Personas

Platform

Security

Authentication and Identity Providers

Use Case 10

Add two different identity providers and authenticate users from both communities.

#hub-spoke-model #fleet-management #Authentication #Authorization #identity

Red Hat OpenShift

Red Hat Advanced Cluster Management

Access Your cluster!

X.509 Certificate

```
$ export KUBECONFIG=/home/user/auth/kubeconfig
$ oc get nodes
```

you can use the `--kubeconfig` option of the `oc` command.

```
$ oc --kubeconfig /home/user/auth/kubeconfig get
nodes
```

Kubeadmin

After installation completes, OpenShift creates the `kubeadmin` virtual user.

```
...output omitted...
INFO The cluster is ready when 'oc login -u
kubeadmin -p XYZ'
...output omitted...
```

Deleting `kubeadmin` [Virtual User]

A `kubeadmin` user with cluster-admin role needs to be deleted after you configure your providers and grand cluster-admin role to user[s].

```
$ oc delete secret kubeadmin -n kube-system
```

Identity Providers

The Authentication Operator

It runs an OAuth server

An identity provider must be configured and available to the OAuth server.

Multiple providers can be configured at the same time

Examples: HTPasswd, LDAP, and OpenID Connect

```
$ htpasswd -c -B -b /tmp/htpasswd user1 redhat123
$ htpasswd -b /tmp/htpasswd user2 redhat1234

$ oc create secret generic htpasswd-secret \
  --from-file htpasswd=/tmp/htpasswd -n openshift-config
```

Update the OAuth CRD instance and wait for OAuth pods to restart.

```
apiVersion: config.openshift.io/
v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
  - name: my_htpasswd_provider
    mappingMethod: claim
    type: HTPasswd
    htpasswd:
      fileData:
        name: htpasswd-secret
```

Use Case Catalog

Day 1

1. UC01 : Cluster as a service
2. UC02: VM as a service
3. UC03: Namespace as a service
4. UC04: Container as a service
5. UC05: Cloud native as a service
6. UC06: VM migration as a service
7. UC07: Baseline Configuration
8. UC08: Custom Policies
9. UC09: Control Policy Scope
10. UC10: AuthN and Identity Providers
11. UC11: Authorization and RBAC
12. UC12: Zero Trust enforcement
13. UC13: Workload network policies

Day 2

14. UC14: Cross provider connectivity
15. UC15: Hybrid workload
16. UC16: Workload scalability
17. UC17: Cluster autoscaling
18. UC18: Metrics and Logging
19. UC19: Network graphs
20. UC20: Policy violation dashboard
21. UC21: Day 2 Operations
22. UC22: Cluster upgrades
23. UC23: Developer onboarding
24. UC24: Trusted SW supply chain

Day 3 (hands-on workshop)

25. UC25: Node Resiliency
26. UC26: Cluster and site resiliency
27. UC27: Backup & Restore

Hands-on labs

1. UC02: VM as a service
2. UC04: Container as a service
3. UC06: VM migration as a service
4. UC11: Authorization and RBAC
5. UC12: Zero Trust enforcement
6. UC16: Workload scalability
7. UC24: Trusted SW supply chain