KubeCon | CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Remote Control Planes With Konnectivity; What, Why And How?

Remote Control Planes With Konnectivity

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2021

Rastislav Szabo
Senior Sw. Engineer
Kubermatic

Jussi Nummelin
Sr. Principal Engineer
Mirantis

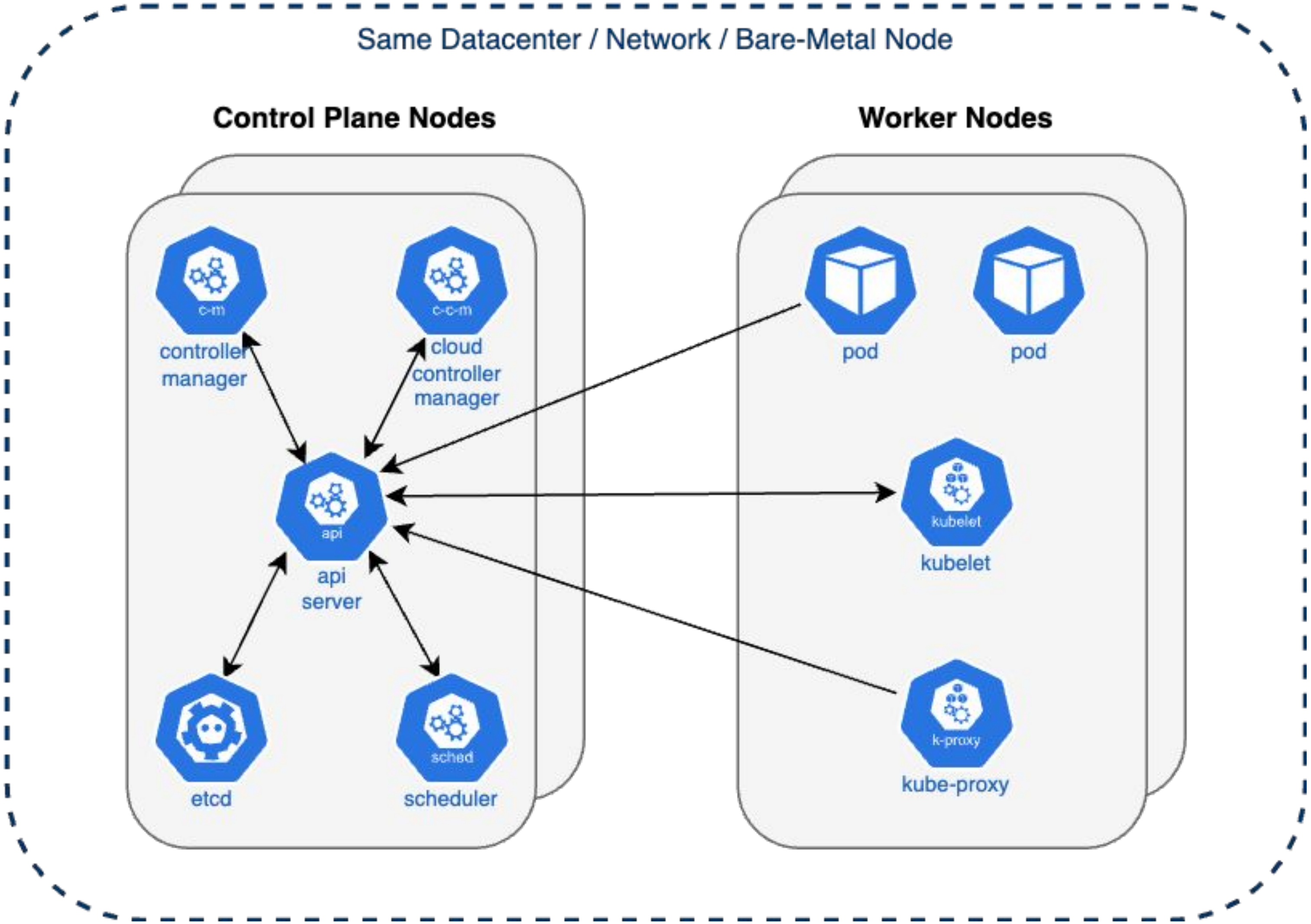
Outline

- What?
  - What do we mean by “Remote Control Planes”
- Why?
  - Example use-cases for remote control planes
- How?
  - Building blocks and concepts to make this happen with a bit of history
  - Real-world integration examples

Acknowledgements

- We’re not the inventors, merely happy users
- There’s very little documentation on the topic → We wanted to raise awareness
- Kudos to the original “inventors” and maintainers

