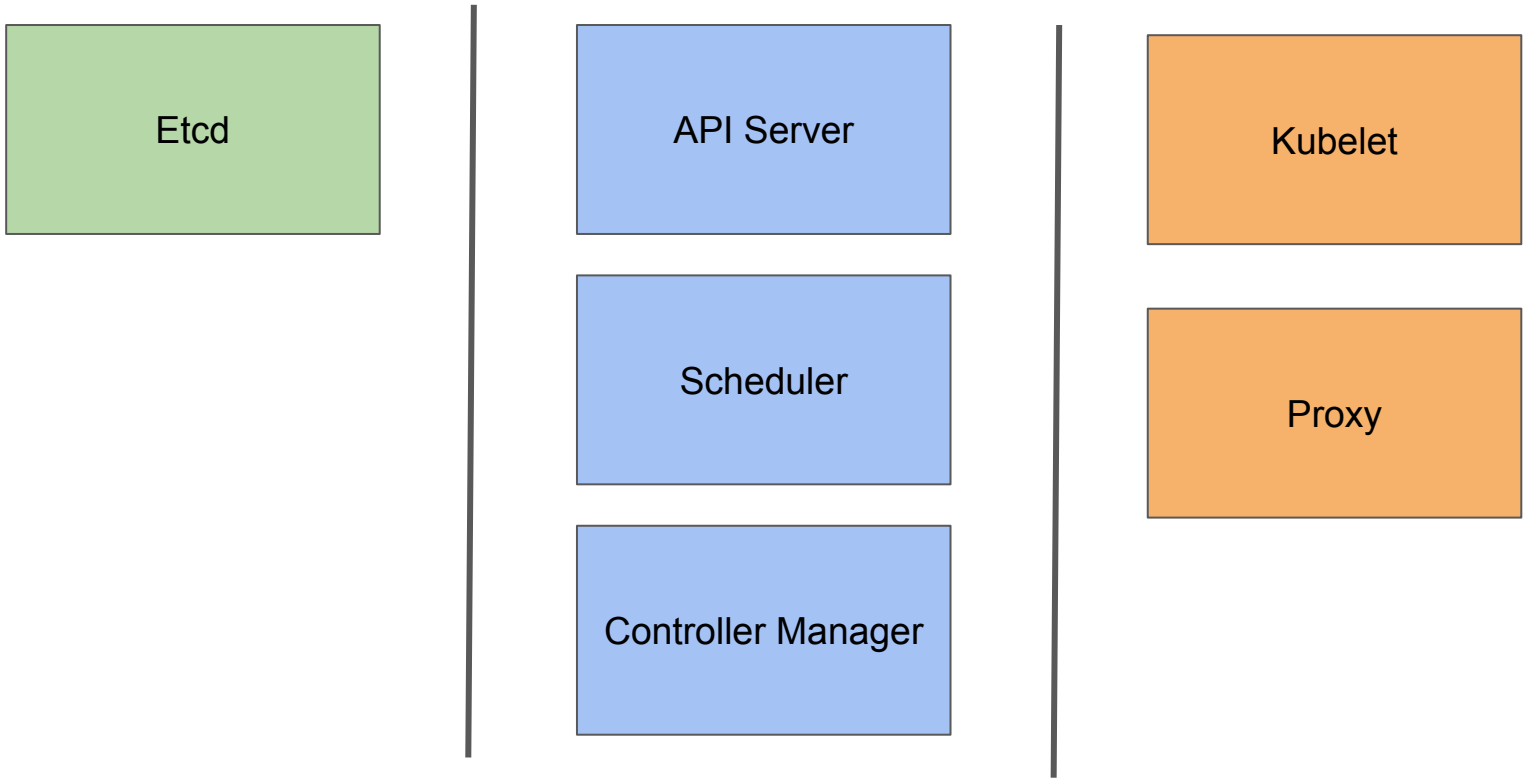
Descomponiendo Kubernetes

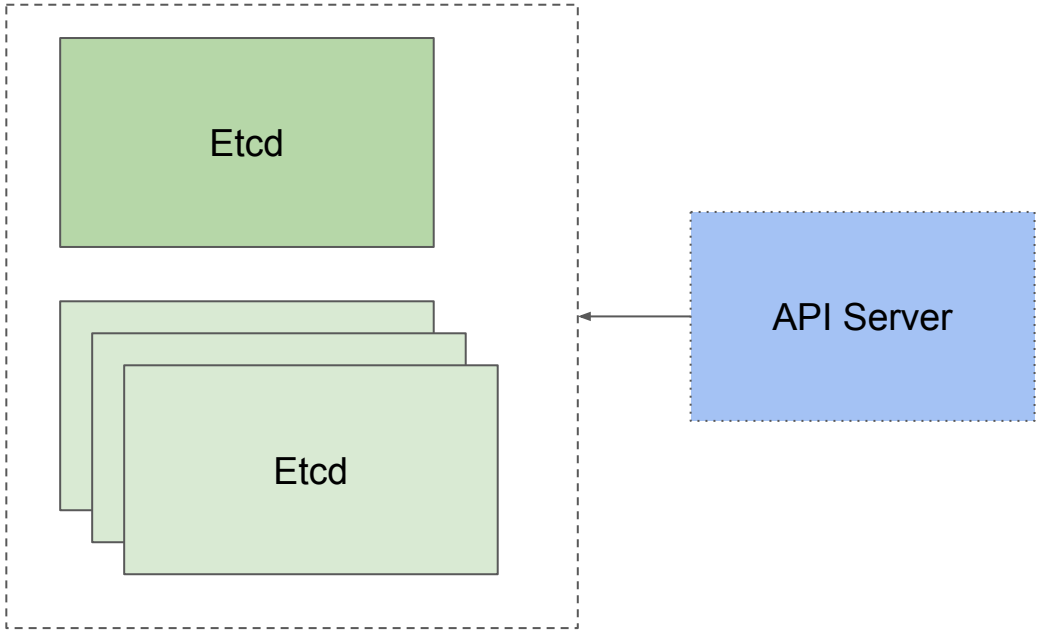
STACKPOINTCLOUD

Pablo
@pablme
pablo (at) stackpointcloud.com

Kubernetes Components

