

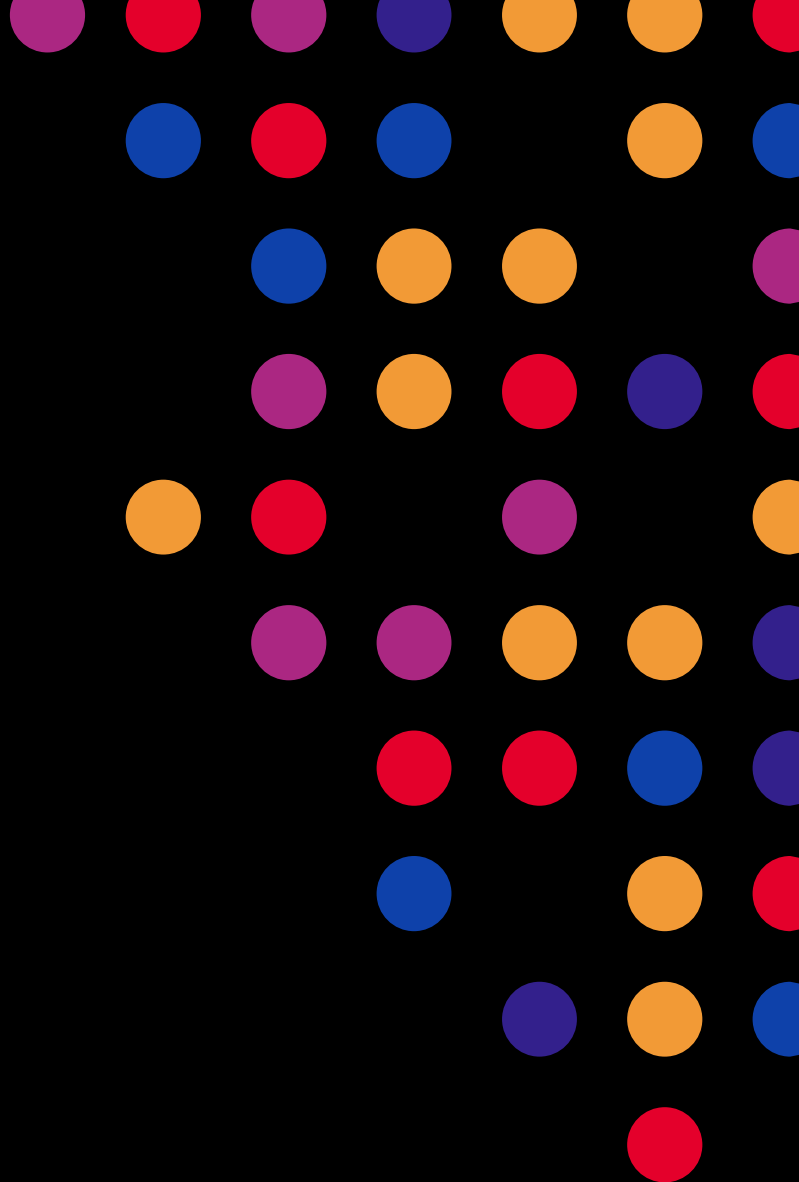


NGINX+ Ingress Controller & F5 Container Ingress Services

Christopher Sheehan | Solution Engineer

Daniel Cayer | Solution Engineer

March 20, 2024



Agenda

K8s and Networking Discussion

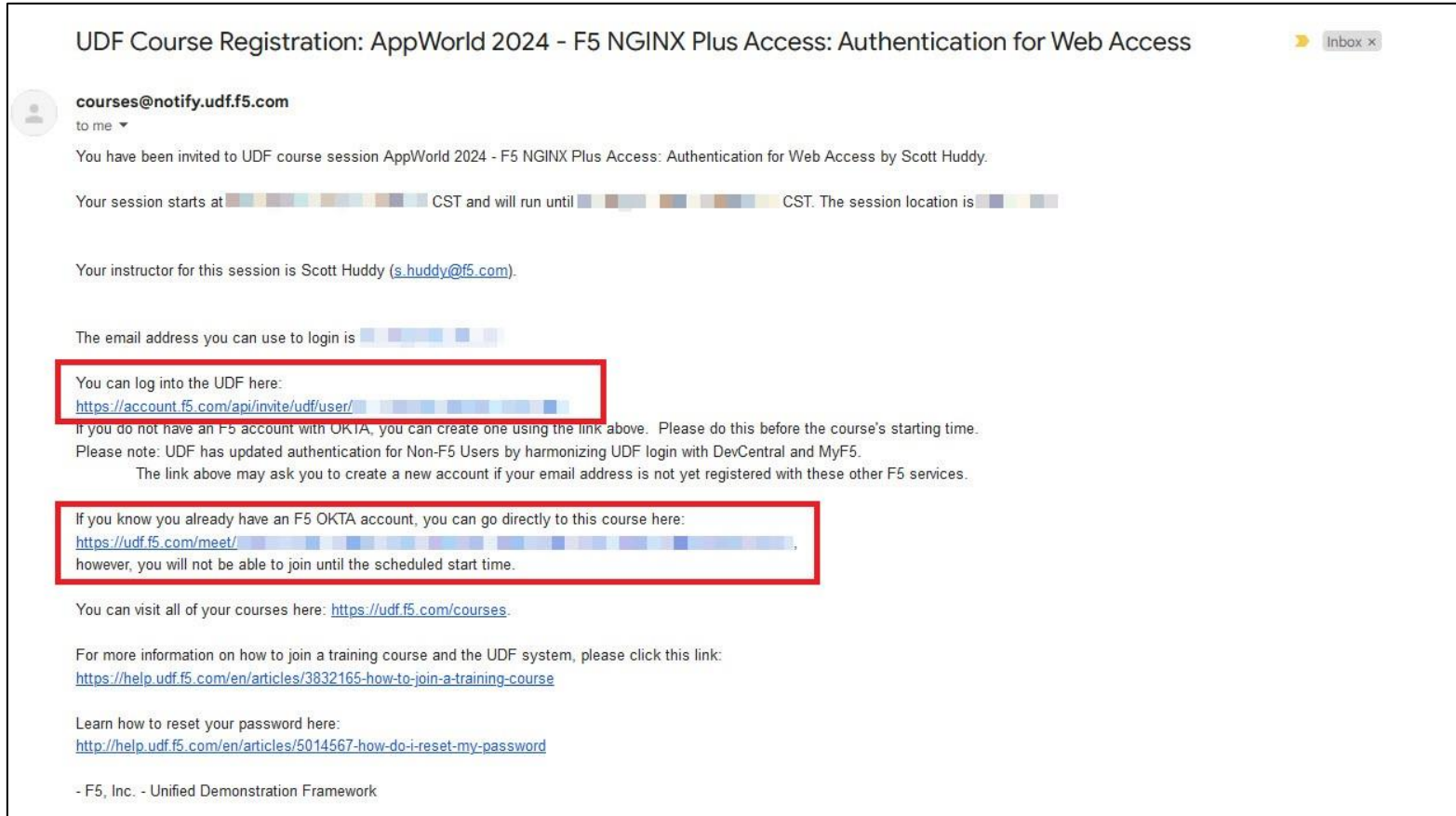
Ingress Controllers

Container Ingress Services

F5 IngressLink

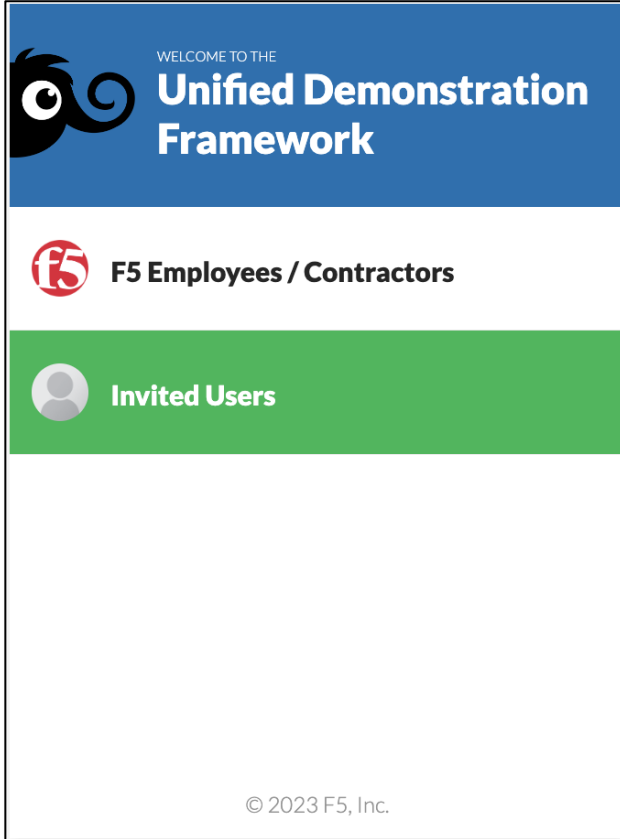
Lab fun

Lab Attendee Experience



- Lab Attendees will receive an invite email from: courses@notify.udf.f5.com
- Lab Attendees can click the provided link

Lab Attendee Experience



Sign in with your email and password

Email

Password

[Forgot your password?](#)


Sign in

- Lab Attendees will select *Invited Users*
- Lab Attendees can enter username and password if a returning user, or username and “Forgot your password”


Lab Attendee Experience

SET UP 2-STEP AUTHENTICATION


F5 requires you to set up 2-step authentication to add an additional layer of security when signing in to your account

 Google Authenticator
Enter single-use code from the mobile app.

