NetApp Astra Control Center Overview: Red Hat OpenShift with NetApp

NetApp Solutions

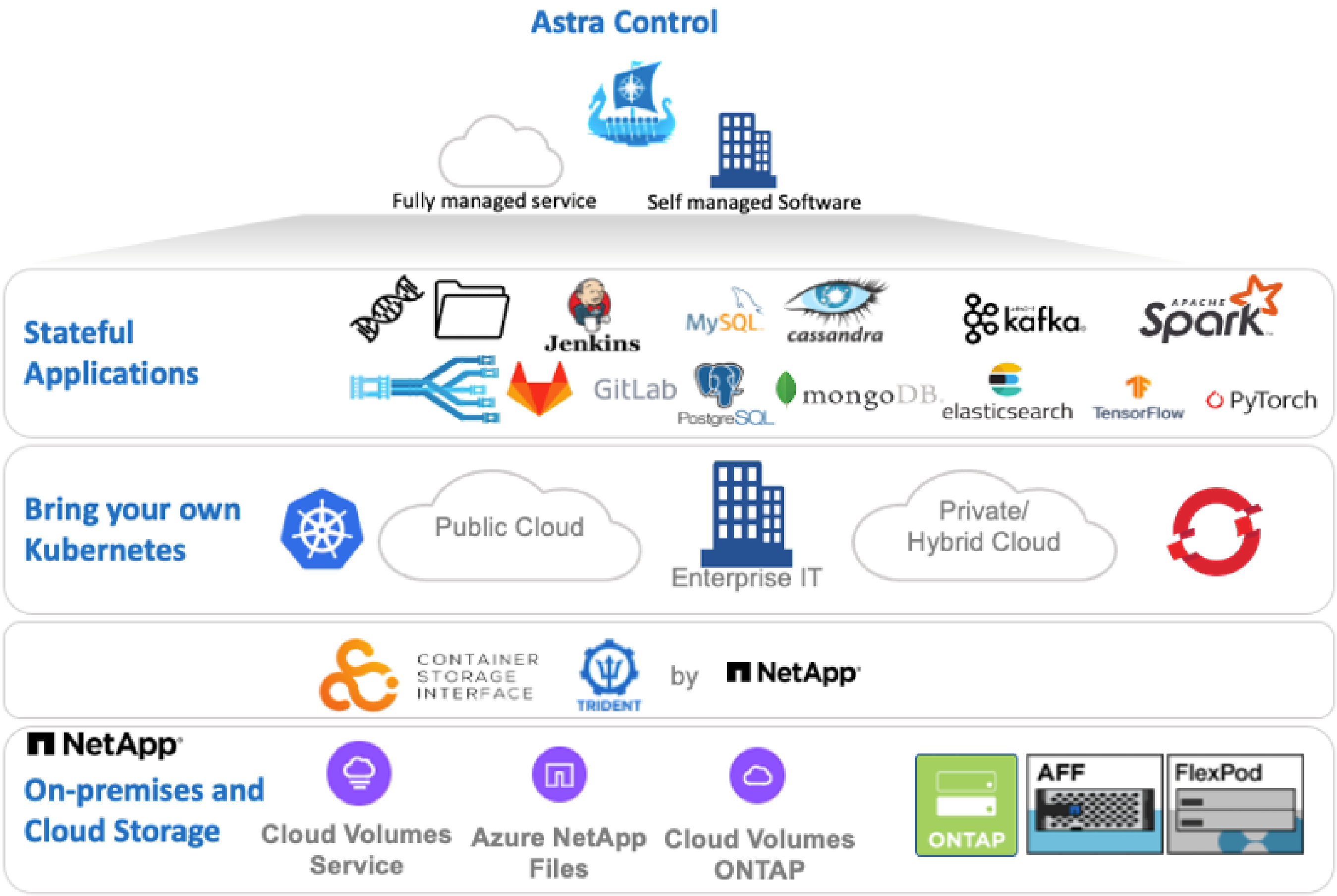
Alan V Cowles, Nikhil M Kulkarni

August 12, 2021

Table of Contents

NetApp Astra Control Center Overview: Red Hat OpenShift with NetApp

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads, deployed in an on-premises environment, powered by NetApp's trusted data protection technology.



NetApp Astra Control Center can be installed to a Red Hat OpenShift cluster which has Astra Trident storage orchestrator deployed, configured with storage classes, and storage backends to NetApp ONTAP storage systems.