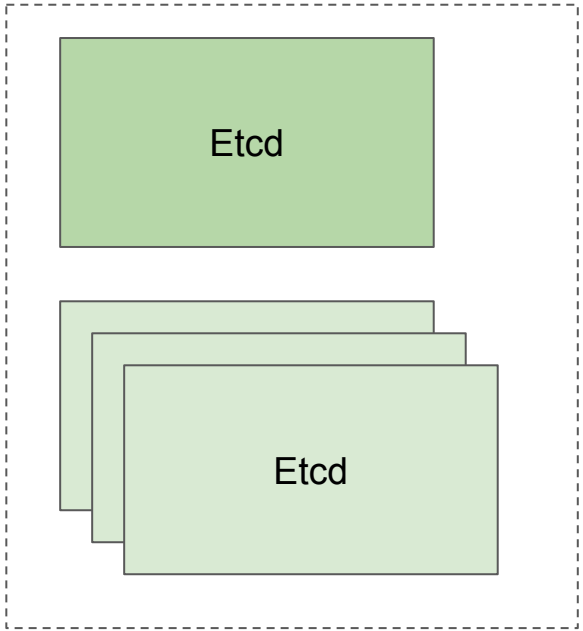


Etcd

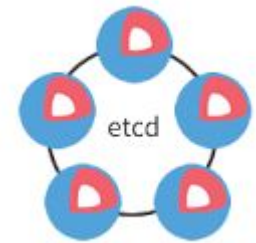


- ❏ Distributed KV
- ❏ Raft based
- ❏ HTTP
- ❏ TLS
- ❏ Auth Client Certificates
- ❏ gRPC
- ❏ Watch
- ❏ TTL - Leases
- ❏ Multiversion