Setup

 SMS Authentication
Enter a single-use code sent to your mobile phone.

Setup

 Email Authentication
Enter a verification code sent to your email.

Setup


SET UP 2-STEP AUTHENTICATION

You can configure any additional optional factor or click finish


Enrolled factors

 Email Authentication 

Additional optional factors

 Google Authenticator
Enter single-use code from the mobile app.

Setup

 SMS Authentication
Enter a single-use code sent to your mobile phone.

Setup

Finish

Welcome

Privacy Policy

+

Terms and Conditions

+

Cookie Policy

+

☒ AGREE & CONTINUE

- MFA setup for invited guests
- Users will be given MFA options for Google Authenticator, SMS and Email authentications
- Agree to the UDF use policy

Lab Attendee Experience

F5's UDF: Password Reset

noreply@registration.udf.f5.com

To i@chas.one

Reply

Reply all

Forward

Delete

Add to Safe Senders

Add to Blocked Senders

Here is your temporary reset password code for F5's Unified Demonstration Framework **535580**. If you did not request a password reset, please contact your instructor.

We have sent a password reset code by email to I***@c***. Enter it below to reset your password.

Code

.....

New Password

.....

Enter New Password Again

.....

✓ Password must contain a lower case letter

✓ Password must contain an upper case letter

✓ Password must contain a number

✓ Password must contain at least 8 characters

Change Password

- Screenshots show the forgot password experience

Lab Attendee Experience

 COURSE SESSIONS





Happening now					
Date & Time	Course	Region	Location	Instructors	
Tue 09 Jan 8:00 AM - 8:00 PM CST Duration: 12 hours	AppWorld 2024 - F5 NGINX Plus Access: Authentication for Web Access	Oregon, USA	Austin, TX	 Scott Huddy	UNREGISTER → LAUNCH


LOBBY

AppWorld 2024 - F5 NGINX Plus Access:
Authentication for Web Access

TUE 9 JAN 08:00 AM TO TUE 9 JAN 08:00 PM CST

 Ends in 10 hours

 Austin, TX

 Oregon, USA

Join

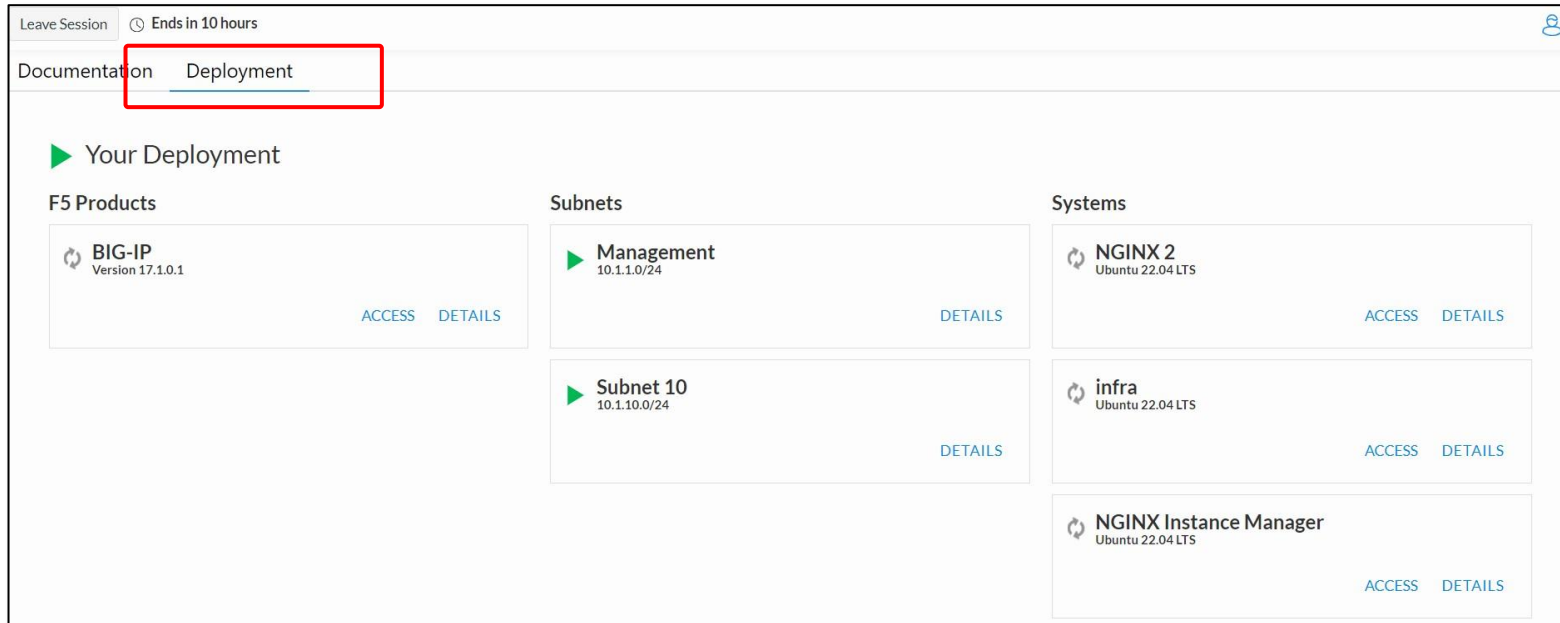
Course Overview

Course Documentation

Instructors

- Upon, successful access, click *Launch* and then *Join*

Lab Attendee Experience



- This screenshot shows the Lab environment and resources
- Note: experiences may differ

Show of hands

- First lab today? First lab ever?
- How many are familiar with Kubernetes (K8s)?
- How many are familiar with F5 CIS/NGINX Ingress Controller? AS3?
- Anyone not familiar with Big-IP in general?

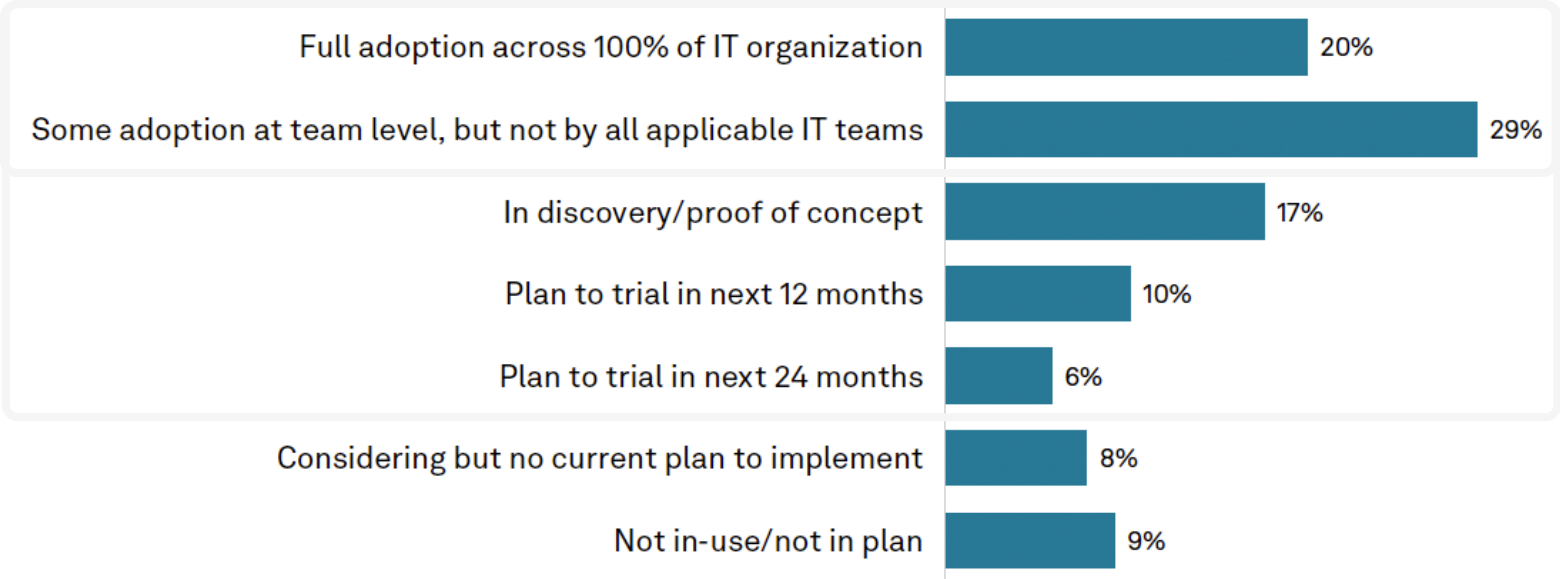


Why Talk about K8S & CIS/NGINX Ingress Controller?