For the installation and configuration of Astra Trident to support Astra Control Center, see the section in this document, here.

In a cloud-connected environment, Astra Control Center uses Cloud Insights to provide advanced monitoring and telemetry. In the absence of a Cloud Insights connection, limited (7-days worth of metrics) monitoring and telemetry will be available and also exported to Kubernetes native monitoring tools (Prometheus/Grafana) through open metrics endpoints.

Astra Control Center is fully integrated into the NetApp AutoSupport/Active IQ ecosystem to provide support for users, provide assistance with troubleshooting, and display usage statistics.

In addition to the paid version of Astra Control Center, a 90-day evaluation license will be made available to customers. The evaluation version will be supported through the email and community (Slack channel). Customers have access to these and other knowledge-base articles and the documentation available from the in-product support dashboard.

To get started with NetApp Astra Control Center, visit https://cloud.netapp.com/astra.

Astra Control Center Installation Prerequisites

1. One or more Red Hat OpenShift clusters.

   Currently versions 4.6 EUS and 4.7 are supported.

2. Astra Trident must be already installed and configured on each Red Hat OpenShift cluster.
3. One or more NetApp ONTAP storage systems running ONTAP 9.5 or greater.

   It's best practice for each OpenShift install at a site to have a dedicated SVM for persistent storage. Multi-site deployments would require additional storage systems.

4. A Trident storage backend must be configured on each OpenShift cluster with an SVM backed by an ONTAP cluster.
5. A default StorageClass configured on each OpenShift cluster with Astra Trident as the storage provisioner.
6. A load balancer must be installed and configured on each OpenShift cluster for load balancing and exposing OpenShift Services.

   Refer to the link here for information about load balancers that have been validated for this purpose.

7. A private image registry must be configured to host the NetApp Astra Control Center images.

   Refer the link here to install and configure an OpenShift private registry for this purpose.

8. You must have Cluster-Admin access to the Red Hat OpenShift cluster.
9. You must have Admin access to NetApp ONTAP clusters.
10. An admin workstation with docker or podman, tridentctl, and oc or kubectl tools installed and added to your $PATH.

    Docker or Podman installations must be at least version 20.10.

Install Astra Control Center

1. Log into NetApp Support Site and download the latest version of NetApp Astra Control Center. This requires a license to be attached to your NetApp account. Once you download the tarball, transfer it to the admin workstation.

   To get started with a trial license for Astra Control, visit the site here

2. Unpack the tar ball and change the working directory to the resulting folder.

```
[netapp-user@rhel7 ~]$ tar -vxzf astra-control-center-21.08.57.tar.gz
[netapp-user@rhel7 ~]$ cd astra-control-center-21.08.57
```

3. Before we start the installation, we need to push the Astra Control Center images to an image registry.

> You can choose to do this with either Docker or Podman, instructions for both are provided in this step.

podman

a. Export the registry FQDN with the organization/namespace/project name as a environment variable ‘registry’.

```
[netapp-user@rhel7 ~]$ export registry=astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra
```

b. Log into the registry.

```
[netapp-user@rhel7 ~]$ podman login -u ocp-user -p password --tls
-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```

c. Create a shell script file and paste the below content in it.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar); do
   astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image(s): //')
   podman tag $astraImage $registry/$(echo $astraImage | sed
's/^[^\/]\+\///')
   podman push $registry/$(echo $astraImage | sed 's/^[^\/]\+\///')
done
```

If you are using untrusted certificates for your registry, edit the shell script and use --tls-verify=false for the podman push command - `podman push $registry/$(echo $astraImage | sed 's/[\/]\+\///') --tls -verify=false`

d. Make the file executable.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. Execute the shell script.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

docker

a. Export the registry FQDN with the organization/namespace/project name as a environment variable ‘registry’.

```
[netapp-user@rhel7 ~]$ export registry=astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra
```

b. Log into the registry.

```
[netapp-user@rhel7 ~]$ docker login -u ocp-user -p password --tls
-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```

c. Create a shell script file and paste the below content in it.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar); do
   astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //')
   docker tag $astraImage $registry/$(echo $astraImage | sed
's/^[^\/]\+\///')
   docker push $registry/$(echo $astraImage | sed 's/^[^\/]\+\///')
done
```