Etcd setup



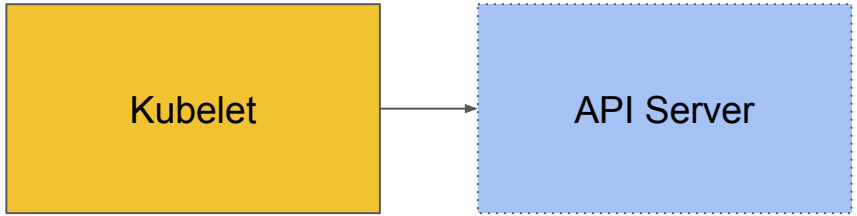
Etcd
Proxy



Static cluster
Discovery
- URL
- Reverse DNS

Etcd Operator

Kubelet



- Creates PODs
  - API Server
  - Manifest dir
  - Remote endpoint
  - Kubelet API (WIP)

Also deals with Network and Volume plugins

Kubelet setup

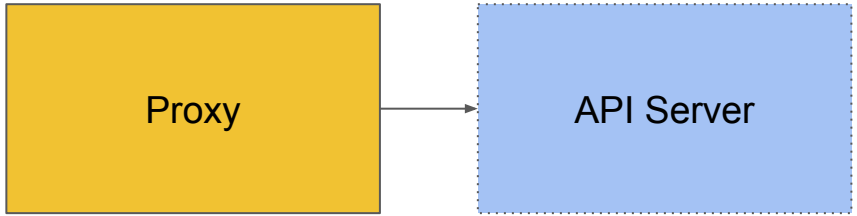
- Deployment
  - Init System
  - Self Hosted (WIP)
- Parameters

  --kubeconfig=...
  --allow-privileged
  --cluster-dns-ip=...
  --cluster-domain=...
  --pod-manifest-path=...
  --network-plugin=cni

Kubelet tips

- Kubelet is able to start pods with host network, without need to setup CNI
- If a Pod needs to access itself through a service, check the --hairpin-mode parameter
- Node name is taken from the hostname. You can override it with --hostname-override
- Kubelet files can be found at /var/lib/kubelet
- Can speed up pulls --serialize-image-pulls=false

Proxy



- Manages service routing
  - pods to services
  - out of cluster routing
  - Nodeports

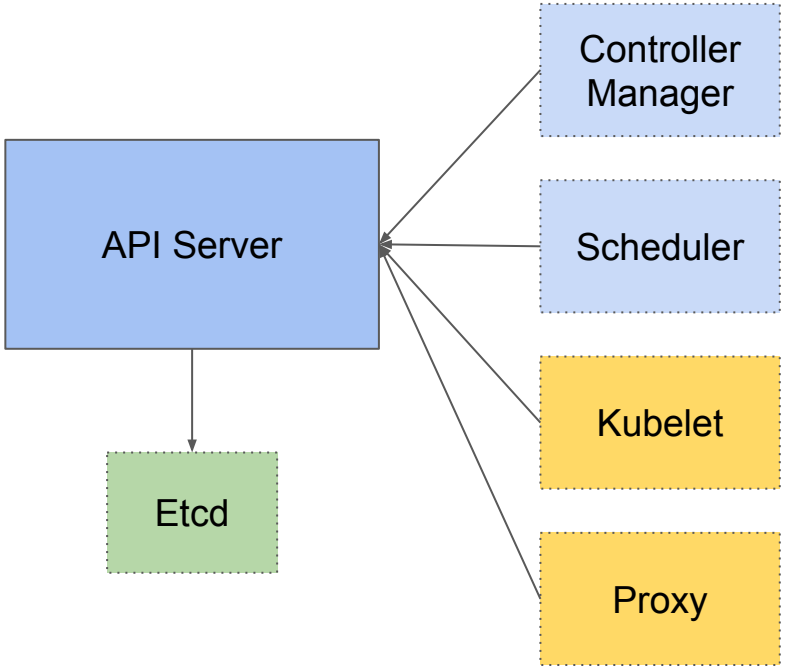
- Deployment
  - Init System
  - Daemonset
- Parameters

  --kubeconfig=...
  --proxy-mode=iptables
  --cluster-cidr=...
  --hostname-override=

Proxy tips

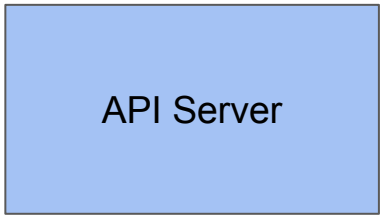
- If you need to remove iptables generated by kube-proxy, use --cleanup-iptables
- Under heavy traffic, conntrack parameters should be tuned

