KubeCon | CloudNativeCon

OPEN SOURCE SUMMIT

China 2023

KubeCon | CloudNativeCon
OPEN SOURCE SUMMIT
China 2023

Kubernetes Namespaces Unleashed: Unlocking the Full Potential of Your Infrastructure

Victor Varza & Adrian Aneci, Adobe Inc

Agenda

Project Ethos

Namespaces

Capacity Management

Governance Policies

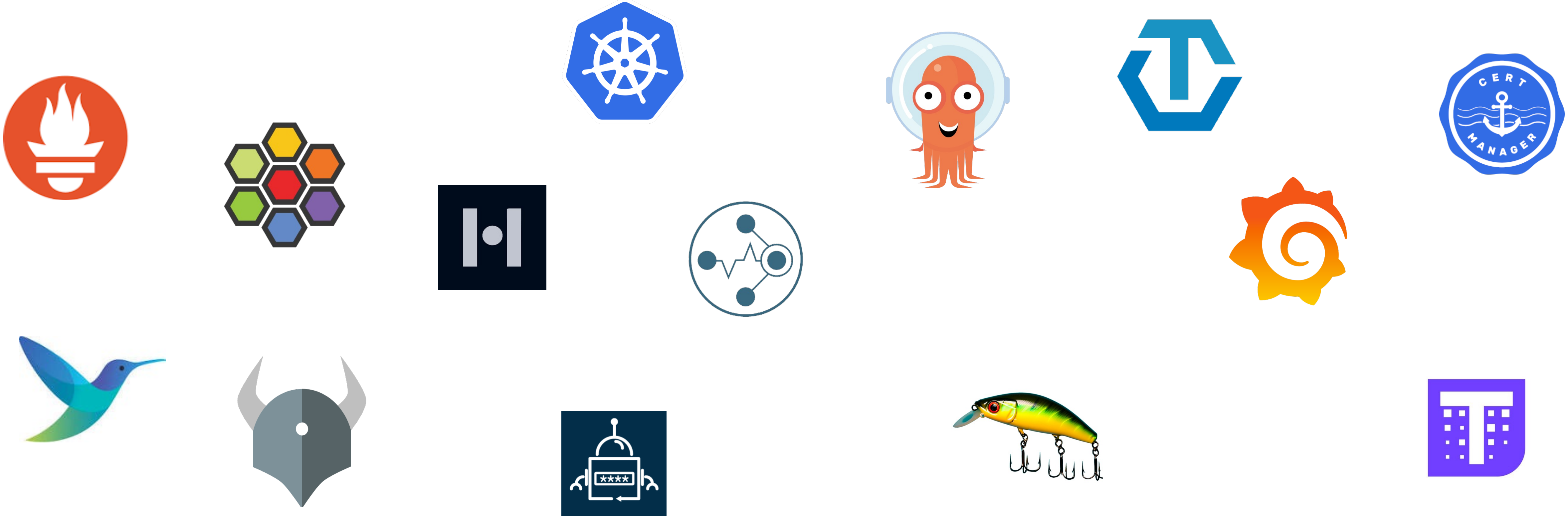
Non-disruptive Kubernetes Upgrades

Multi-tenancy at Scale

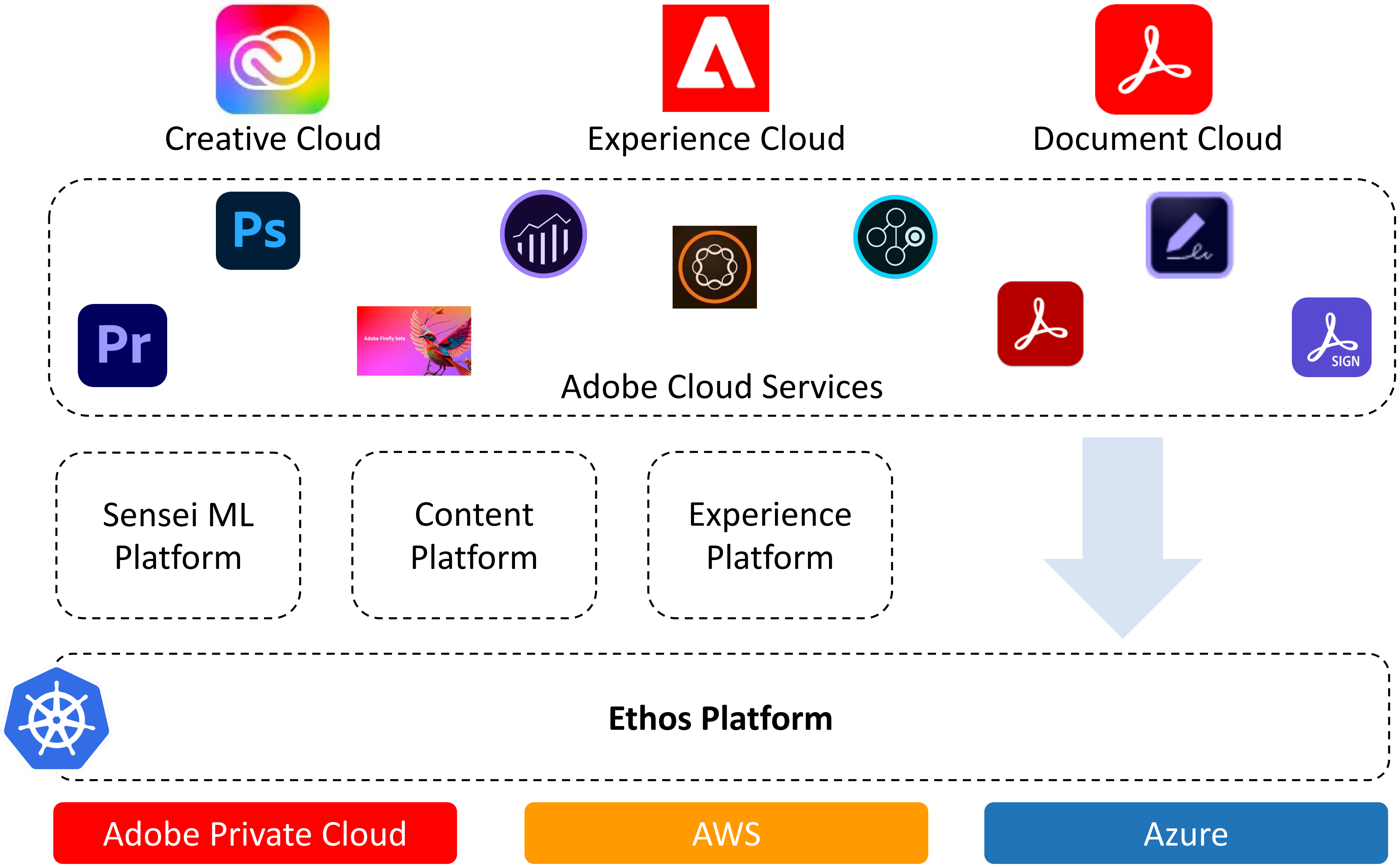
Conclusion

Project Ethos

A synergistic, multi-tenant Kubernetes based platform established through a collaborative effort between the infrastructure and product development teams at Adobe.