Containers/Kubernetes Adoption Trends

Enterprise Adoption of Kubernetes

- By 2026:
 - 20% of all apps will be running in containers (up from less than 10% in 2020).
 - 90%+ of global organizations will be running containerized applications in production (up from fewer than 40% in 2021).
 - 80%+ of ISVs will offer their application software in container format (up from 10% in 2020).



Q. What is your organization's adoption status for Kubernetes?
Base: All respondents (n=463)
Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2022

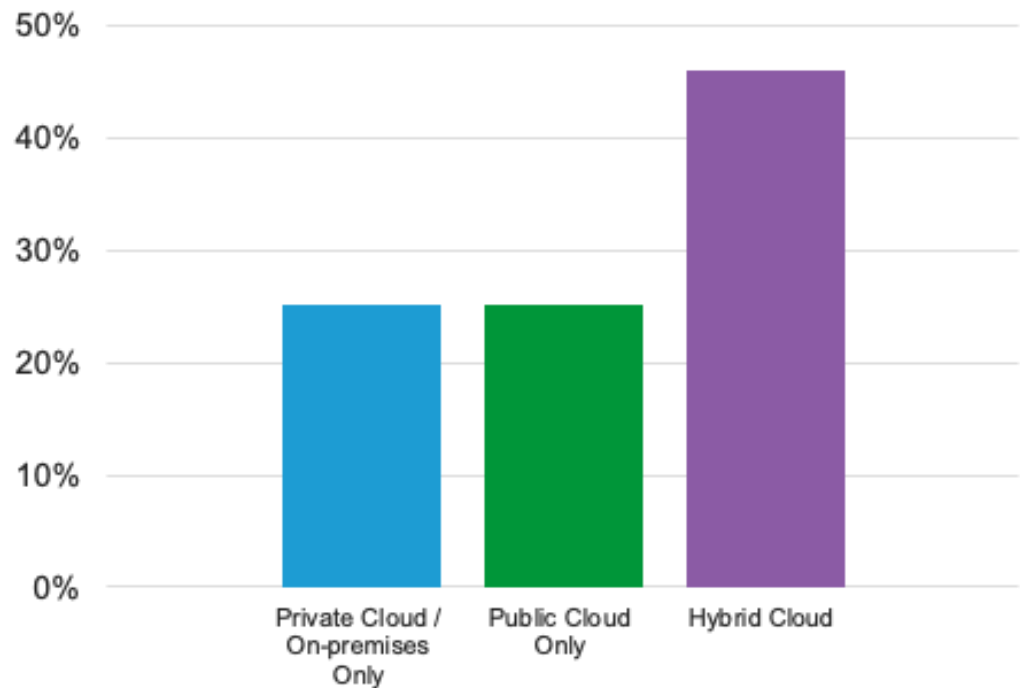
Source: Gartner 2022



Containers/Kubernetes Deployment Environments

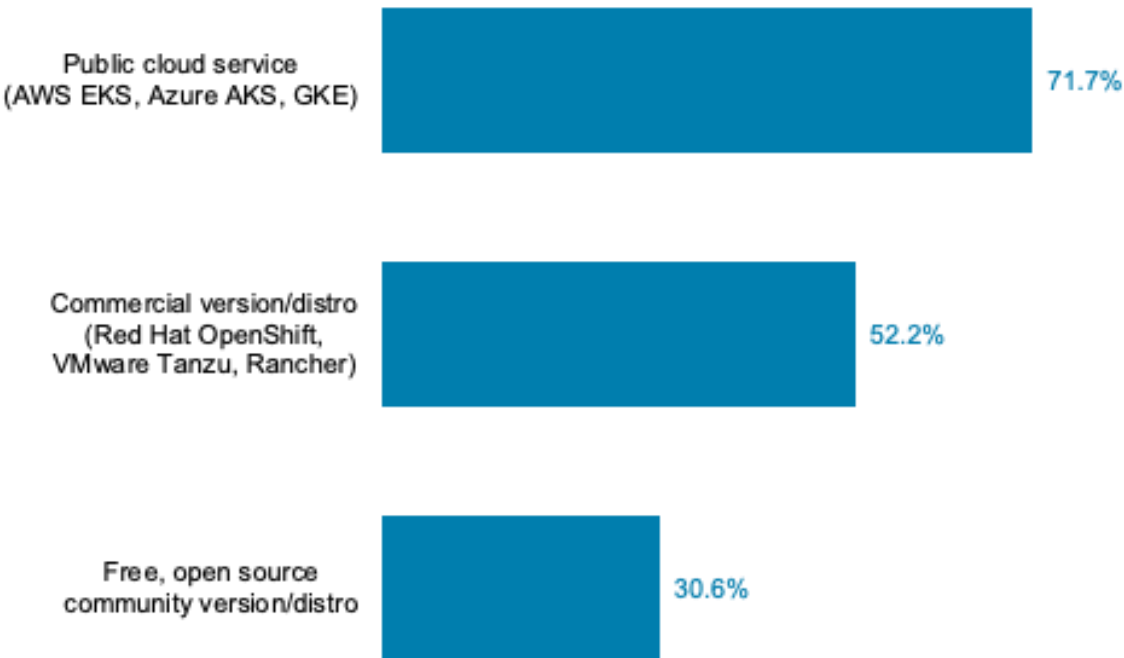
Cloud-native technologies for application development

Where do customers run containers?



Source: CNCF 2021

Which K8s offerings do customers use?



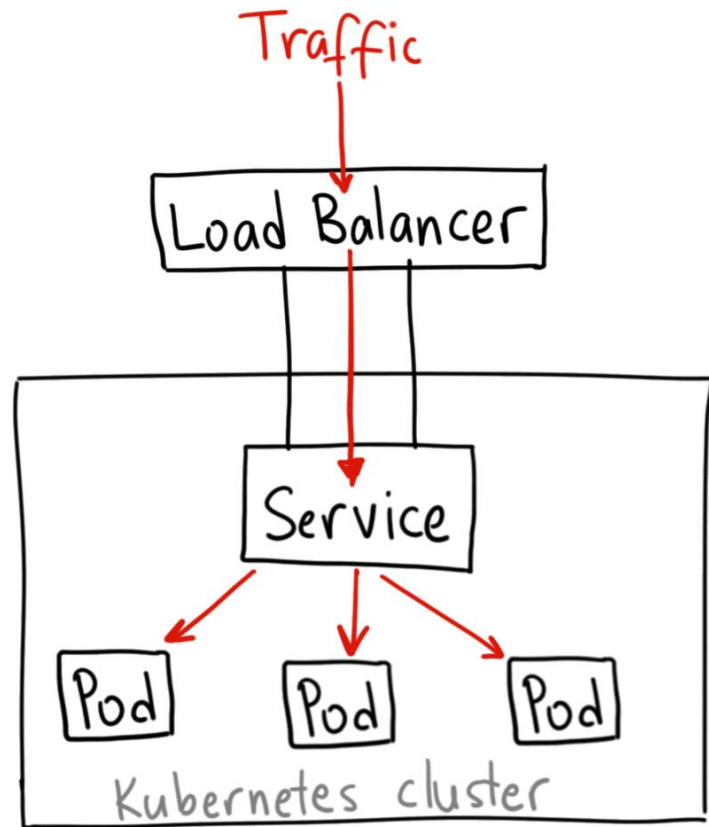
Source: 451 Research





K8s Overview

Applications in Kubernetes



- **Pods**

- Containers run workloads on nodes in a Kubernetes cluster

- **Services**

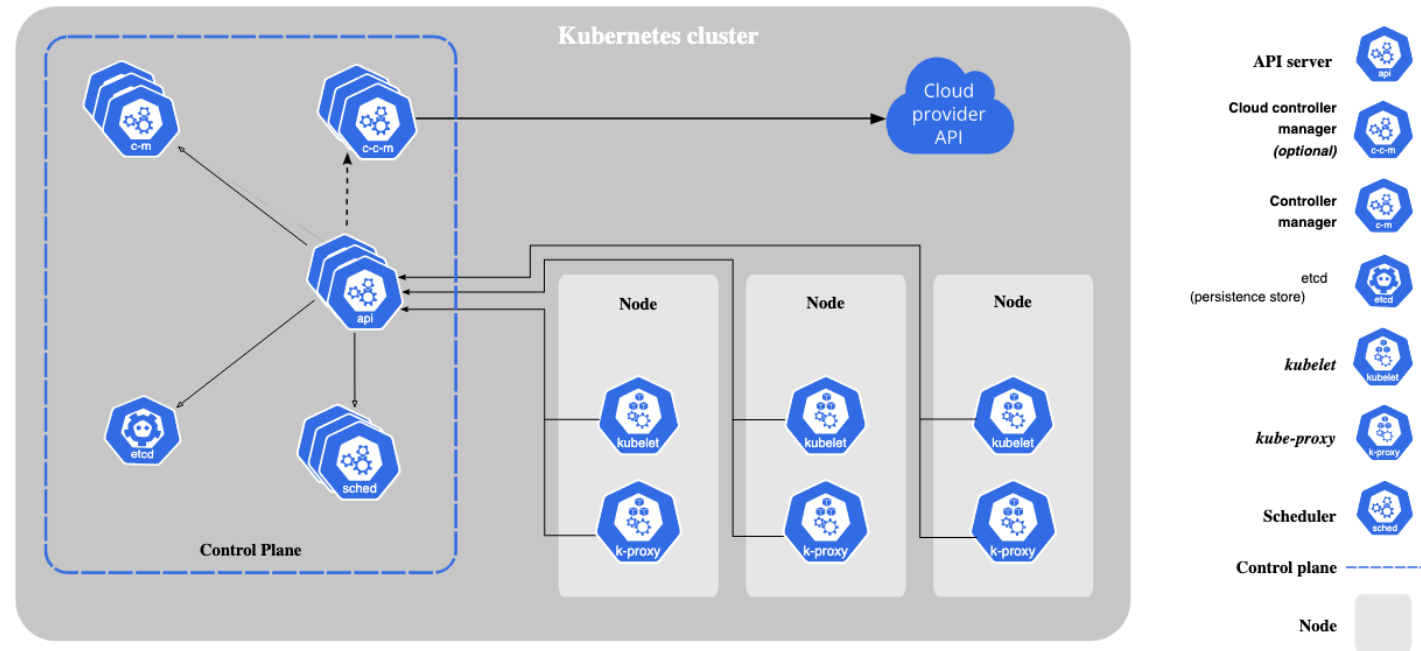
- A logical grouping of pods that perform the same function

