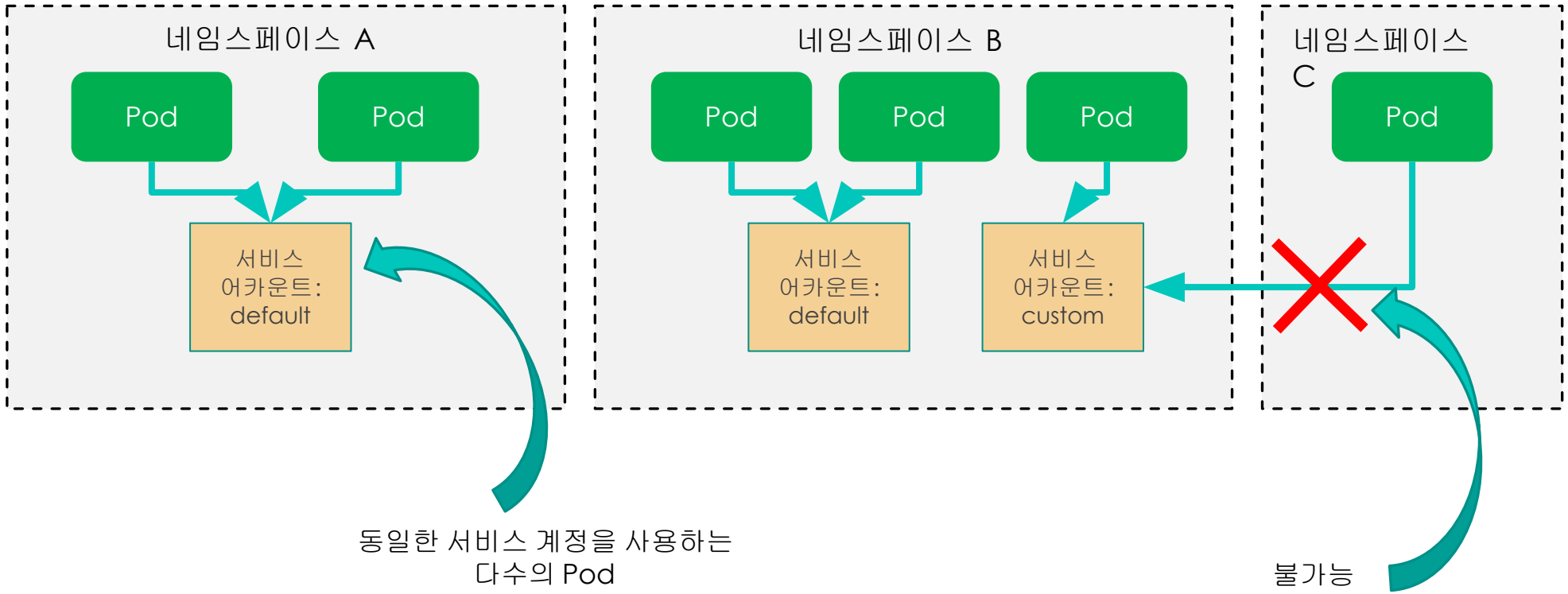
22. 서비스 어카운트 및 RBAC

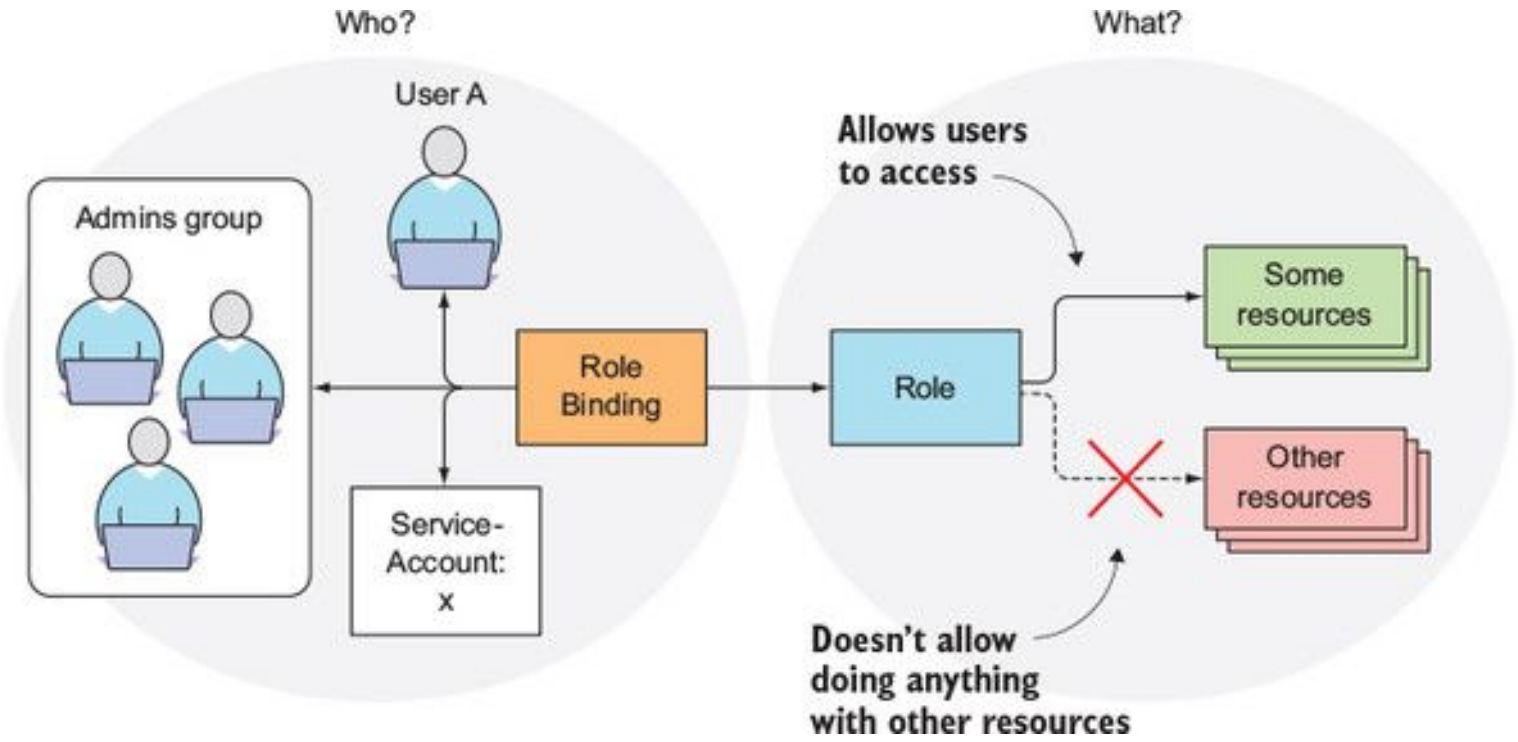
서비스 계정 (Service Account)

