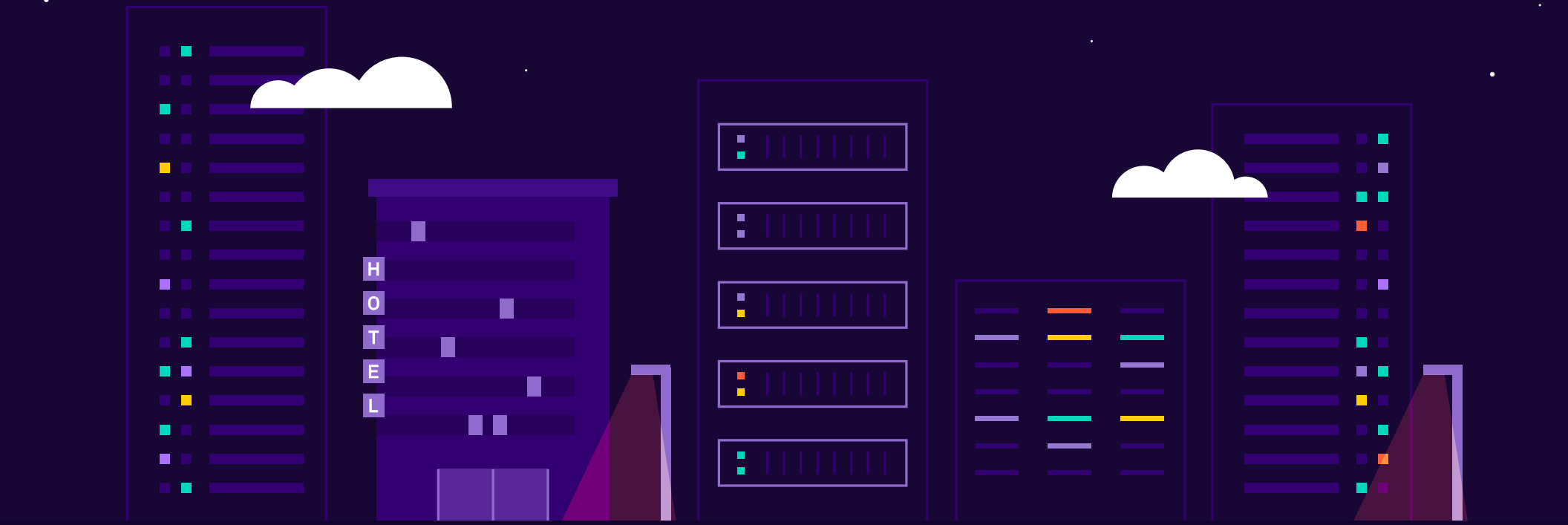
# Multi-Tenancy for Kubernetes: A Smarter Approach to Identity and Access Management

D2IQ



# Introduction

Identity and access management are critical components of many applications. However, enterprise companies that are using Kubernetes for various projects may find it challenging to identify the right level of access for different users, especially when there are multiple users and groups of users who are coming, going, and moving between teams.

## How do you ensure that applications and workloads have the proper level of isolation and resource availability?

## And how do you safely delegate management and operational responsibilities at various levels to those who require them?

In this ebook, we'll walk through the challenges of managing multi-tenancy for Kubernetes. We'll also share how D2iQ Kommander simplifies identity and access management for your multi-cluster operations.

CHAPTER 1

# The Challenges of Multi-tenancy for Kubernetes

Multi-tenancy for Kubernetes addresses the needs of governing access for multiple users or groups across Kubernetes clusters. Clusters can either be dedicated or shared depending on the needs of the users.