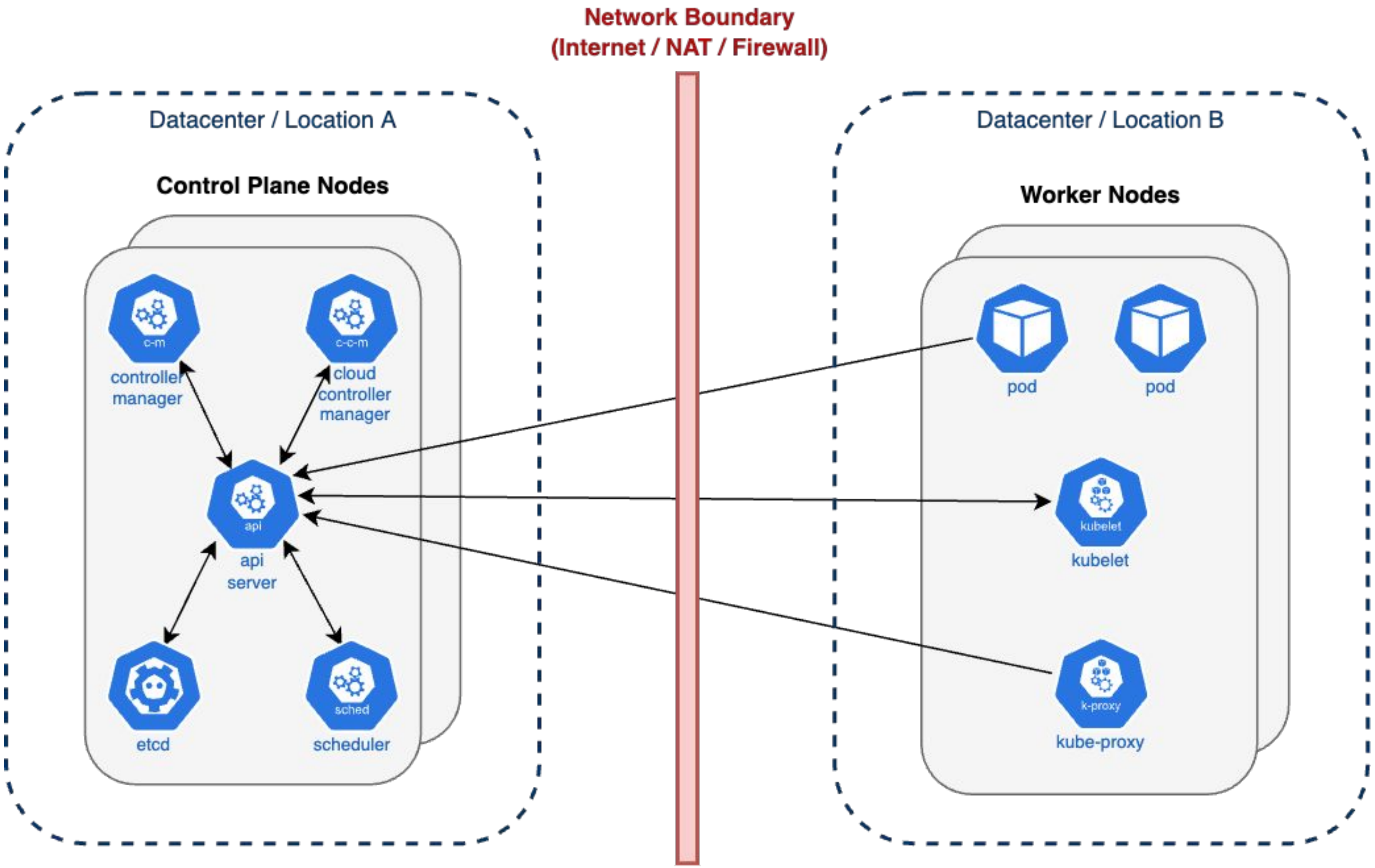
Local Kubernetes Control Plane



Control plane nodes ⇔ worker nodes connection:

- Bidirectional
- Unrestricted
- Fast
- Reliable
- Secure
- Often node-local / rack-local / same L2 network / same datacenter