Ethos Overview



Creative Cloud

Experience Cloud

Document Cloud

Adobe Cloud Services

Sensei ML Platform

Content Platform

Experience Platform

Ethos Platform

Adobe Private Cloud

AWS

Azure

Ethos in Numbers

2.1 million containers

0.9 million pods

40k namespaces

310 K8s Clusters

AWS

Azure

APC

28 regions

> 32k compute nodes

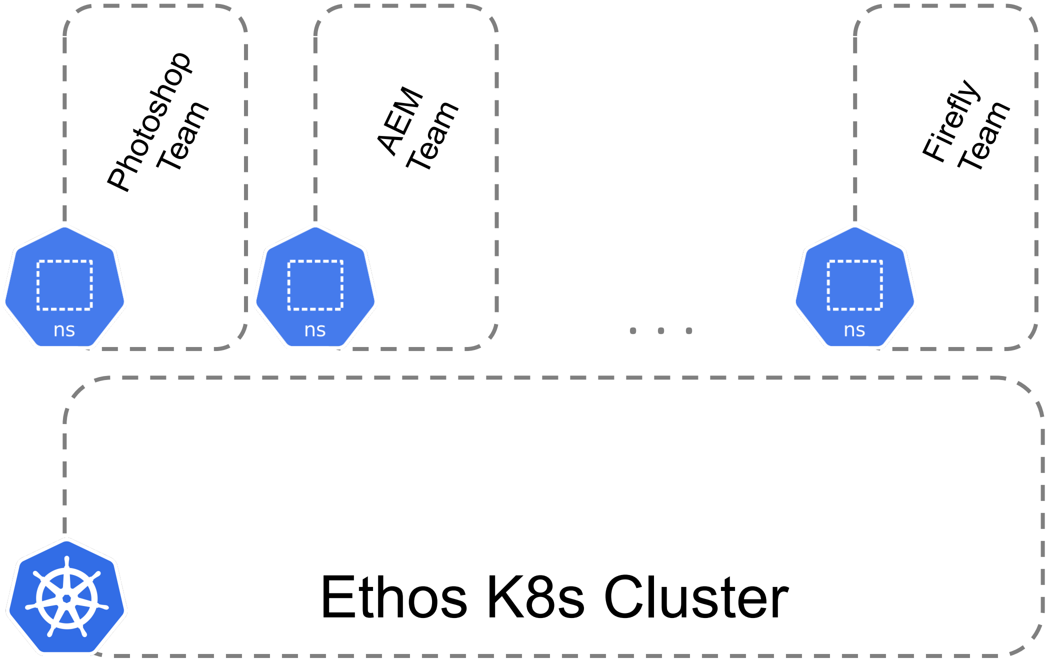
2.7PB Memory
750k CPUs
2.1k GPUs

Multi-tenancy @Adobe

Multi-tenancy = multiple different teams share multiple k8s clusters

> Shared Clusters

> Dedicated Clusters

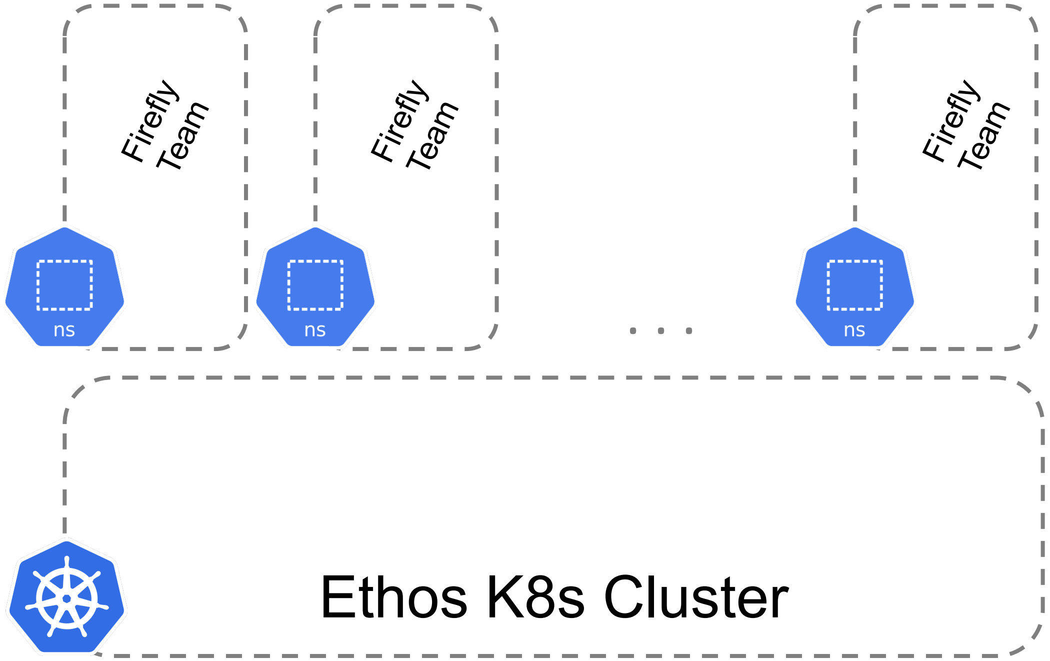


Multi-tenancy @Adobe

Multi-tenancy = multiple different teams share multiple k8s clusters

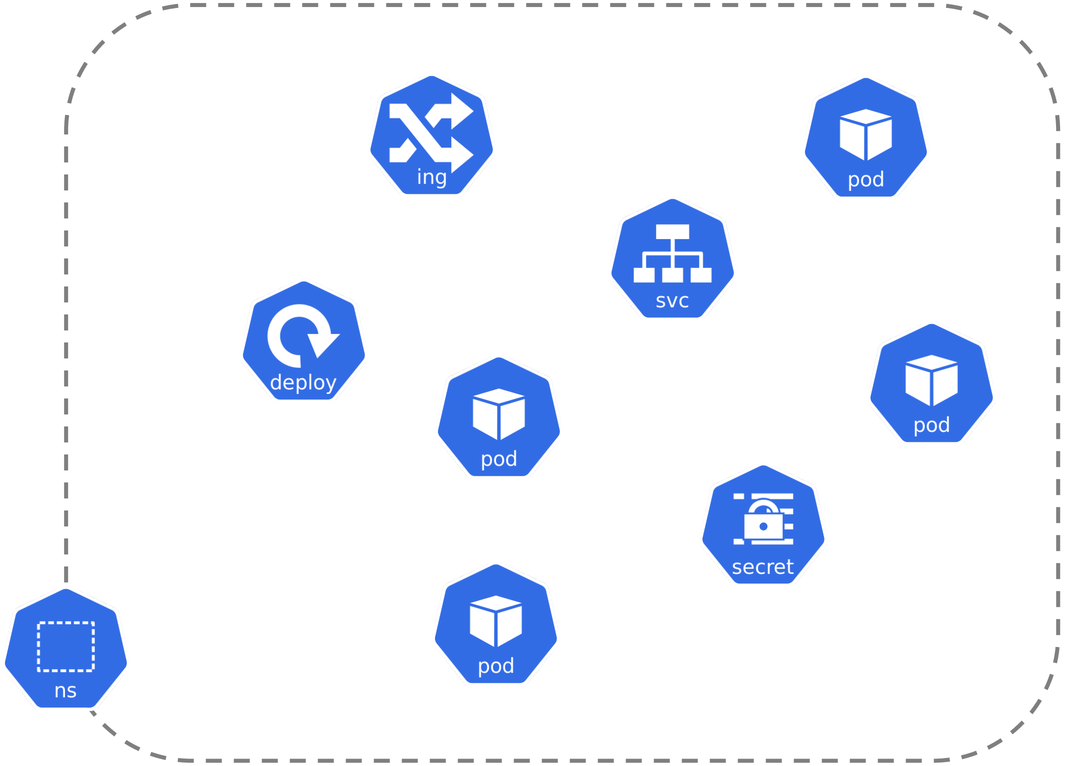
> Shared Clusters

> Dedicated Clusters



Namespaces aka Virtual K8s Clusters

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

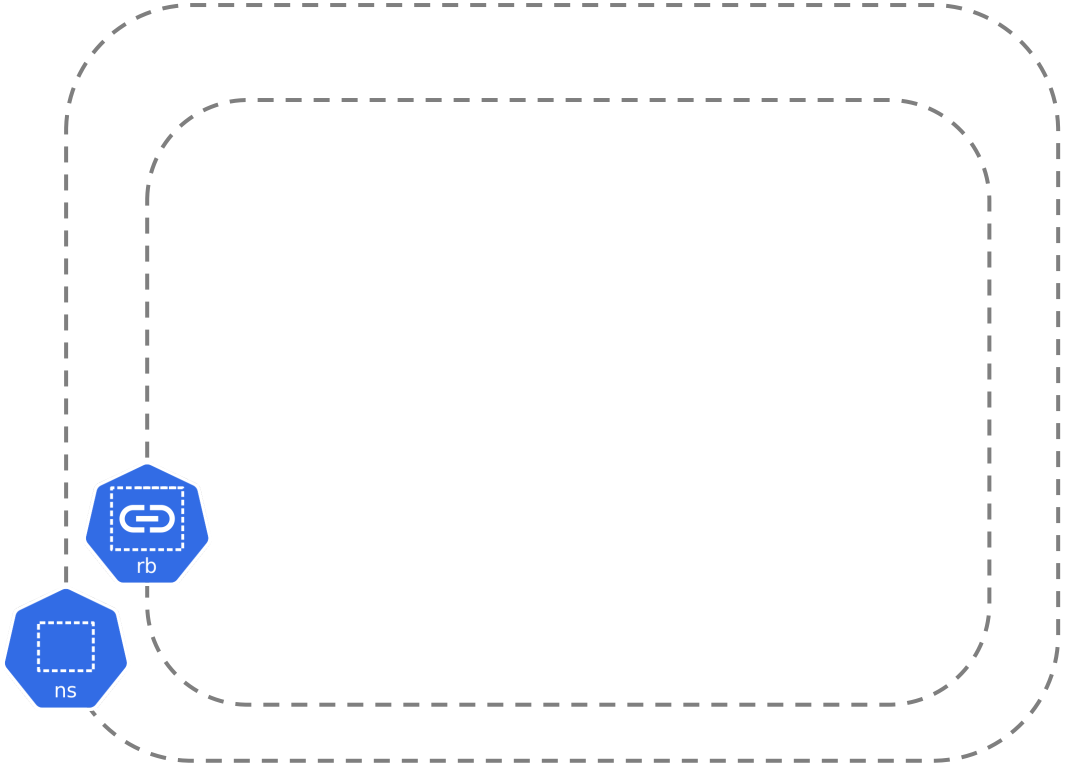


Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies

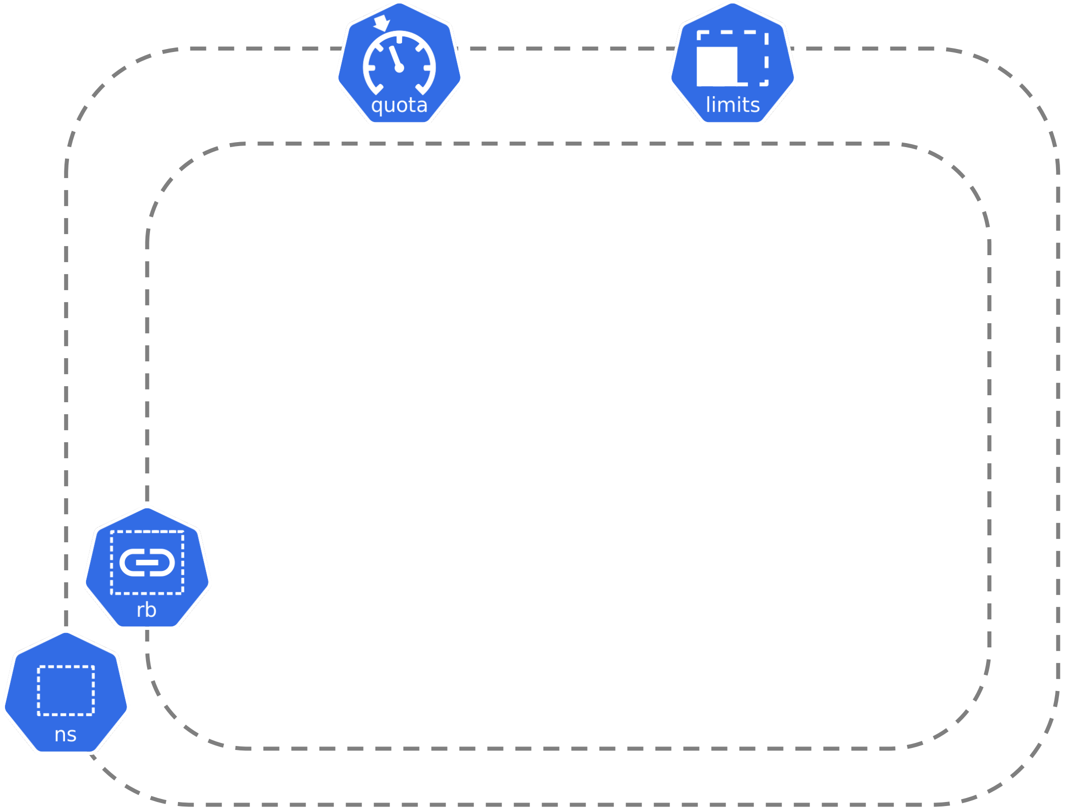
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



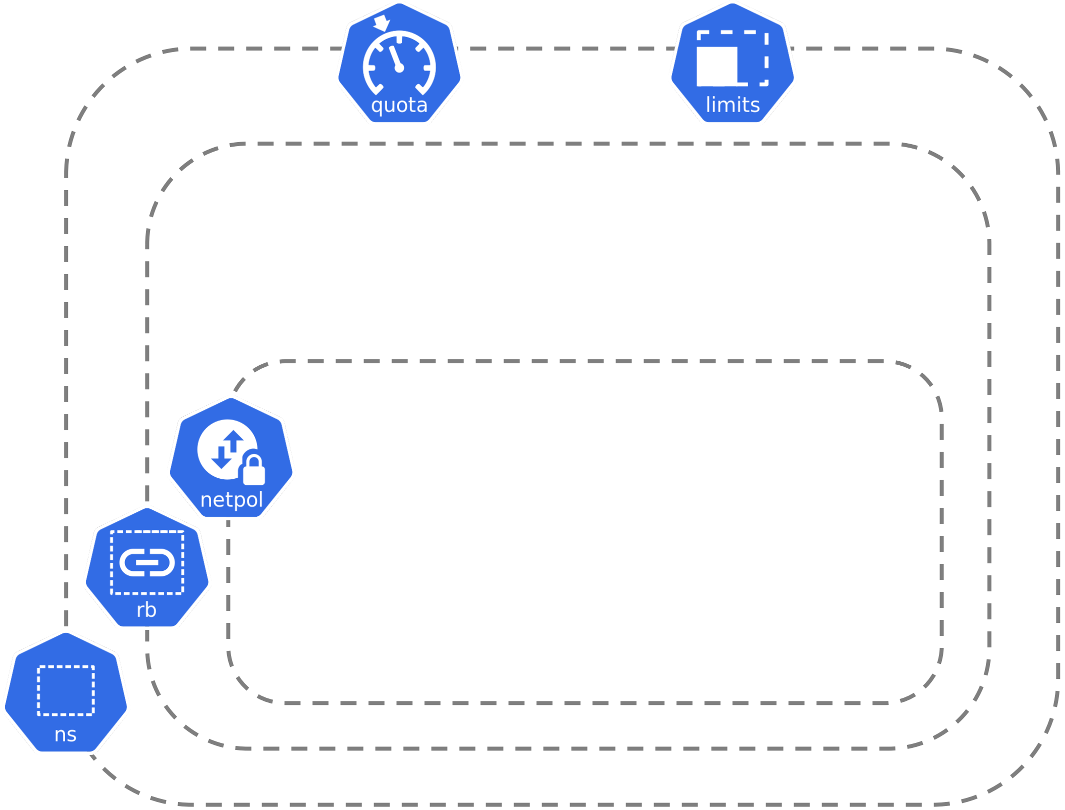
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



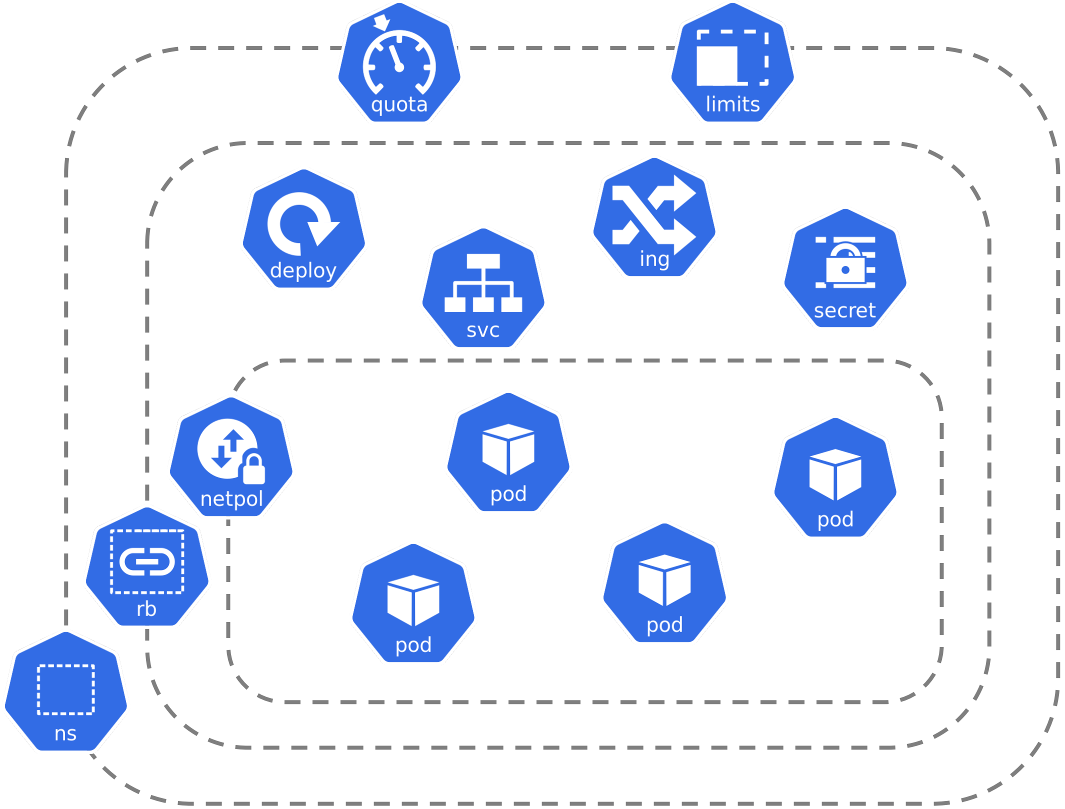
Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