API Server



- Exposes the API
- Control Plane coordinator
  Scheduler
  Controller Manager
- Kubelet interaction
- Pod interaction
  Fetch pod logs through kubelet
  Attach to pod through kubelet

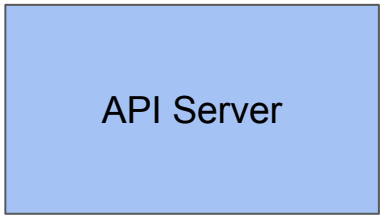
API Server setup (I)



- Deployment
  - Init System
  - DaemonSet + nodeSelector
- Parameters
  - --advertise-address
  - --etcd-servers
  - --storage-backend
  - --allow-privileged
  - --service-cluster-ip-range
  - --admission-control

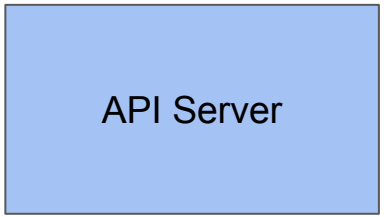
The admission control param hold a list of plugins that modify the acceptance/behaviour/ content of the request

API Server setup (II)



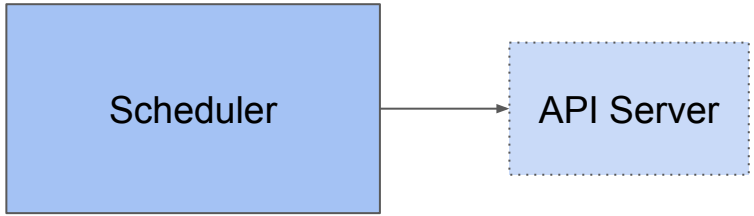
- Parameters (continued)
  - --runtime-config=api/all=true
  - --tls-cert-file=
  - --tls-private-key-file=
  - --service-account-key-file=
  - --client-ca-file=
  - --authorization-mode=RBAC
  - --anonymous-auth=false
  - --apiserver-count=
  - --etcd-cafile=
  - --etcd-cert-file=
  - --etcd-key-file=
  - --audit-log-maxsize=

API Server tips



- Backup etcd and certificates
- HA is not fault tolerant yet. You can try a balancer in front of multiple API Servers #22609
- RBAC is the way to go, but is alpha
- Operate with kubectl, Automate with HTTPS

Scheduler

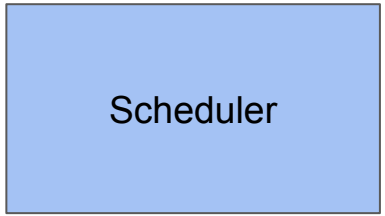


- Assign pods to nodes
  - Watch pod requests
  - Resources aware
  - Policies aware
- Deployment
  - Init System
  - Deployment
- Parameters

  --kubeconfig=...

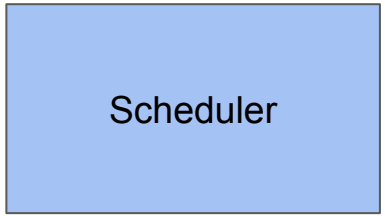
  --algorithm-provider=...

Scheduler tips



- Use --leader-elect to HA
- You can use --policy-config-file, but defaults should be OK for most scenarios
- Can have policies per Pod using multiple schedulers with --scheduler-name (Alpha)

Scheduler predicates and policies



Scheduler customization via
--policy-config-file

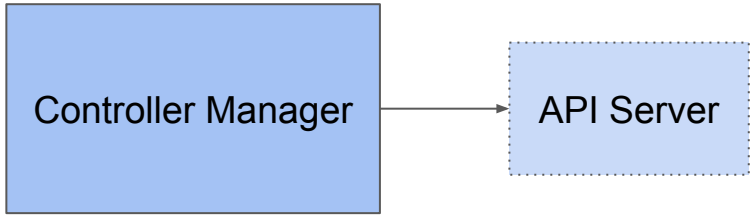
- Predicates to filter nodes
- Priority to rank nodes