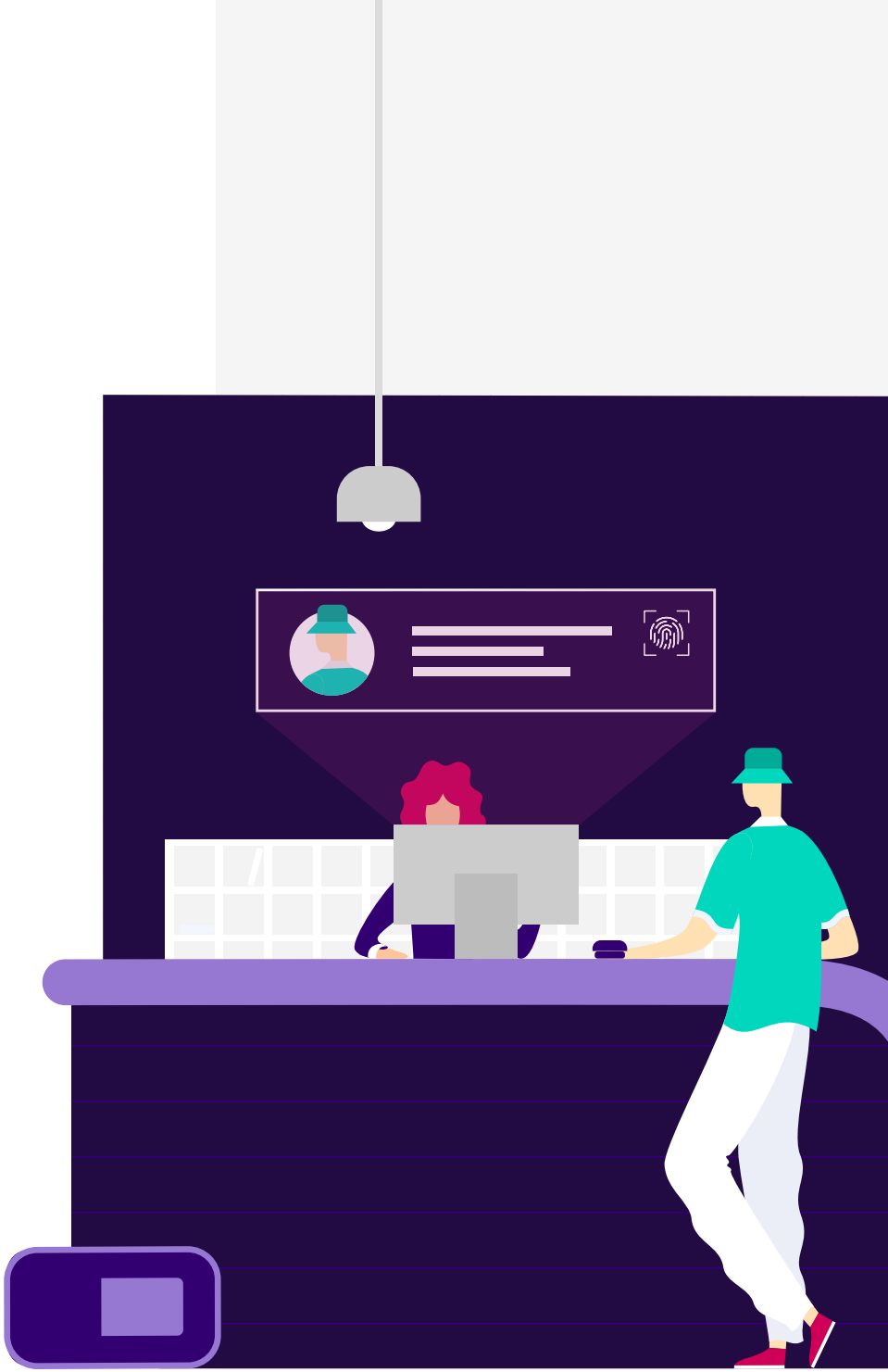
Kubernetes deployments would be much easier if they hosted just a single tenant—in other words, if only one cluster or workload was deployed in the entire environment.