Namespace profile

Namespace
Rolebinding
Quota
LimitRange
Network Policies
Cilium Network Policies



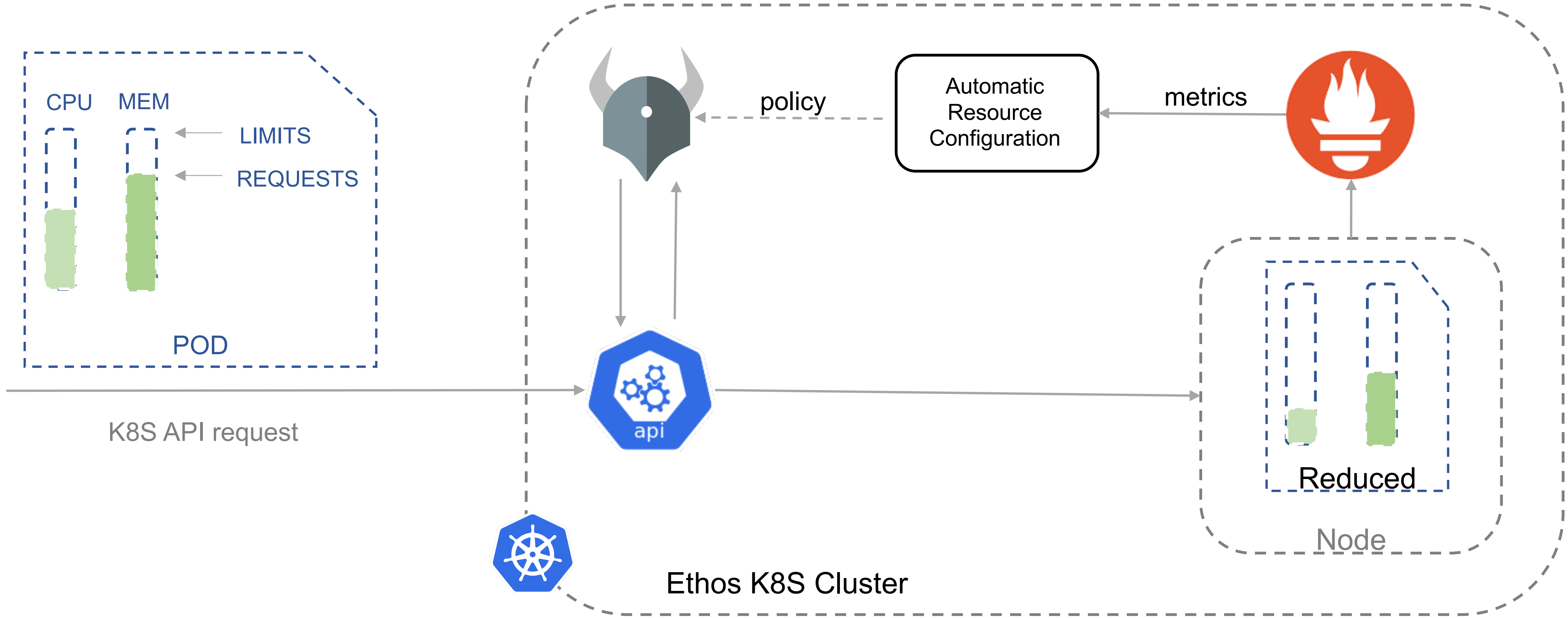
Capacity Management

Capacity issues = higher costs

Three levels:

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

Capacity Management

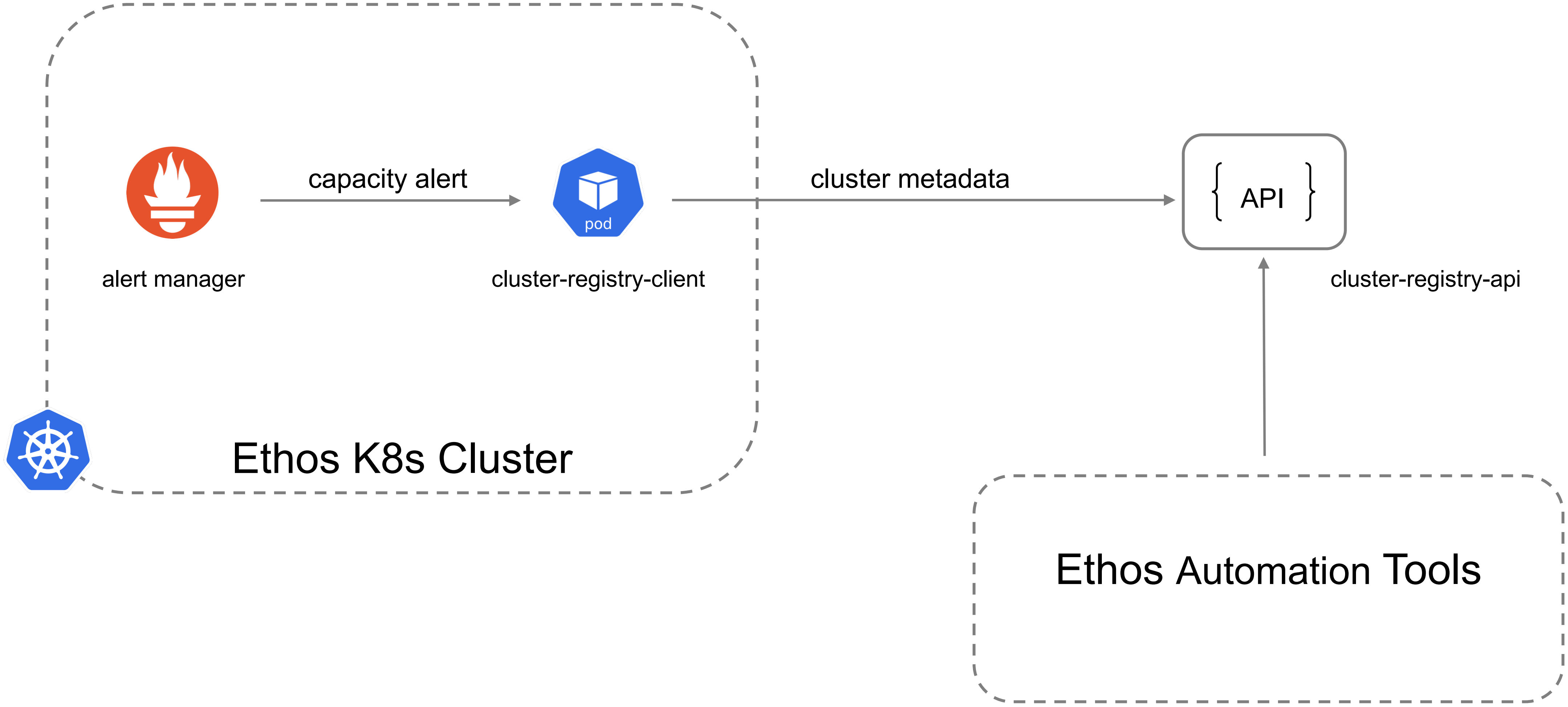


Capacity Management

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



Governance policies

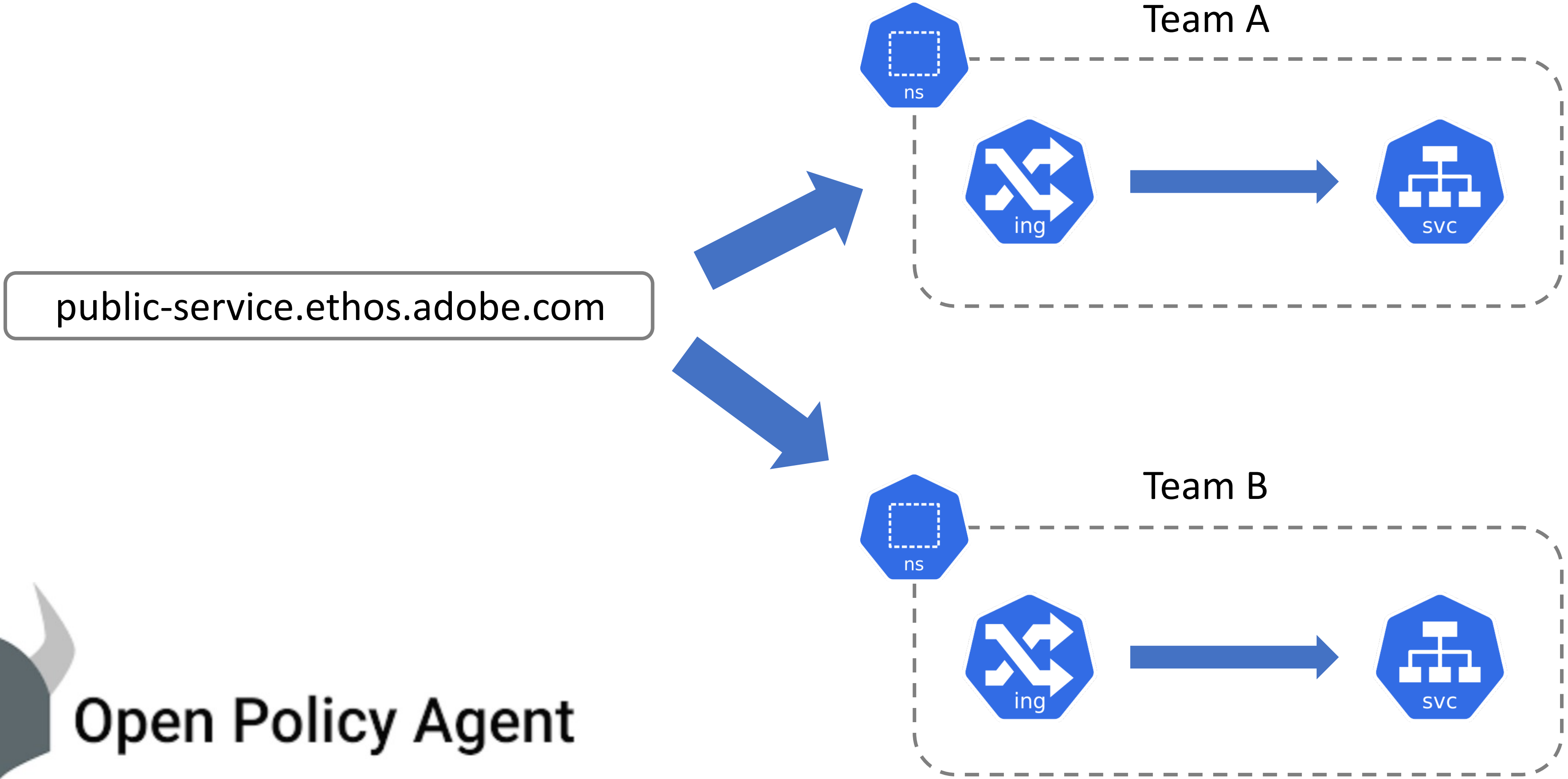
Business is governed by a set of rules => so does a multi-tenant k8s cluster.

Why are these policies mandatory?

