
KubeCon
CloudNativeCon
North America 2023


KubeCon | CloudNativeCon

North America 2023

Beyond the Cluster: Harnessing the Power of Kubernetes Namespaces

Victor Varza & Adrian Aneci, Adobe Inc

Co-author - adobe/k8s-shredder, adobe/cluster-registry

Kubernetes Org Member

@email: aneci@adobe.com

@github: adriananeci

@linkedin: adrian-aneci

Co-author - adobe/k8s-shredder, adobe/cluster-registry

Organizer of KCD Romania, 25th of April 2024

@email: vvarza@adobe.com

@github: victorvarza

@linkedin: victorvarza

Agenda

Project Ethos

Kubernetes Namespaces

Capacity Management

Governance Policies

Multi-tenancy at Scale

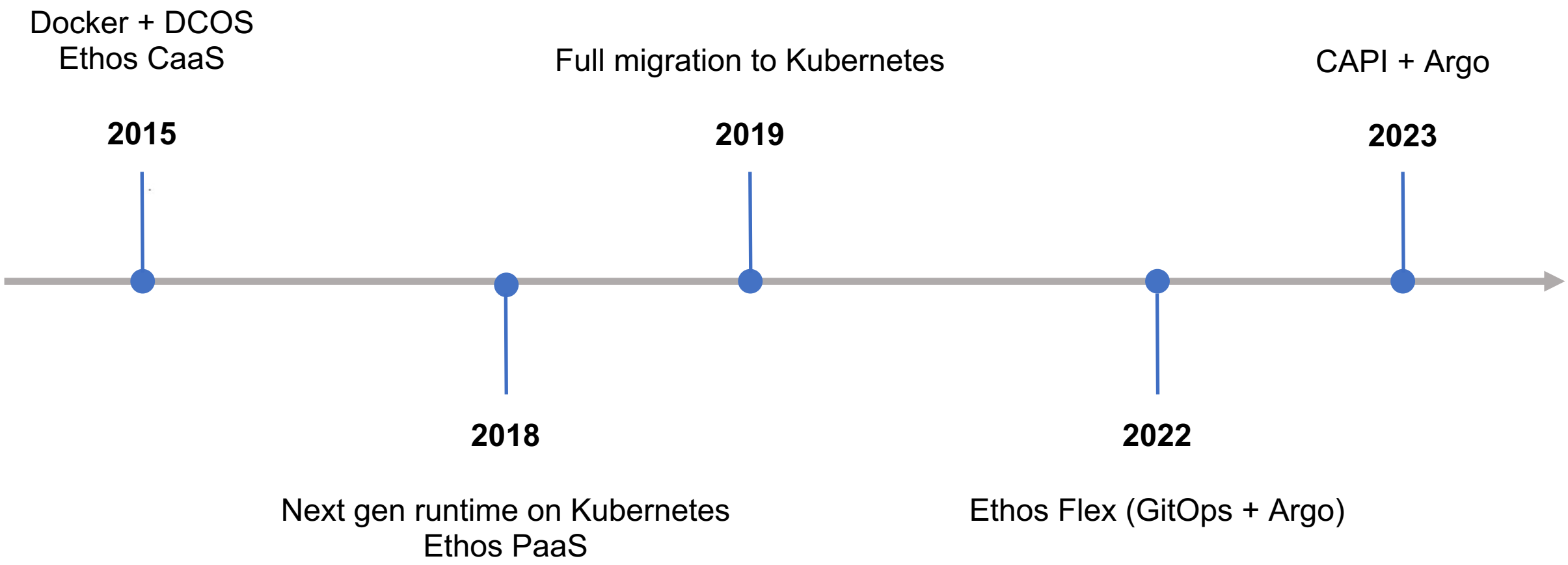
Non-disruptive Kubernetes Upgrades + Live Demo

Project Ethos

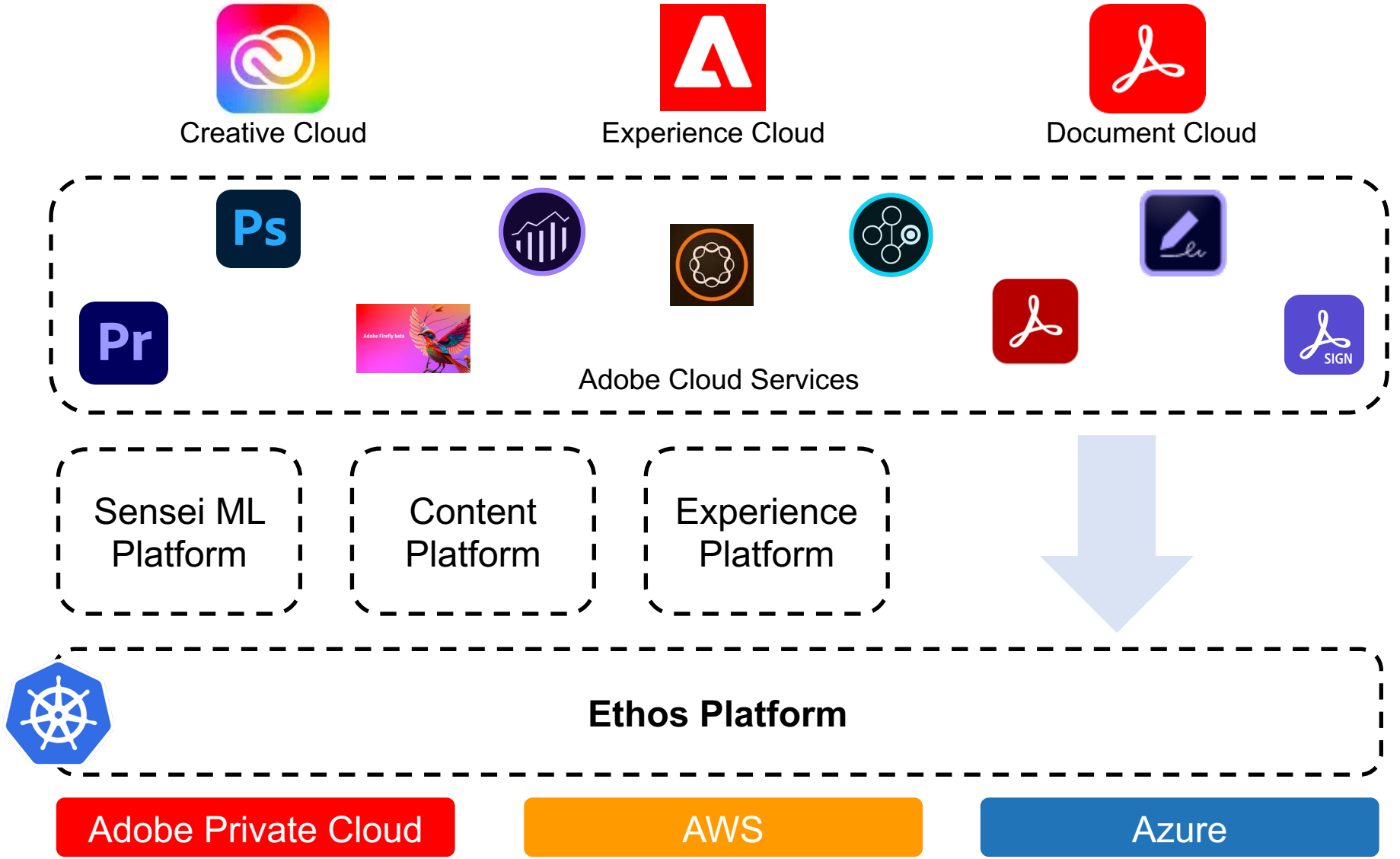
"It doesn't matter how good your engineering team is if they are not given something worthwhile to build."