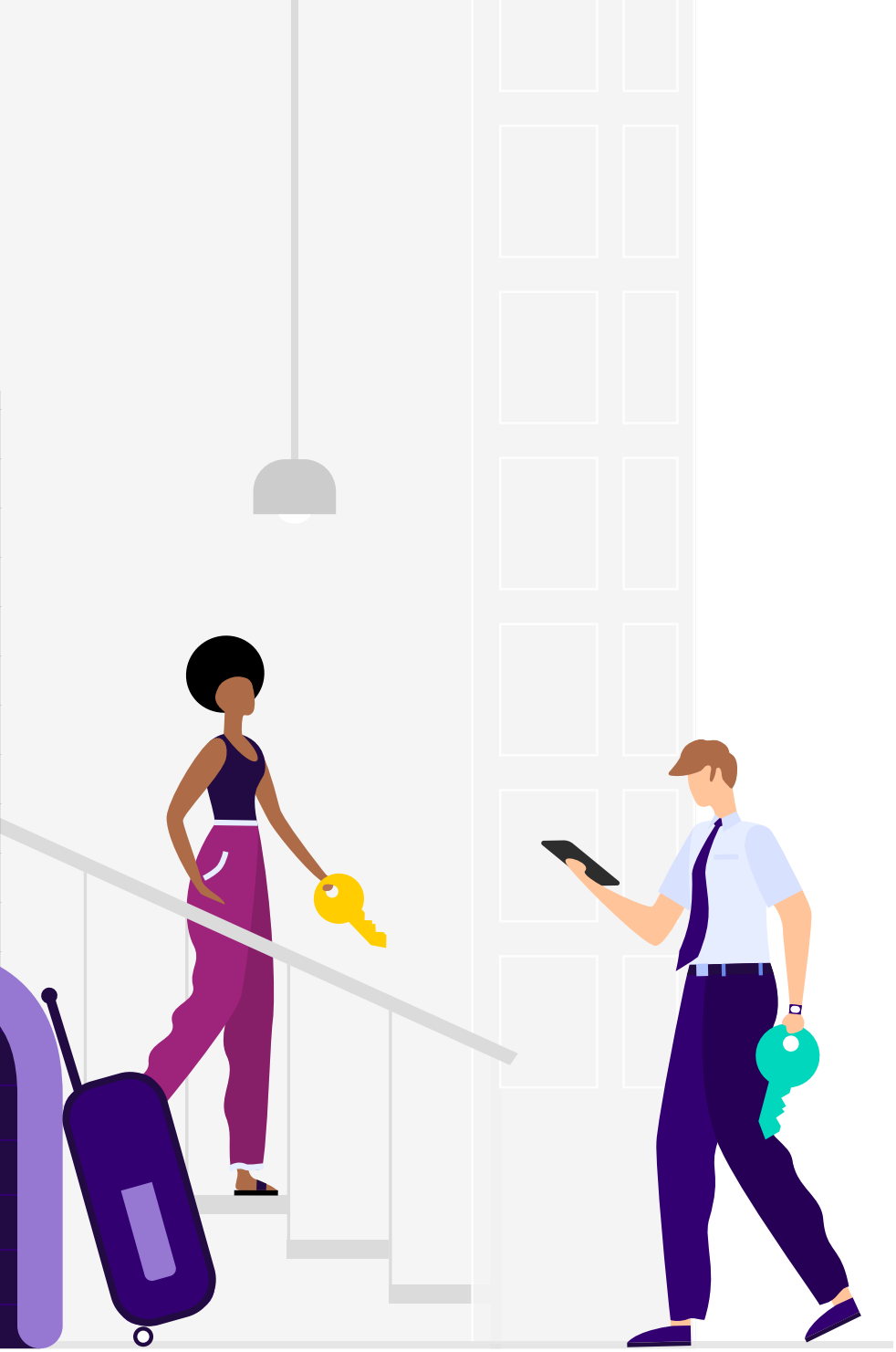
The reality is that for a majority of companies, it's common to have multi-tenant Kubernetes deployments where there is centralized management of either tenant-specific clusters or clusters that host multiple independent tenants.

You can think of multi-tenant Kubernetes in terms of a hotel. When it comes to authentication, a hotel needs to be able to identify guests before they are given access to their rooms. Similarly, Kubernetes administrators need to be able to identify users before they are given access to resources.

When it comes to authorization, not everyone needs the same level of access to resources as others. In a hotel, each room doesn't need to be accessed by everyone at the hotel. You don't want people walking into another guest's room, unless it's security or housekeeping. This level of control not only helps the hotel track who has access to the building, but also their activities during their stay.

**Likewise, each cluster or workload doesn't need to be accessed by everyone at the company, just by the people who need it to do their job. That way, admins can monitor both the resources that users access, as well as the activities users perform on those resources.**





This scenario is much easier to implement if you only have one user and one cluster or workload. But when you have multiple users and multiple clusters and workloads, that's where the challenge begins. As teams expand their usage of Kubernetes, clusters and workloads will exist in different environments.

One team may be creating their cluster on cloud provider "A," a different cluster on cloud provider "B," and a third cluster at the edge or in a data center, each with differing roles, configurations, and policies in their usage. This makes tracking all of the individual logins and permissions across the organization next to impossible, especially when there are multiple accounts and access levels to manage. And the problem only grows in complexity as more people on-board, off-board, or change teams, and projects multiply.