Remote Kubernetes Control Plane



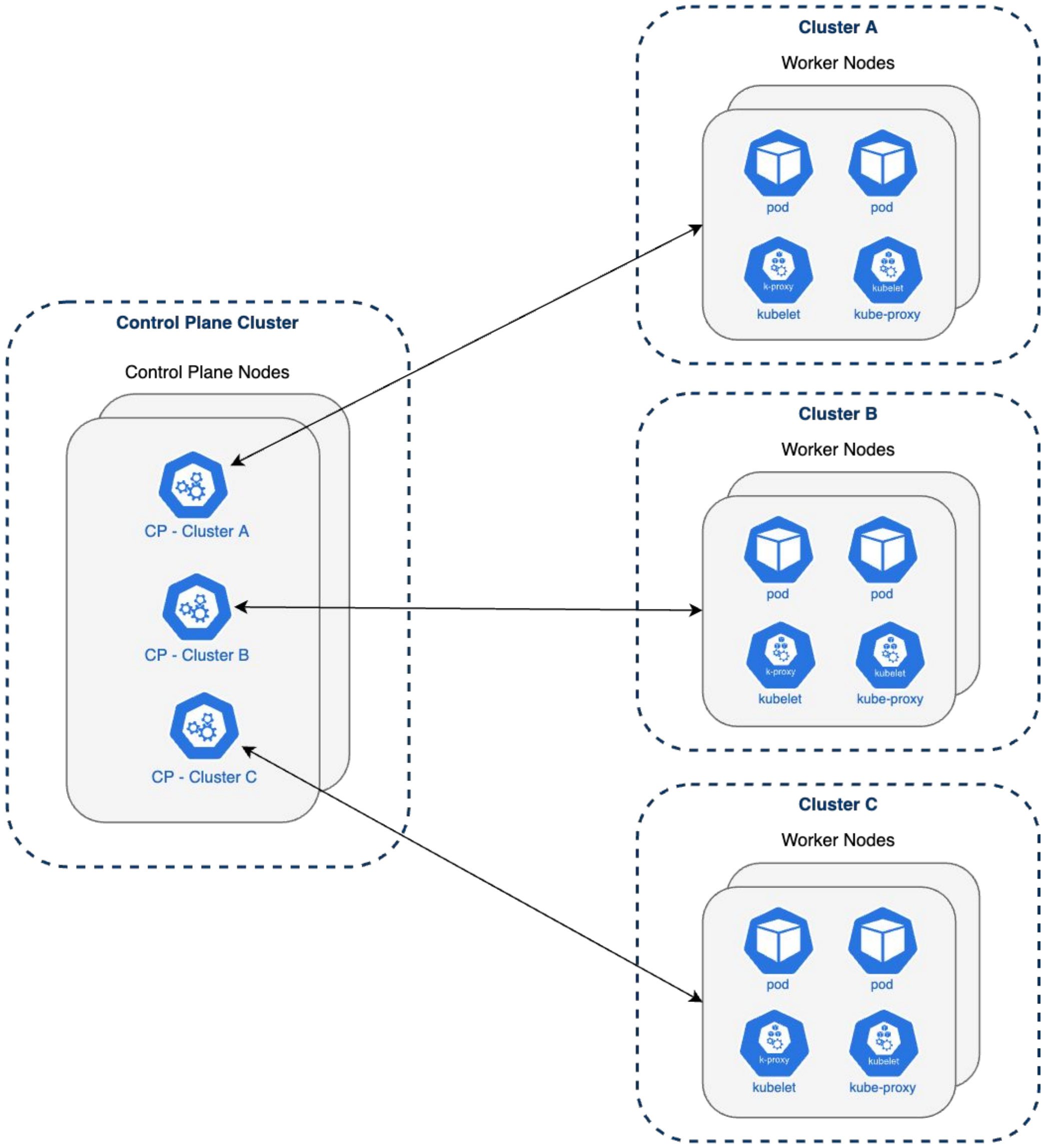
Control plane nodes ⇔ worker nodes connection:

- One-directional (NAT)
- Restricted (Firewall)
- Slower
- Less reliable
- Insecure
- Possibly over public Internet

Remote Control Plane Use Cases / 1

- Trust Segmentation
  - Control Plane in “protected / trusted” network, worker nodes in “untrusted” network
- Human Error Reduction
  - Only specialized personnel can access the control plane nodes / infrastructure
- Kubernetes at Edge
  - Worker nodes (e.g. resource-constrained) at edge, control plane in a datacenter
- Hybrid Cloud
  - Worker nodes on different platform / cloud than the control plane
  - Easy migration of worker-nodes between platforms

Remote Control Plane Use Cases / 2



Co-located control-plane for multiple clusters:

- Easy operation for 100s / 1000s clusters
- HA control plane with wise resource usage
- Same control-plane experience across different (hybrid) cloud platforms
- Fast cluster spin-up time - good for temporary / short-lived clusters
- Build your own Kubernetes as a service