- **Ingress**

- How to access a set of Pods via a L7 load balancer (Hostname, URI)

Kubernetes Cluster

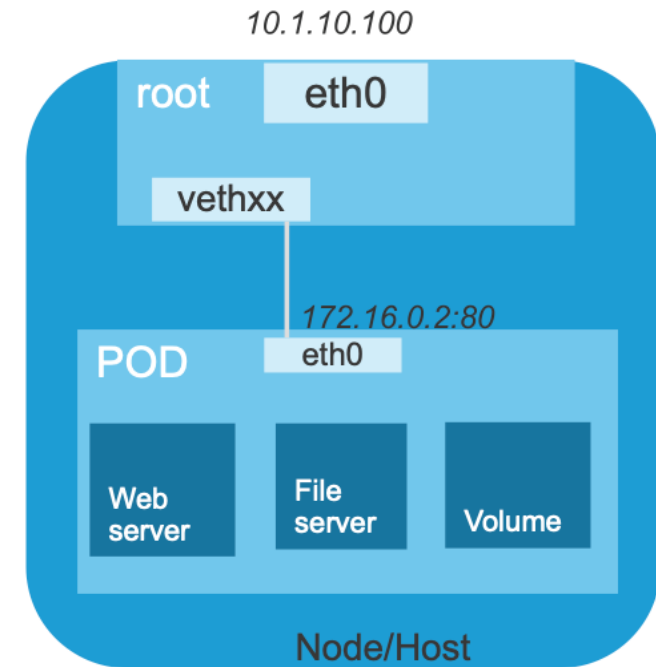
- A **Kubernetes cluster** is a set of nodes that run containerized applications in an efficient, automated and scalable manner.
- Kubernetes clusters allow containers to run across multiple machines and environments: virtual, physical, cloud-based, and on-premises.
- Clusters are comprised of one controller node and a number of worker nodes
- POD replicas spread across nodes in a cluster
- **Control Plane Node(s) must communicate with each worker Node which necessitates tunneling**
- The API server is a component of the Kubernetes [control plane](#) that exposes the Kubernetes API. The API server is the front end for the Kubernetes control plane.



What is a K8s POD?



- Small group of related Containers on same host machine and share the same life cycle
- Ephemeral and Replaceable
- Pods gets a new unique new IP at every launch from the Pod subnet
- Containers reach each other using Pod IP (localhost) on specific ports
- A ReplicaSet ensure that a specified number of Replicas are running at one time.
- Pods have the following auto assigned DNS resolution:
 - pod-ip-address.my-namespace.pod.cluster-domain.example
 - 172-16-0-2.default.pod.cluster123.company.com



Types of Services

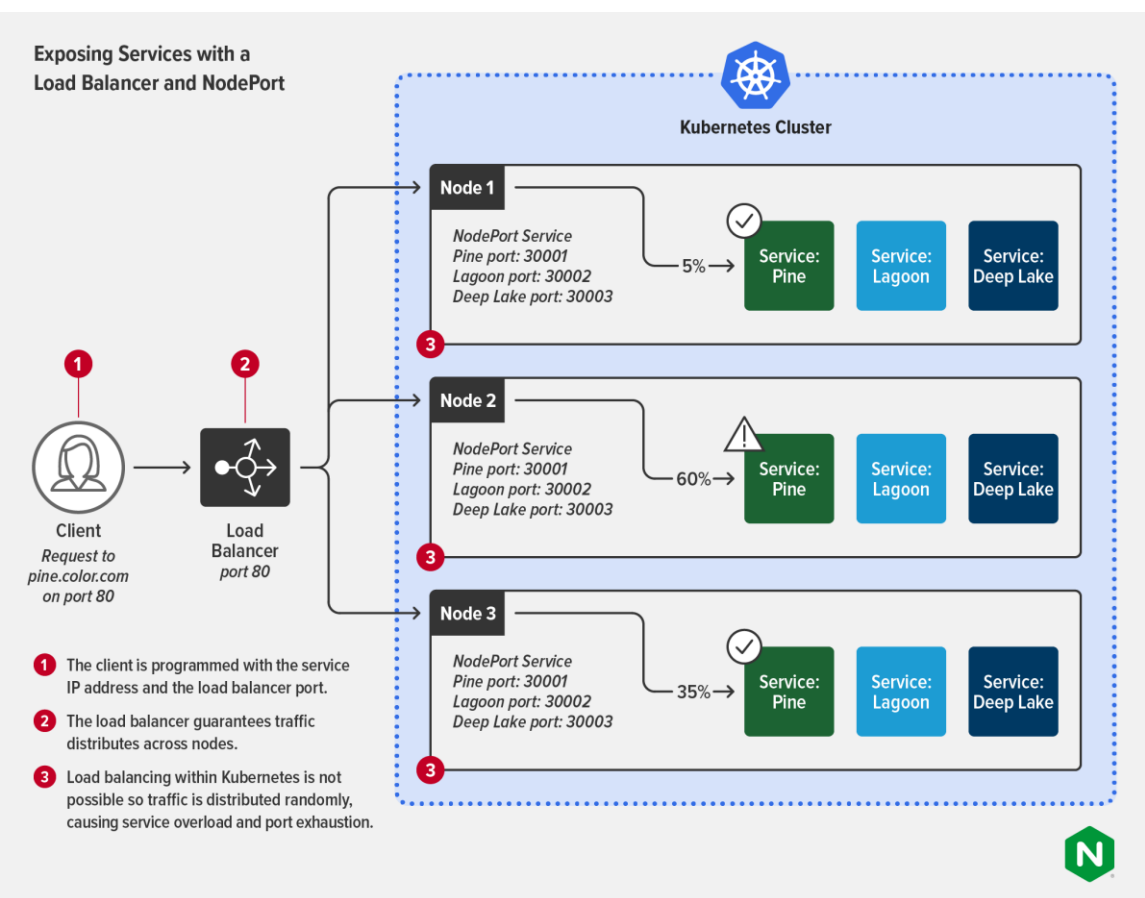


- **NodePort:** Accessible via port mapping of IP:Port to Pod (similar to vanilla Docker). Allows connection from outside cluster.
- **ClusterIP** (default): Only accessible internally
- **LoadBalancer:** Utilize external load balancer (i.e. AWS NLB, Azure LB, GCP LB) , sets up NodePort service inside cluster and Cloud-LB outside.
- **Service without Selectors:** Allows for creating manual endpoints that can be other Services. Service Chaining.
- **External:** uses an FQDN instead of a pool of endpoints.
- **Headless:** No Cluster IP, No LB internally. Each endpoint gets a DNS name. LB via external DNS.