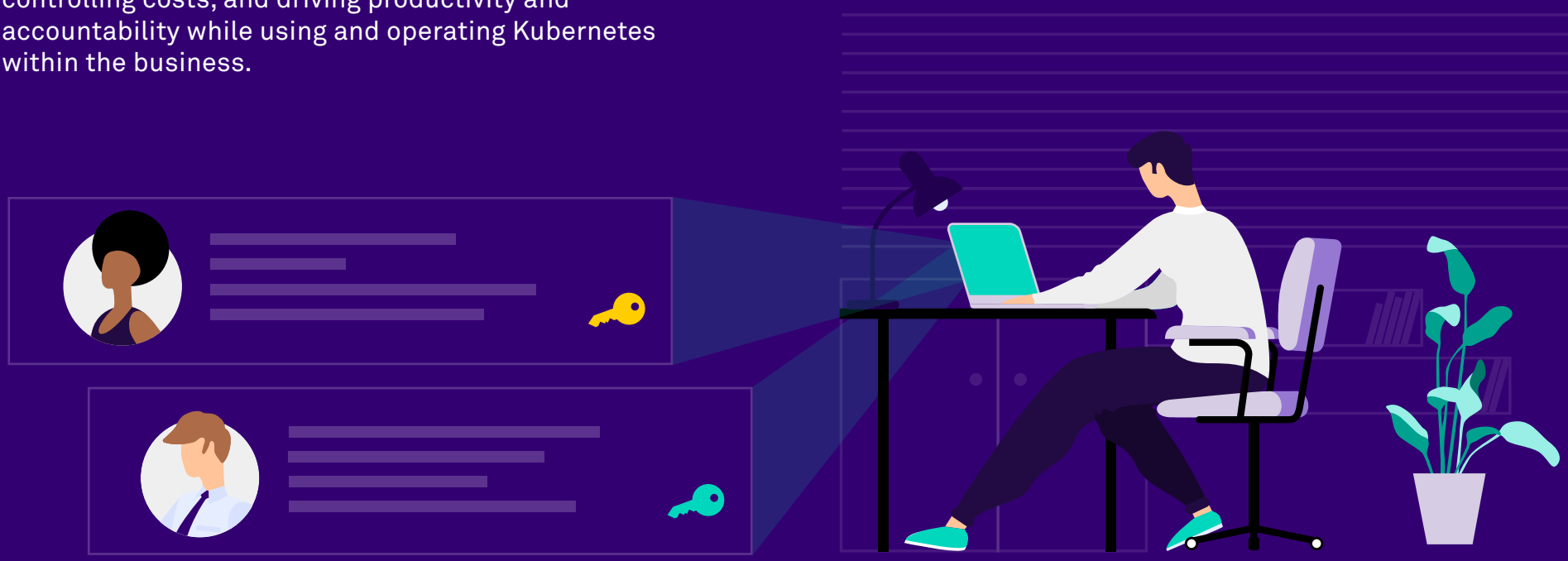
## Admins need to create a consistent environment where they can define and enforce policy across Kubernetes deployments and create standardization across identities and access to resources.

A lack of consistency will lead to more overhead for your operations team to manage. Operators won't be able to identify users that are allowed access to resources, or govern the use of resources. Even worse, they won't be able to track role violations, assess governance risk, and perform compliance checks. More time will be spent putting out fires and less time on efficient operations.

CHAPTER 2

# Why Kubernetes Governance is Essential for Enterprises

Kubernetes governance refers to a set of rules codified as policies aimed at minimizing risk, controlling costs, and driving productivity and accountability while using and operating Kubernetes within the business.