History

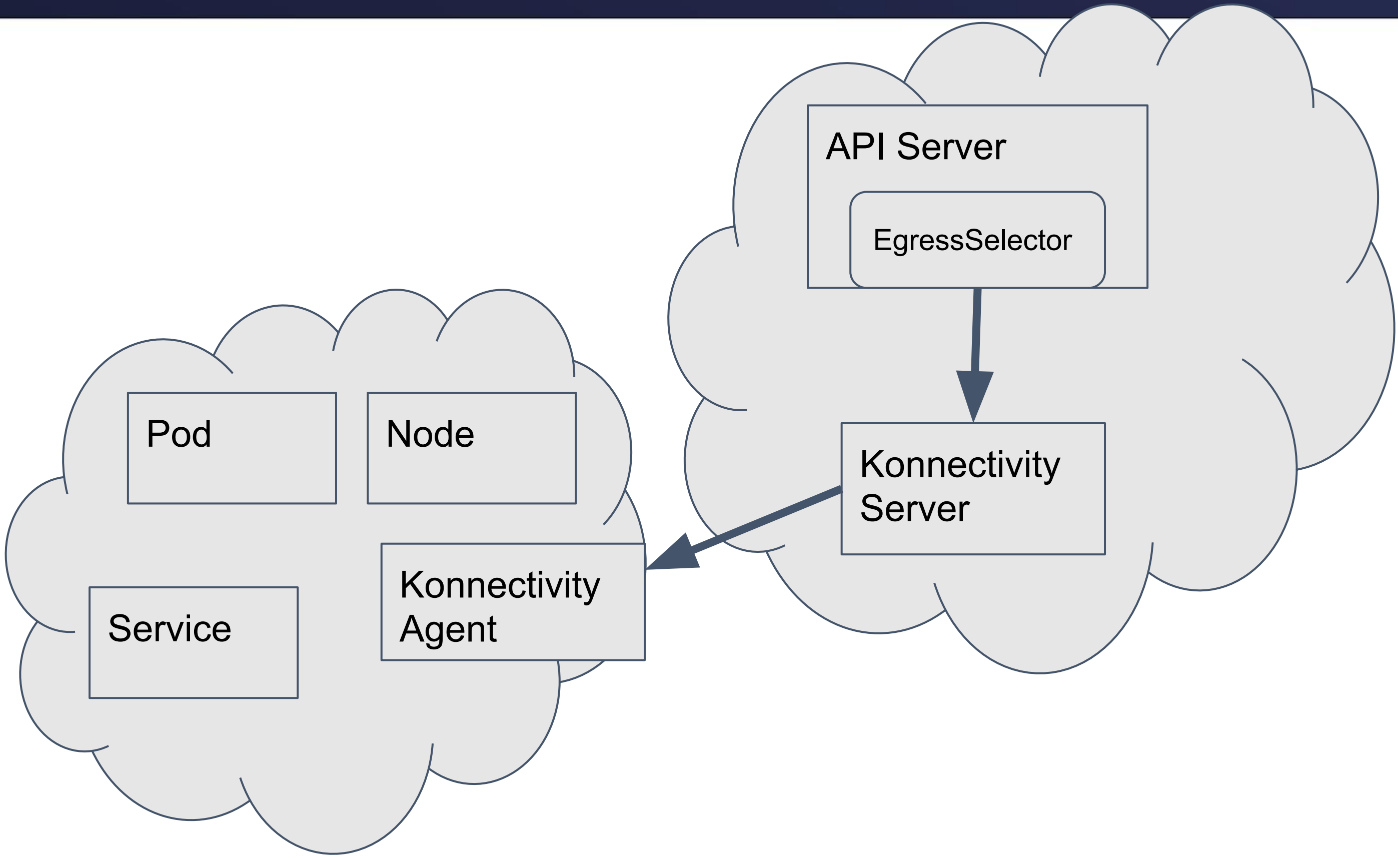
- Kubernetes supported SSH tunnels in the past, deprecated at v1.9
- Various custom solutions using things like VPN tunnels
- KEP-1281 was born in Spring 2019
- KEP-1281 is the architectural foundation for API server → workerplane communication routing

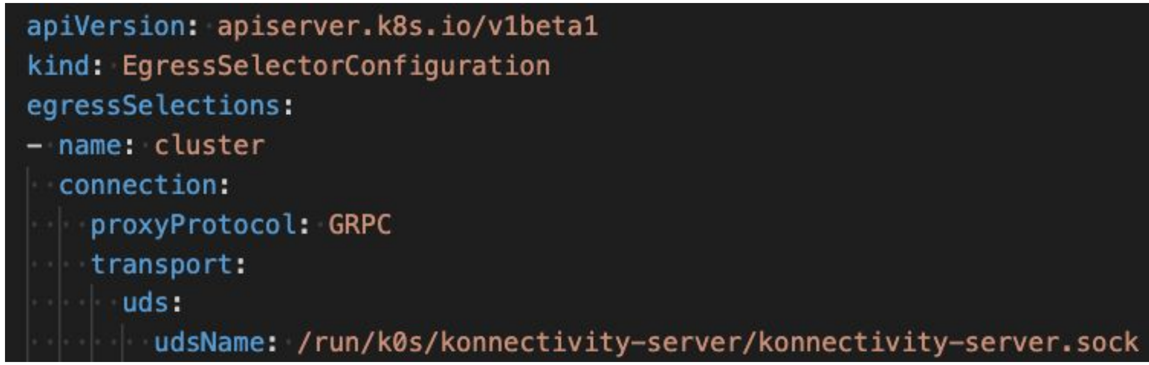
Concepts - EgressSelector

- *EgressSelector* defines how API talks to external components

- Almost like a typical network proxy

- Types: cluster, etcd, controlplane
  - cluster: pods/logs,pods/exec,svc/proxy,...
  - etcd: obviously KAS -> etcd connections
  - controlplane: admission etc. webhooks