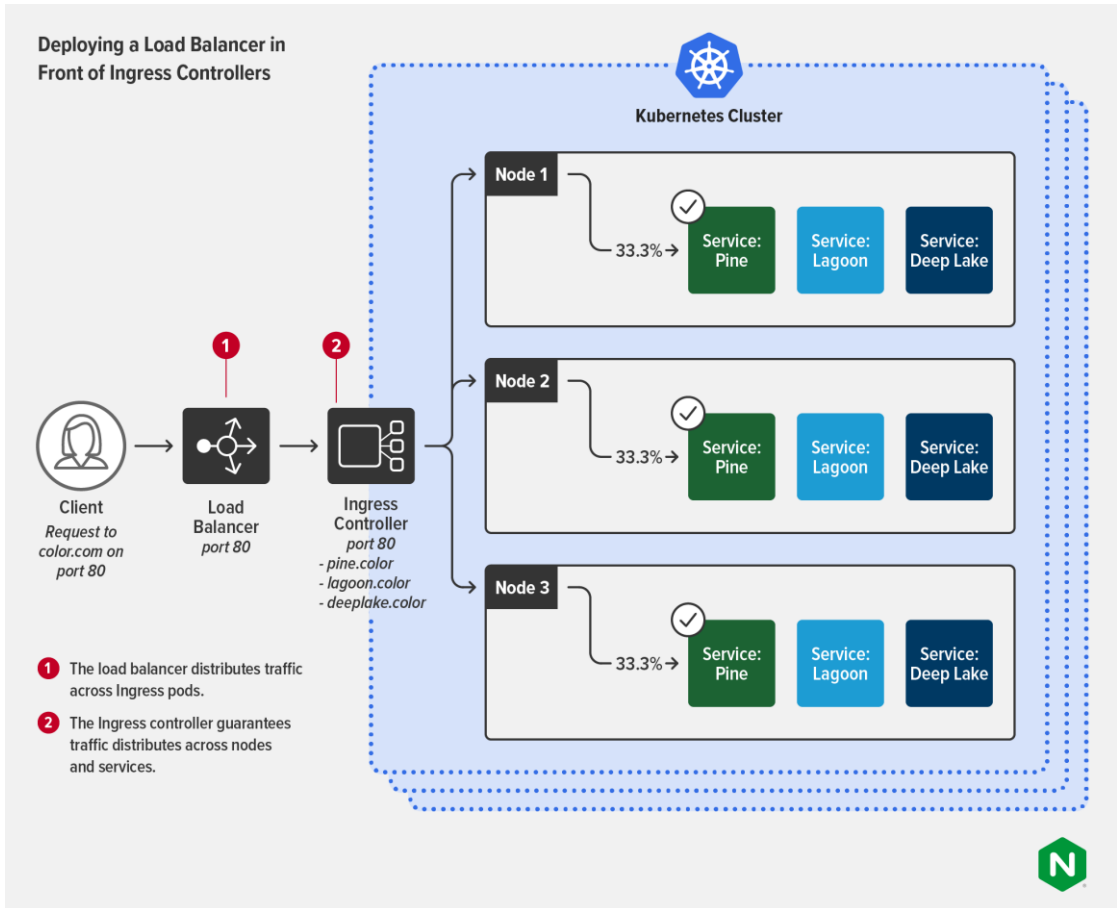
```
apiVersion: v1
kind: Service
metadata:
  name: my-frontend
  labels:
    run: my-frontend
spec:
  ports:
    - port: 80
      protocol: TCP
      targetPort: 80
    type: NodePort
  selector:
    run: my-frontend
```

Exposing Apps in Kubernetes

Small, static deployments

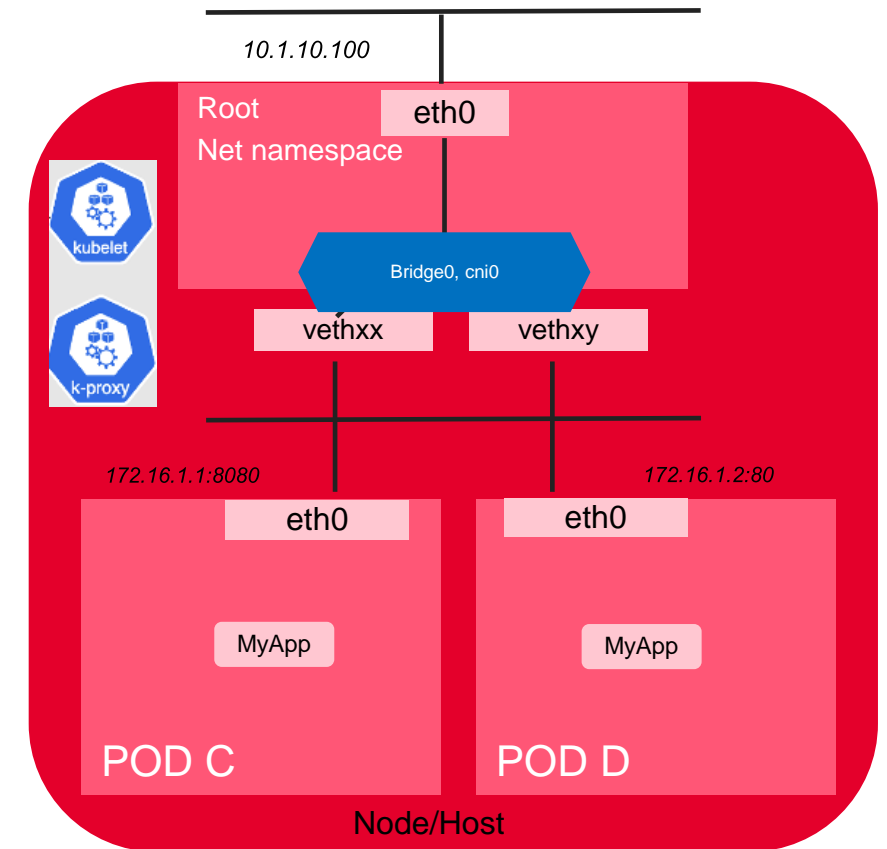


Scalable, dynamic deployments



K8s Network subnets

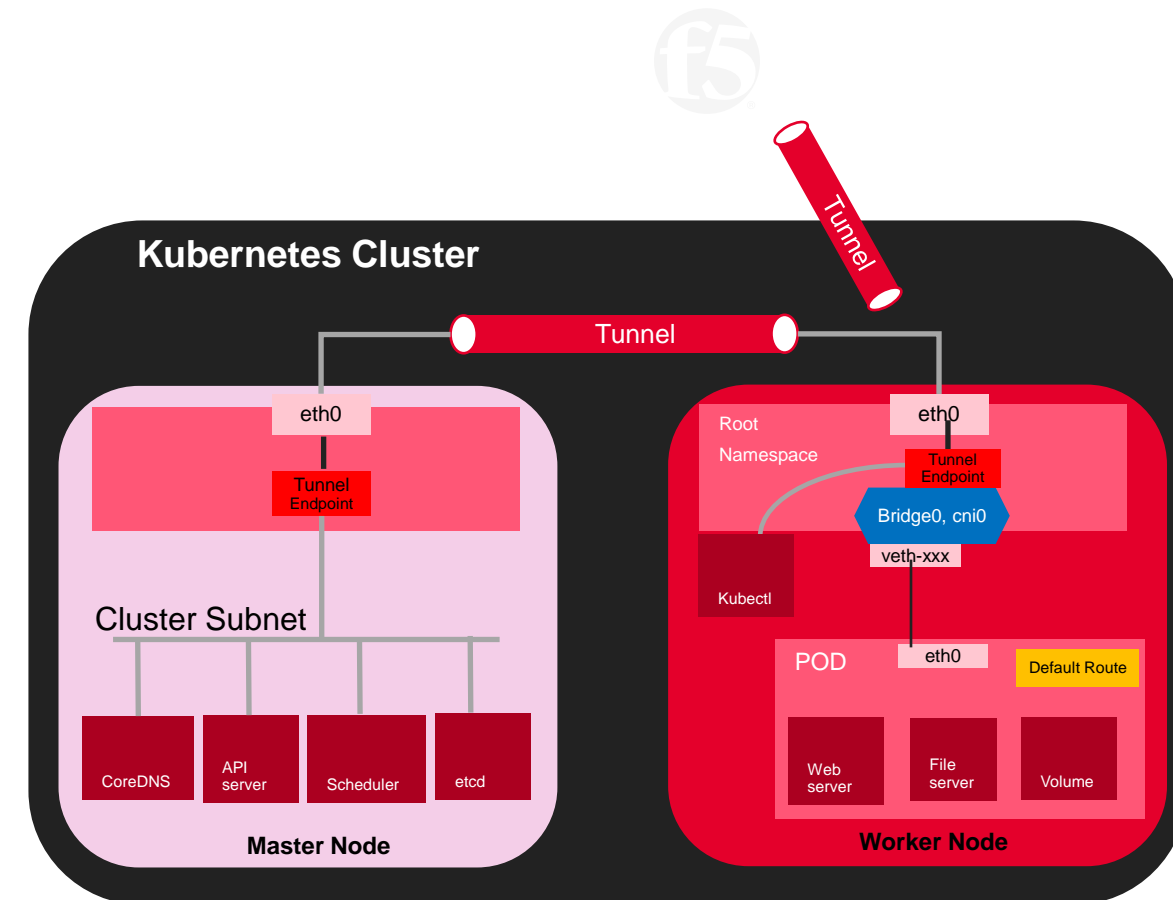
- **Node Network** (external subnet)
- **Pod Network** (specified as Pod CIDR block)
 - Local to a Node.
- **Cluster Network** for API server, K8s controllers and other services.
 - Stretches across nodes of a Cluster.
 - Also used for Cluster-IP type services
- Default K8s CNI or third-party plugins are responsible for interconnecting cluster network.