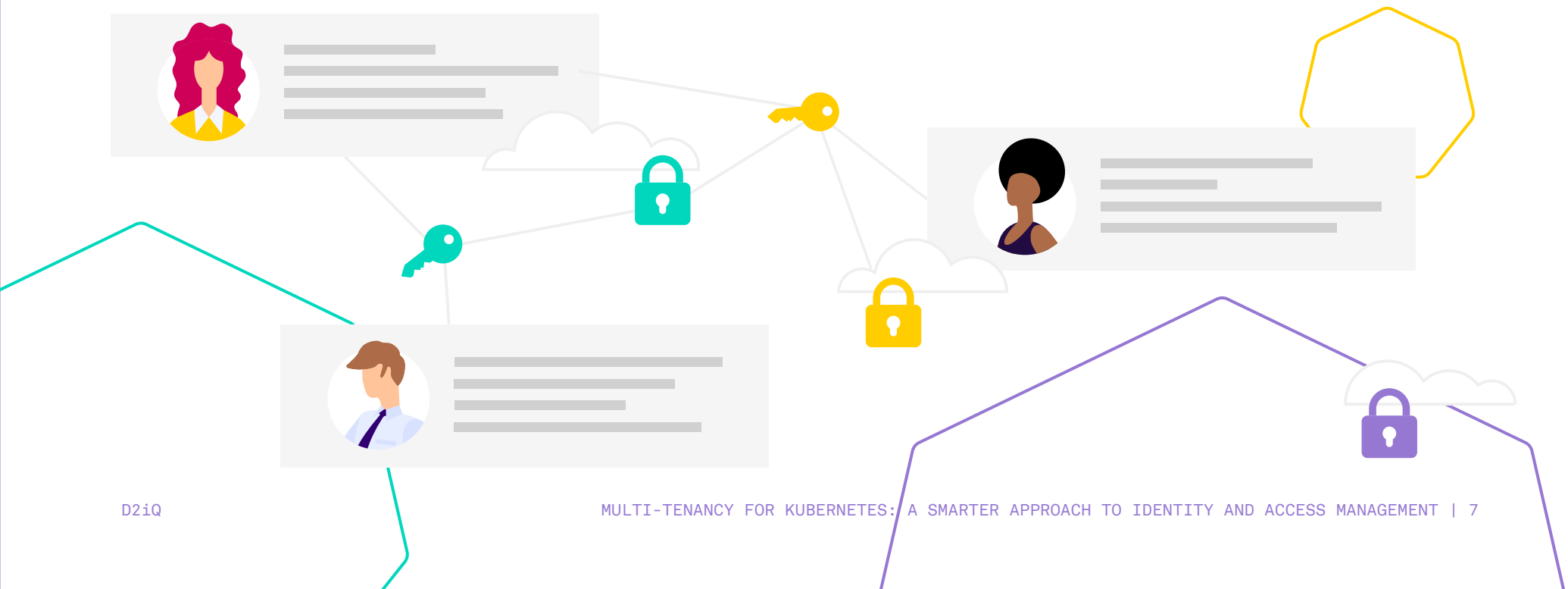


Whether you're a seasoned vet or just getting started with Kubernetes, you need a solid plan in place to drive policy and create consistency across identities and levels of access to resources. Governance is not to be taken lightly or something you can bypass before you start using Kubernetes. Unless you want to deal with the headache of managing a chaotic IT environment, starting with proper governance is a must.

As you begin defining policies for Kubernetes, it's important to note that there is no "one size fits all" type of governance framework. Different organizations, as well as different teams within the same organization, can have differing governance and access control requirements depending on the type of industry or organizational structure they are in. In addition, access requirements for different roles will evolve as employees change job roles or responsibilities, or leave the company.

That said, you'll want to define and implement policy at the top level, as well as create lines of separation across clusters. This not only allows for a consistent governance framework across the enterprise, but empowers division of labor across a wide variety of roles and projects.

