Enable a Data Plane for Workspaces

To support workspaces, the data plane must be configured so that users can connect directly to the data plane to access interactive workloads, as described below.

Configure the hostname

The data plane must be served from a *subdomain* of the domain used for the control plane. In other words, if users connect to Domino at **example.com**, then data planes must be served from **data-plane.example.com.**

Configure load balancing

The hostname above should resolve to a load balancer which routes traffic to port 8080 on Pods with the following label selector:

```
app.kubernetes.io/component: auth-proxy
app.kubernetes.io/instance: auth-proxy
app.kubernetes.io/name: auth-proxy
```

You can do this with a combination of a **NodePort** service and load balancer if on-premises, or using **LoadBalancer** service types in major cloud providers.

Configure TLS

Users must connect to data planes using TLS (HTTPS). If you are using a load balancer to route traffic to the data plane, it might be easiest to configure the load balancer to serve valid TLS certificates for the domain.

To configure the data plane to serve TLS certificates that you provide:

1. Create a Kubernetes secret containing the certificates:

```
kubectl create secret tls custom-certs -n <data plane namespace> --cert=<cert file> --key=<key file>
```

2. Set the following value when deploying the data plane Helm chart:

```
--set auth-proxy.config.nginx.tlsSecretName=custom-certs
```