What are Tunnels



- *IP-in-IP Encapsulates [layer 3 IP Packets](#) within [layer 3](#) IP packets.*
- *“Virtual Extensible LAN (VXLAN) Encapsulate [layer 2 Ethernet frames](#) within [layer 4 UDP](#) datagrams, using 4789. VXLAN endpoints are known as VXLAN tunnel endpoints (VTEPs).”*
- *GENEVE, similar to VXLAN , created by VMWARE for use with NSX-T*
- *Used for:*
 1. *Bridging the Cluster Subnet*
 2. *Connecting outside devices to POD subnet*
 3. *Other Intra-Cluster communication*

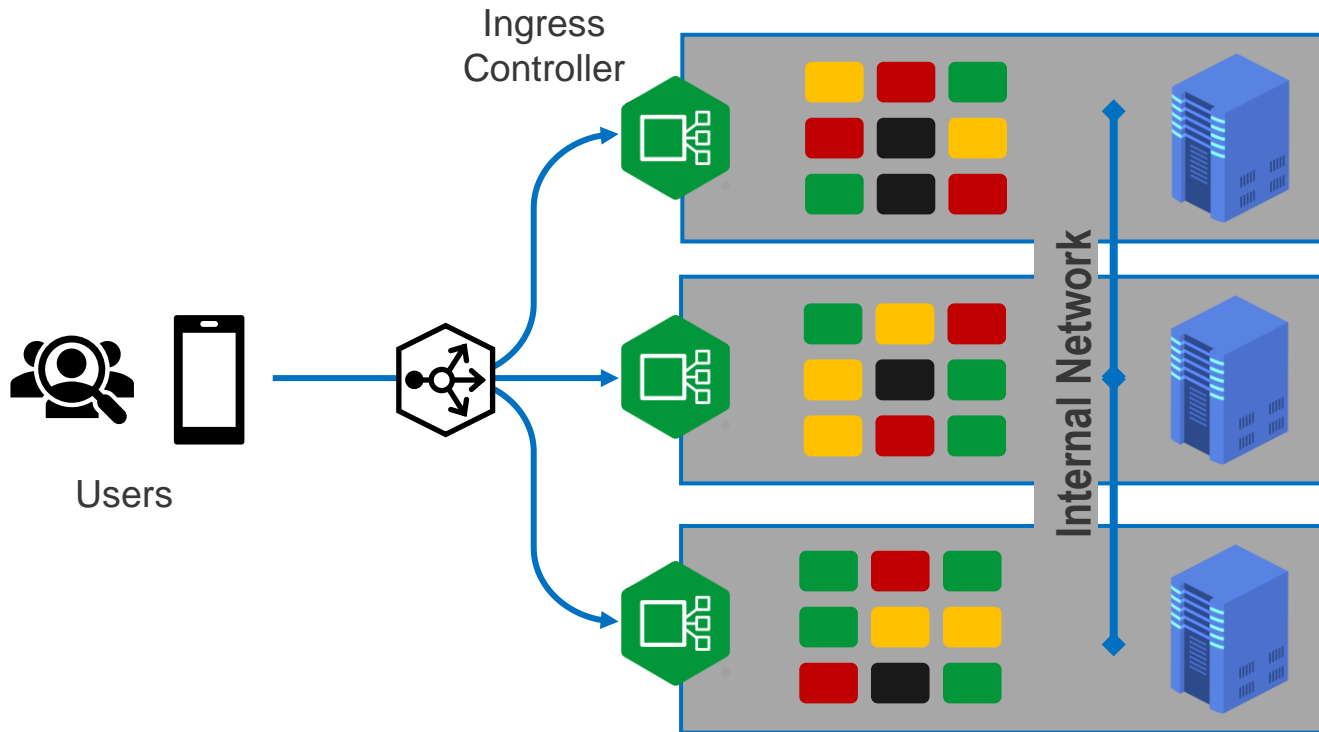




Ingress Controllers

The K8S Ingress Controller

A specialized load balancer for Kubernetes environments:



- Accepts traffic from outside the Kubernetes platform, and load-balances it to pods (containers) running inside the platform
- Configured using the Kubernetes API, with objects called 'Ingress Resources'
- Monitors the pods running in Kubernetes, and automatically updates the load balancing rules if, for example, pods are added or removed from a service



Container Ingress Services

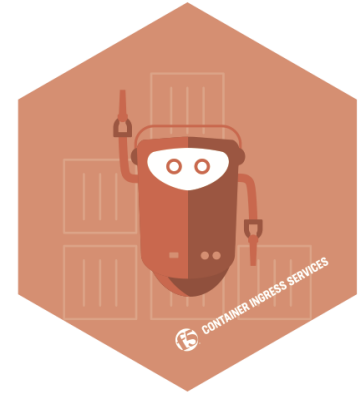
F5 Container Ingress Services



- Automate provisioning of ingress (L4) services
- Automate Ingress (L7) services
- BIG-IP Configurations are deployed FROM Kubernetes
- Application Deployments use meta-data (Configmap/Ingress) to reference BIG-IP configuration
- Container Ingress Services translates meta-data to BIG-IP configuration

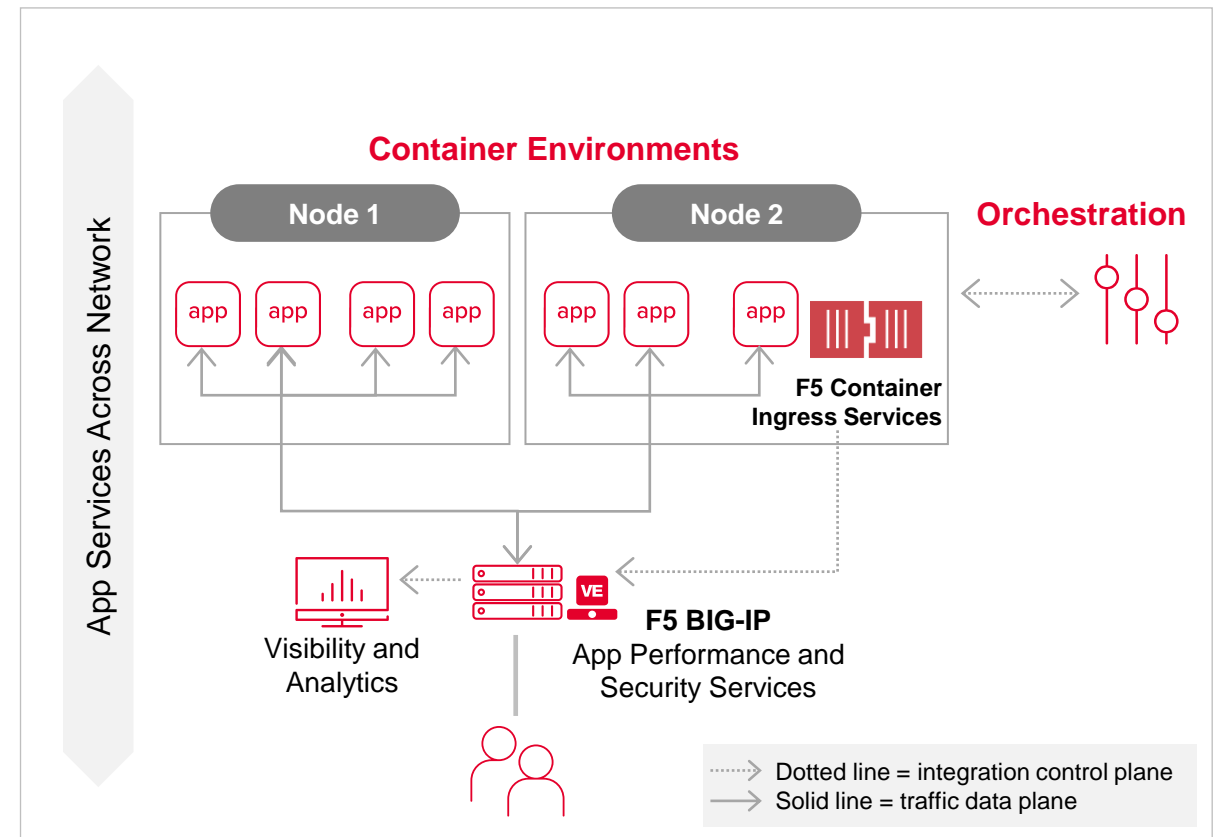
```
apiVersion: v1
kind: Service
metadata:
  name: my-frontend
  labels:
    run: mv-frontend
    cis.f5.com/as3-tenant: AS3
    cis.f5.com/as3-app: MyApp
    cis.f5.com/as3-pool: frontend_pool
spec:
  ports:
    - name: my-frontend
      port: 80
      protocol: TCP
      targetPort: 80
  type: LoadBalancer
  selector:
    run: my-frontend
```


