proxy node

ICP Components Backup and Restore Tools and Techniques

Scripts and procedures for the backup and restore of etcd can be found here: https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/etcd.md

Depending on your topology and environment, your Docker Registry may be located on shared storage. Notes on backing up and restoring the registry may be found here: https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/registry.md

The MariaDB is optional for restoration of the master node, but you can find procedures to do so here: https://github.com/ibm-cloud-architecture/icp-backup/blob/master/docs/mariadb.md

Persistent Workload

Each persistent storage provider will have best-practices for that solution

For vSphere Persistent Volumes use a suitable backup tool that can access vmdk files directly from a vSphere datastore (e.g. vmkfstools)

NFS Persistent Volumes can be backed up using a suitable tool for the NFS system

HostPath Persistent Volumes can be backed up using tools or agents running on the Worker nodes

Other tools such as GlusterFS and Ceph will have their own best-practices for meeting the resiliency requirements, these should be considered prior to deployment

Further and Current Information

https://github.com/ibm-cloud-architecture/icp-backup