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

Governance policies

FQDN Conflicts day



Open Policy Agent

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", [])
}
```

Non disrupting cluster upgrades

Disruptions:

- Voluntary
- Involuntary

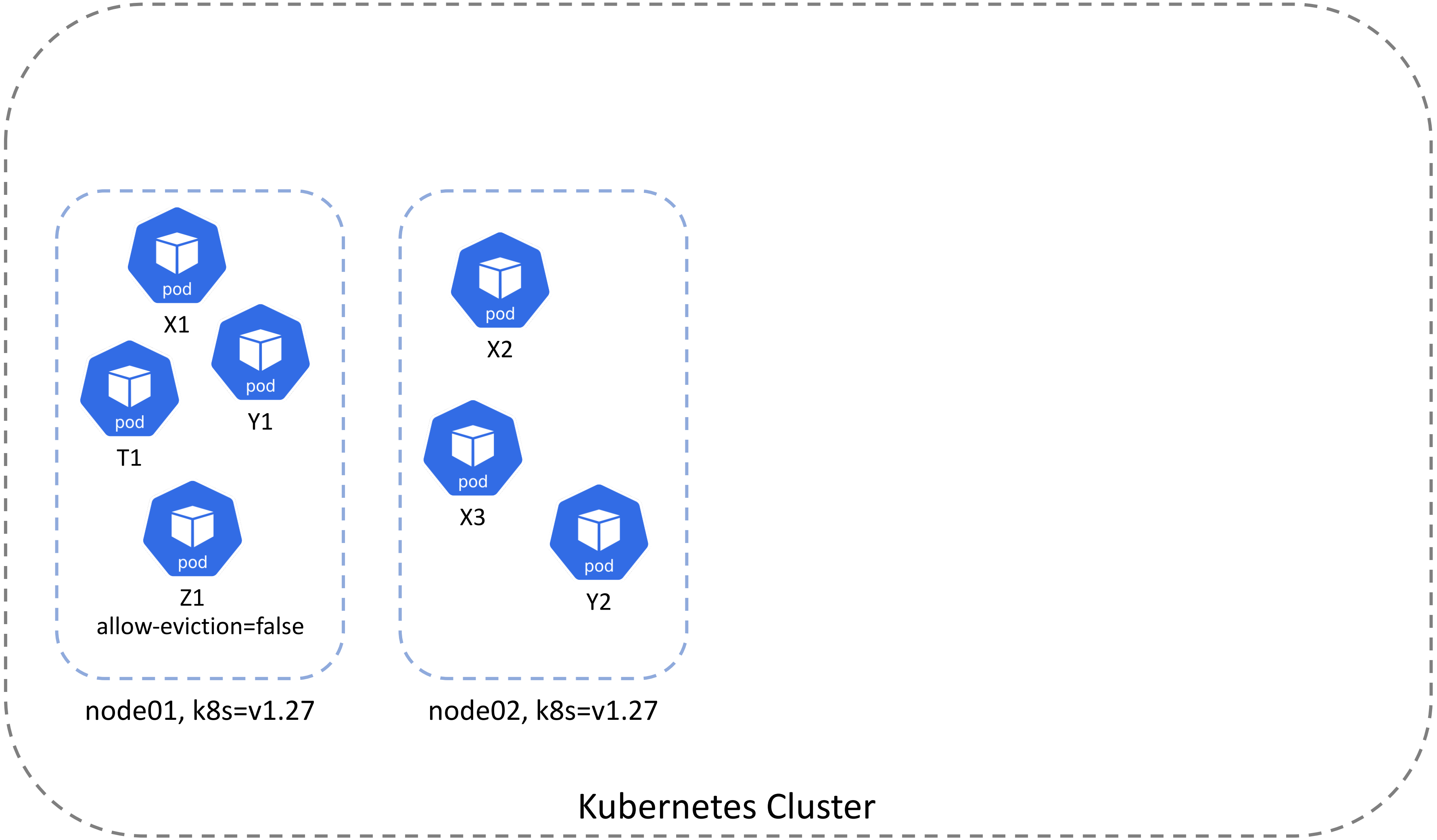
Pod Disruption Budget (PDB)

- contract between the cluster administrator and the developer