If you are using untrusted certificates for your registry, edit the shell script and use --tls-verify=false for the docker push command - `docker push $registry/$(echo $astraImage | sed 's/[\/]\+\///') --tls -verify=false`

d. Make the file executable.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. Execute the shell script.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

4. The next step is to upload the image registry TLS certificates to the OpenShift nodes. For that, create a configmap in openshift-config namespace using the TLS certificates and patch it to the cluster image config to make the certificate trusted.

```
[netapp-user@rhel7 ~]$ oc create configmap default-ingress-ca -n
openshift-config --from-file=astra-registry.apps.ocp
-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"default-ingress-ca"}}}'
--type=merge
```

> ℹ If you are using OpenShift internal registry with default TLS certificates from the ingress operator with a route, you will still need to follow the above step to patch the certificates to the route hostname. To extract the certificates from ingress operator, you can use the command - `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`

5. Create a namespace `acc-operator-system` for installing the Astra Control Center Operator.

```
[netapp-user@rhel7 ~]$ oc create ns acc-operator-system
```

6. Create a secret with credentials to log into the image registry in `acc-operator-system` namespace.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-
cred --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com --docker
-username=ocp-user --docker-password=password -n acc-operator-system
secret/astra-registry-cred created
```

7. Edit the Astra Control Center Operator CR `astra_control_center_operator_deploy.yaml` which is a set of all resources Astra Control Center deploys. In the operator CR, find the deployment definition for `acc-operator-controller-manager` and enter the FQDN for your registry along with the organization name as it was given while pushing the images to registry (in this example, astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra) by replacing the text `[your.registry.goes.here]` and provide the name of the secret we just created. Verify other details of the operator, save and close.

```
[netapp-user@rhel7 ~]$ vim astra_control_center_operator_deploy.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: acc-operator-system
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-
astra/kube-rbac-proxy:v0.5.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-
astra/acc-operator:21.05.68
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 100m
            memory: 150Mi
          requests:
            cpu: 100m
            memory: 50Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: [name: astra-registry-cred]
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

8. Create the operator by running the following command.

```
[netapp-user@rhel7 ~]$ oc create -f
astra_control_center_operator_deploy.yaml
```

9. Create a dedicated namespace for installing all the Astra Control Center resources.

```
[netapp-user@rhel7 ~]$ oc create ns netapp-astra-cc
namespace/netapp-astra-cc created
```

10. Create the secret for accessing image registry in that namespace.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-
cred --docker-server= astra-registry.apps.ocp-vmw.cie.netapp.com
--docker-username=ocp-user --docker-password=password -n netapp-astra-cc

secret/astra-registry-cred created
```

11. Next step is to edit the Astra Control Center CRD file `astra_control_center_min.yaml` and fill the FQDN, image registry details, administrator email address and other details.

```
[netapp-user@rhel7 ~]$ vim astra_control_center_min.yaml

apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  astraVersion: "21.08.57"
  astraAddress: "astra-control-center.cie.netapp.com"
  autoSupport:
    enrolled: true
  email: "solutions_tme@netapp.com"
  imageRegistry:
    name: "astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra"
# use your registry
    secret: "astra-registry-cred"             # comment out if not
needed
```

12. Create the Astra Control Center CRD in the namespace created for it.

```
[netapp-user@rhel7 ~]$ oc apply -f astra_control_center_min.yaml -n
netapp-astra-cc
astracontrolcenter.astra.netapp.io/astra created
```

The above file `astra_control_center_min.yaml` is the minimum version of the Astra Control Center CRD. If you want to create the CRD with more control like defining storageclass other than default for creating PVCs or providing SMTP details for mail notifications, you can edit the file `astra_control_center.yaml`, fill those details and use it to create the CRD.

Installation Verificaton

1. It might take several minutes for the installation to complete. Verify that all the pods and services in netapp-astra-cc namespace are up and running.

```
[netapp-user@rhel7 ~]$ oc get all -n netapp-astra-cc
```

2. Check the `acc-operator-controller-manager` logs to ensure that the installation is completed.

