Operate reliably and securely with Air-Gapped Kubernetes

Challenges

Security-conscious organizations in the military, law enforcement, and national security arena as well as companies in industries like banking, finance, healthcare, and manufacturing face total disruption of operations, theft of critical Intellectual Property, and limitations due to lack of network connection or bandwidth.

To balance between the myriad risks of connecting to the Web, particularly in public cloud environments, and the need to operate offline, air-gapped Kubernetes is ideal. However, custom implementations typically require months of development work and ongoing maintenance. Instead, D2iQ gives you everything you need to run production Kubernetes in an air-gapped environment – both the right technology and the right expertise to implement that technology. D2iQ's purpose-built automation provides fast implementation with flexible configuration in place of time-consuming customization.

## On-Premises or Private Cloud

The diagram depicts an air-gapped Kubernetes implementation that is physically isolated from the Public Internet. D2iQ provides local repositories for container images, Helm charts, the OS package, and platform services. It enables Docker images to pull from these internal registries and repositories. And it makes software and open-source components locally accessible to your application and deployment environment.

PUBLIC INTERNET

AIR GAPPED PHYSICAL NETWORK BOUNDARY
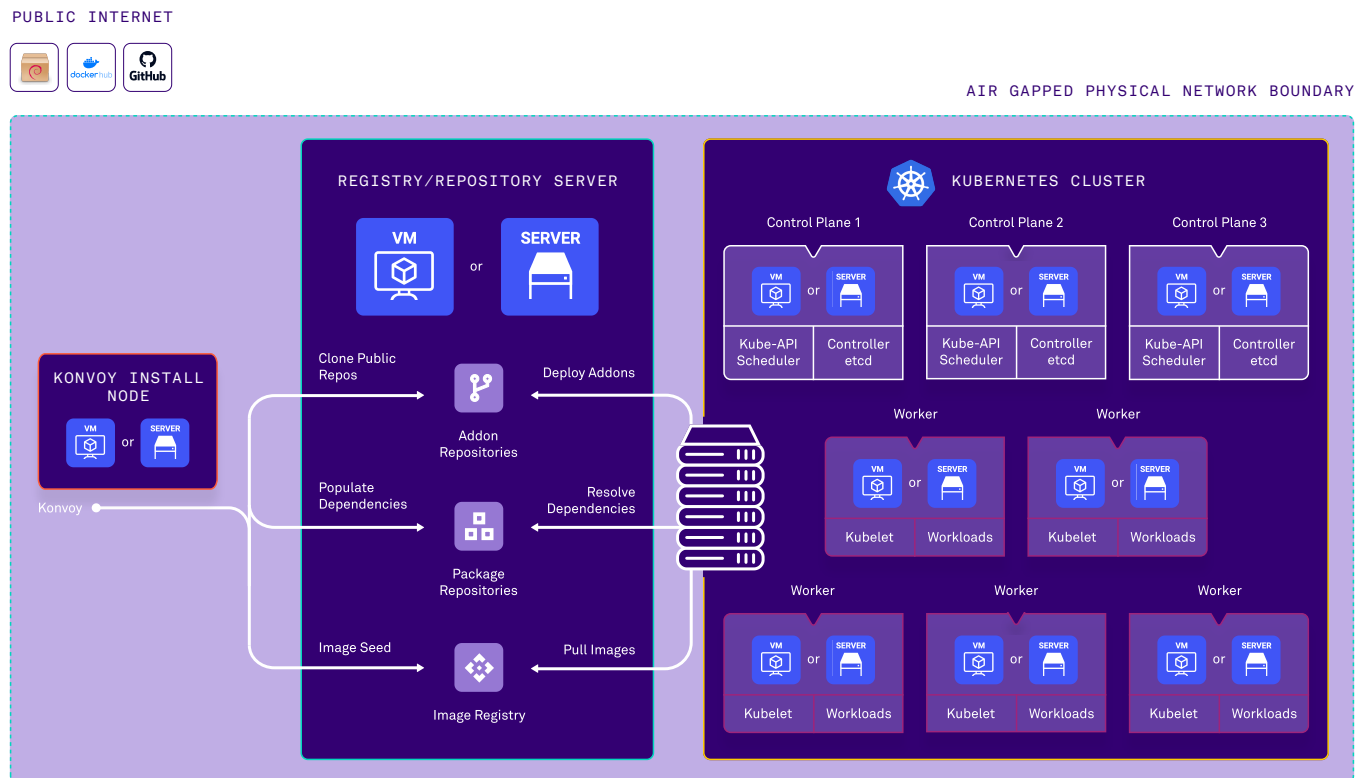
While operations are air-gapped, the Kubernetes implementation is fully functional and does not limit the applications or functions executed within the containers. Further, the implementation is consistent across all environments.

