
CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

# When Sys-Admins Quit

## Protecting Kubernetes Clusters when Cluster-Admins Quit

*Arun Krishnakumar, VMware Inc*

# Problem


- Usually, humans are operators and owners of Clusters.
- Humans change teams or companies
- When Cluster-Owners leave a team, they need to have a way to cleanly transfer ownership of their Kubernetes Cluster (*)

- This is with regard to Kubernetes Clusters created using kubeadm

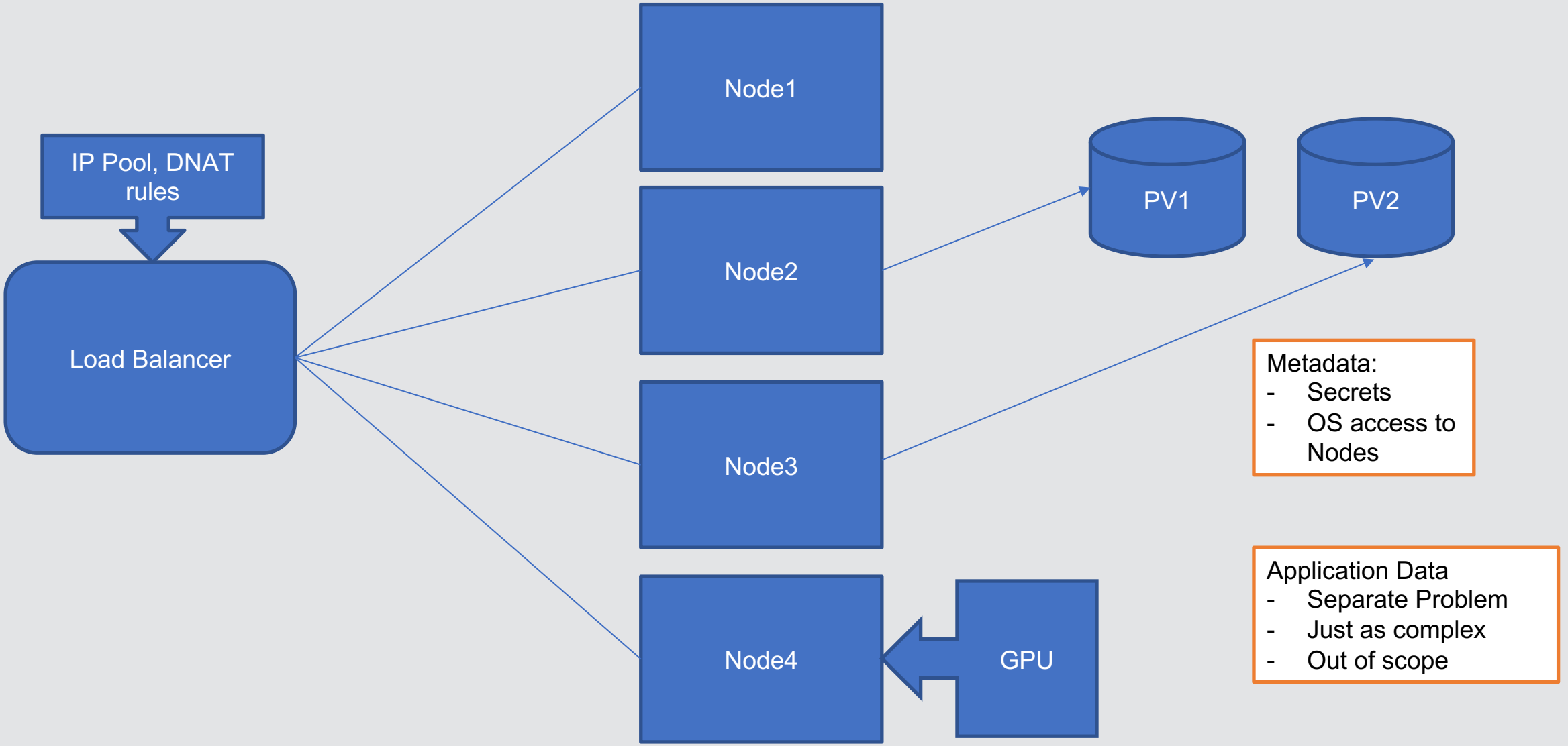
# Solution


- Transfer Cluster ownership to a new user
- Revoke access from old user

- Scope of Solution clear, but building for this is an afterthought
- When the problem appears, developers scramble and present hacky solutions