Marty Cagan - INSPIRED

Project Ethos



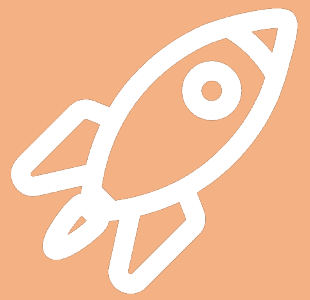
Ethos from 10k ft



Ethos in numbers

2.2 million containers

1.0 million pods



41k namespaces

330

K8s Clusters

AWS

Azure

APC

28 regions

> 35k compute nodes

2.9PB Memory

830k vCPUs

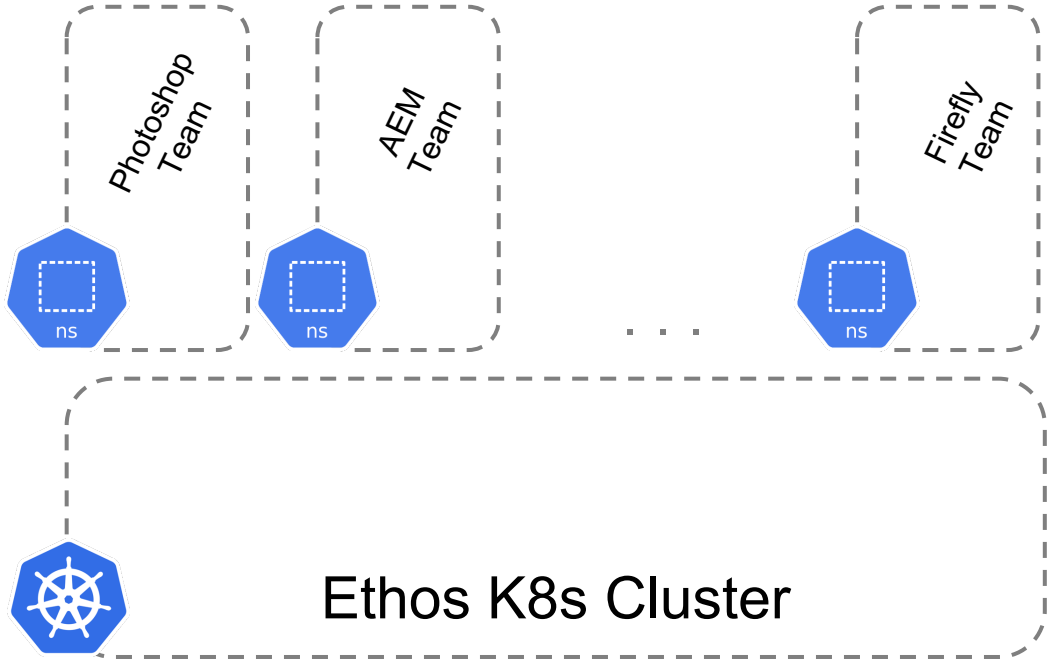
7.8k GPUs

Multi-tenancy @Adobe

Multi-tenancy = multiple different teams share multiple k8s clusters

> Shared Clusters

> Dedicated Clusters

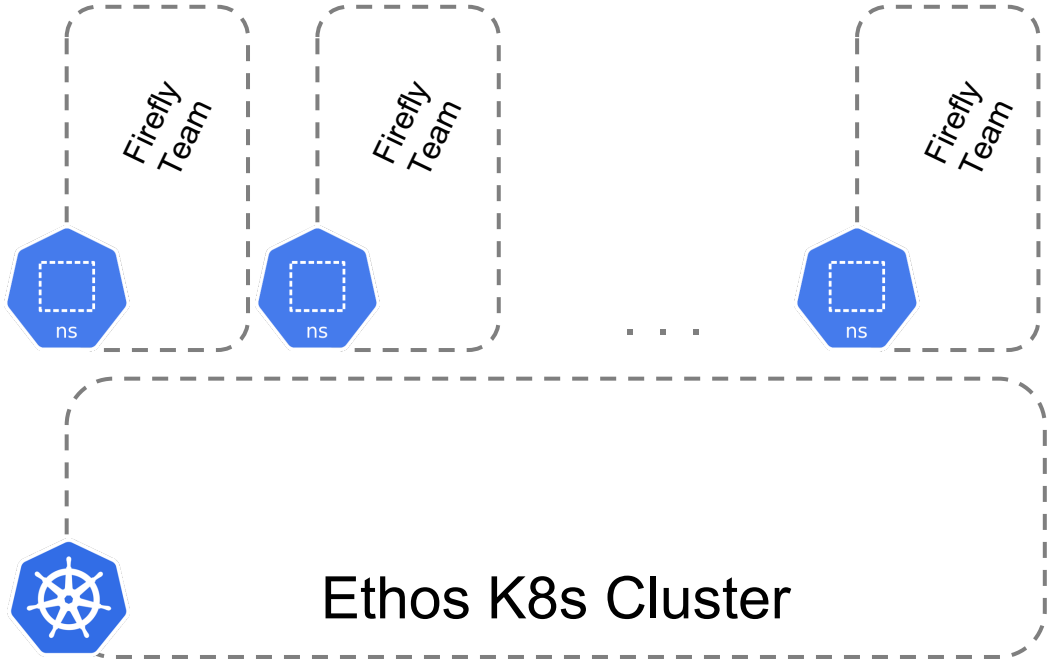


Multi-tenancy @Adobe

Multi-tenancy = multiple different teams share multiple k8s clusters

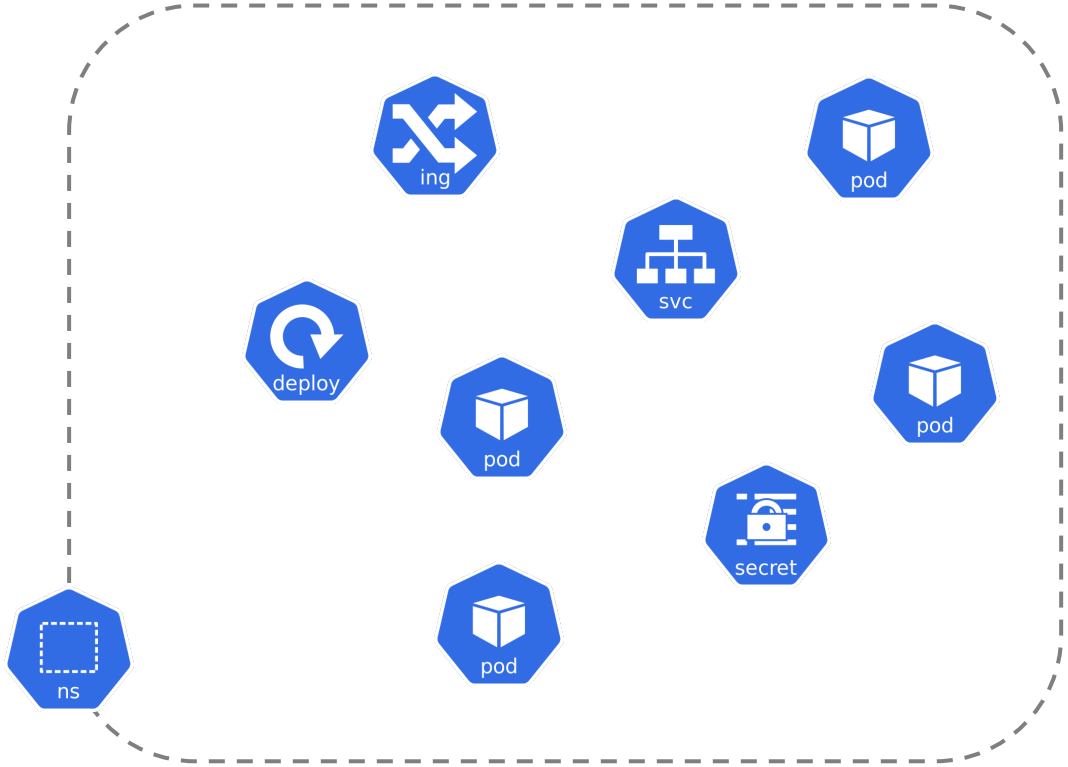
> Shared Clusters

> Dedicated Clusters



Kubernetes Namespaces

Developers ❤ namespaces
Unique namespace across the fleet
Compile a ns profile template

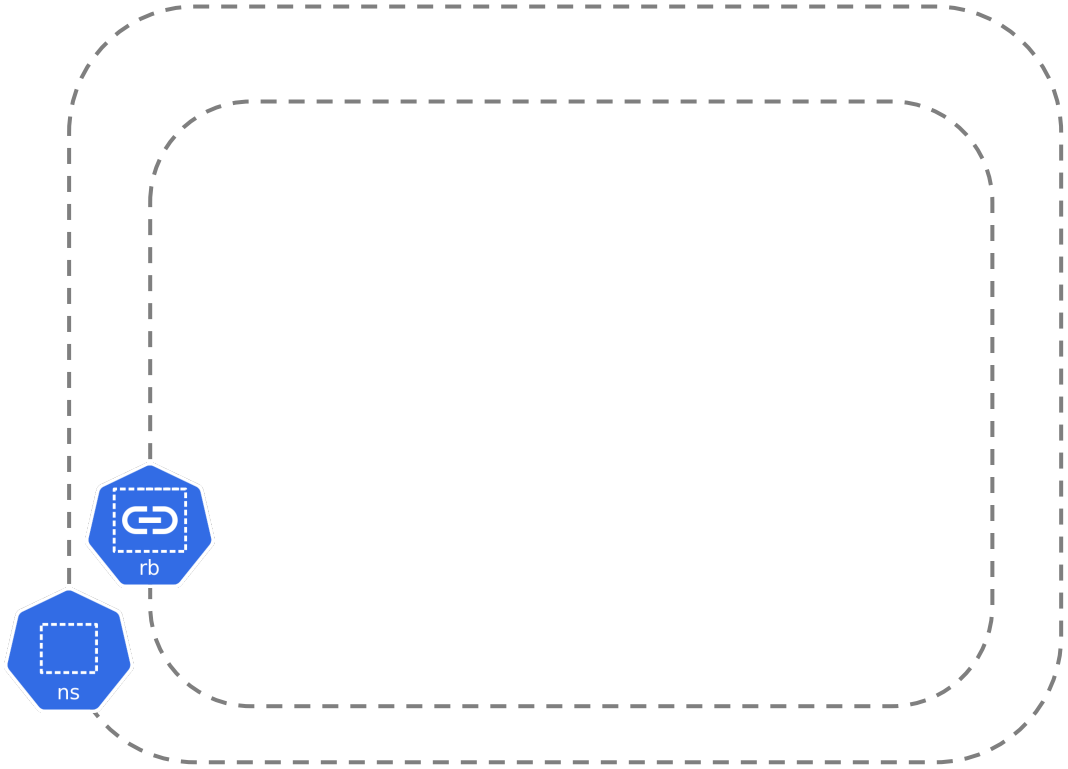


Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies

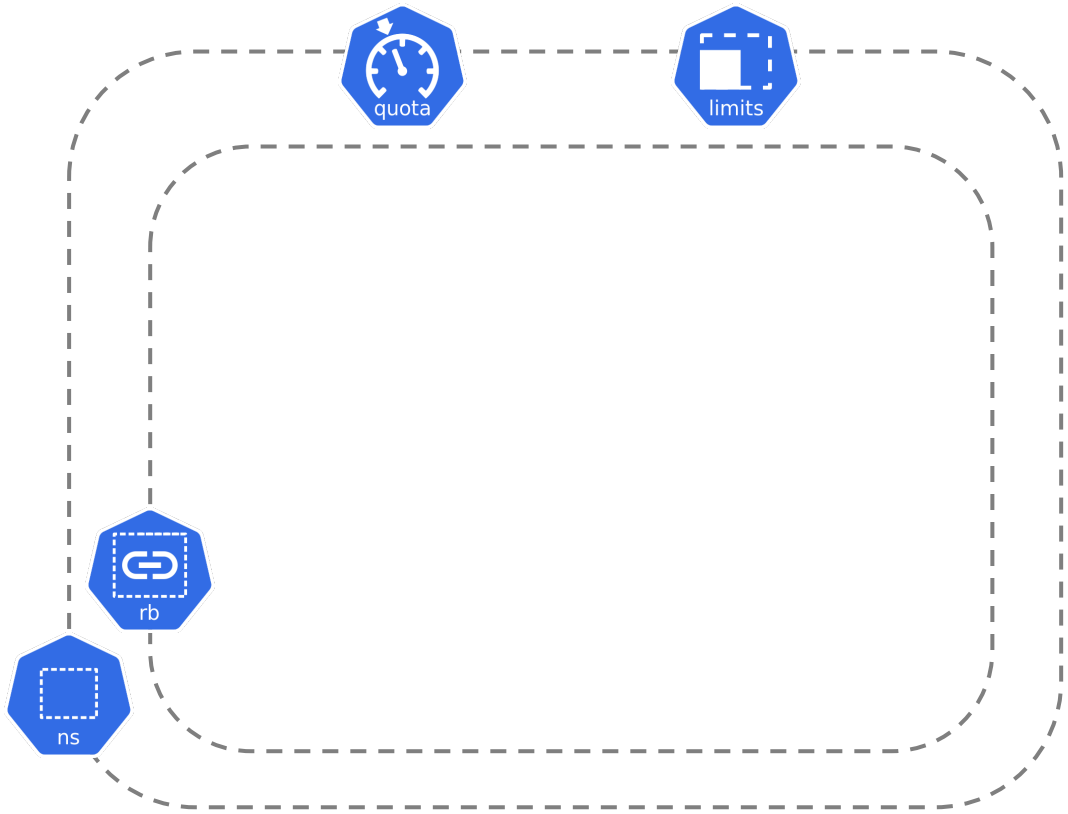
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



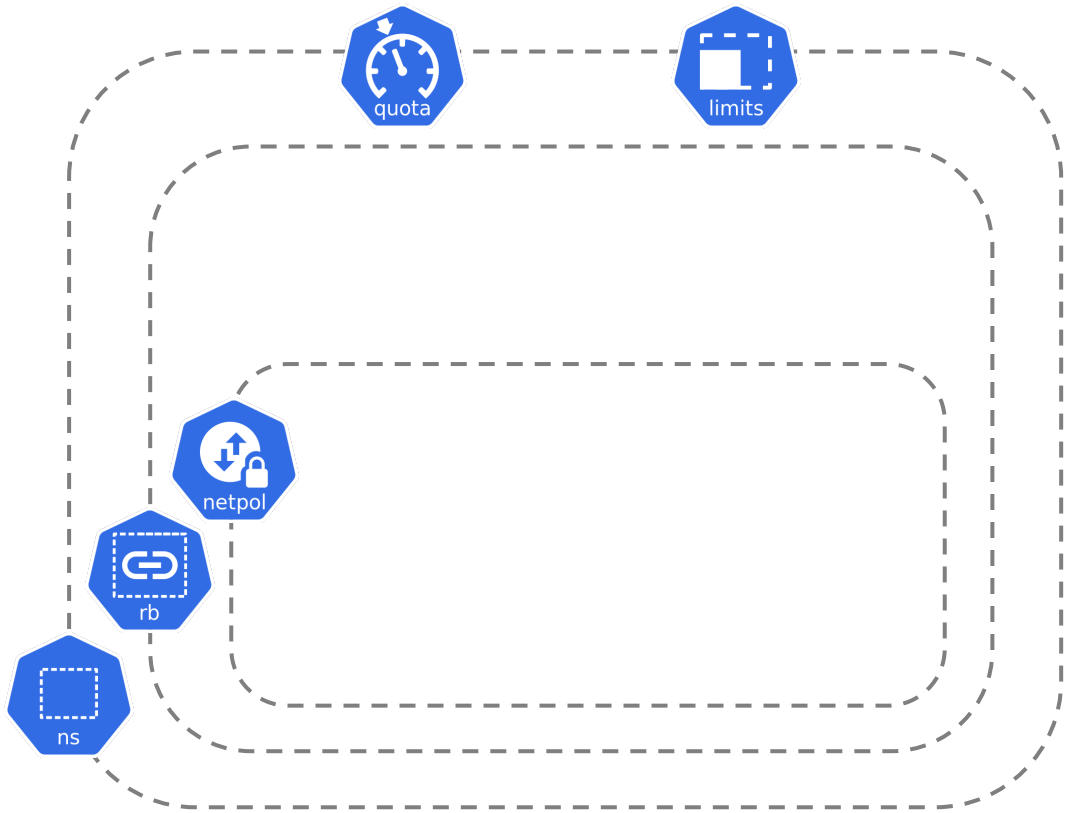
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



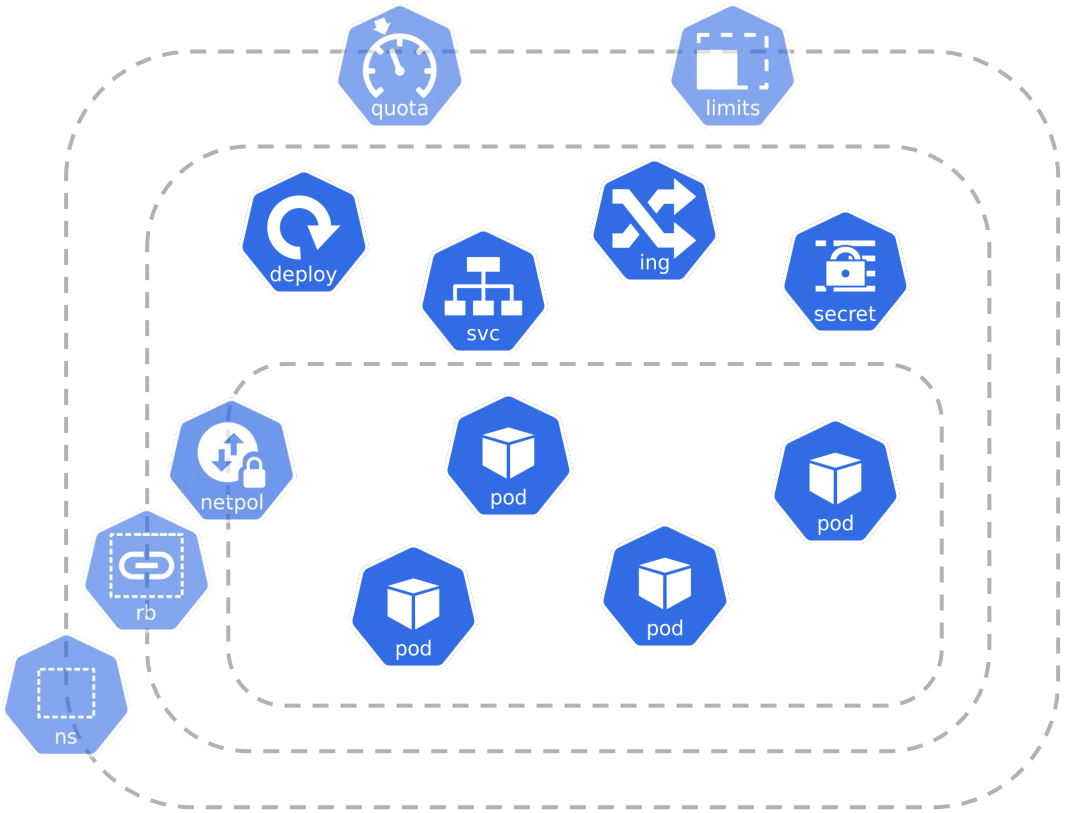
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



