# Demo Policies

# Table of Contents



These are policies that my ficticious company "TofuOrg" wants to ensure are applied consistently to our OpenShift Kubernetes environments.

These policies have an annotation `policy.open-cluster-management.io/standards: TofuOrg-Standards` to group them in the ACM console.

*Be sure to see more example policies*

- https://github.com/stolostron/policy-collection
- https://github.com/SimonDelord/ACM-Templates/tree/master/resources12

# Deploy

These policies may be applied by deploying the demo-acm-policies app in this repo and placing it on the ACM hub cluster.

# Policies

## Policy ACS-Operator

### Description

Ensure that the RHACS Operator is installed.

This work is derivative of Simon Delord's https://github.com/SimonDelord/ACM-Templates/tree/master/resources12

*Effect*

- Install RHACM Operator

*Remediation*

- Enforce

*Scope*

- environment=infra

### Deploy

```
oc apply -k .
oc label managedcluster/demo-aws-tofu-org -n demo-aws-tofu-org environment=infra
```

## Policy ACS-Central

Once the RHACS operator is installed it must be configured to act as the "manager" (Central) or an "agent" (SecuredCluster).

To act as the ACS "manager hub" for an environment a `Central` must be created.

The same cluster can be central and secured of course.

*WIP*

- See ../../../apps/acs-instance.yaml

### Description

Ensures that a cluster is configured to host ACS Central services

*Effect*

- Create Application to deploy ACS Central and generate cluster init
- Create Subscription to above Application
- Apply Subscription

*Remediation*

- Enforce

*Scope*

- environment=infra

### Deploy

```
oc apply -k .
oc get central -n stackrox
oc get secrets -n stackrox | grep tls
```

### Todo

*Bugs*

- Because it uses `Channel` CR, this policy fails when applied to a custer that does not have ACM operator and associated open-cluster-management.io API groups installed. Installing RHACM provides the `Channel` resource, but the `Subscription` resource is not recognized. Is that because a `MulticlusterHub` must be created first or a flaw in my policy?
  - Possible fix: write a policy to install RHACM, use GitOps instead?
  - Symptom: *NonCompliant; violation - couldn't find mapping resource with kind Subscription, please check if you have CRD deployed View details*
  - Note: Maybe reconciliation is lagging. Waiting. TBD

## Policy ACS-SecuredCluster

### Description

Ensure that cluster is secured by ACS.

See also https://github.com/stolostron/policy-collection/tree/main/policygenerator/policy-sets/community/openshift-plus

*Effect*

- Create SecuredCluster resource with proper endpoint and TLS secretes from Stackrox cluster init bundle.

*Remediation*

- Enforce

*Scope*

- vendor=OpenShift

### Deploy

```
oc apply -k .
```