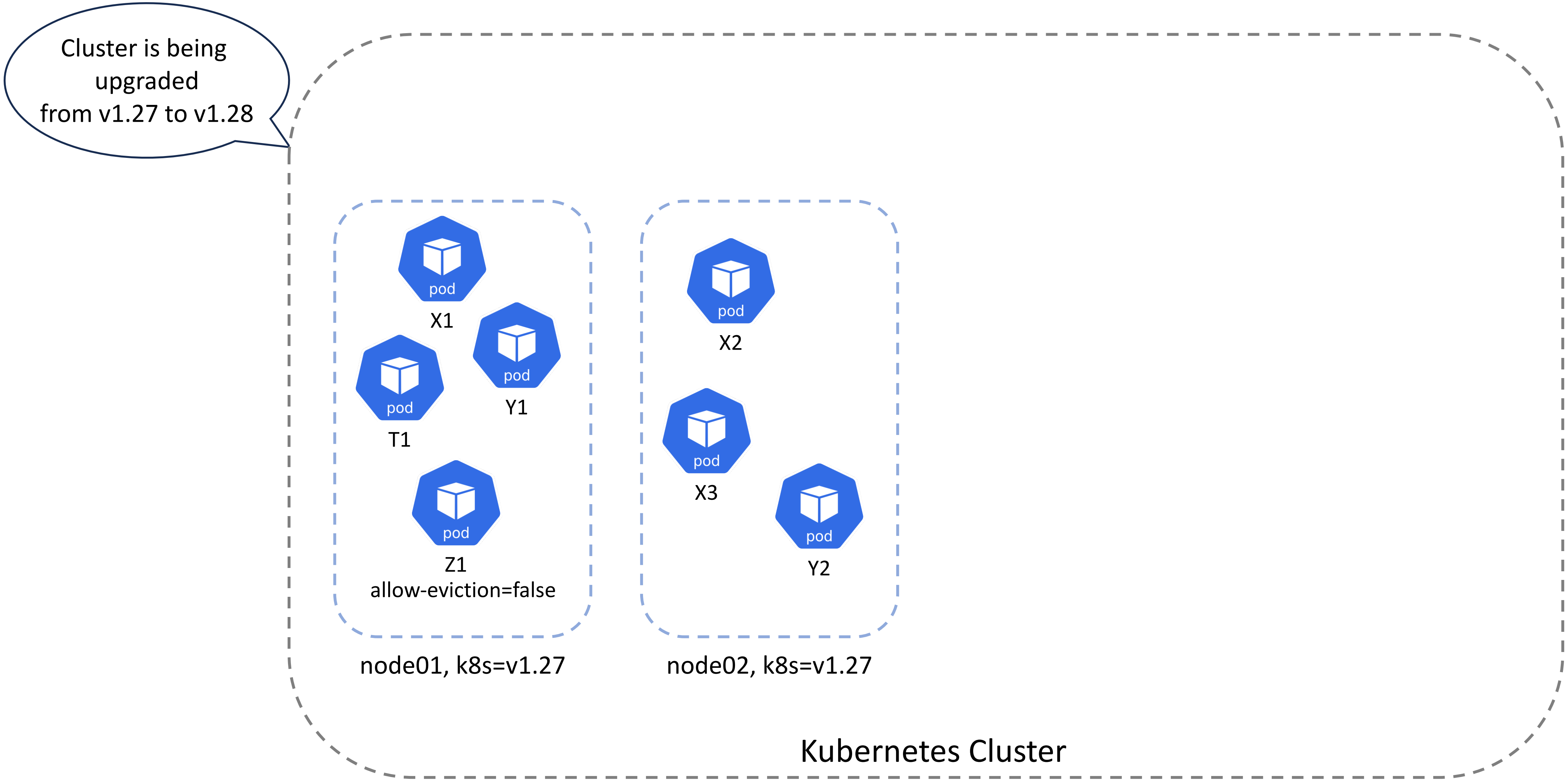
https://github.com/adobe/k8s-shredder

Non disrupting cluster upgrades

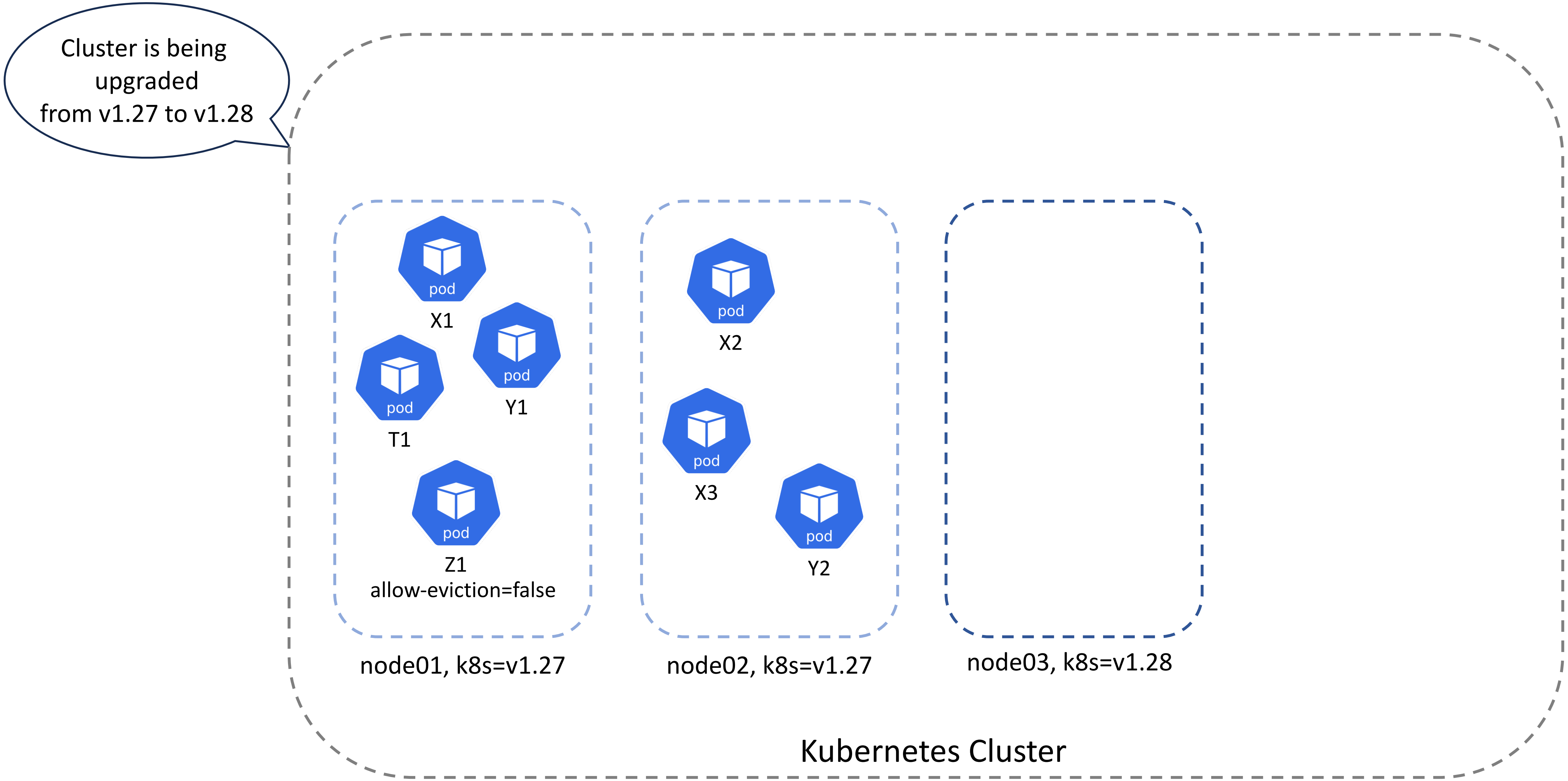
KubeCon CloudNativeCon OPEN SOURCE SUMMIT China 2023



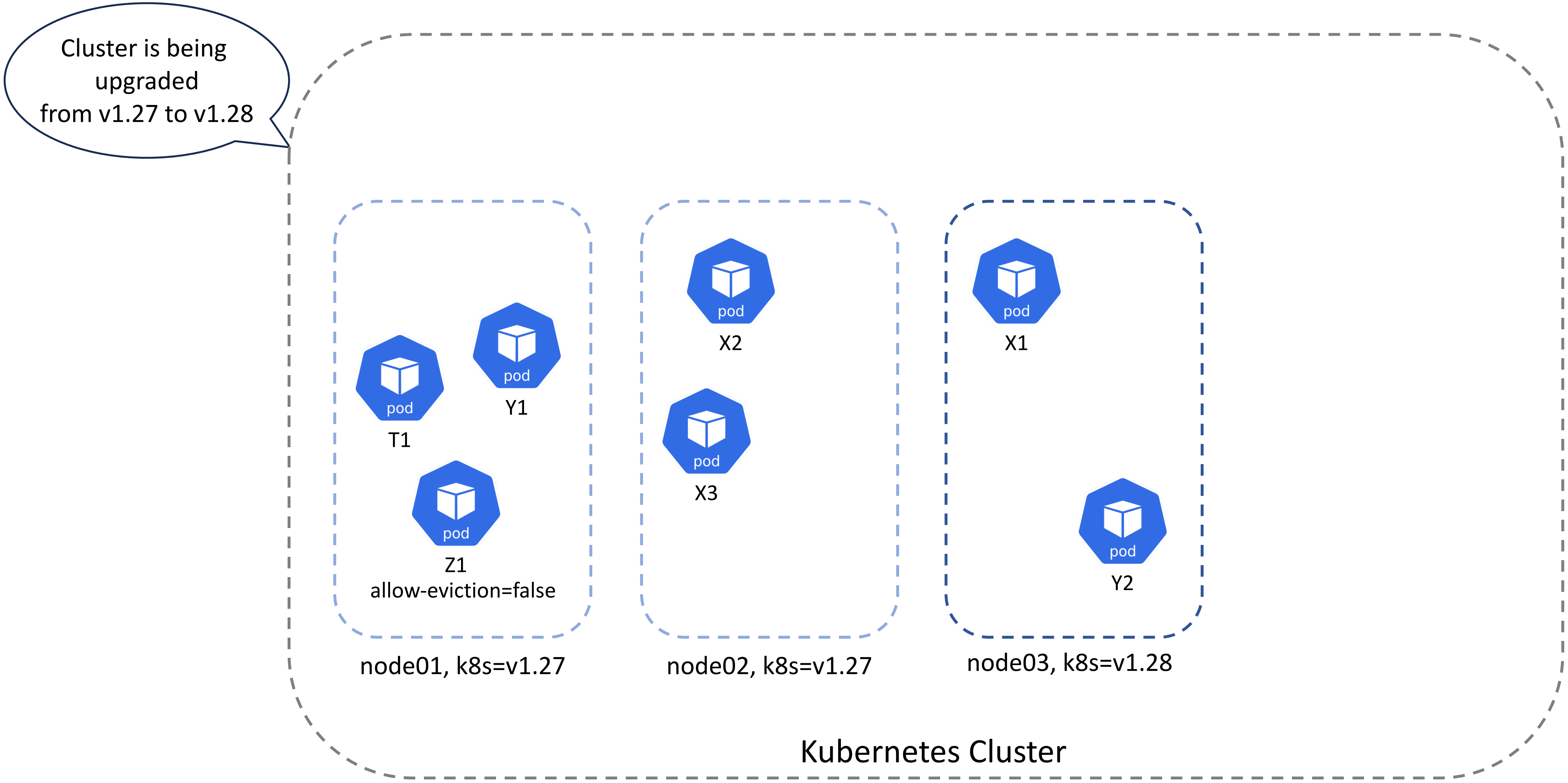
Non disrupting cluster upgrades



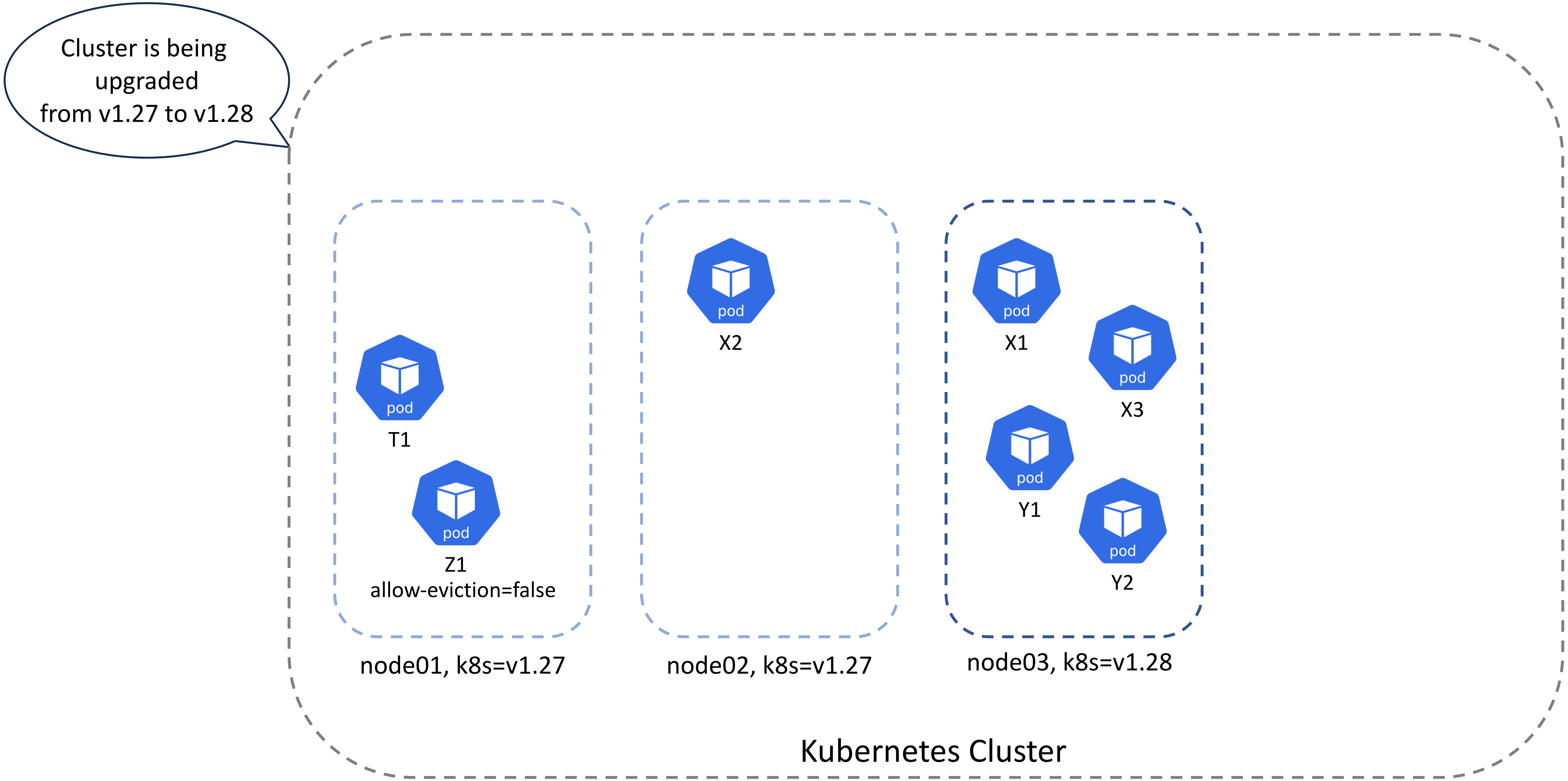
Non disrupting cluster upgrades