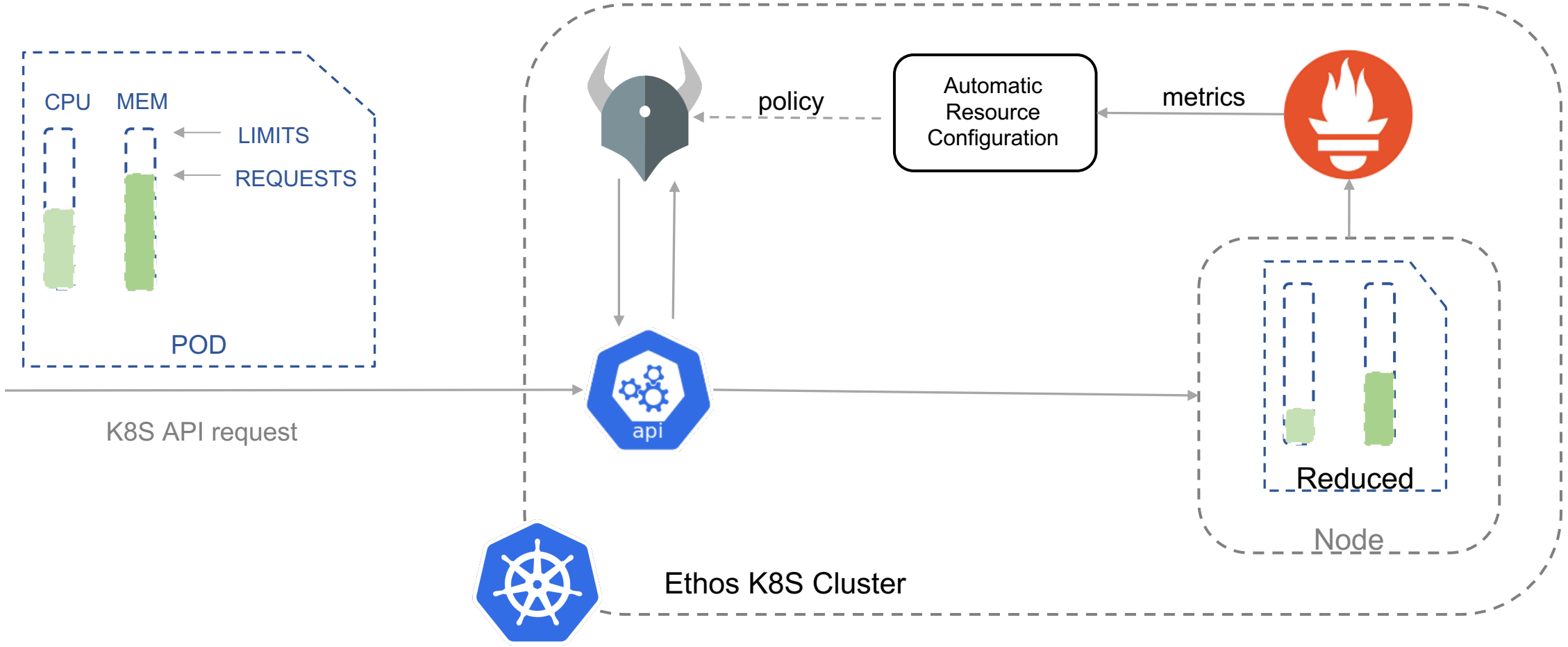
Capacity management

Capacity issues = higher costs

Three levels:

- ✓ Pod - Automatic Resource Configuration
- ✓ Namespace – Baseline Quota Unit
- ✓ Cluster – Capacity Alerts

Capacity management



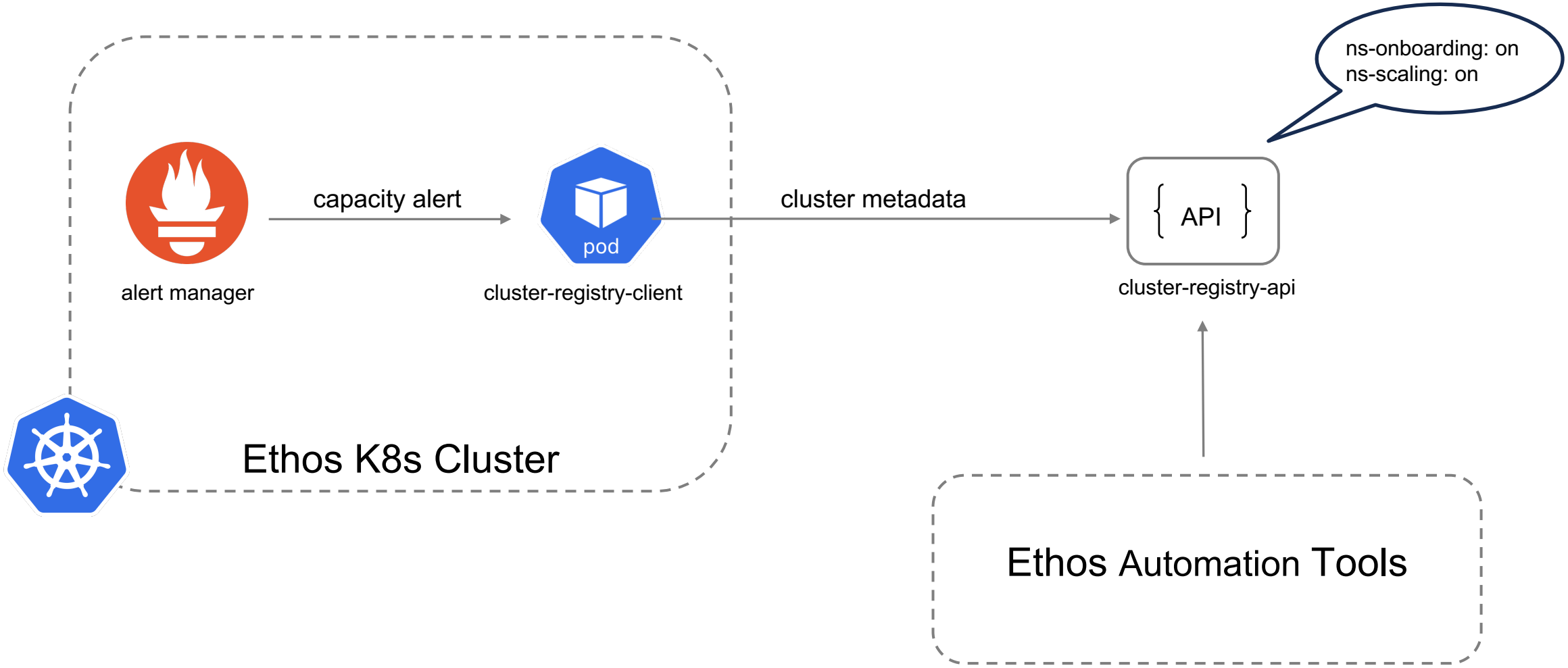
Capacity management

1 Baseline Quota Unit (BQU) = 16 vCPUs
32 GiB of RAM
30 PODs (Running)
…

Resource	Used	Hard
count/ciliumnetworkpolicies.cilium.io	0	30
count/configmaps	0	15
count/ingresses.networking.k8s.io	0	0
count/ingressroutes.contour.heptio.com	0	5
count/networkpolicies.extensions	0	10
count/networkpolicies.networking.k8s.io	7	10
count/pods	0	300
count/secrets	1	15
count/serviceaccounts	1	15
count/services	0	10
limits.cpu	**0**	**16**
limits.memory	**0**	**32Gi**
persistentvolumeclaims	0	5
pods	**0**	**30**
services.loadbalancers	0	0
services.nodeports	0	0

Capacity management

https://github.com/adobe/cluster-registry



Governance policies

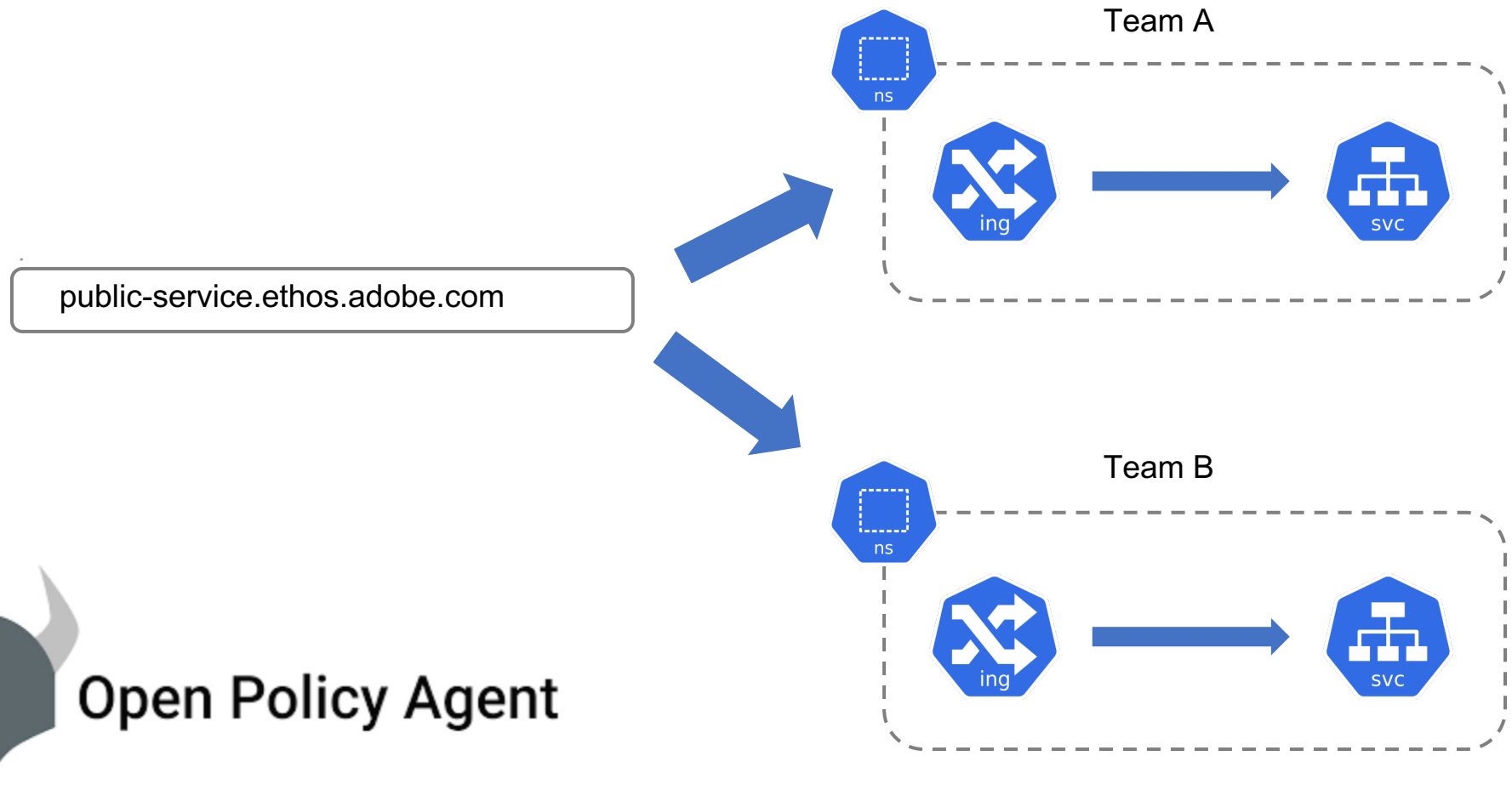
Business is governed by a set of rules => so does a multi-tenant k8s cluster.

Why are these policies mandatory?