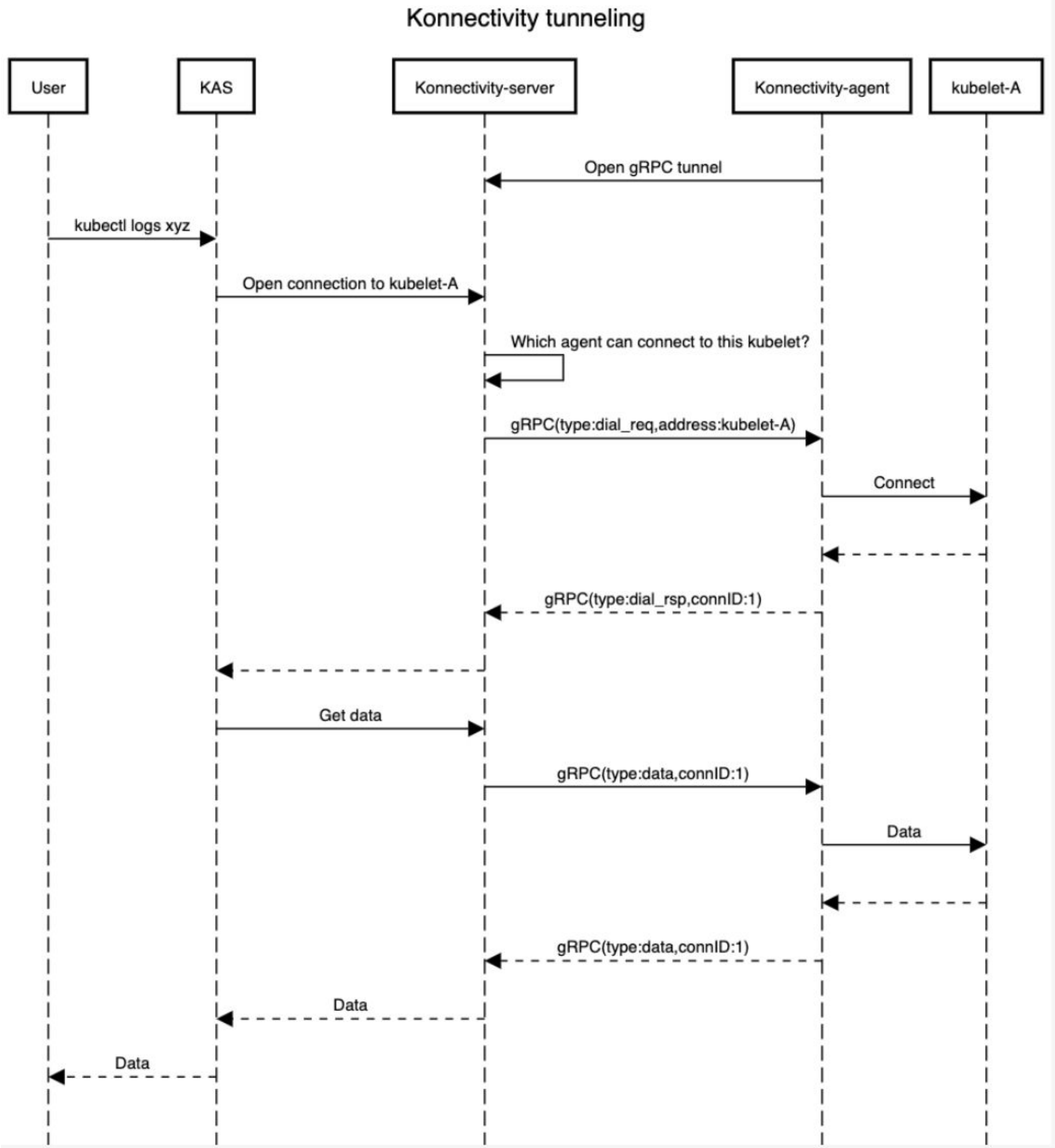




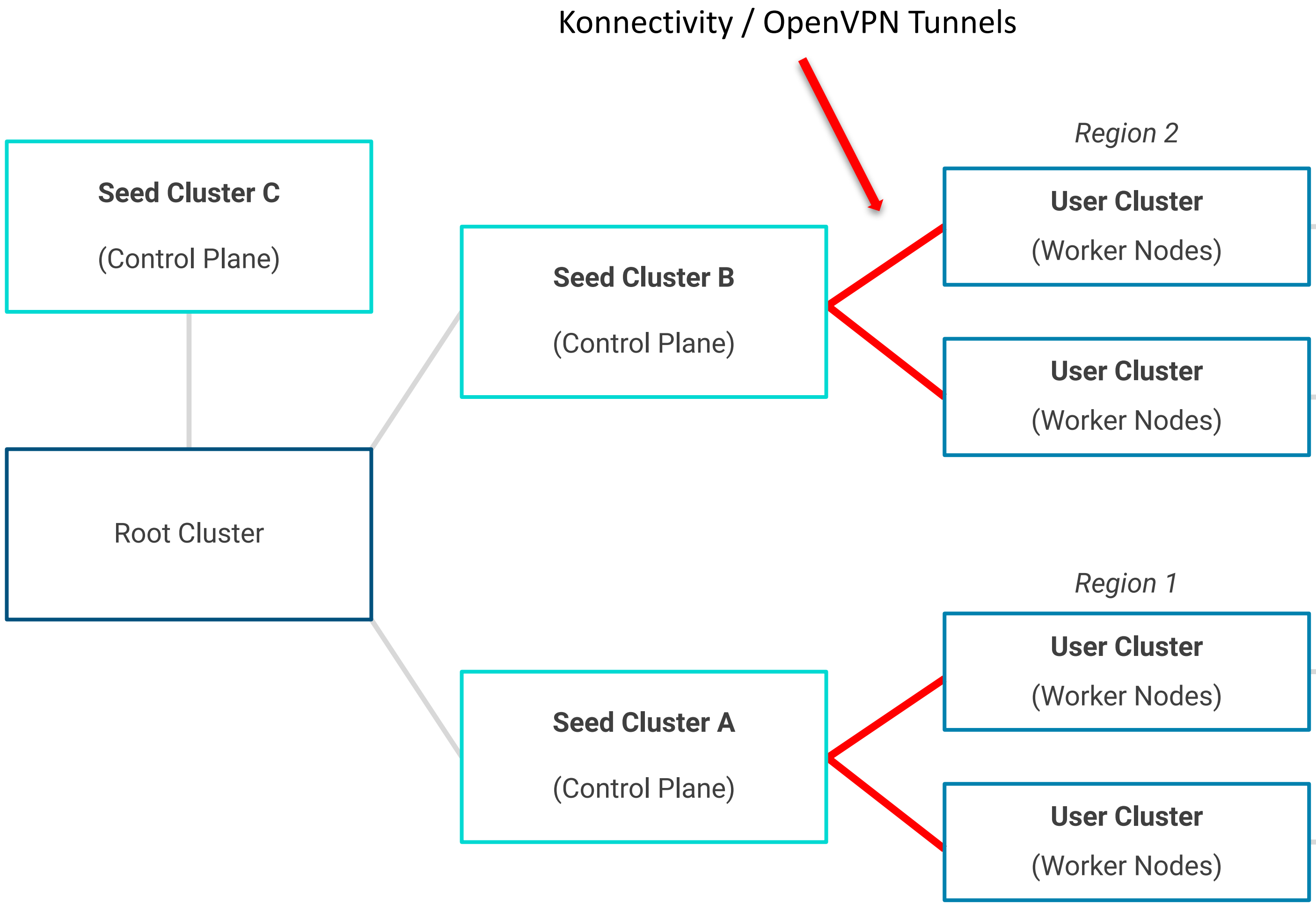
```yaml
apiVersion: apiserver.k8s.io/v1beta1
kind: EgressSelectorConfiguration
egressSelections:
- name: cluster
  connection:
    proxyProtocol: GRPC
    transport:
      uds:
        udsName: /run/k0s/konnectivity-server/konnectivity-server.sock
```