```
[netapp-user@rhel7 ~]$ oc logs deploy/acc-operator-controller-manager -n
acc-operator-system -c manager -f
```

The following message should be displayed to indicate the successful installation of Astra Control Center

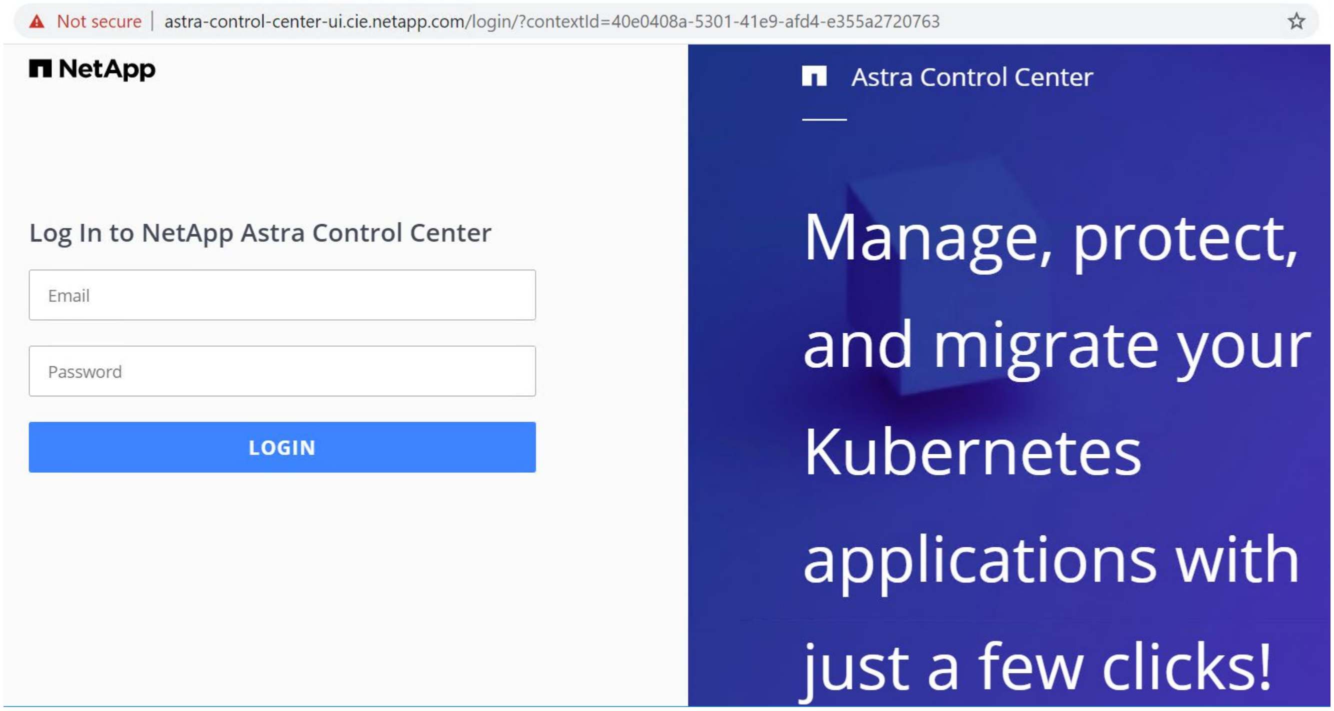
```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[21.08.57]"}
```

3. The username for logging into Astra Control Center is the email address of the administrator provided in the CRD file and the password is a string ‘ACC-’ appended to the Astra Control Center UUID. Run the following command –

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME    UUID
astra   345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```

In this example, the password is – `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`

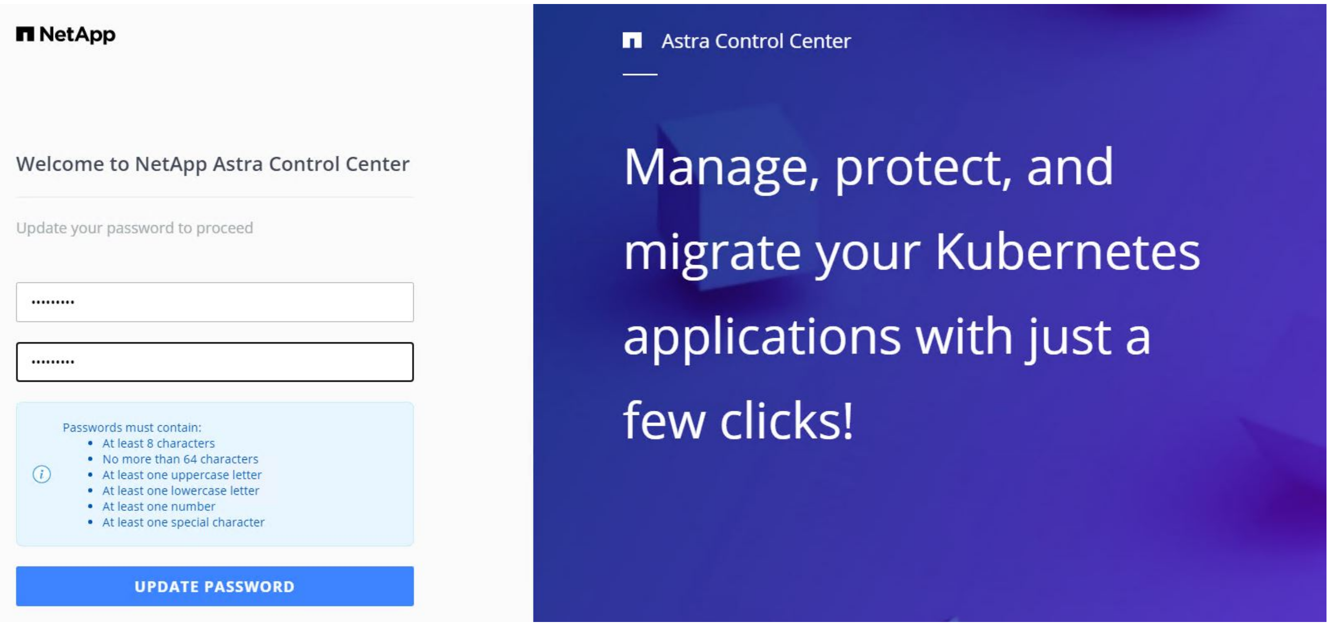
4. Now log into the Astra Control Center GUI by browsing to the FQDN you provided in the CRD file.