F5: Container Ingress Service, CIS



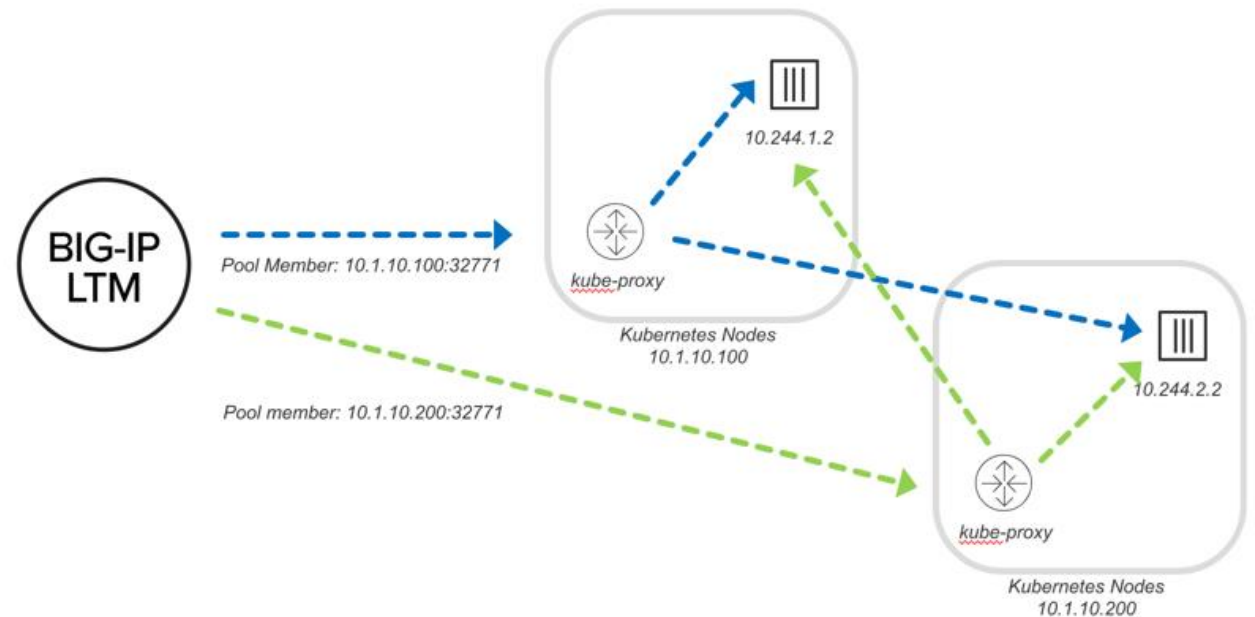
Best-in-class app services for containerized applications

- Control Ingress into container and PaaS environments via native, open-source, **enterprise-grade** F5 BIG-IP integrations
- Ensure performance, security, and availability of container apps **and** ingress controllers
- Enable self-service selection in orchestration for app services
- Scale and secure apps through automated event discovery and service insertion
- Inject automation into CIS and ecosystems with F5 Application Services 3 (AS3) extension and declarative APIs
- Increases flexibility of F5 application delivery and security services via K8s Custom Resource Definitions integration



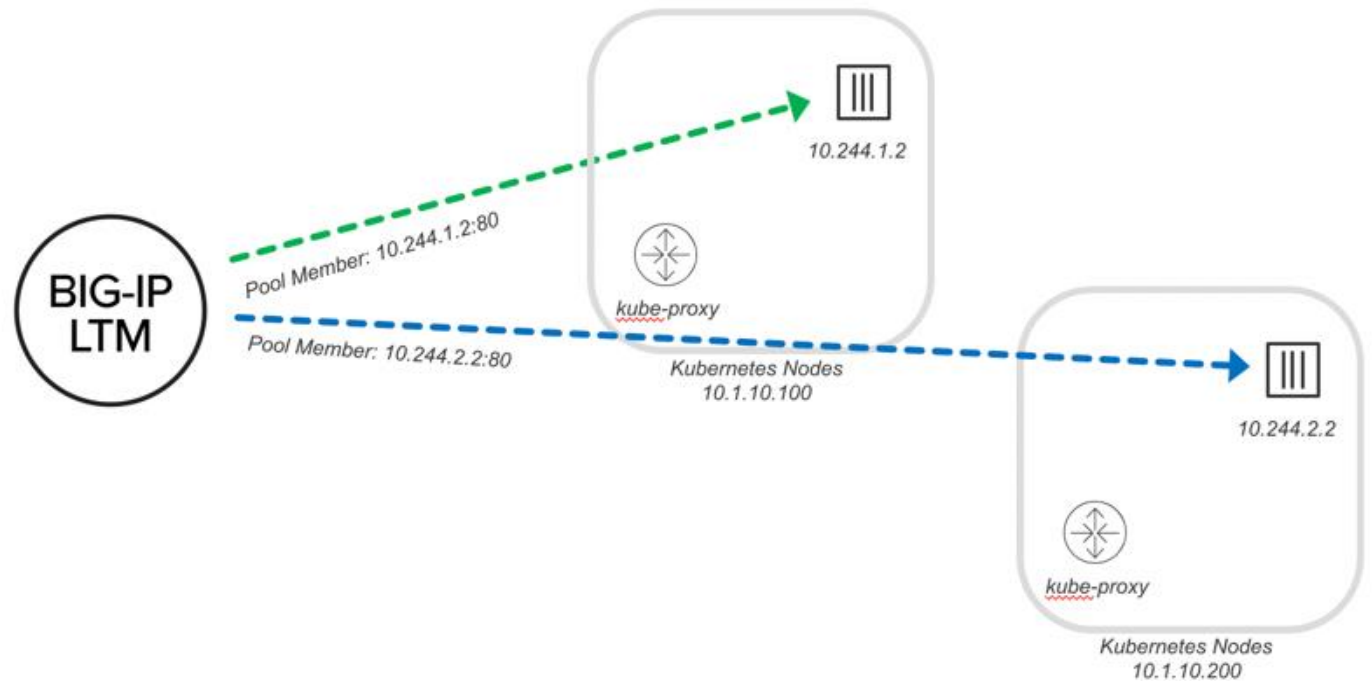
CIS: NodePort Deployment

- BIG-IP communicates with an ephemeral port, but in this case the kube-proxy keeps track of the backend Pod (container).
- Advantages:
 - Works in any K8S environment.
 - No persistence/visibility to backend Pod.
- Disadvantages:
 - Additional layer of load balancing with the kube-proxy.



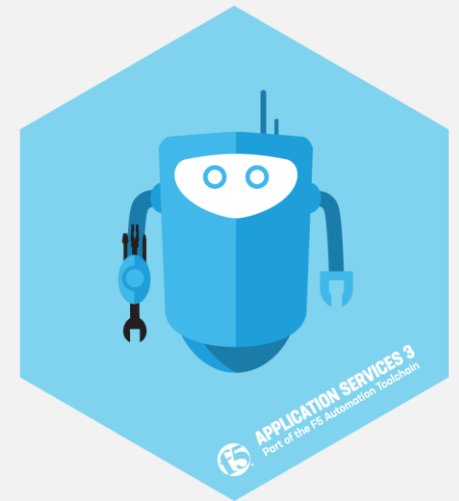
CIS: ClusterIP Deployment

- Ingress traffic bypasses the Kube-proxy and routes traffic directly to the pod.
 - Requires the BIG-IP have the ability to route to the pod.
 - Requires overlay network that F5 supports (Flannel VXLAN, or OpenShift VXLAN).
- Advantages:
 - Visibility to pod layer.
- Disadvantages:
 - Must setup and use overlay network.



Simplify automation with AS3

- Application Services 3 Extension – BIG-IP API extension that accepts a declarative API call
- Configures BIG-IP L4-7 services
- Minimizes need for BIG-IP domain expertise
- Minimizes deployment errors
- Makes it easy to integrate F5 automation into orchestration systems
- Runs on BIG-IP, on BIG-IQ, or in a container
- Create application dashboards / monitoring / alerts when used with BIG-IQ