Concepts - Tunneling protocol

- Custom protocol on top of gRPC over TLS
  - Works through NAT/FW/etc.
- Agent opens the bi-directional connection to server
- Much like SSH reverse tunnels



Real-World Integrations - Kubermatic



User Clusters are independently managed

Scales above 2500 clusters easily

Runs on more than 21 Cloud Providers

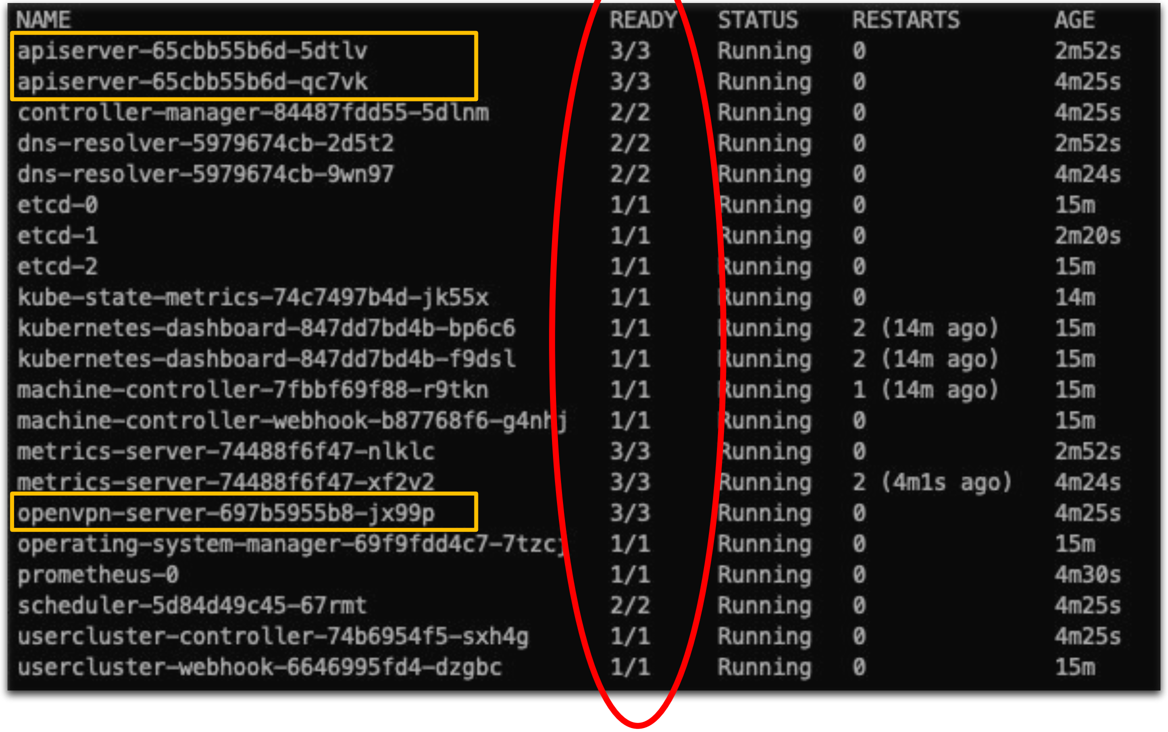
Delivers additional features like Integrated Monitoring