- 쿠버네티스는 유저계정(User Account) 및 서비스 계정(Service Account) 두가지를 지원함
- 유저 계정은 주로 클러스터 관리에 사용 되며, 서비스 계정은 응용 프로그램의 API 접근을 위해 사용됨
- 각 Pod 는 네임스페이스 있는 단일 서비스 어카운트와 연관돼 있음



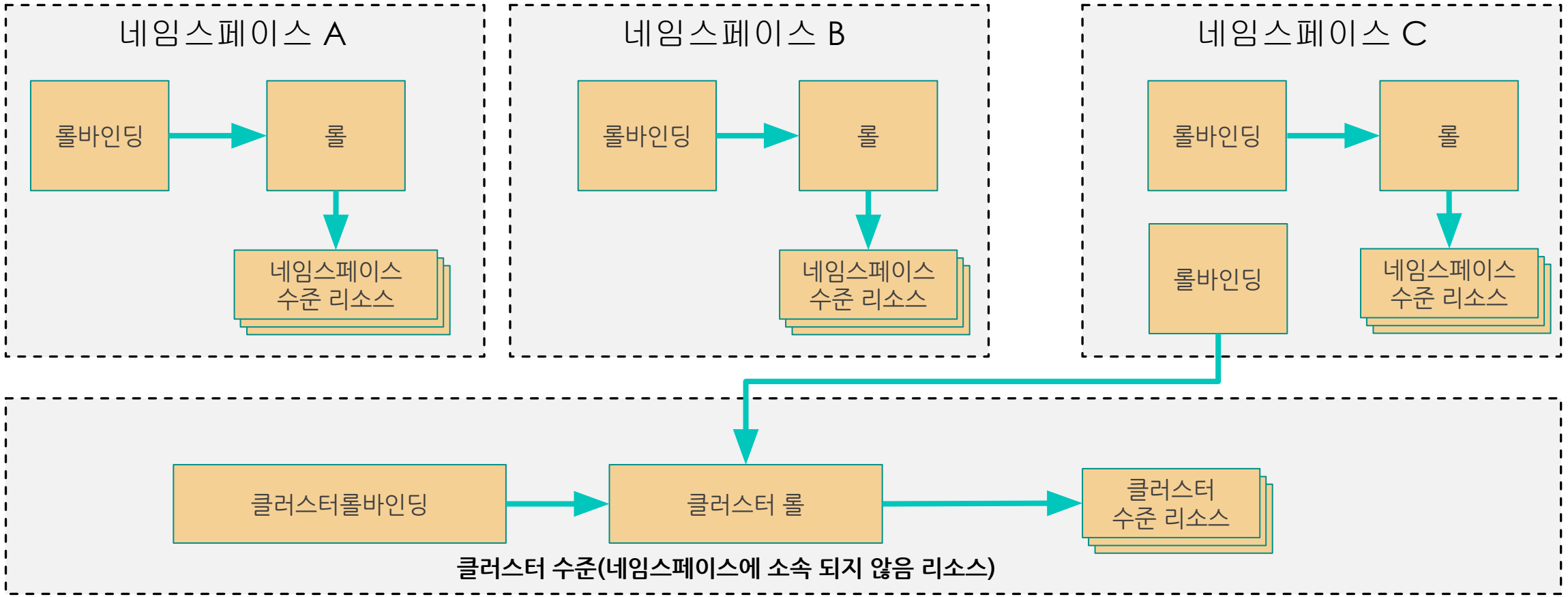
Role and Role Binding

- 특정 리소스에 접근 가능한 롤을 만들고 롤 바인딩을 통해 사용자나 그룹에 롤을 부여함
- 바인딩은 유저 계정 및 서비스 계정 모두에 바인딩 가능함
- 하나의 유저는 여러 개의 롤을 바인딩을 통해 부여 받을 수 있음



