AppArmor Administration

Kubernetes does not provide in native mechanisms for loading AA profiles onto nodes.

Possible methods to setup profiles

1. DaemonSet that runs on pods to ensure correct profiles are loaded. Example.
2. At node initialization time, using your node initialization scripts (e.g. Salt, Ansible, etc.) or image. (YAML file)
3. By copying the profiles to each node and loading them through SSH, as demonstrated in the Example.

Or you can add a node label for each profile on the node, and use a selector to ensure the Pod is run on a node wit the required profile.

You can enable cluster-wide AA restrictions if the PodSecurityPolicy extension is enabled. The flag must be set on the apiserver

```
--enable-admission-plugins=PodSecurityPolicy[,others...]
```

The AppArmor options can be specified as annotations on the PodSecurityPolicy:

```
apparmor.security.beta.kubernetes.io/defaultProfileName: <profile_ref>
apparmor.security.beta.kubernetes.io/allowedProfileNames: <profile_ref>[,others...]
```

default → profile to apply for containers when none are specified.

allowed → specifies a list of profiles that Pod containers are allowed to be run with

If both provided, default must be allowed.