Real-World Integrations - Kubermatic

OpenVPN

35 containers

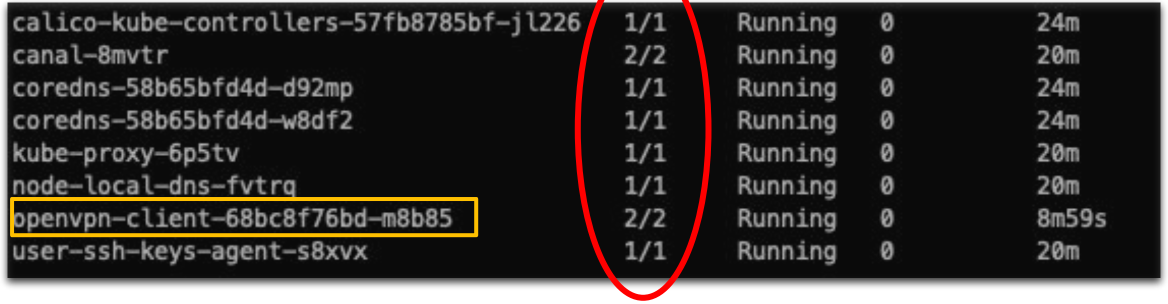
Seed Cluster (Control Plane)



```
NAME                                        READY   STATUS    RESTARTS       AGE
apiserver-65cbb55b6d-5dtlv                  3/3     Running   0              2m52s
apiserver-65cbb55b6d-qc7vk                  3/3     Running   0              4m25s
controller-manager-84487fdd55-5dlnm         2/2     Running   0              4m25s
dns-resolver-5979674cb-2d5t2                2/2     Running   0              2m52s
dns-resolver-5979674cb-9wn97                2/2     Running   0              4m24s
etcd-0                                      1/1     Running   0              15m
etcd-1                                      1/1     Running   0              2m20s
etcd-2                                      1/1     Running   0              15m
kube-state-metrics-74c7497b4d-jk55x         1/1     Running   0              14m
kubernetes-dashboard-847dd7bd4b-bp6c6       1/1     Running   2 (14m ago)    15m
kubernetes-dashboard-847dd7bd4b-f9dsl       1/1     Running   2 (14m ago)    15m
machine-controller-7fbbf69f88-r9tkn         1/1     Running   1 (14m ago)    15m
machine-controller-webhook-b87768f6-g4nhj   1/1     Running   0              15m
metrics-server-74488f6f47-nlklc             3/3     Running   0              2m52s
metrics-server-74488f6f47-xf2v2             3/3     Running   2 (4m1s ago)   4m24s
openvpn-server-697b5955b8-jx99p             3/3     Running   0              4m25s
operating-system-manager-69f9fdd4c7-7tzcj   1/1     Running   0              15m
prometheus-0                                1/1     Running   0              4m30s
scheduler-5d84d49c45-67rmt                  2/2     Running   0              4m25s
usercluster-controller-74b6954f5-sxh4g      1/1     Running   0              4m25s
usercluster-webhook-6646995fd4-dzgbc        1/1     Running   0              15m
```

10 containers

User Cluster (Worker Nodes)



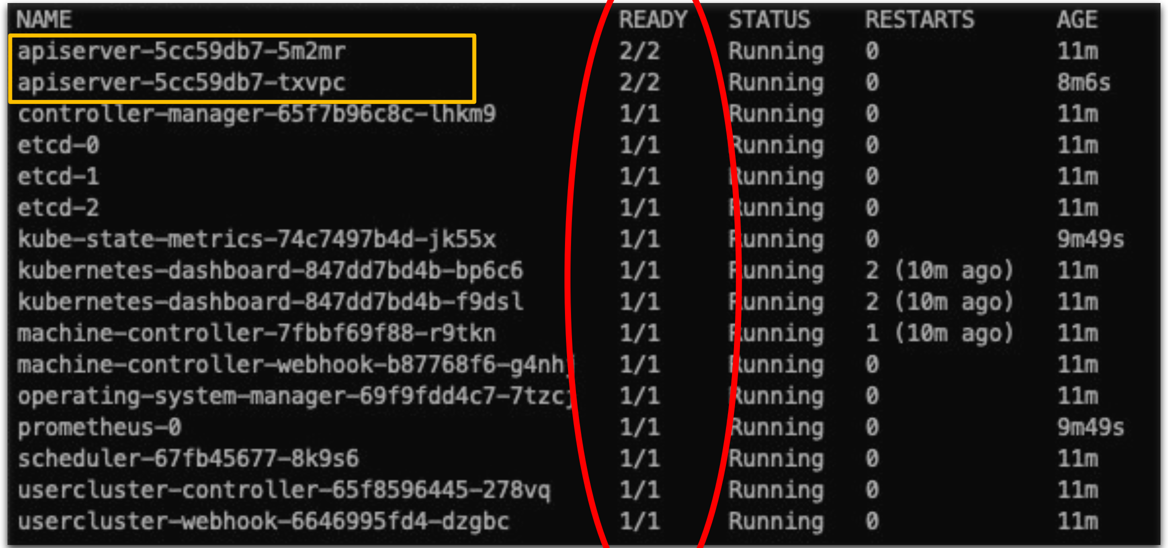
```
calico-kube-controllers-57fb8785bf-jl226   1/1   Running   0   24m
canal-8mvtr                                2/2   Running   0   20m
coredns-58b65bfd4d-d92mp                   1/1   Running   0   24m
coredns-58b65bfd4d-w8df2                   1/1   Running   0   24m
kube-proxy-6p5tv                           1/1   Running   0   20m
node-local-dns-fvtrq                       1/1   Running   0   20m
openvpn-client-68bc8f76bd-m8b85            2/2   Running   0   8m59s
user-ssh-keys-agent-s8xvx                  1/1   Running   0   20m
```