- safeguarding teams against inter-team collisions
- protecting cluster stability

Governance policies

FQDN Conflicts day



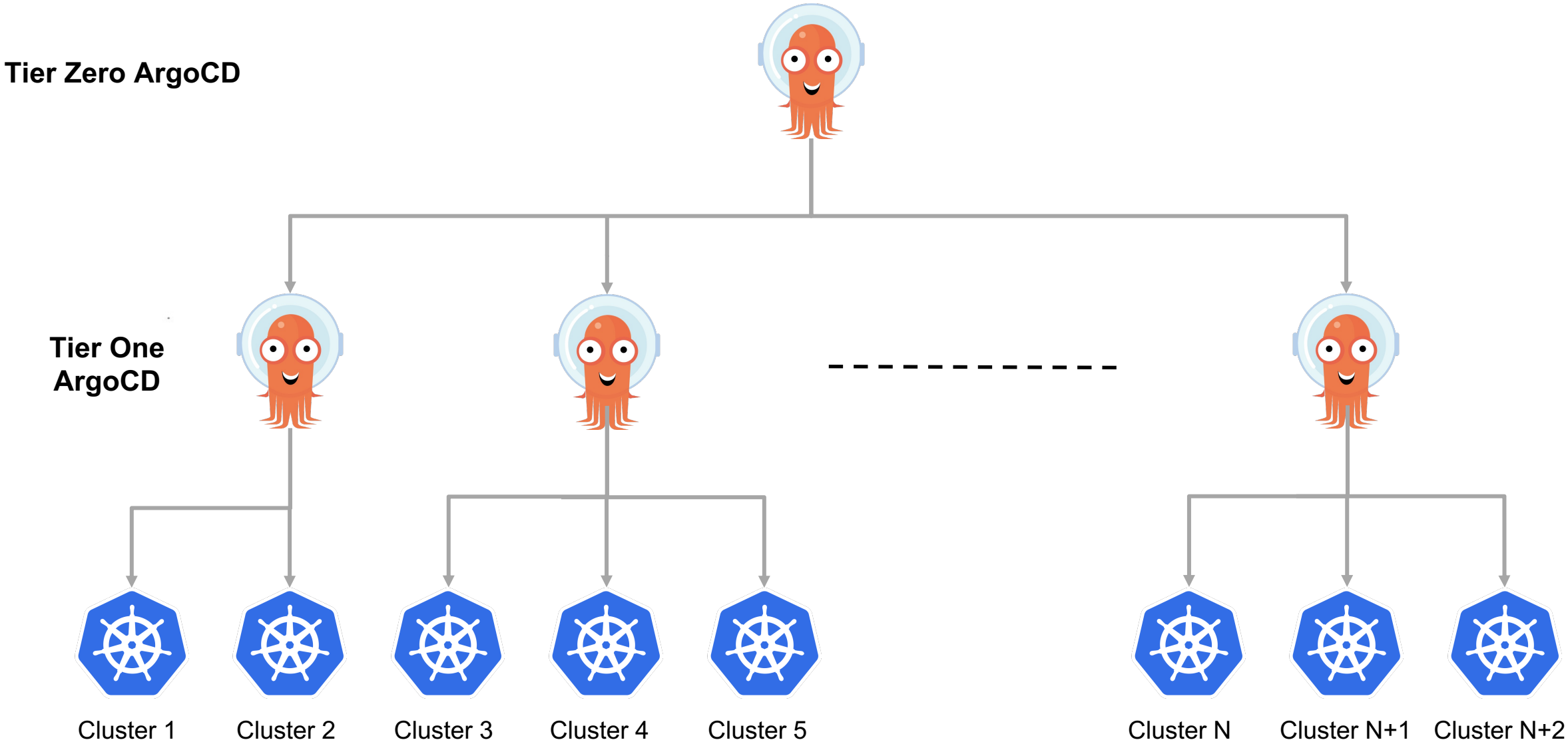
Governance policies

Other example policies:

- Control Plane Toleration
- CronJob History
- Default Ingress Class
- Namespace Limit
- External IP Services

```
# Deny any Service which defines spec.externalIPs
# https://github.com/kubernetes/kubernetes/issues/97076
violation[msg]{
      input.request.kind.kind = "Service"
      isCreateOrUpdate
      input.request.object.spec.externalIPs
      msg = sprintf("External IP Services are not
permitted due to CVE-2020-8554", [])
}
```

Multi-tenancy at scale



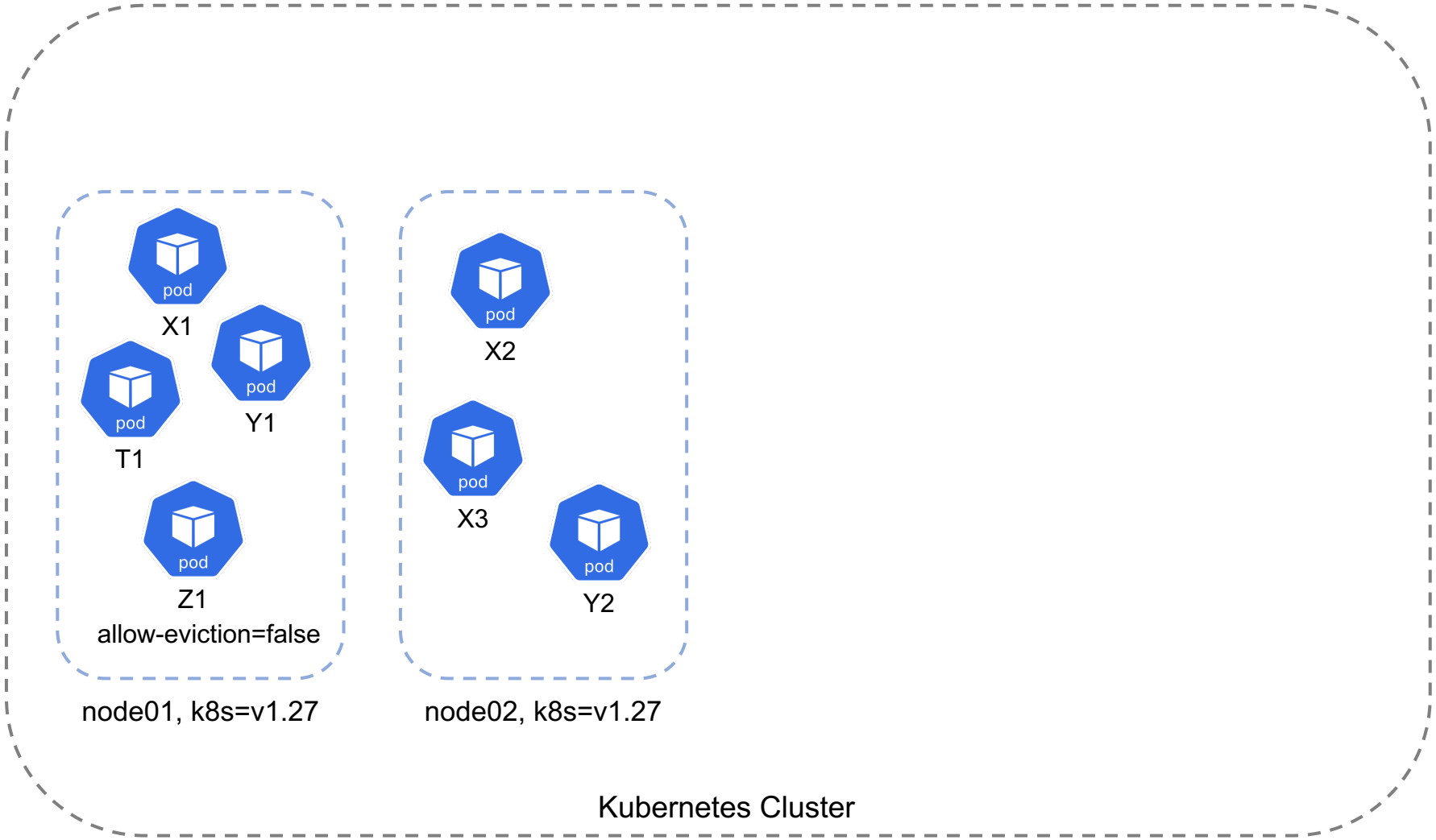
Non disrupting cluster upgrades

Disruptions:
- Voluntary
- Involuntary

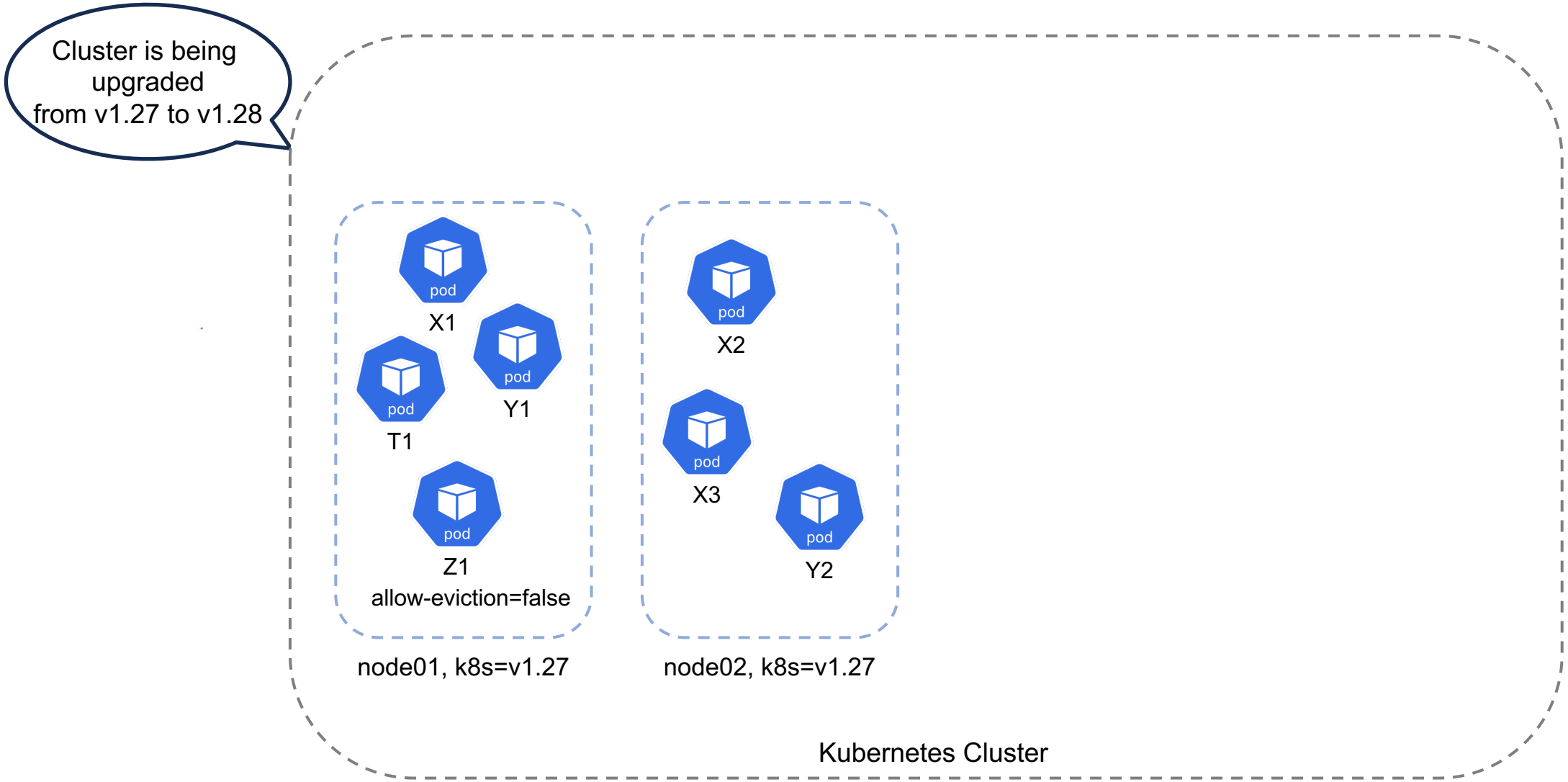
Pod Disruption Budget (PDB)
- contract between the cluster administrator and the developer