# Kubernetes Cluster





# Kubernetes Cluster Objects


## Cloud Infrastructure Objects: Multitenant Cloud

Objects to be transferred to another user:

- Nodes
- Networking components such as Load-Balancer, DNAT Rules, IP Addresses etc.
- Storage

# Kubernetes Cluster Objects


## Cloud Infrastructure Objects: Multitenant Cloud

- Quota Considerations for new user
- Permission considerations: new user must have access to resources that old user has
- Every object of the cluster needs to be transferred to the new user: both logical and physical objects
- Administrator to have access to both objects and be able to transfer

# Kubernetes Cluster Objects


## Cloud Infrastructure Objects: Logical

- Certificates
- Root-Access to Nodes
- User Accounts
- (Port Profiles)
- (Defined Entities)
- (VM metadata)

# Kubernetes Cluster Objects


## Kubernetes Objects

- User-created Secrets
- Cluster Secrets
- User RBAC
- User Accounts
- User KUBECONFIGs

- ***ADMIN KUBECONFIG***

# But…


- ADMIN KubeConfig is a Break-glass Kubeconfig
- Root-access to node is revoked, but a copy could exist
- If earlier Cluster-Admin still has network access, the cluster is still accessible

- Network Access cannot be revoked unless there are provisions from the infrastructure
- Cluster IP cannot be changed since the certificate SAN includes it.

# Solution?


- Revoke the ADMIN KubeConfig?

- Admin Kubeconfig cannot be revoked (easily).
- Open Ticket: https://github.com/kubernetes/kubeadm/issues/2414

# Solution


- **Manual Revocation of Certificates**

- Not a simple process.
- Documentation is at very high level
- Some resources available for advanced users

- But it can be done

- https://kubernetes.io/docs/setup/best-practices/certificates/
- https://kubernetes.io/docs/tasks/tls/manual-rotation-of-ca-certificates/
- https://github.com/kelseyhightower/kubernetes-the-hard-way

# Manual Revocation of certificates

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

**Overall Procedure:**

1. Create a Root-CA
2. Create certs for etcd, kube-controller-manager, kube-apiserver, kubelet, kube-scheduler (Order matters)
3. Copy certs to control-plane and worker nodes
4. Create new KUBECONFIG files for node, kube-proxy, kube-controller-manager, kube-scheduler, **admin**
5. Copy all kubeconfig files to nodes
6. Update static manifests to point to new certs and copy them to nodes. This restarts services. The old **admin** kubeconfig is not usable anymore at this point.
7. Create cluster role to access kubelet using new admin.conf
8. Update kubelet service files to point to new kubeconfig files and certificates. Restart kubelet.

And we are done. Note that some pods will be down from steps 6-8. And due to the restart of core pods in step 6, there will be some control-plane outage.

# Demo

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

# Limitations


**Cluster Downtime**

- etcd, kube-apiserver, kube-controller-manager will be restarted
- kubelet service needs to be restarted on every node

**General Risk**

- Once started, cluster will be in an invalid state until completed
- All of this needs to be managed by custom scripts.

# Tying it all together


- Be prepared to move resources from the Infrastructure perspective
- Use External CA Infrastructure of Kubernetes: https://kubernetes.io/docs/setup/best-practices/certificates/
- Use an Intermediate CA and keep keys of root-CA secure.
- If an intermediate CA is compromised, revoke intermediate cert and manually rotate certs
- Delete and Recreate all Users that existed earlier

# Q&A

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

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