Kubernetes SIG-Auth Update

KubeCon Austin - Dec, 2017

Overview: this session

- Overview of recent Kubernetes SIG-auth features
  - See this for up to date recommendations: https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/
- Future roadmap
- Questions

RBAC (1.6+)

- https://kubernetes.io/docs/admin/authorization/rbac/
- GA in 1.8
- Enabled by default by almost all install tools

Kubelet client cert bootstrapping and rotation (1.7+)

- https://kubernetes.io/docs/admin/kubelet-tls-bootstrapping/
- Kubelets request credentials via CSR API for initial bootstrap and renewal
- Credentials and identity are unique to each node
- Approval of CSRs can be controlled through RBAC (1.7)

Node authorizer and admission controller (1.7+)

- https://kubernetes.io/docs/admin/authorization/node/
- Nodes can only access resources required to run pods scheduled to them
  - Can no longer request arbitrary secrets
- Requires unique credentials for nodes (Pairs well with TLS bootstrapping)
- Use in combination with RBAC

Pod security policies (1.8+)

- https://kubernetes.io/docs/concepts/policy/pod-security-policy/
- Restricts the kind of pods that can be created in a namespace
- Administered through RBAC (or external authorizer)
- Can prevent a user from creating pods that:
  - mount arbitrary volumes
  - run in the host network
  - use privileged containers
  - run processes as root
  - etc.

Advanced audit logs (1.8+)

- https://kubernetes.io/docs/tasks/debug-application-cluster/audit/
- Improved audit logging:
  - Policy to control what events get audited and at what level (headers, request body, etc.)
  - JSON formatted audit logs
  - Webhook mode to aggregate audit events across multiple API servers
- Tooling can consume/act on the new audit format:
  - https://github.com/liggitt/audit2rbac
  - ...

Authorizer improvements (1.8-1.9)

- RBAC aggregated cluster roles (1.9+)
  - Easily contribute custom permissions to default “user-facing” roles
- External authorizer short-circuit deny (1.9+)
  - External authorizers can now override RBAC
- SelfSubjectRulesReview (1.8+)
  - Authorizer API for determining what the current user can do

Planned for 1.10: NodeRestriction enhancements

- https://github.com/kubernetes/community/pull/911
- Lock down kubelet self-modification
- Remove kubelets' ability to label themselves arbitrarily
- Remove kubelets' ability to untaint themselves

Planned for 1.10: Secret encryption at rest

- https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/
- Alpha since 1.7
- New external encrypt/decrypt extension point planned for 1.10
- External KMS integration (Vault, Google, Azure) via extension point

Planned for 1.10: Service account improvements

- https://github.com/kubernetes/community/pull/1460
- Service account credential improvements
- Goal is to allow moving service account tokens out of Secret API objects
- Point of use creation, attenuated by node/pod, with bounded lifetime

Planned for 1.10: kubectl auth providers

- https://github.com/kubernetes/kubernetes/issues/55968
- Pluggable bearer token rotation for kubectl

Ongoing efforts: Container Identity WG

- https://github.com/kubernetes/community/tree/master/wg-container-identity
- Better identities for containers than service accounts
  - Differentiate between pods running on different nodes
  - Scoped identities that only work for target services
- Improved container identities enable external secret management
- Focus on mechanisms for delivering credentials/identity directly to pods

Future efforts: TLS bootstrapping and rotation

- https://github.com/kubernetes/features/issues/267
- Server certificate rotation to beta
- Kubelet address validation
- Attestation as part of CSR process

Future efforts: external authorizers

- https://github.com/kubernetes/community/pull/1458
- Improve ability to self-host webhook authorizers

Future efforts: PodSecurityPolicy

- https://github.com/kubernetes/kubernetes/issues/56174
- Move out of extensions/v1beta1
- GCE enabled
- API improvements

Future efforts: docs

- https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/
- https://github.com/kubernetes/kubernetes/issues/52184
- Keep security recommendations up to date
- Continue to refine and improve docs for new and existing features

Questions?

https://github.com/kubernetes/community/tree/master/sig-auth