https://github.com/adobe/k8s-shredder

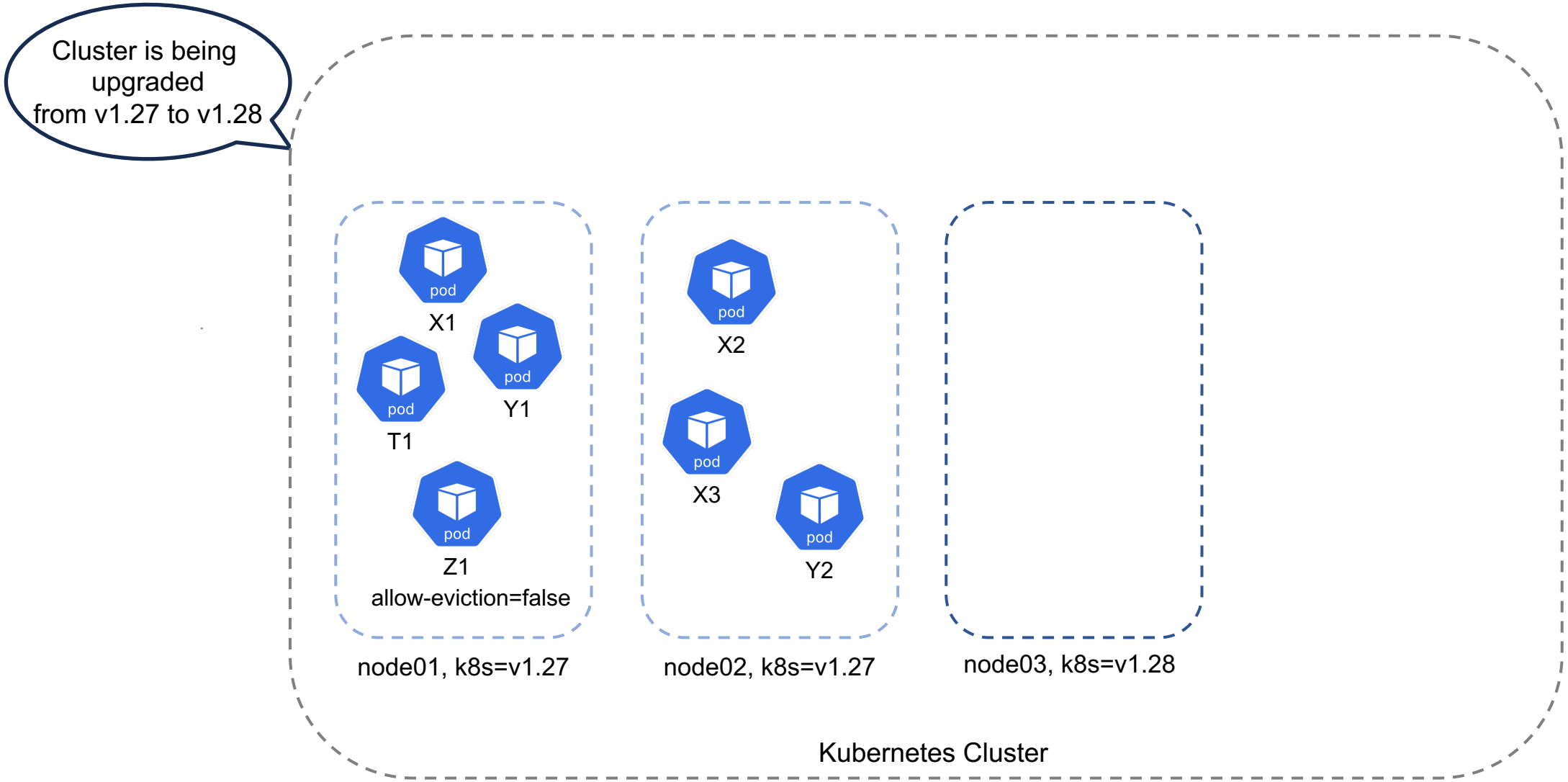
Non disrupting cluster upgrades



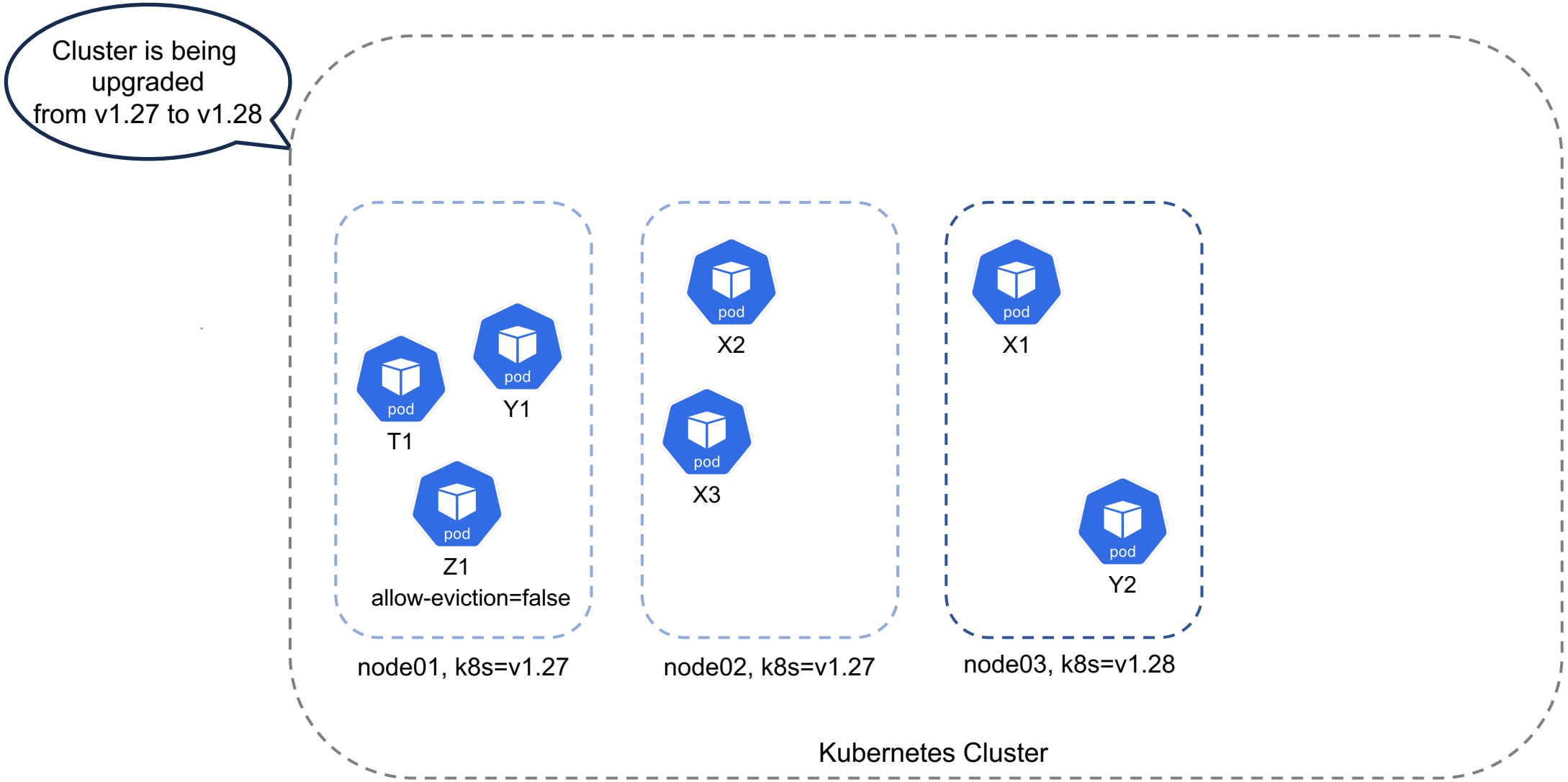
Non disrupting cluster upgrades



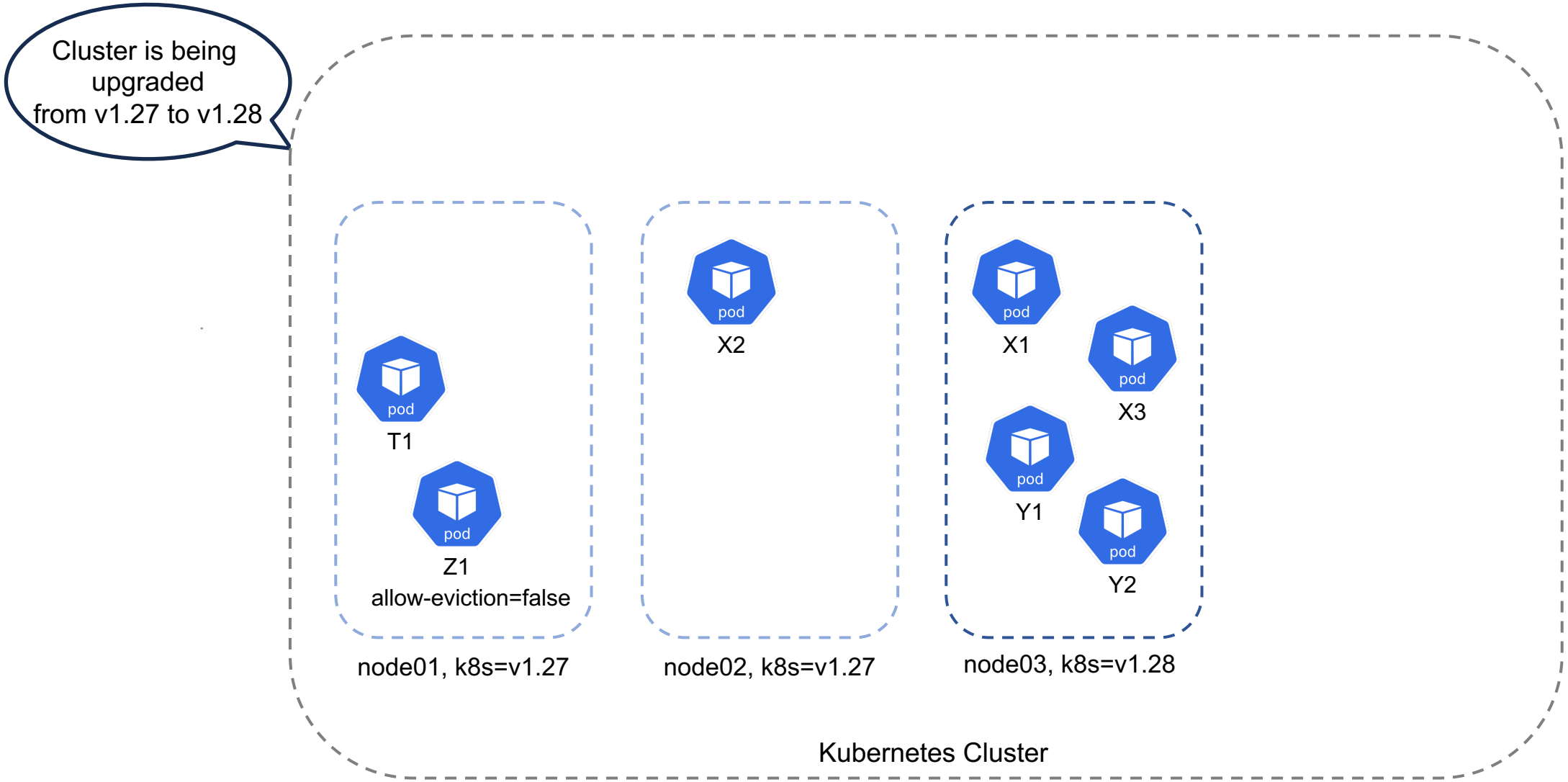
Non disrupting cluster upgrades



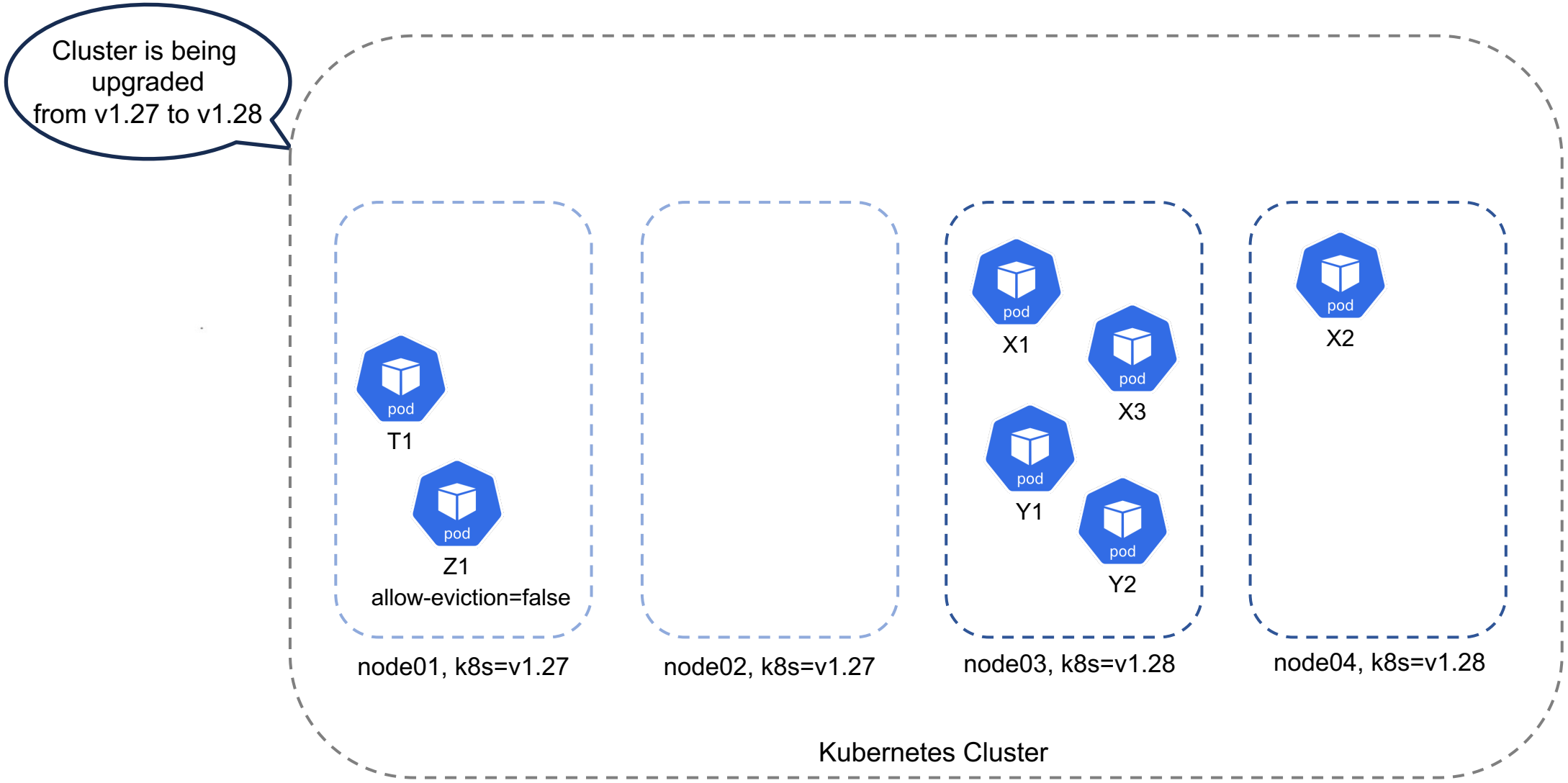
Non disrupting cluster upgrades



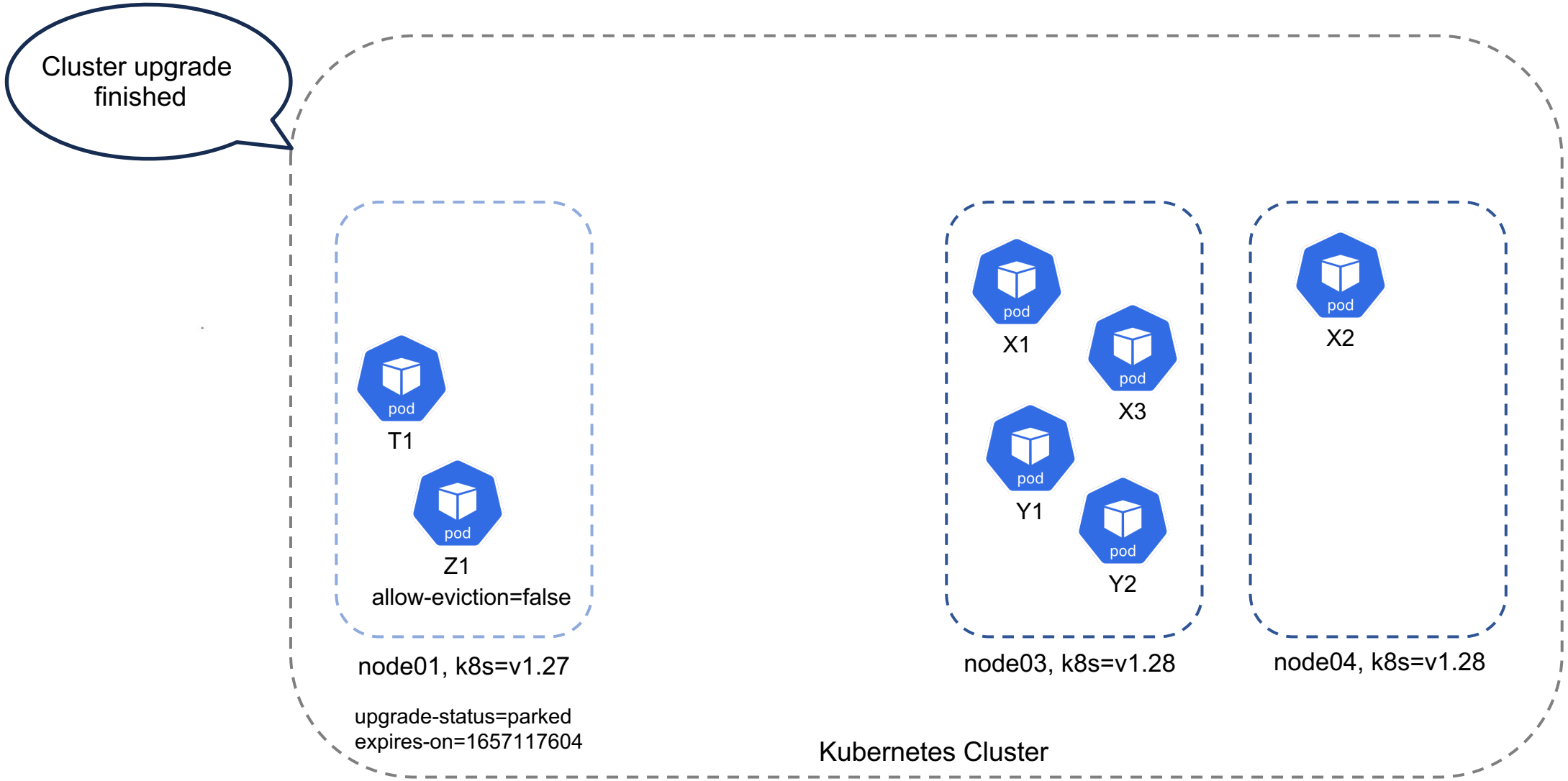
Non disrupting cluster upgrades