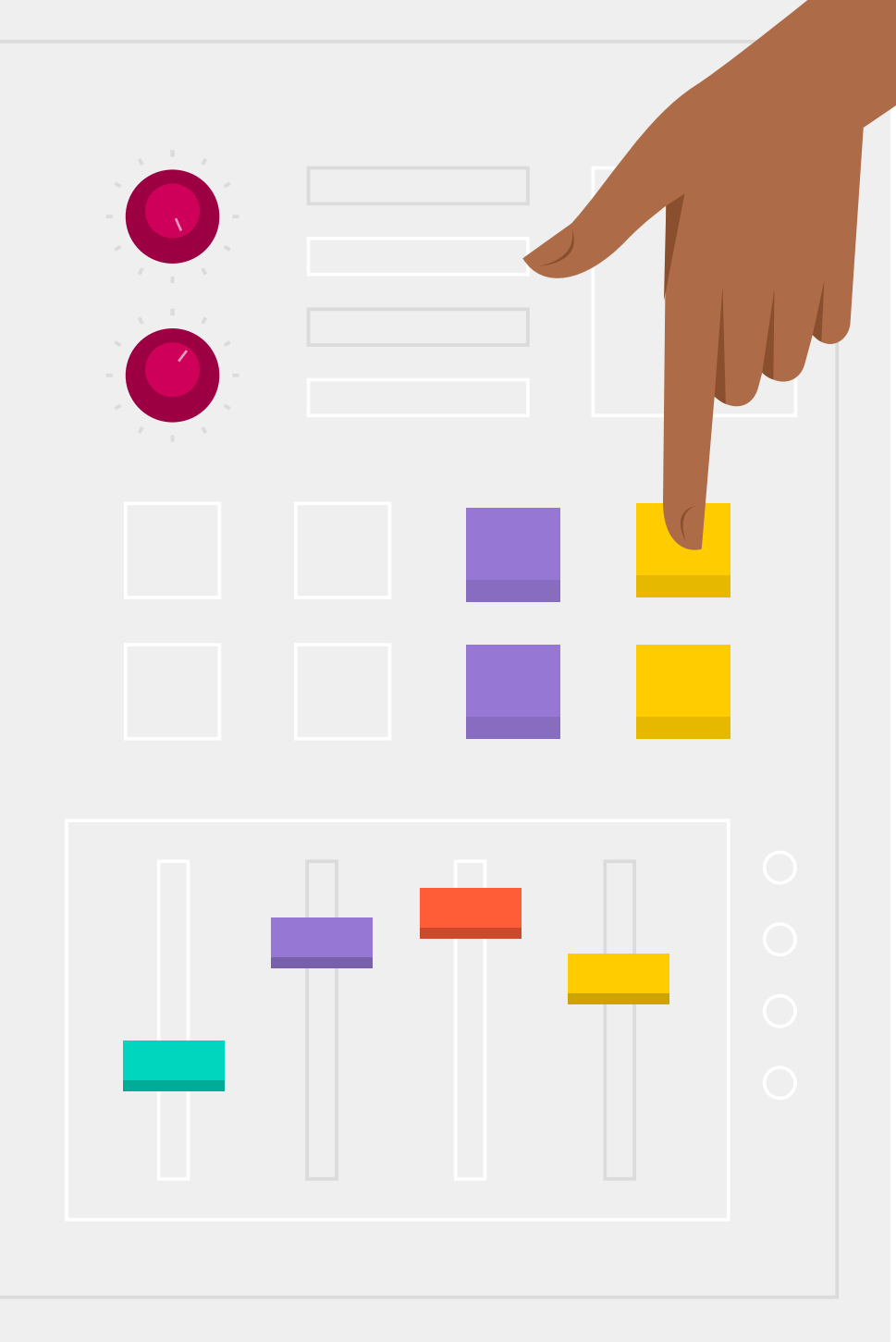
Putting all of this together may sound like a daunting task, but it doesn't have to be. With the right solution and a tested framework, you can effectively govern identities and resource utilization.



CHAPTER 3

# Take Control of Identity and Access Management with D2iQ Kommander

Developed to address the exploding demand of Kubernetes, D2iQ Kommander delivers federated management, governance, and visibility across your multi-tenant Kubernetes deployments.



Developed to address the exploding demand of Kubernetes, D2iQ Kommander delivers federated management, governance, and visibility across your multi-tenant Kubernetes deployments.

**D2iQ Kommander provides single sign-on and Role-Based Access Control (RBAC) to simplify the process of identity and access management.**

**D2iQ Kommander provides operators with a centralized dashboard to define tenant roles and responsibilities, as well as the activities that can be performed on those resources.**

This ensures a significantly simpler experience when it comes to creating consistency across clusters in the environment. On top of that, role-based responsibilities ensure the right people are performing the right activities within the environment.

Single sign-on provides your organization with secure access and authentication across different services. This capability not only makes it easier for developers to access the resources they need, but for operators to authenticate and manage access, as well as monitor cluster activities with consistent identities. And because D2iQ Kommander ensures that access is limited to authenticated users, it prevents you from running into potential security threats and data leaks down the road.