Konnectivity

-15 containers

18 containers

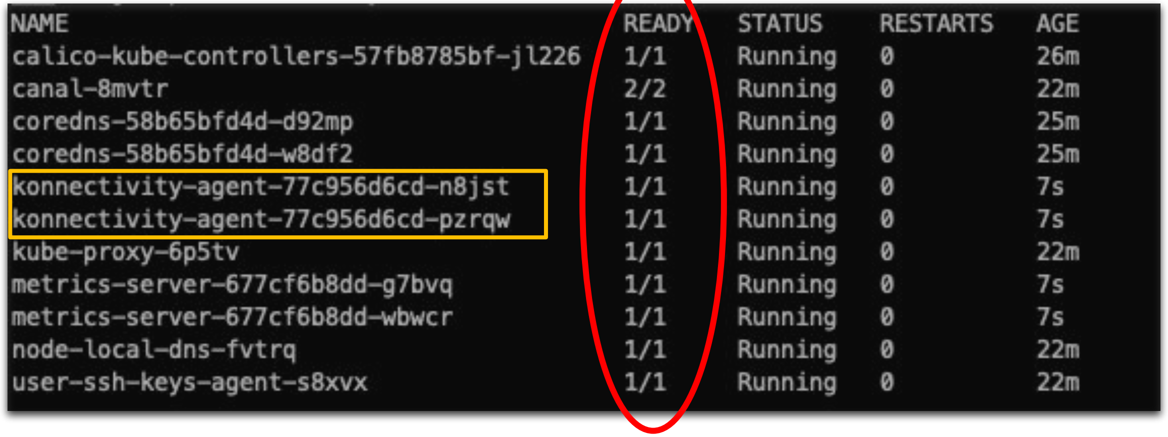
Seed Cluster (Control Plane)



```
NAME                                        READY   STATUS    RESTARTS      AGE
apiserver-5cc59db7-5m2mr                    2/2     Running   0             11m
apiserver-5cc59db7-txvpc                    2/2     Running   0             8m6s
controller-manager-65f7b96c8c-lhkm9         1/1     Running   0             11m
etcd-0                                      1/1     Running   0             11m
etcd-1                                      1/1     Running   0             11m
etcd-2                                      1/1     Running   0             11m
kube-state-metrics-74c7497b4d-jk55x         1/1     Running   0             9m49s
kubernetes-dashboard-847dd7bd4b-bp6c6       1/1     Running   2 (10m ago)   11m
kubernetes-dashboard-847dd7bd4b-f9dsl       1/1     Running   2 (10m ago)   11m
machine-controller-7fbbf69f88-r9tkn         1/1     Running   1 (10m ago)   11m
machine-controller-webhook-b87768f6-g4nhj   1/1     Running   0             11m
operating-system-manager-69f9fdd4c7-7tzcj   1/1     Running   0             11m
prometheus-0                                1/1     Running   0             9m49s
scheduler-67fb45677-8k9s6                   1/1     Running   0             11m
usercluster-controller-65f8596445-278vq     1/1     Running   0             11m
usercluster-webhook-6646995fd4-dzgbc        1/1     Running   0             11m
```

12 containers

User Cluster (Worker Nodes)



```
NAME                                       READY   STATUS    RESTARTS   AGE
calico-kube-controllers-57fb8785bf-jl226   1/1     Running   0          26m
canal-8mvtr                                2/2     Running   0          22m
coredns-58b65bfd4d-d92mp                   1/1     Running   0          25m
coredns-58b65bfd4d-w8df2                   1/1     Running   0          25m
konnectivity-agent-77c956d6cd-n8jst        1/1     Running   0          7s
konnectivity-agent-77c956d6cd-pzrqw        1/1     Running   0          7s
kube-proxy-6p5tv                           1/1     Running   0          22m
metrics-server-677cf6b8dd-g7bvq            1/1     Running   0          7s
metrics-server-677cf6b8dd-wbwcr            1/1     Running   0          7s
node-local-dns-fvtrq                       1/1     Running   0          22m
user-ssh-keys-agent-s8xvx                  1/1     Running   0          22m
```

Real-World Integrations - K0s

- Konnectivity built-in in k0s
- Enables our “controlplane isolation” feature
- Enables some very interesting deployment architectures

Challenges

- Lack of documentation
- HA setup is bit tricky; Especially in dynamic environments
- Debuggability; When things are not working as expected users see bit obscure errors
- Lack of contributors; PRs can take quite a while to land
- Real-world Testing; Resource leaks are known to happen

Please scan the QR Code above to leave feedback on this session