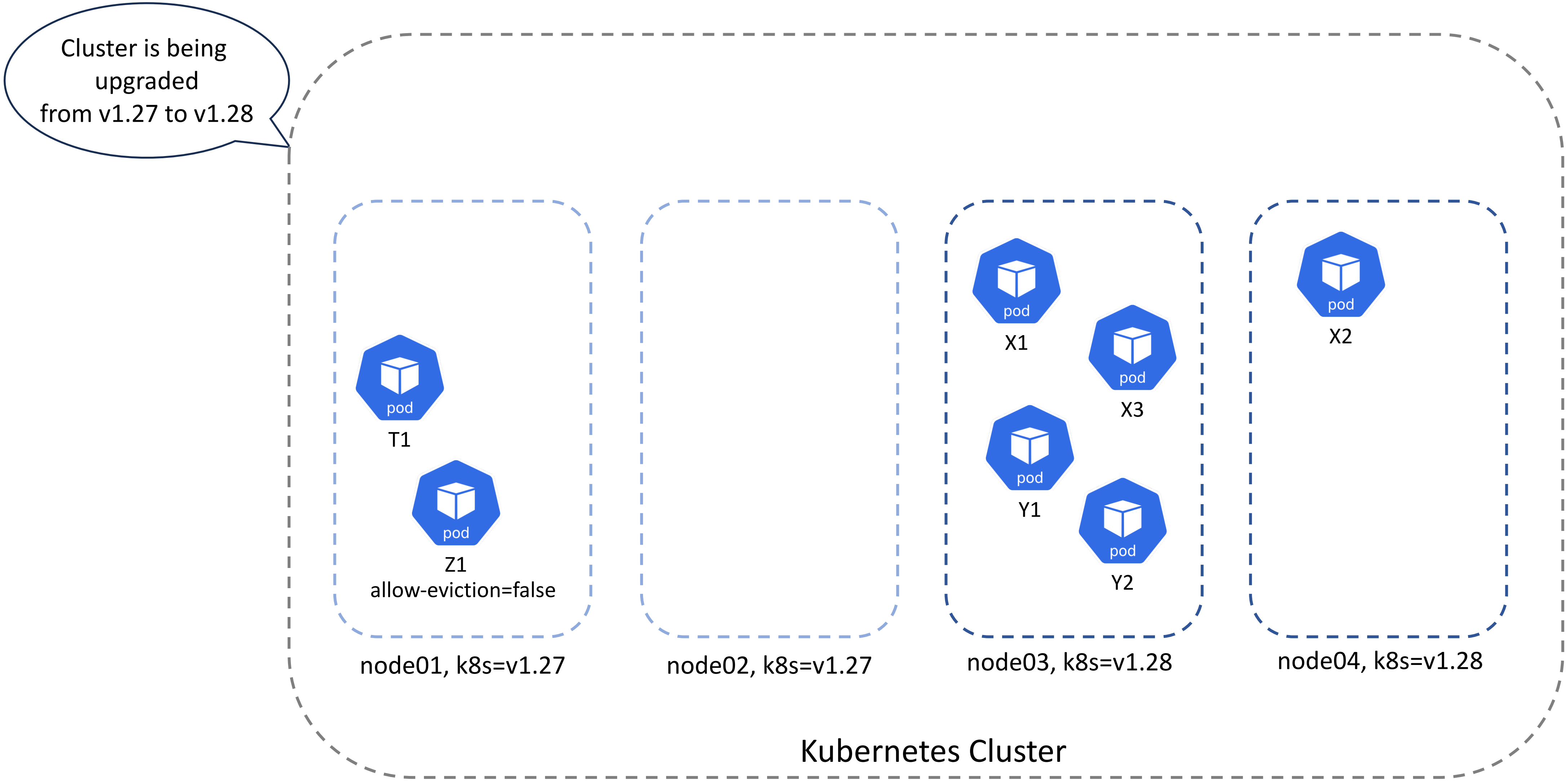
Non disrupting cluster upgrades



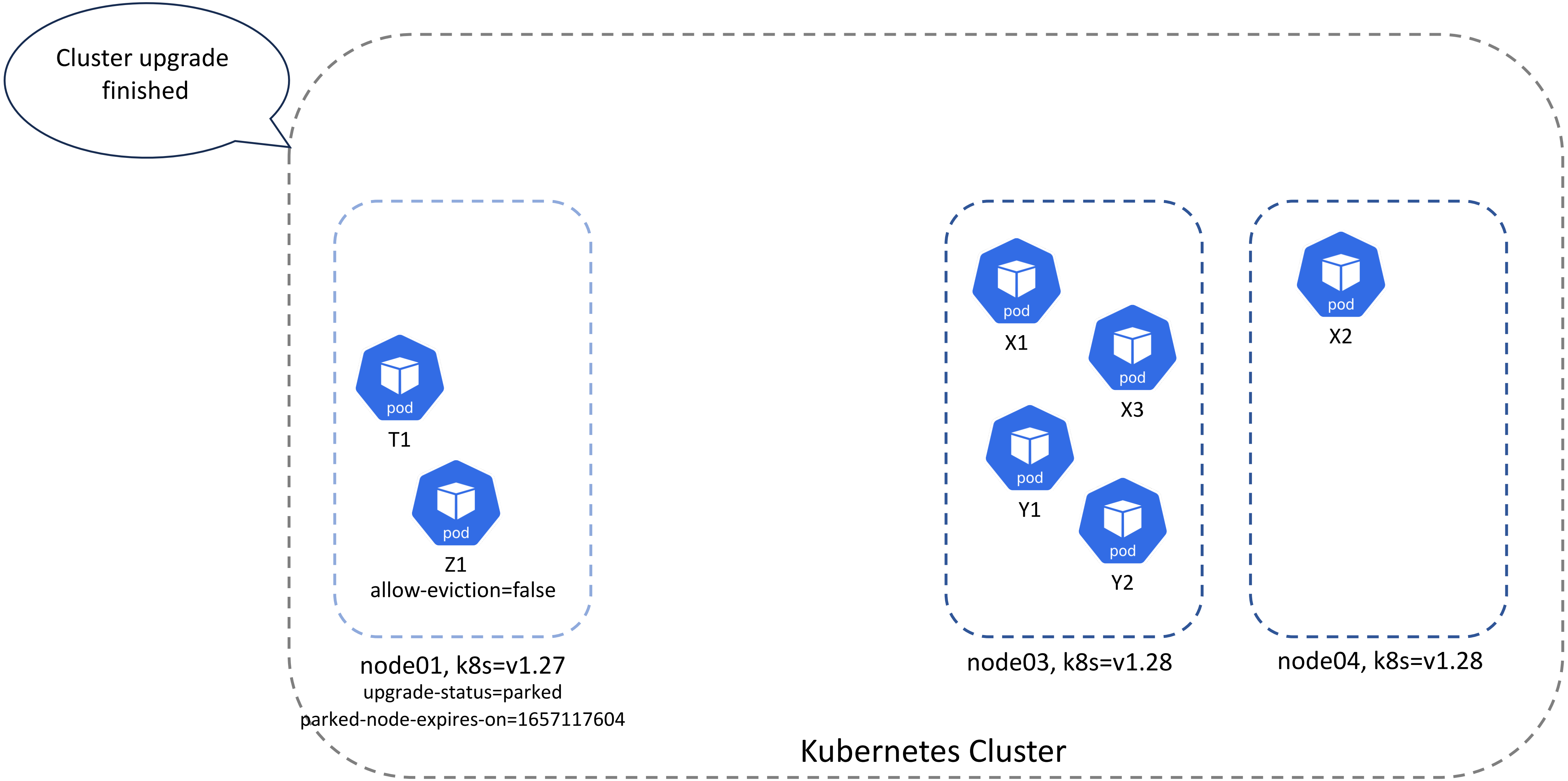
Non disrupting cluster upgrades



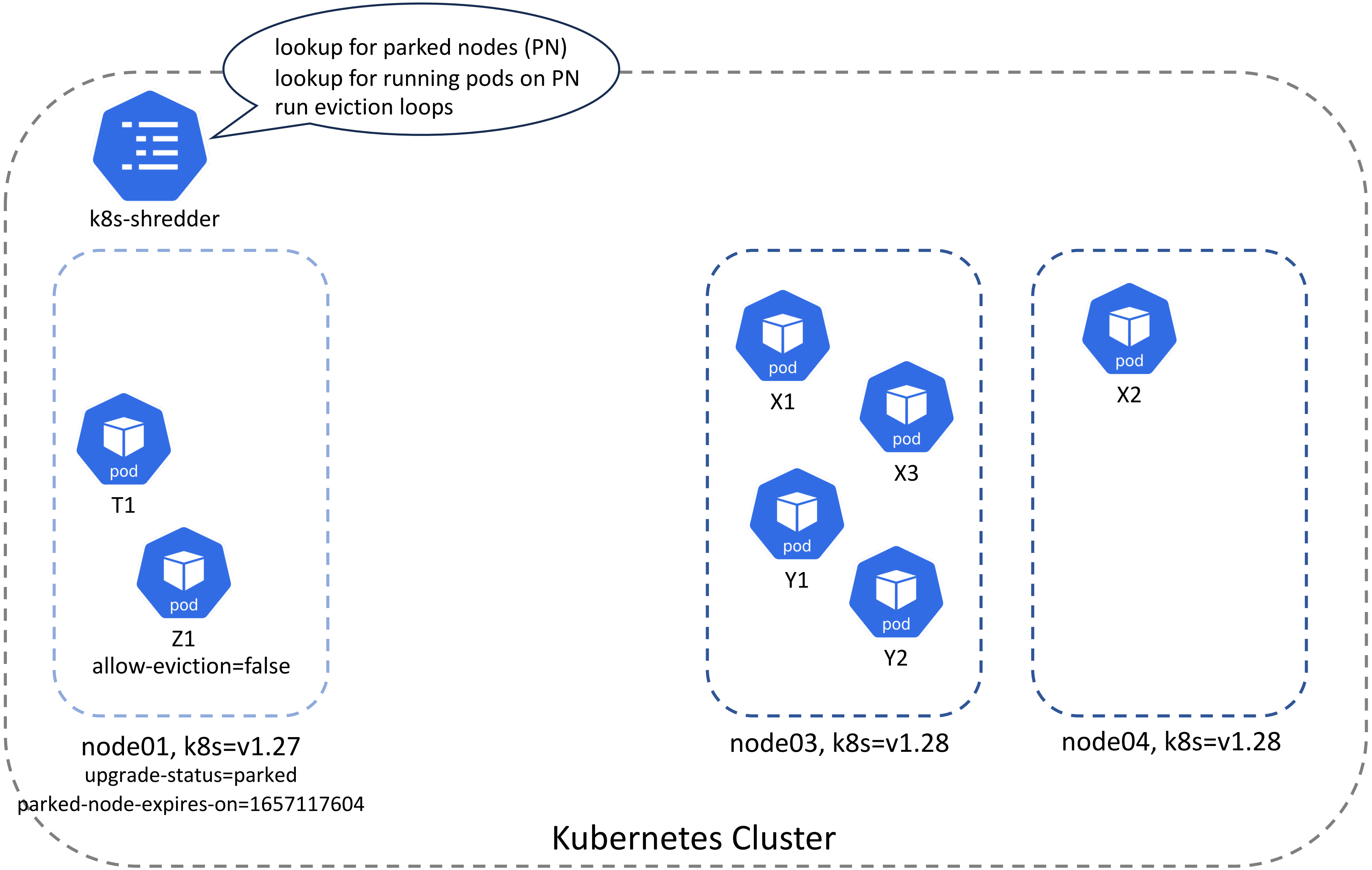
Non disrupting cluster upgrades



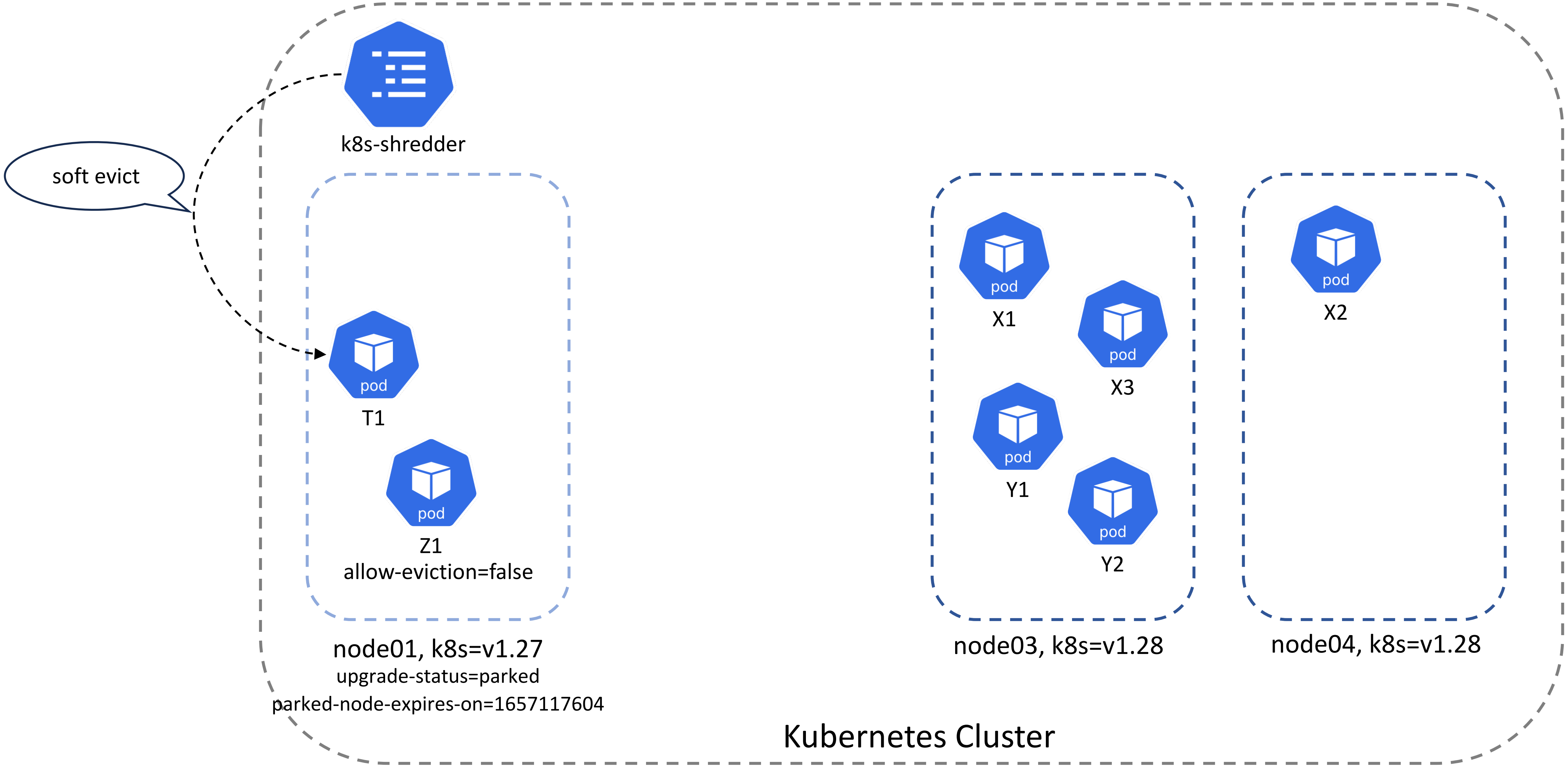
Non disrupting cluster upgrades



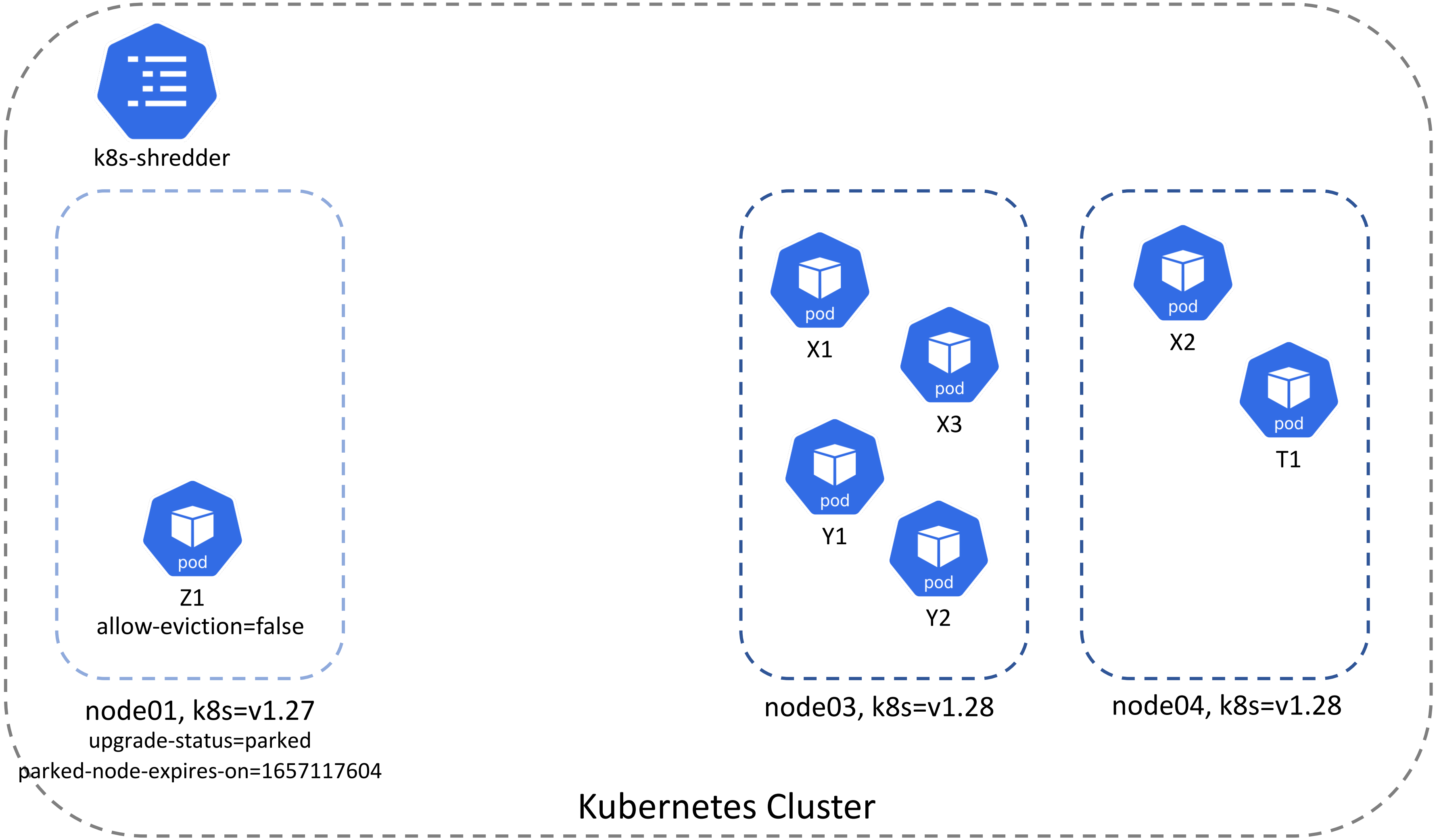
