Backing Up and Restoring Cisco Container Platform

This chapter contains the following topics:

Backing Up Cisco Container Platform

You can back up the Cisco Container Platform application data that pertains to the following components:

- Application users
- Virtualization providers
- Tenant clusters

Note The logging or monitoring data from Prometheus, Grafana, and the EFK stack is not included in the backup archive.

You must ensure that you use an up-to-date backup archive for a restore operation. Tasks such as creating, deleting, upgrading, or scaling tenant clusters or altering the number of Load Balancer Virtual IP addresses will create changes in the data that will not be present in the backup. If you perform such tasks after a backup and use an outdated backup archive to restore your Cisco Container Platform environment, unexpected IP address conflicts, unmanageable tenant clusters, or an unsuccessful restore may occur.

Backing Up Cisco Container Platform with IP Pool Management v3.0.x+

Before you begin

Ensure that at least 6 consecutive IP addresses are available in the same pool where the Cisco Container Platform Control Plane is deployed.

When the target for a restore is a new cluster, you must ensure that additional free IP addresses are available to avoid conflicts with the IP addresses that are currently in use.

For more information on the requirement for additional free IP addresses, refer to the *Managing Networks* section of the *Cisco Container Platform User Guide*.

Step 1 Log in to the console of the master node of the Cisco Container Platform Control Plane.

Step 2 Run the following command.

```
/ccp_related_files/percona_backup.sh ./backup.tar
```

The backup script displays the following information on the console:

- The valid IP pool ranges with enough free IP addresses to create a replacement Cisco Container Platform Control Plane

  You must save the IP ranges for future use while specifying the **IP Address Range** on the **Network Settings** screen during an install, see Deploying Cisco Container Platform.

- The encryption key that is needed to decrypt the backup data encryption key that is stored on your disk.

  You must save the encryption key for future use while restoring the database to a new Cisco Container Platform Control Plane. For more information, see Restoring Cisco Container Platform, on page 2.

  Caution Losing the encryption key will prevent restoration of the Cisco Container Platform Control Plane cluster.

Step 3 Copy the `backup.tar` backup archive to a secure location.

Note You must ensure that the backup archive is maintained securely as anyone with access to it has administrative capabilities on all tenant clusters.

Restoring Cisco Container Platform

You can restore a valid backup in one of the following ways:

- To the same cluster, in case of database corruption.
- To a new Cisco Container Platform Control Plane instance of the same version that has control over all the existing Cisco Container Platform settings and tenant clusters.

When restoring a backup archive to a new Control Plane, the Ingress, kube-apiserver, and node IP addresses will not be restored, they will remain the same as when the new Control Plane was created.

Before you begin

For versions 3.2 and later, you must have the Encryption key provided during the Backing Up Cisco Container Platform with IP Pool Management v3.0.x+.

Step 1 Power off the VMs that belong to the previous Control Plane instance.

Step 2 Install a new Cisco Container Platform Control Plane with the same version as the previous Control Plane with the same subnet configuration used for the previous Control Plane instance, but the IP pool range needs to be one of the smaller

ranges specified during the backup output. All tenant network settings and IP pool ranges from the previous Control Plane instance will be restored as part of the restoration process.

For the 3.1 version, the IP addresses required for the new Control Plane must be from the original IP address pool range of the Control Plane that was created during installation. If this is not possible, you must open a support case for assistance in creating a complete backup. You are allowed to expand the original IP address pool range by modifying the start and end of the range if required.

Step 3 Copy the backup from the secure location to Control Plane master.

```
scp ./backup.tar <control_plane_master>:/tmp/backup.tar
```

Step 4 Log in to the console of the master node of Cisco Container Platform Control Plane.

Step 5 Follow these steps for Cisco Container Platform **version 3.1 only**:

a) Update the **CCP_BACKUP** environment variable to match the filename of the backup file that was created during the Backing Up Cisco Container Platform with IP Pool Management v3.0.x+:

```
CCP_BACKUP="backup.tar"
```

b) Decrypt the database encryption key and store it in an environment variable. When prompted, enter the decryption key from the Backing Up Cisco Container Platform with IP Pool Management v3.0.x+.

```
 AES_KEY="$(read -s -p "Encryption Key: " && echo -n $REPLY | openssl enc -d -aes-256-cbc \ -in
<(tar -f "$CCP_BACKUP" -O -x tmp/backup/aes_key.enc) \ -pass file:/dev/stdin)"
```

c) Update the database decryption key in the new Control Plane:

```
kubectl get secret cx-aes-key --export -o json \| jq ".data[\"aes-key\"] |= \"$(echo -n "$AES_KEY"
 | base64 | tr -d '\n')\"" | kubectl apply -f -
```

Step 6 Run the following command.

```
/ccp_related_files/percona-restore.sh /tmp/backup.tar
```

If prompted to continue the backup, enter the encryption Key from the Backing Up Cisco Container Platform with IP Pool Management v3.0.x+.

Backing Up Harbor Database

The database on Harbor tenant contains information such as user data and audit logs. This information can be backed up as a safety precaution before attempting a tenant upgrade on a Harbor tenant as the upgrade process may perform a database migration.

Note This backup process does not include docker images hosted on the Harbor registry.

Step 1 Log in to the console of the master node of Harbor tenant.

Step 2 Run the following command.

```
/opt/ccp/charts/harbor-db-backup.sh ./harbor_db_backup.sql default ccp-harbor
```

Step 3 Copy the `harbor_db_backup.sql` backup file to a secure location.

Restoring Harbor Database

You can restore a valid Harbor database on a new or an existing Harbor tenant.

Step 1 Copy the backup from the secure location to Harbor tenant master.

```
scp ./harbor_db_backup.sql <harbor_tenant_master>:/tmp/harbor_db_backup.sql
```

Step 2 Log in to the console of the master node of Harbor tenant.

Step 3 Run the following command.

```
/opt/ccp/charts/harbor-db-restore.sh /tmp/harbor_db_backup.sql default ccp-harbor
```