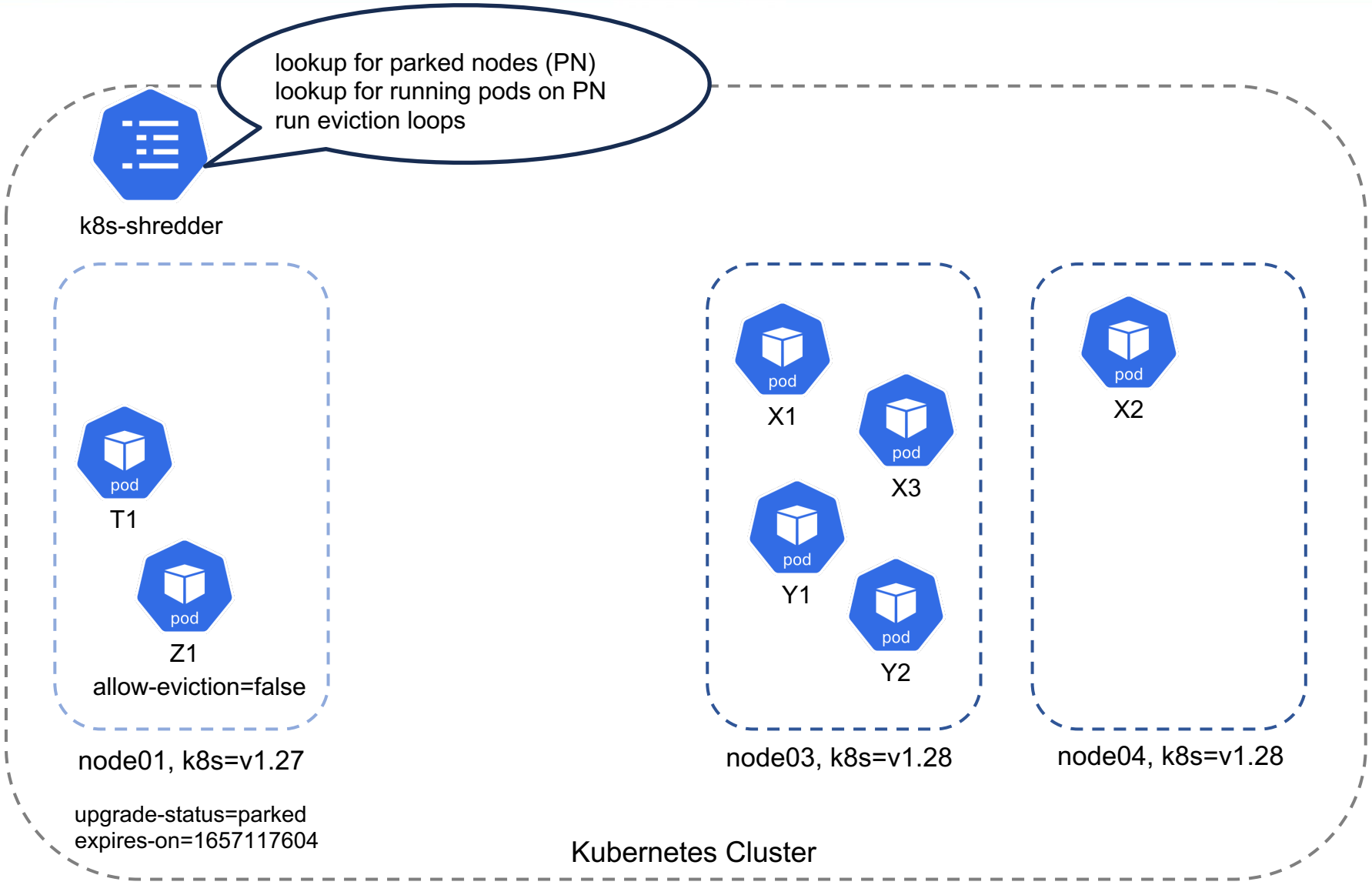
Non disrupting cluster upgrades



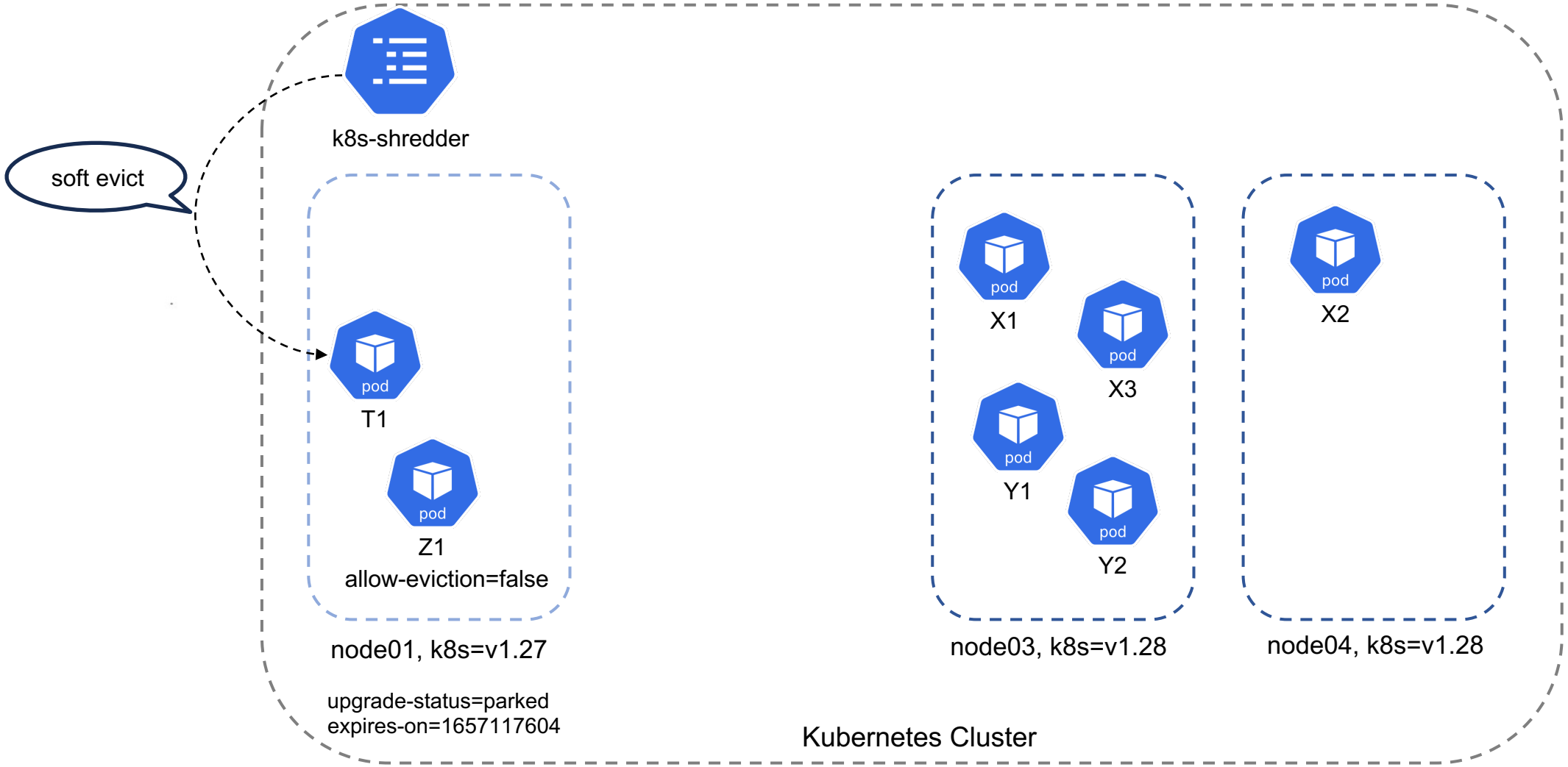
Non disrupting cluster upgrades



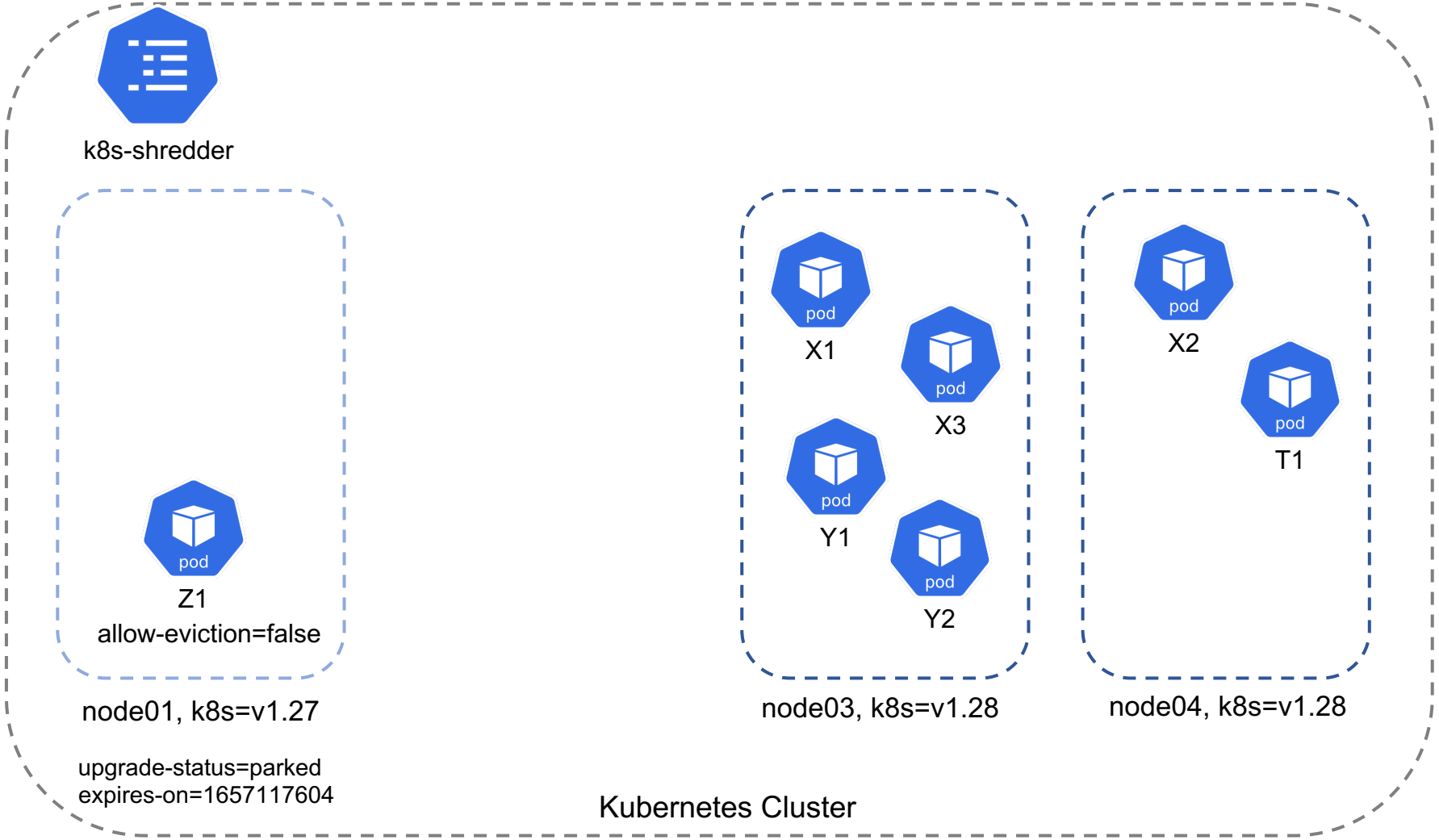
Non disrupting cluster upgrades



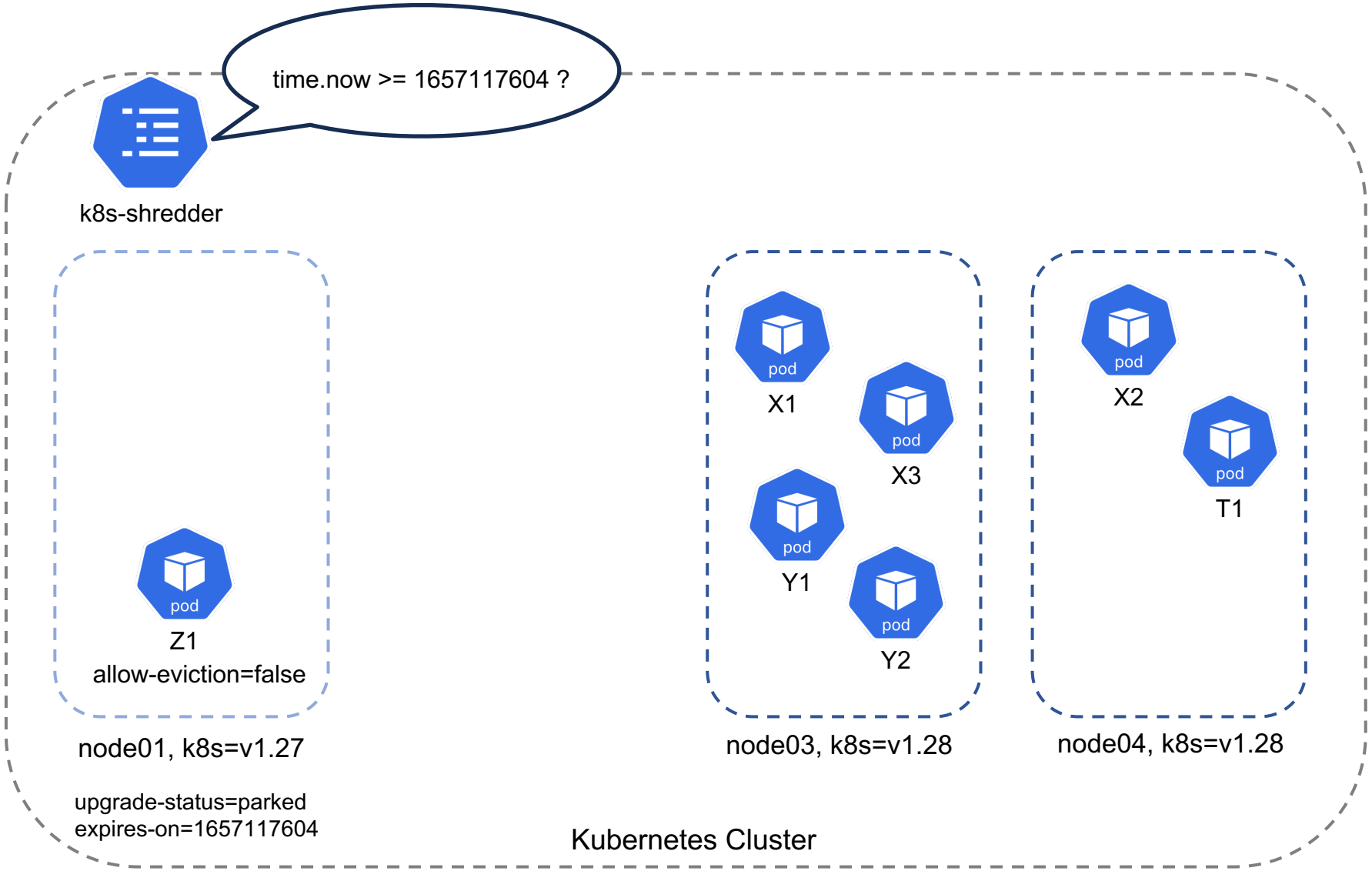
Non disrupting cluster upgrades



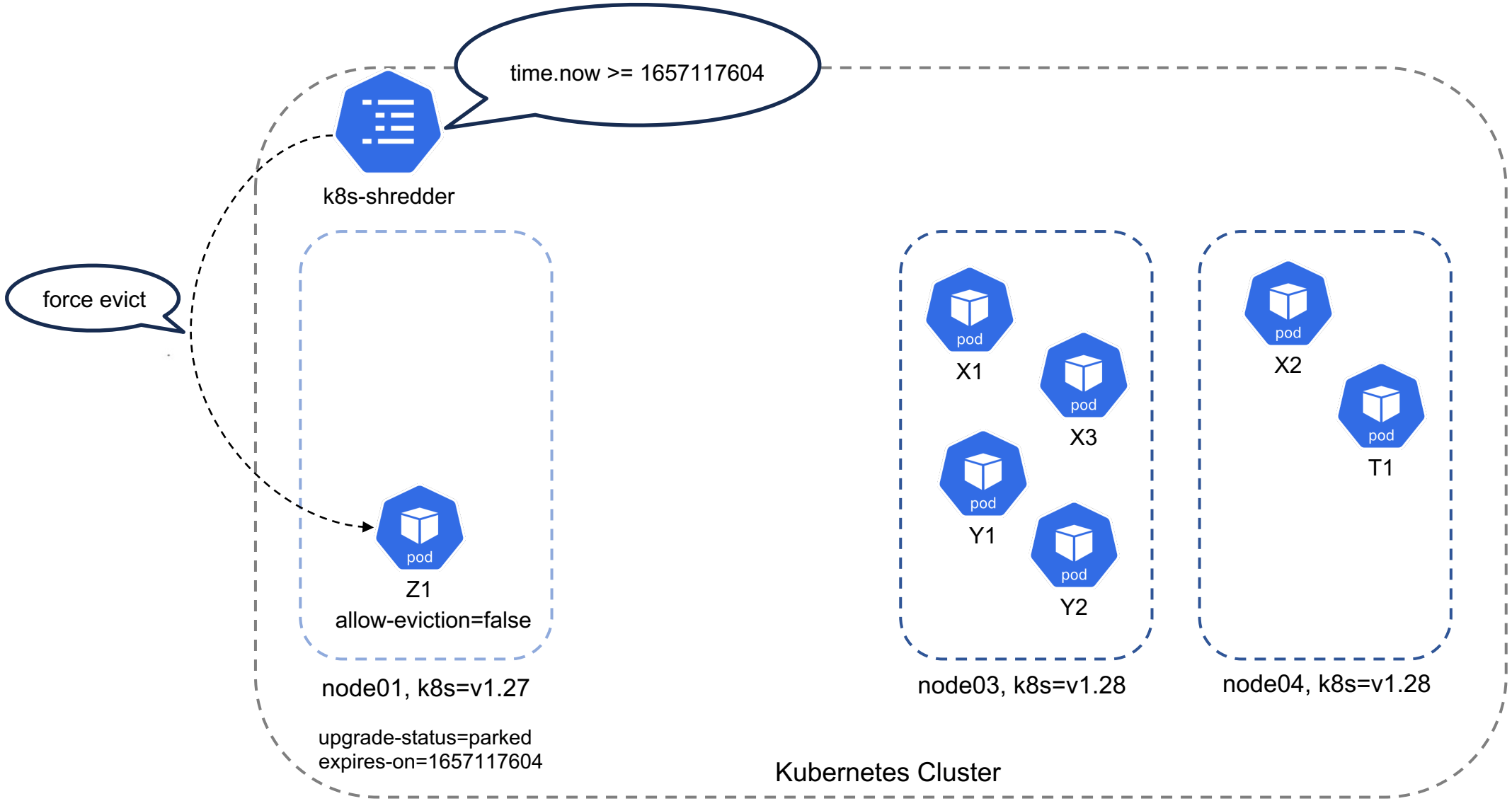
Non disrupting cluster upgrades