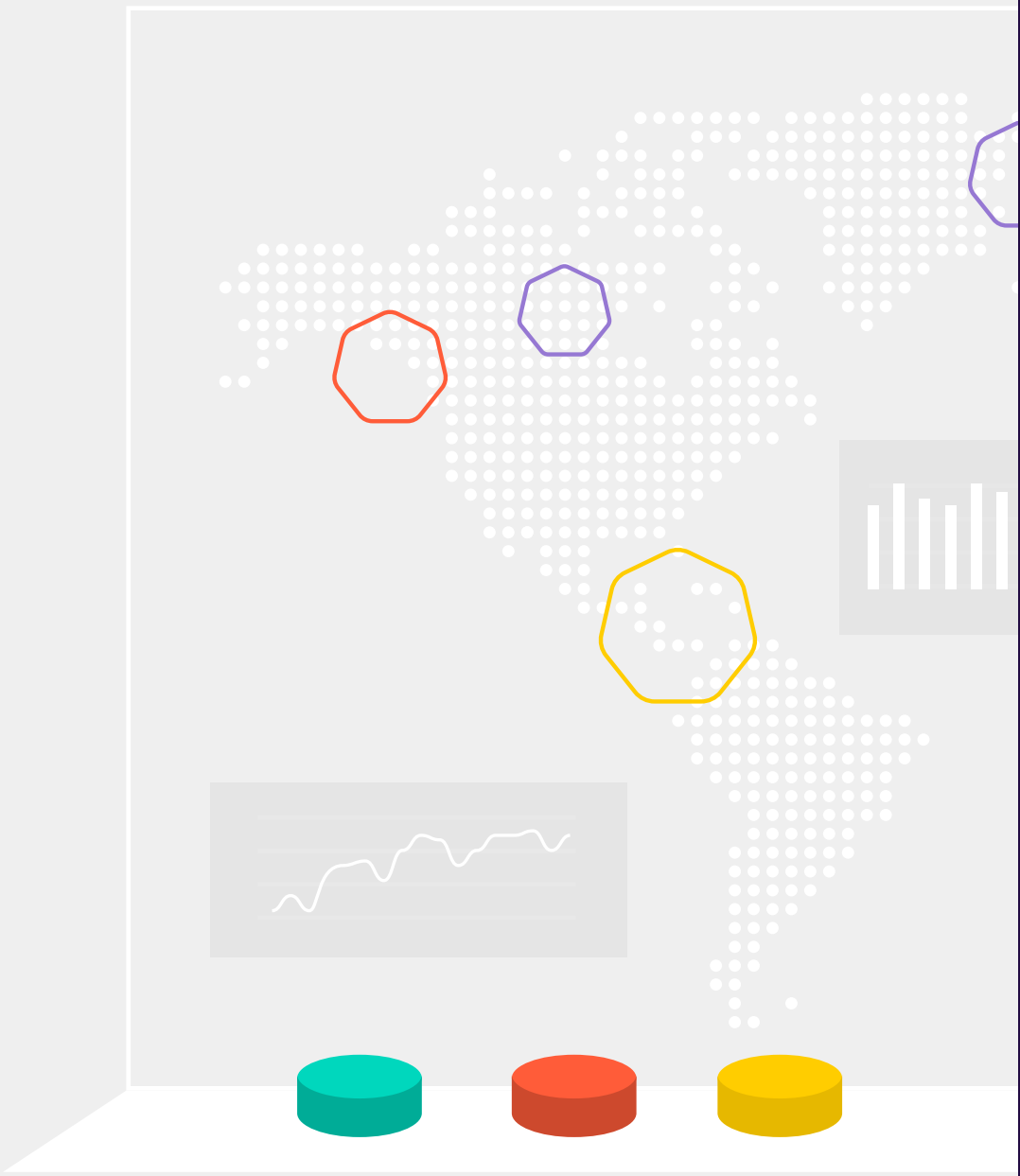
# Conclusion

As your organization adopts new clusters and workloads, you'll need a thoughtful governance framework to help you gain visibility and control over your multi-tenant Kubernetes deployments.

With D2iQ Kommander, your organization can create operational consistency across clusters, making it easier to delegate management and responsibilities at various levels to those that require them.

**To learn more about D2iQ Kommander, click here to contact us.**

Contact us



D2iQ, formerly Mesosphere, is the leading provider of enterprise-grade cloud platforms that enable organizations to embrace open source and cloud native innovations while delivering smarter Day 2 operations. With unmatched experience driving some of the world's largest cloud deployments, D2iQ empowers organizations to better navigate and accelerate cloud native journeys with enterprise-grade technologies, training, professional services and support. Whether you are deploying your first Kubernetes workload, optimizing your business analytics with Spark or Jupyter, or looking to educate your developers on the benefits of cloud native, D2iQ has the expertise, services, and technology to enable you on the journey.

**d2iq.com**