Non disrupting cluster upgrades



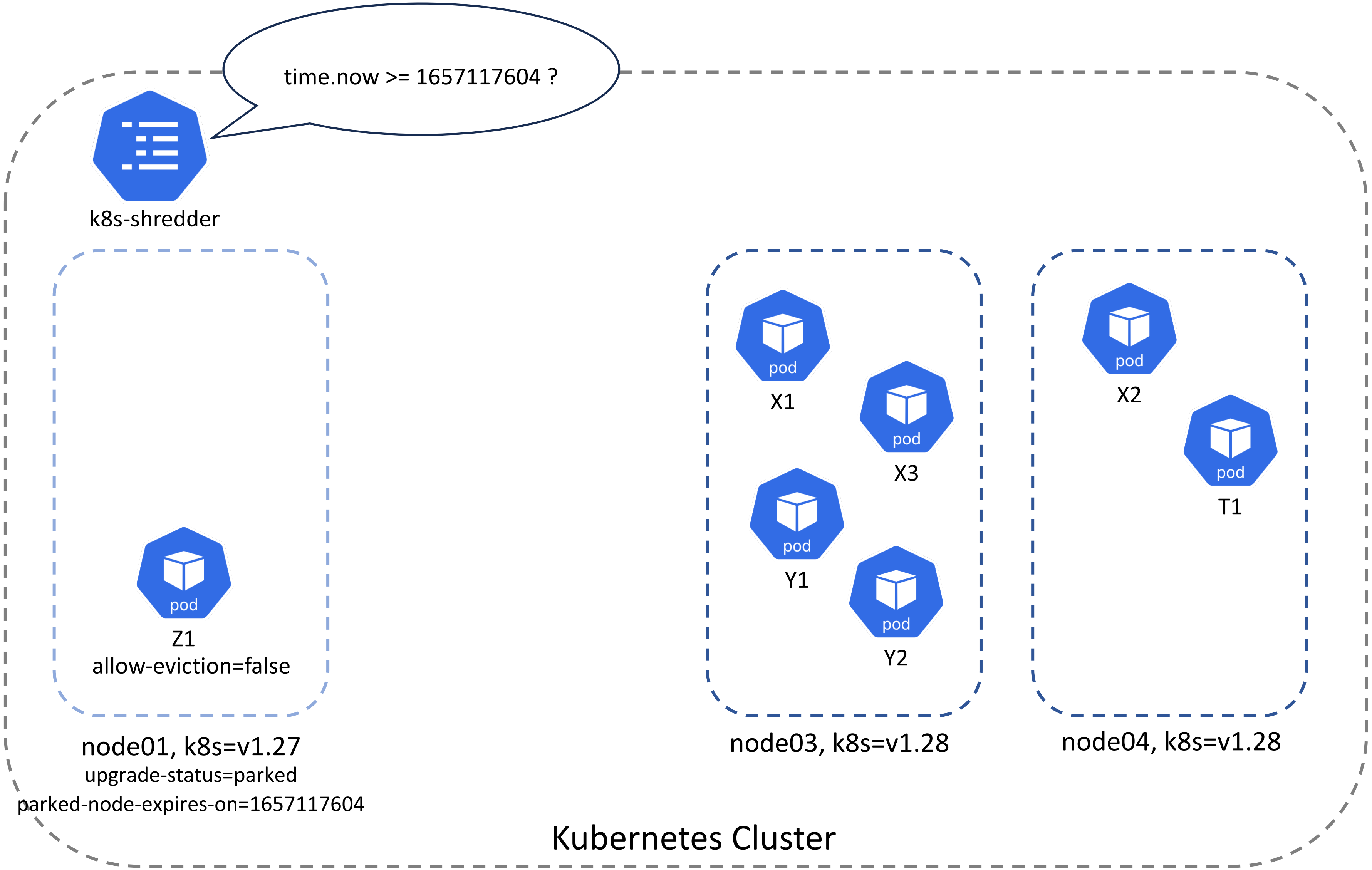
Non disrupting cluster upgrades



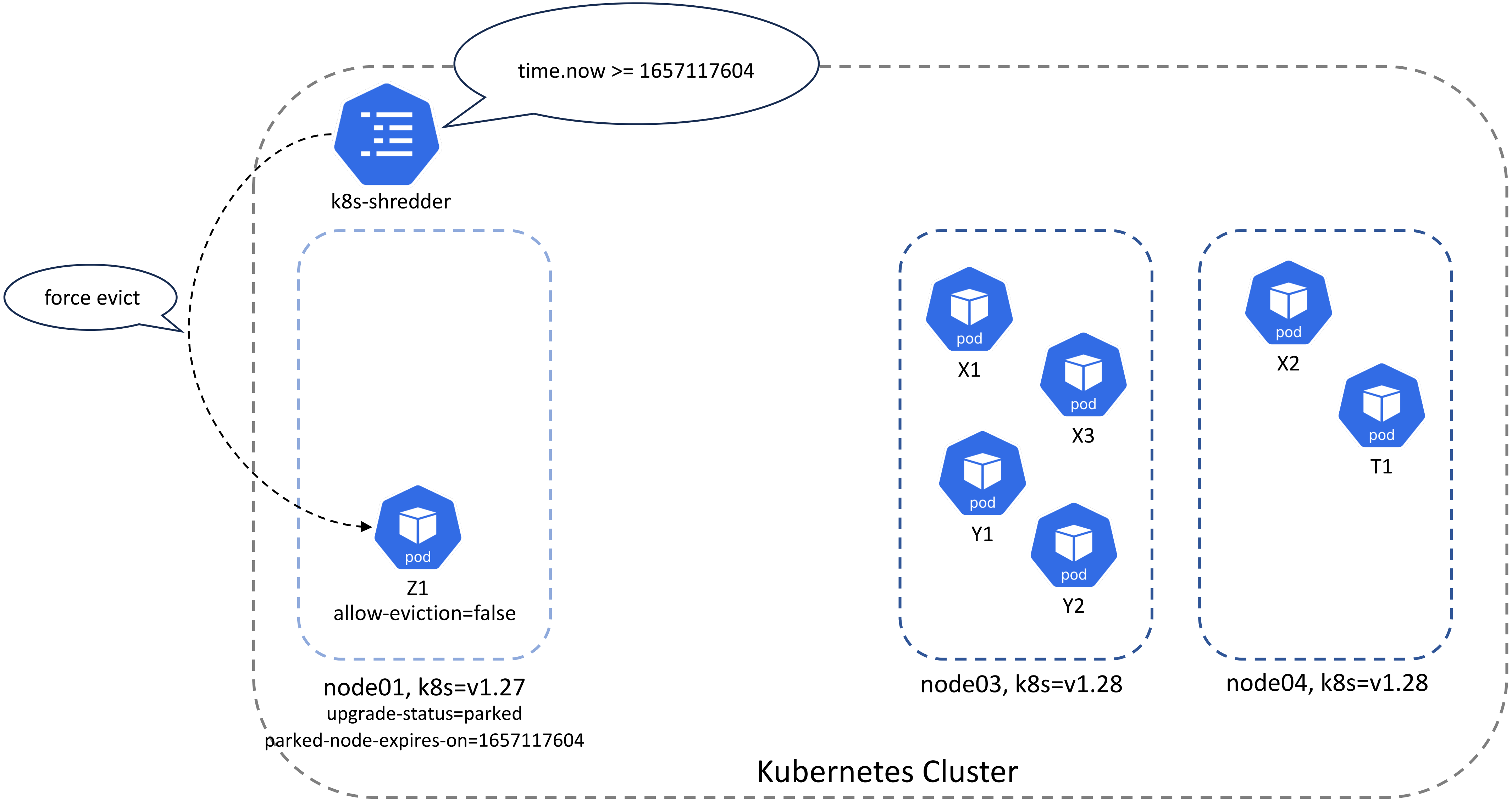
Non disrupting cluster upgrades



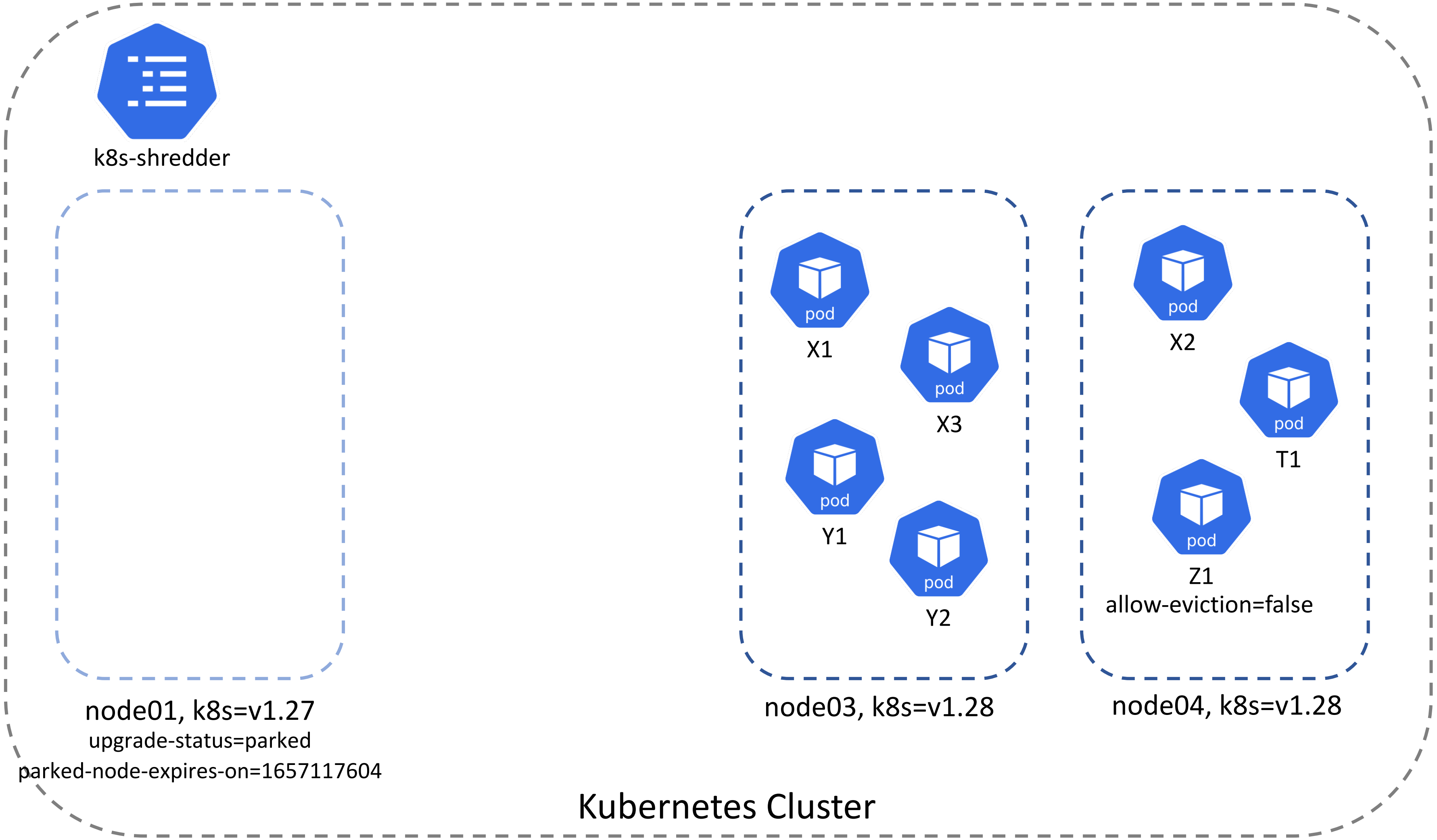
Non disrupting cluster upgrades



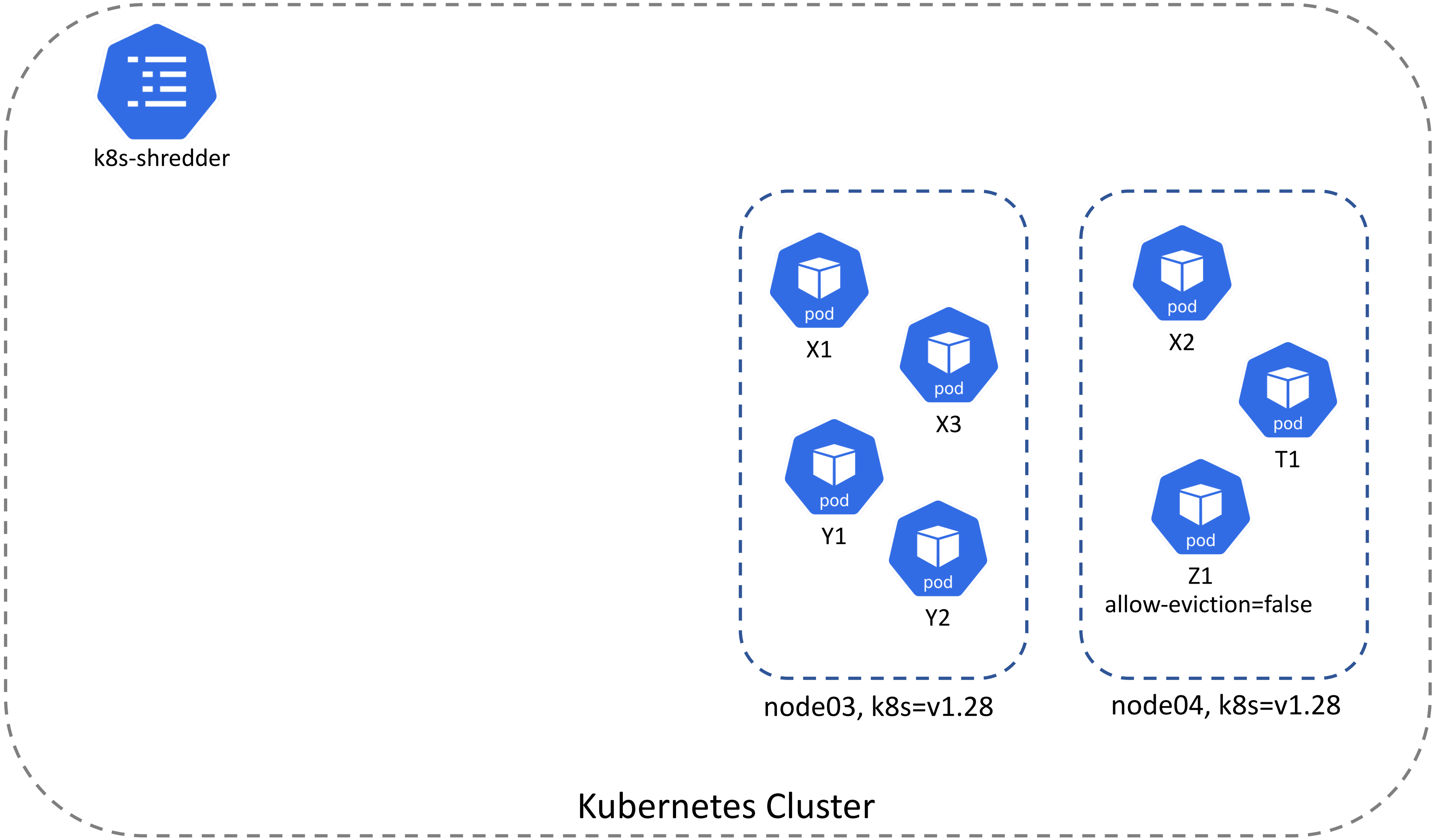
Non disrupting cluster upgrades



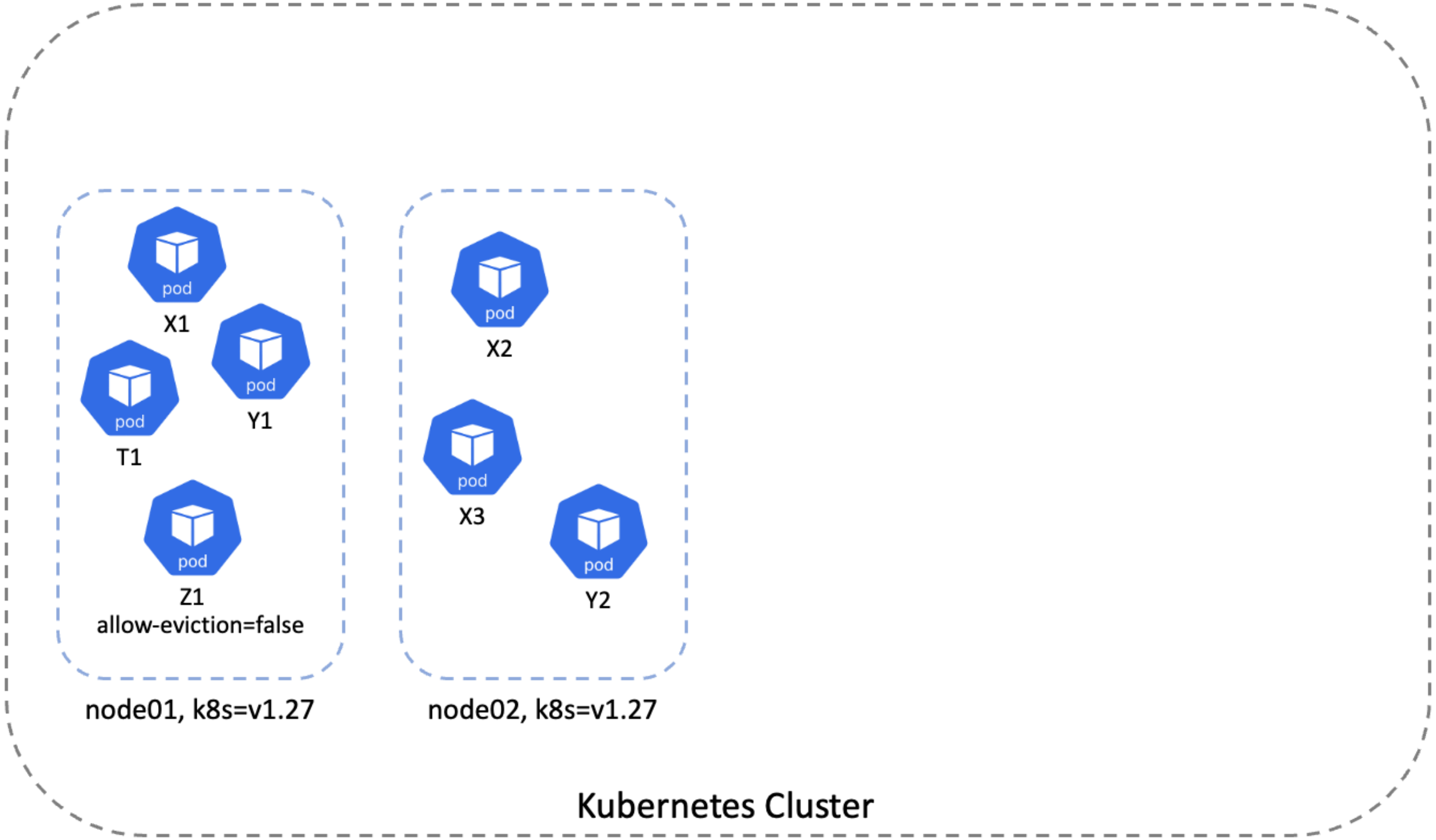