Not secure
astra-control-center-ui.cie.netapp.com/login/?contextId=40e0408a-5301-41e9-afd4-e355a2720763
NetApp
Email
Password
LOGIN
Astra Control Center

Log In to NetApp Astra Control Center

Manage, protect, and migrate your Kubernetes applications with just a few clicks!

5. When you log into Astra Control Center GUI for the first time using the admin email address provided in CRD, you will need to change the password.



NetApp

Welcome to NetApp Astra Control Center

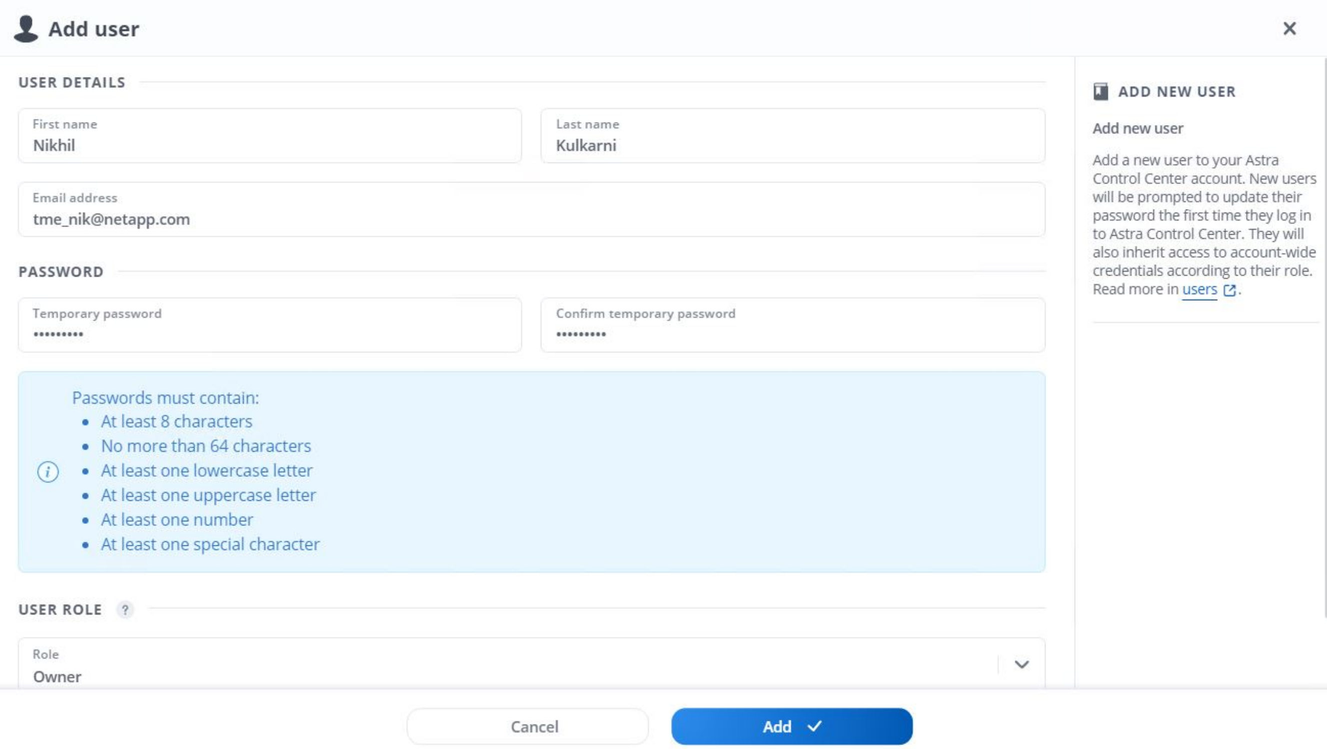
Update your password to proceed

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

UPDATE PASSWORD
Astra Control Center
Manage, protect, and migrate your Kubernetes applications with just a few clicks!

6. If you wish to add a user to Astra Control Center, go to `Account` → `Users` and click on `Add` and enter the details of the user and click `Add`.



Add user