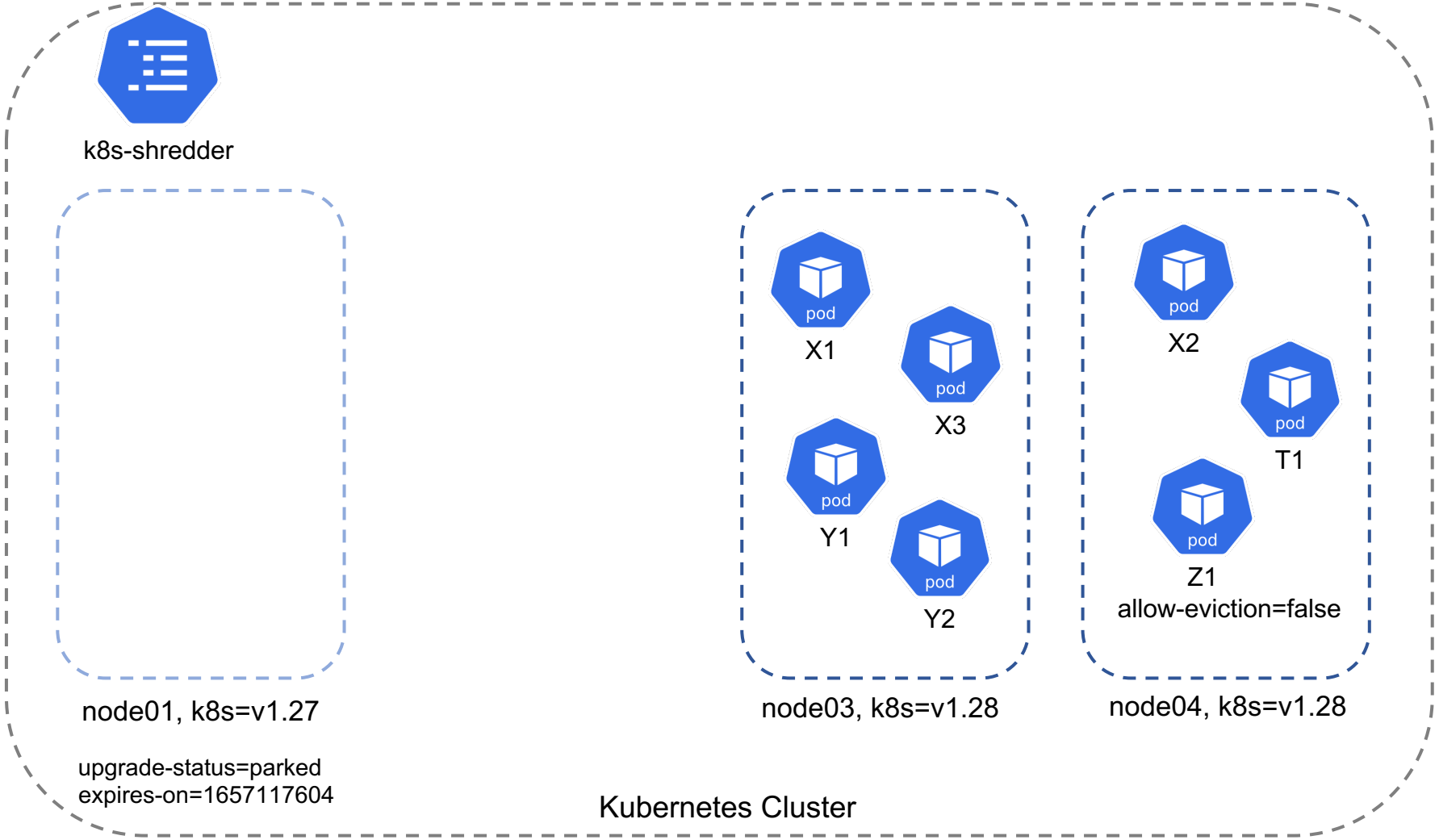
Non disrupting cluster upgrades



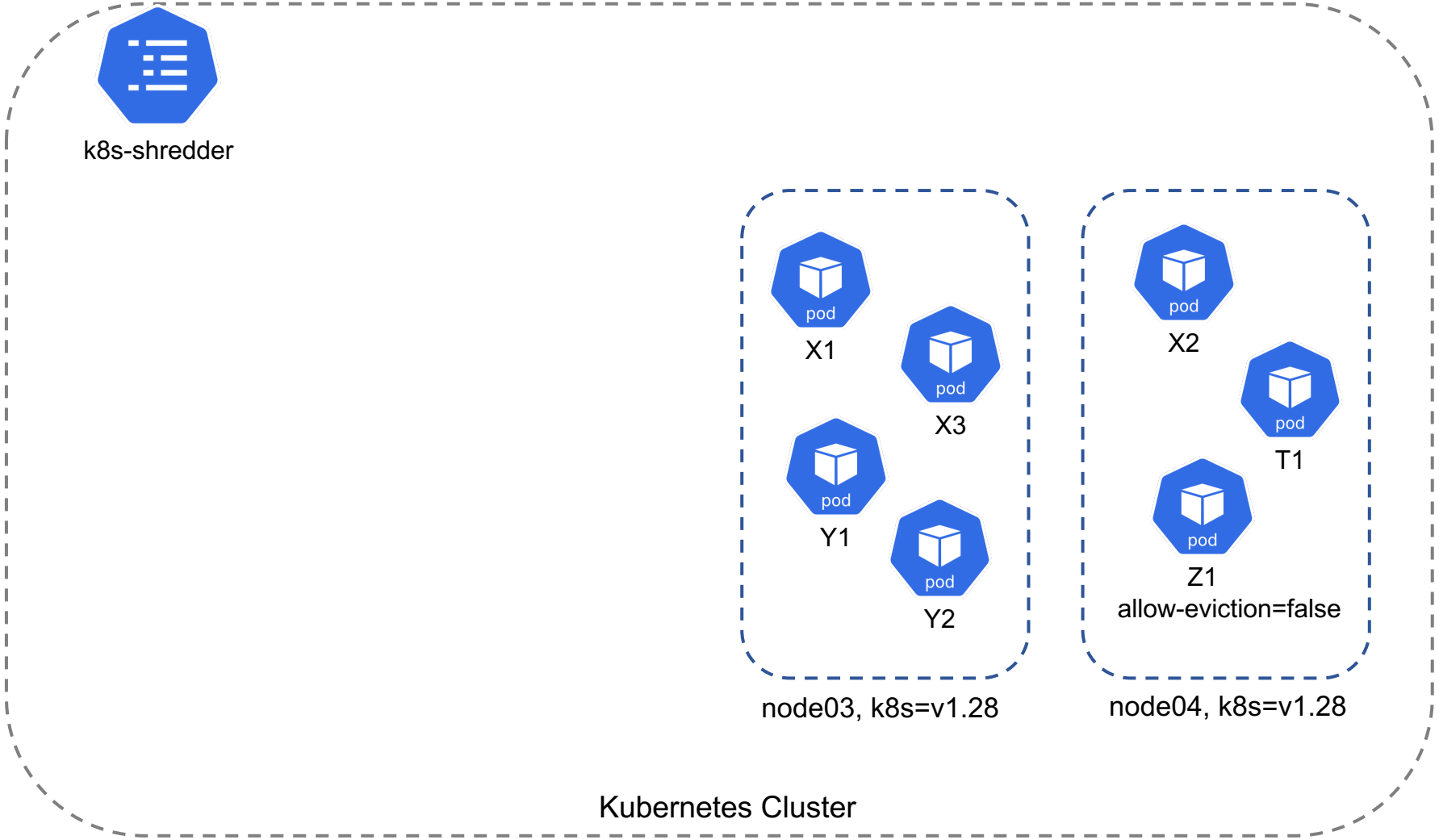
Non disrupting cluster upgrades



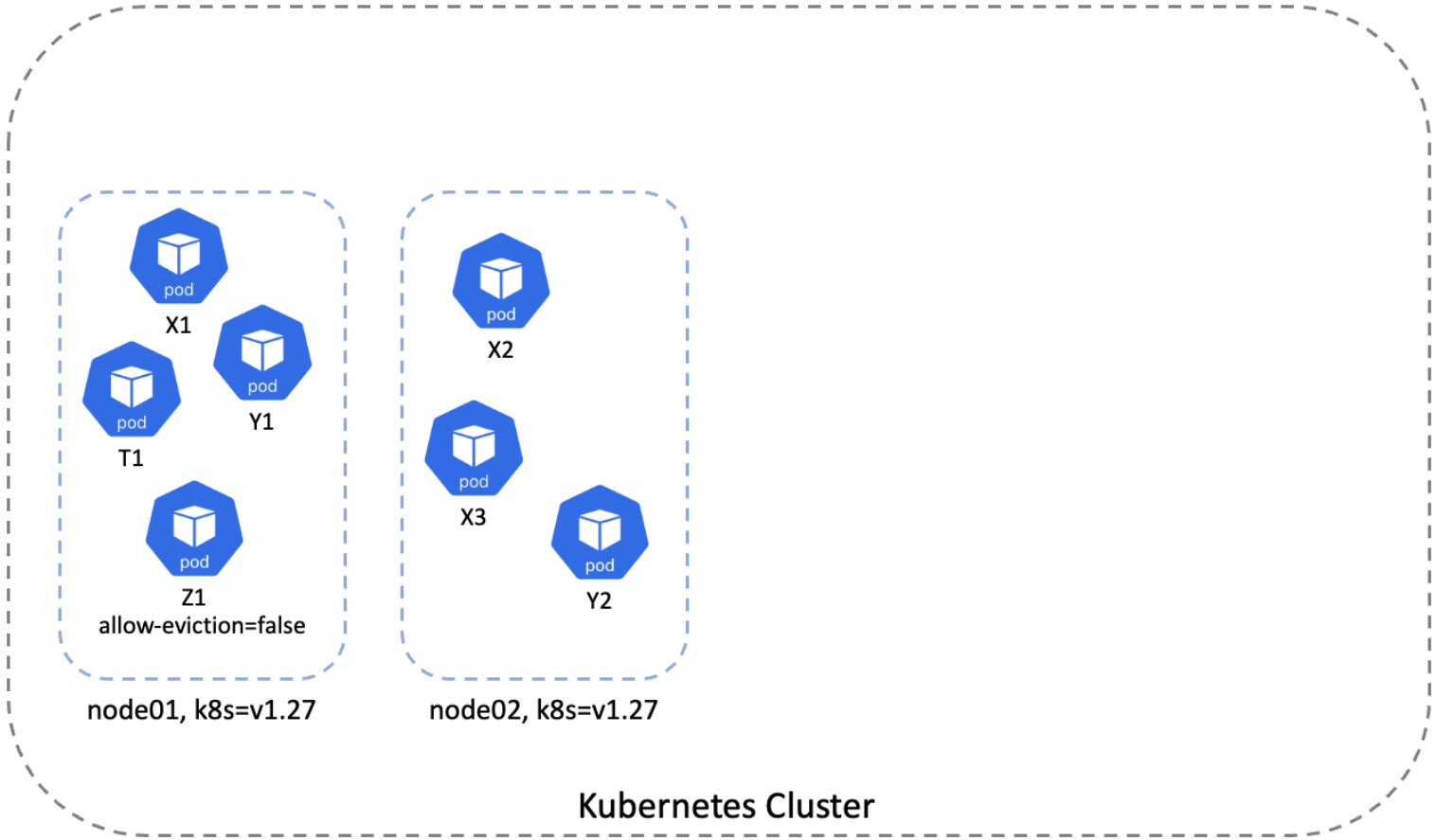
Non disrupting cluster upgrades



Non disrupting cluster upgrades



Non disrupting cluster upgrades



Non disrupting cluster upgrades

Conclusion

There is no silver bullet while building a multi-tenant developer platform