Public Cloud / Public Multi-cloud

D2iQ also supports air-gapped Kubernetes in the public cloud. As shown below, a virtual private cloud takes the place of the physical air-gapped boundary typically used on-premises. D2iQ Konvoy is implemented in a secure, hardened, and isolated Bastion Node. As the Kubernetes Cluster instantiates new containers, the Control Plane accesses the Bastion Node via a Secure Tunnel to pull images, resolve dependencies, and deploy add-ons.
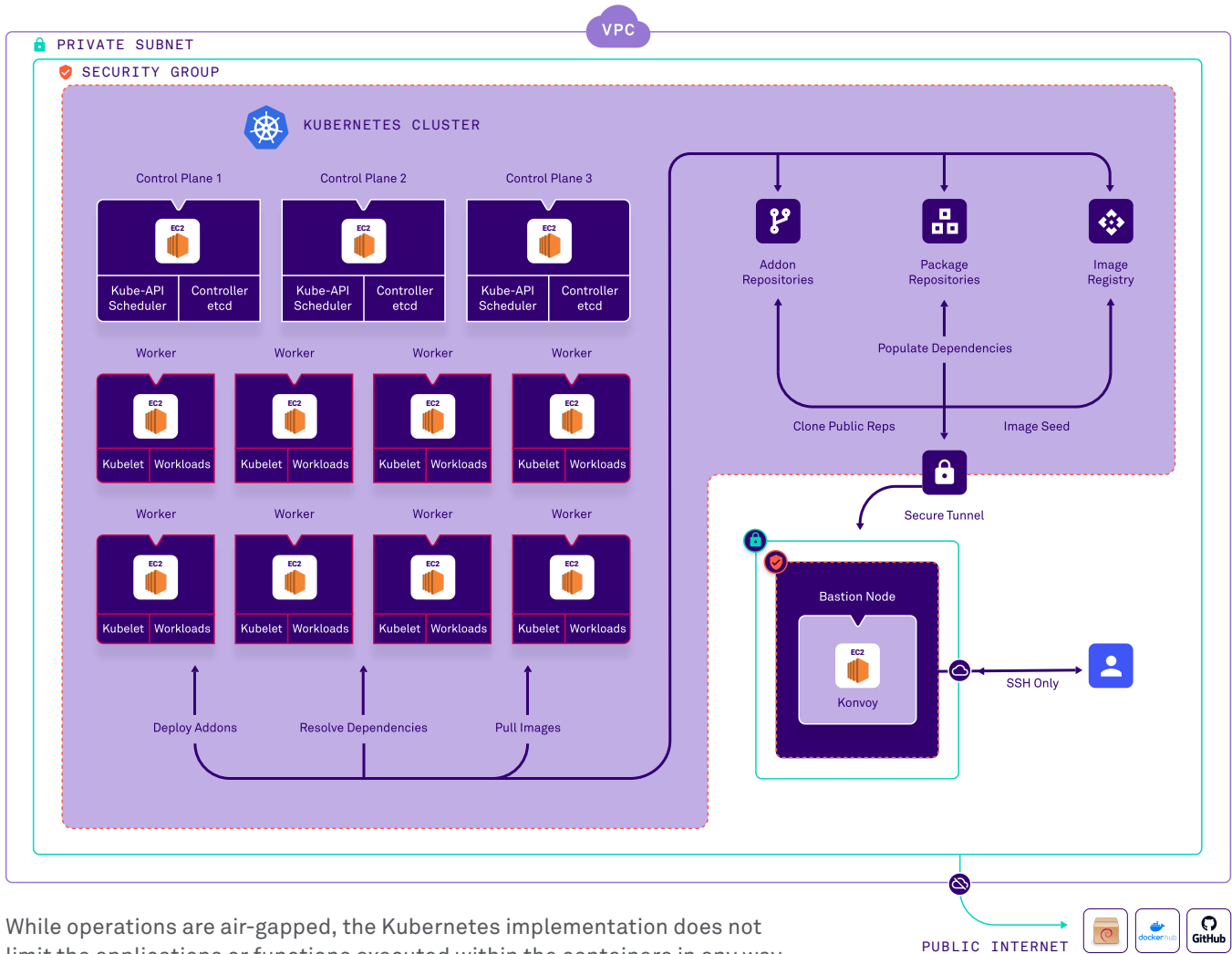
While operations are air-gapped, the Kubernetes implementation does not limit the applications or functions executed within the containers in any way. Further, operations are consistent across one or more public clouds.

Outcomes

Air-gapped Kubernetes with D2iQ helps government agency and business IT teams create unparalleled business outcomes.

Operational Resilience

Protect critical operations against threat actors and IT service disruptions due to network availability.

Security and Compliance

Provide protection against both external and internal threat vectors and compliance with regulations.

Consistency

Applies consistently across all environments including those with connection limitations.

D2iQ delivers the leading independent platform for enterprise-grade Kubernetes. Starting with a comprehensive, enterprise-grade Kubernetes distribution built on pure upstream open-source, D2iQ provides management and ancillary platform applications that are tightly integrated, secured, and tested at scale. To learn more, go to www.D2iQ.com.