RBAC(Role-Based Access Control)

- 쿠버네티스는 ABAC(Attribute-Based Access Control) 과 RBAC 를 지원. 주로 RBAC 사용
- 롤(Role)은 특정 api나 리소스에 대한 권한들을 명시해둔 규칙들의 집합
- 롤에는 그냥 롤(Role)과 클러스터롤(ClusterRole) 2가지 종류가 있음
- 클러스터롤은 특정 네임스페이스에 대한 권한이 아닌 클러스터 전체에 대한 권한을 관리



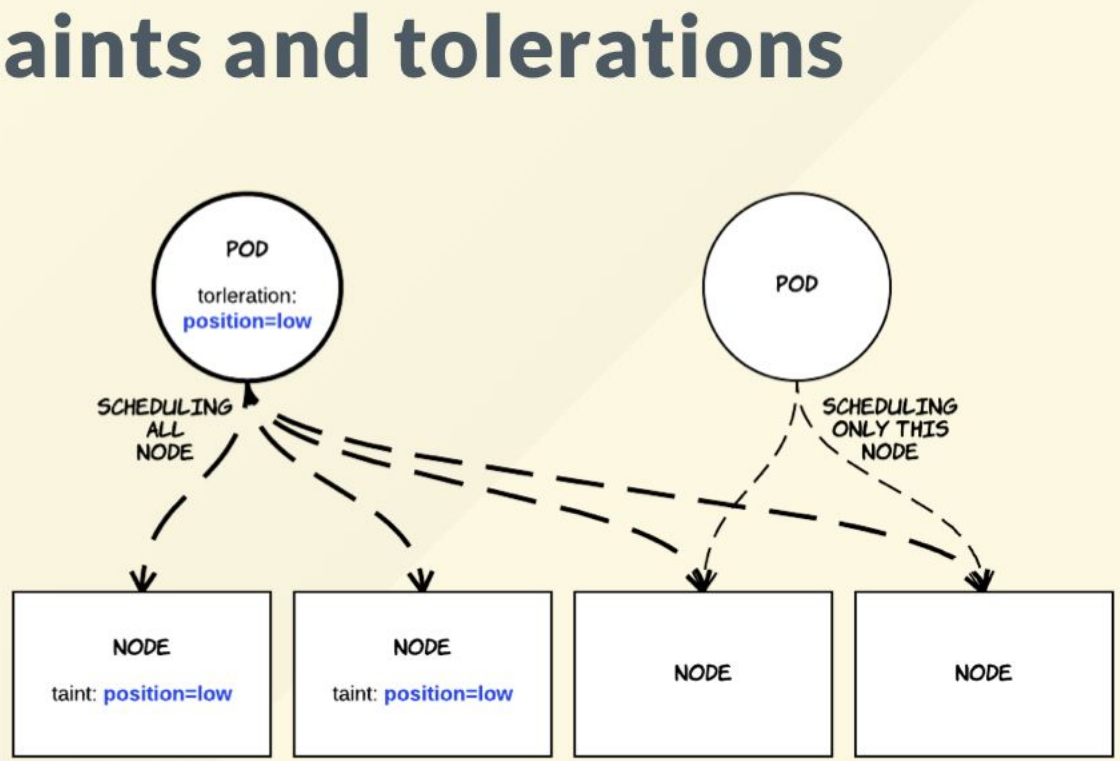
22. Taint 및 Toleration

Taint 및 Toleration

- Taint 는 {key}={value}:{option} 형식으로 이루어짐
- tain : 노드마다 설정 가능 하며, 설정한 노드에는 Pod 가 스케줄 되지 않음
- Toleration: taint를 무시 할 수 있음
- Taint 에는 3가지 종류가 있음

Taint	설명
NoSchedule	toleration이 없으면 pod이 스케쥴되지 않음, 기존 실행되던 pod에는 적용 안됨
PreferNoSchedule	toleration이 없으면 pod을 스케줄링안하려고 하지만 필수는 아님, 클러스터내에 자원이 부족하거나 하면 taint가 걸려있는 노드에서도 pod이 스케줄링될 수 있음
NoExecute	toleration이 없으면 pod이 스케줄되지 않으며 기존에 실행되던 pod도 toleration이 없으면 종료시킴.

사용 방법


taints and tolerations
POD
torleration:
position=low
POD
SCHEDULING
ALL
NODE
SCHEDULING
ONLY THIS
NODE
NODE
taint: position=low
NODE
taint: position=low
NODE
NODE