USER DETAILS

First name: Nikhil

Last name: Kulkarni

Email address: tme_nik@netapp.com

PASSWORD

Temporary password: •••••••••

Confirm temporary password: •••••••••

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE

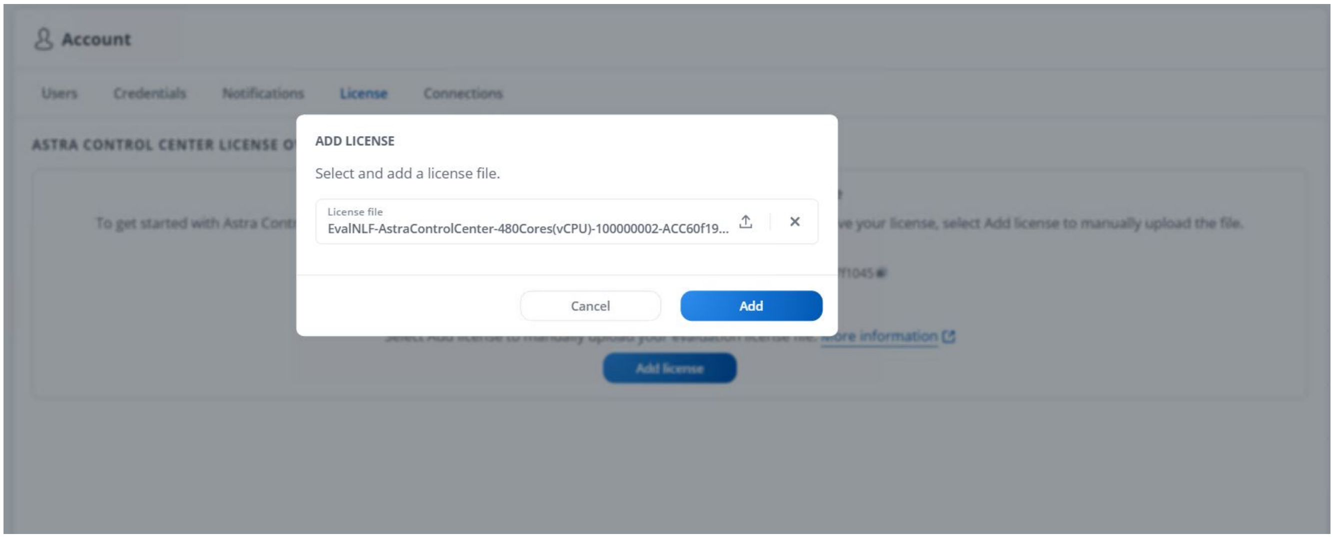
Role: Owner

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in users.

7. Astra Control Center requires a license for all of it’s functionalities to work. To add a license, go to `Account` → `License`, click on `Add License` and upload the license file.



ADD LICENSE

Select and add a license file.

License file
EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

If you encounter issues with the install or configuration of NetApp Astra Control Center, the knowledge base of known issues is available here.

Next: Register your Red Hat OpenShift Clusters: Red Hat OpenShift with NetApp.

Copyright Information

Trademark Information