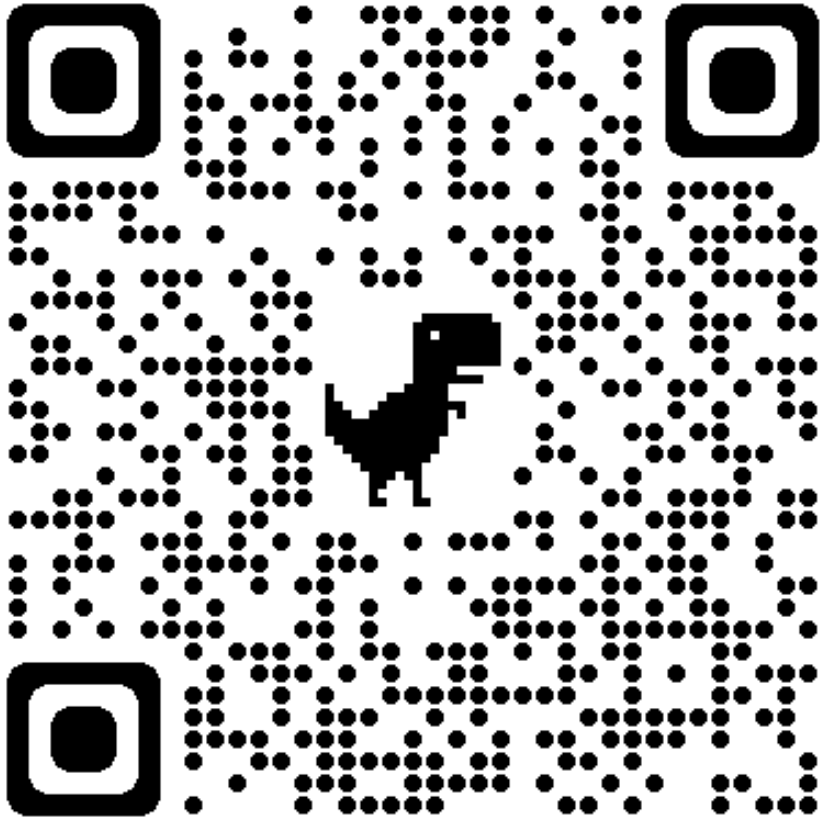
Every company is different and has its own needs and vision regarding multi-tenancy

Namespaces are a viable solution for building the boundaries around multi-tenancy

Challenges while working at scale are different compared to small or medium size platforms.

Thank you!

KubeCon CloudNativeCon North America 2023



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