Non disrupting cluster upgrades



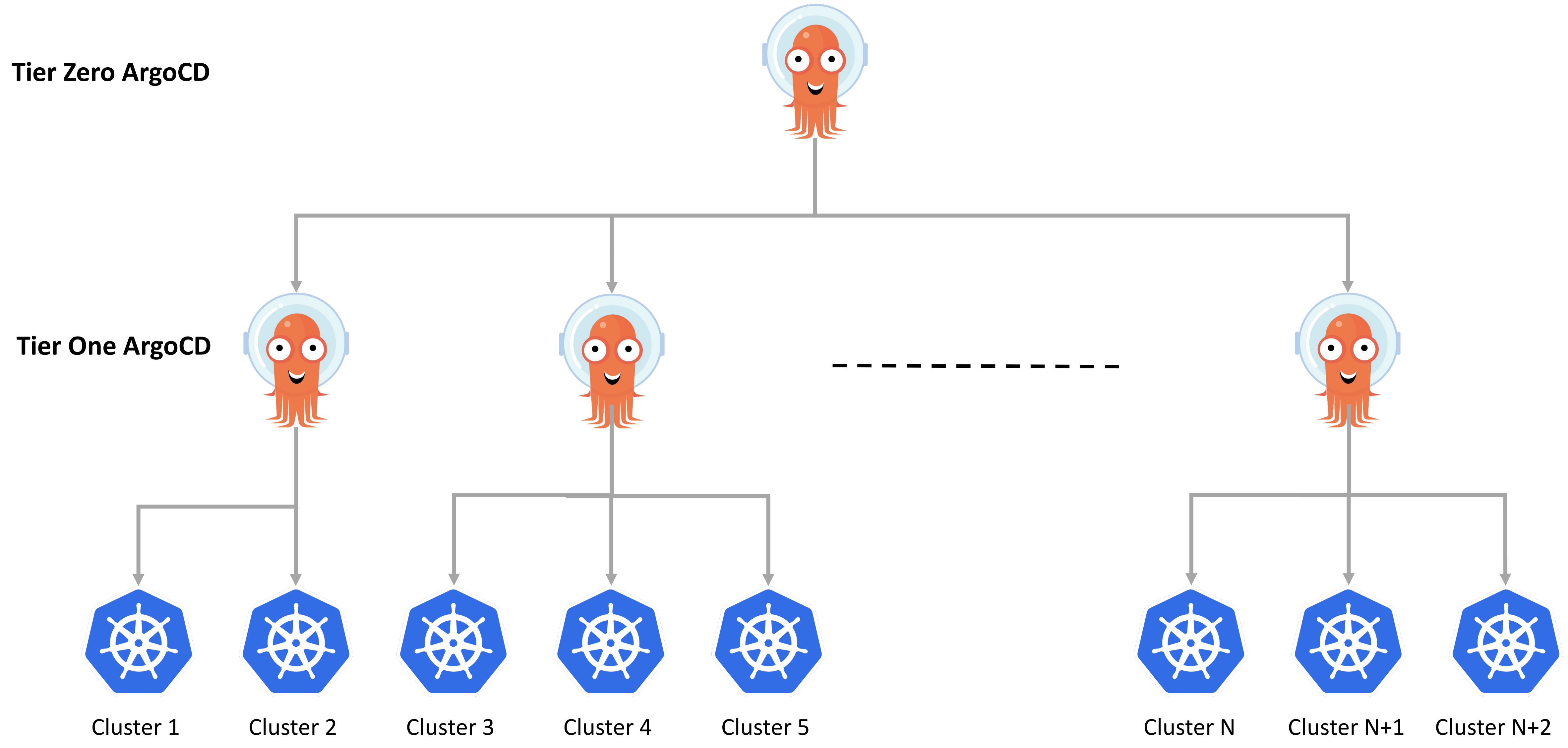
Non disrupting cluster upgrades



Non disrupting cluster upgrades



Multi-tenancy at scale



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.

Q & A

@email: aneci@adobe.com

@github: adriananeci

@linkedin: adrian-aneci

@email: vvarza@adobe.com

@github: victorvarza

@linkedin: victorvarza