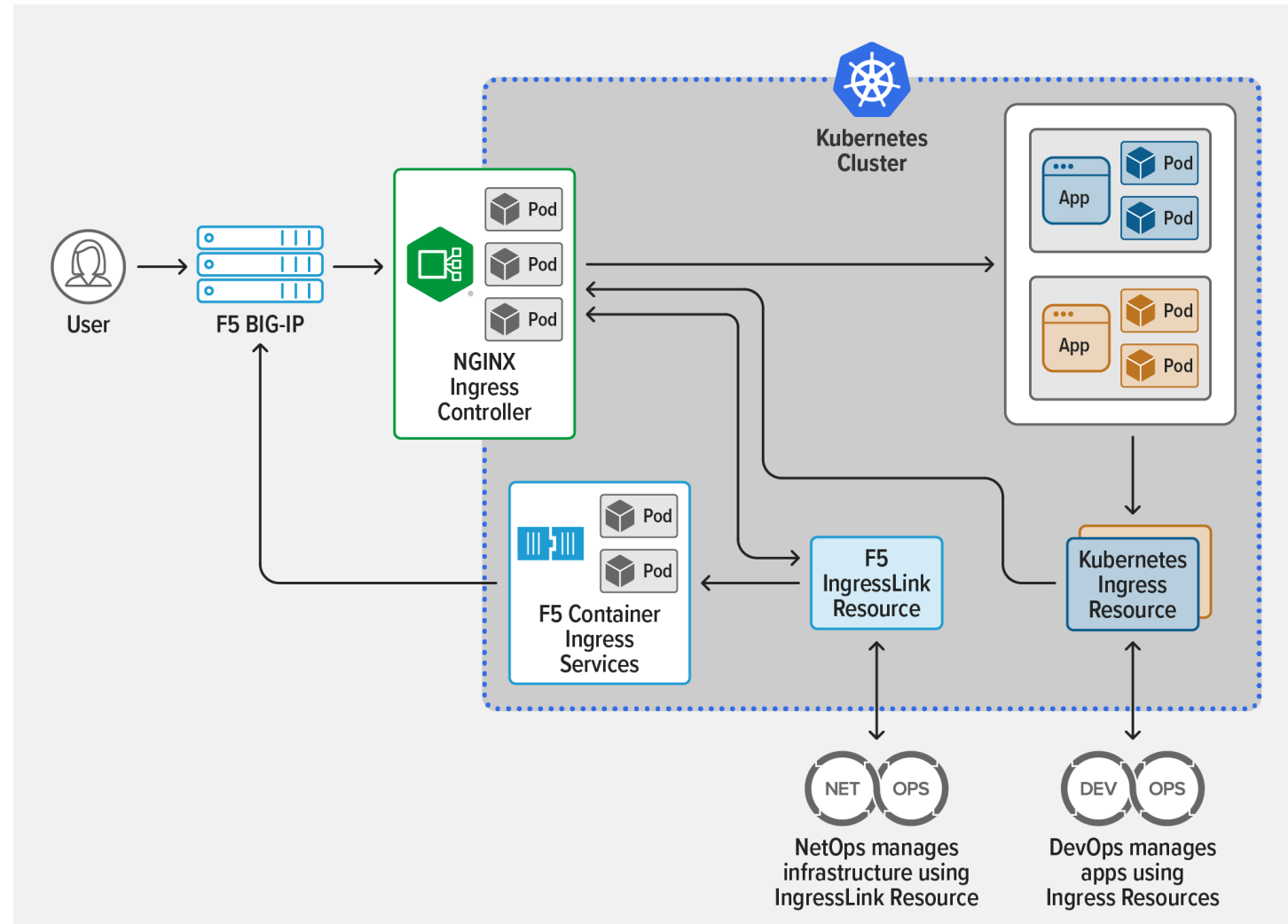




IngressLink

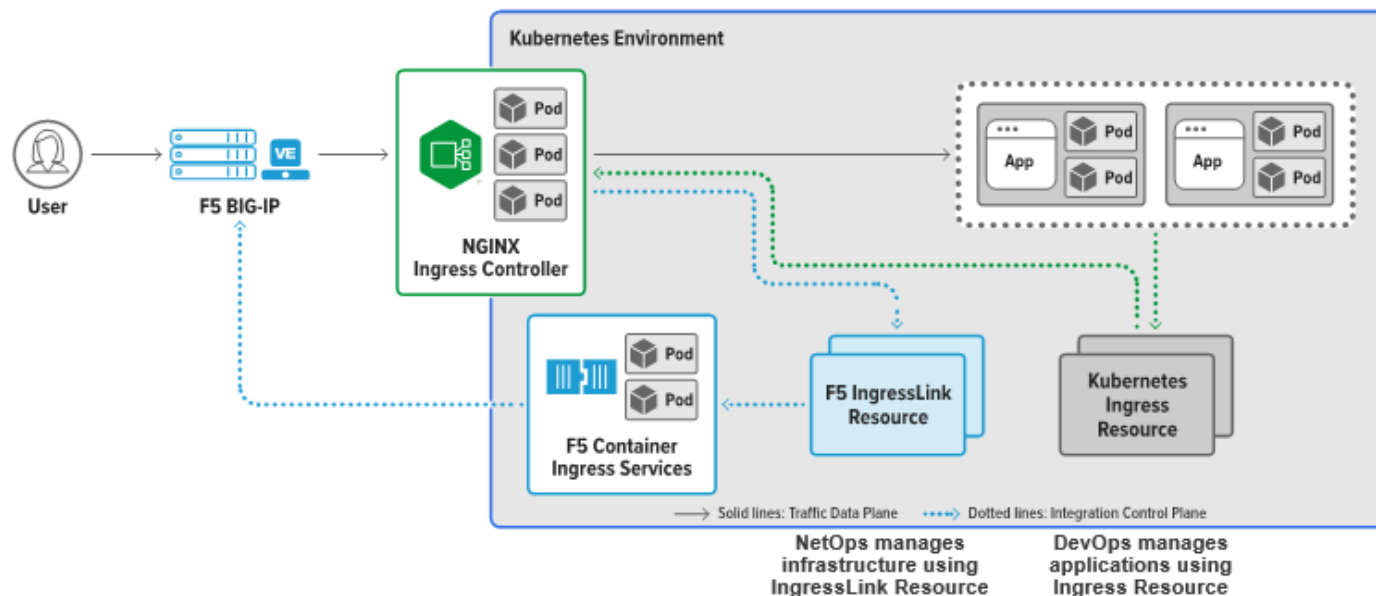
BIG-IP and NGINX in a Kubernetes Environment

- Clear separation between NetOps and DevOps
 - Each has a distinct responsibility for their domain
- Straightforward, familiar Configuration
 - NetOps F5 IngressLink is simple (no required domain knowledge)
 - DevOps use familiar Ingress Resources (no exposure to CIS)
- NGINX Ingress Controller takes the high control-plane load
 - Lightweight demands on the BIG-IP control plane
 - Much better operations experience



IngressLink

Requires NGINX Plus as Ingress Controller



Benefits:

- Unified solution for modern app services at DevOps velocity
- Intuitive management of enterprise-grade performance and security
- Supports DevOps use cases: routing, B/G, circuit breaker
- Advanced attack protection selected in orchestration without expertise

Clear Separation between NetOps and DevOps

- Each has a distinct responsibility for their domain

Straightforward, Familiar Configuration

- NetOps F5 IngressLink is simple (no required domain knowledge)
- DevOps use familiar Ingress Resources (no exposure to CIS)

NGINX IC takes the high control-plane load

- Lightweight demands on the BIG-IP control plane
- Much better operations experience

RedHat OpenShift

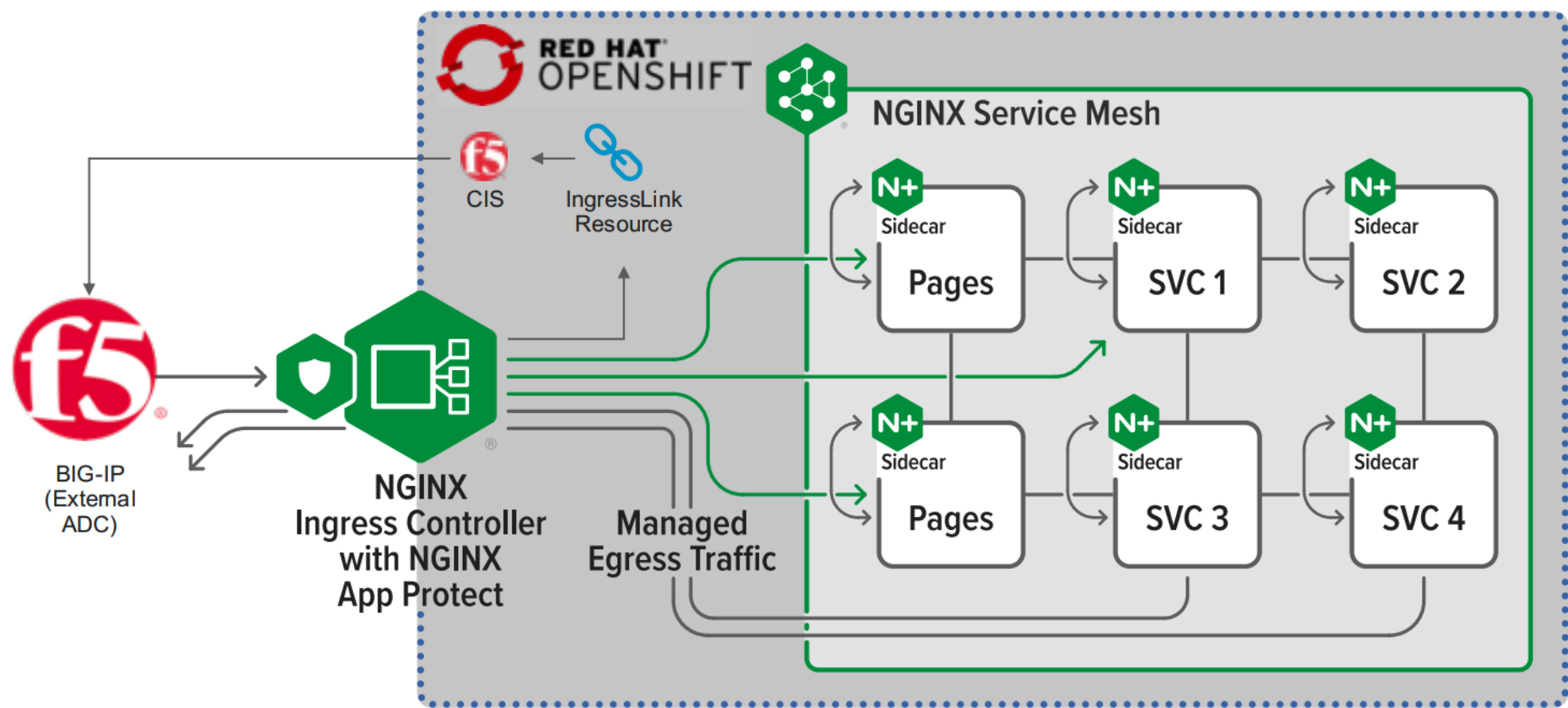


Figure 1 – Deploying NGINX Ingress Controller and BIG-IP in the OpenShift Architecture

Hands On Lab Time

Please complete the Survey.



Survey can be found in the Attendee Hub