Documentation

If you want to group your pods belonging to a service on nodes, use Pod affinity annotations

Documentation

Controller Manager



- Controls lifecycle for kubernetes items
  - Contains the control loop for built-in kubernetes controllers

- Deployment
  - Init System
  - Deployment

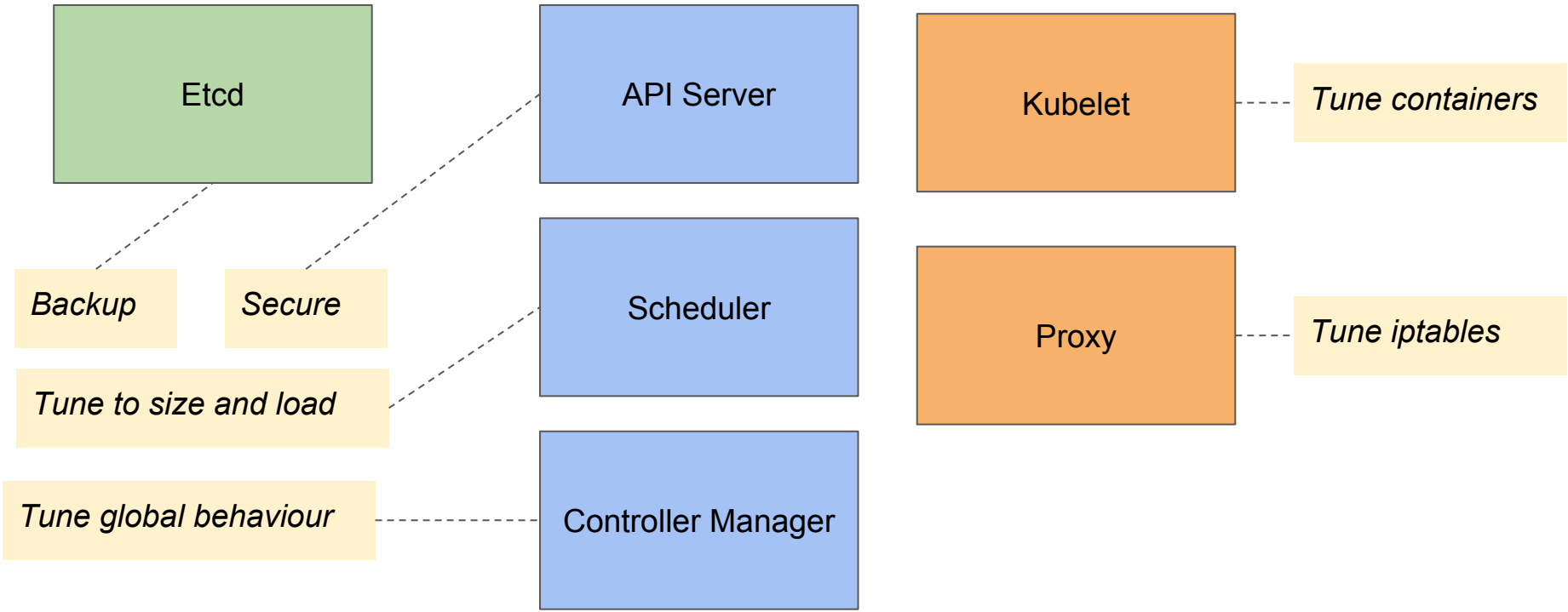
- Parameters
  --kubeconfig=...
  --cluster-cidr=...

Controller Manager tips

- Use --leader-elect to HA
- When in cloud you can
  --allocate-node-cidr
  --configure-cloud-routes
- Using service accounts
  --service-account-private-key
  --root-ca-file
- Special mention:

--insecure-experimental-approve-all-kubelet-csrs-for-group string

Kubernetes Components: oversimplifying our focus



Kubernetes Components: Add-ons and others

DNS	**Overlay**	Ingress	Volumes
Dashboard	Network Policy	Federation	Seccomp
Monitoring	Autoscaler	External DNS	...

Muchas gracias!

Si queréis participar como ponentes en eventos futuros, contactadme:

@pablme
pablo (at) stackpointcloud.com