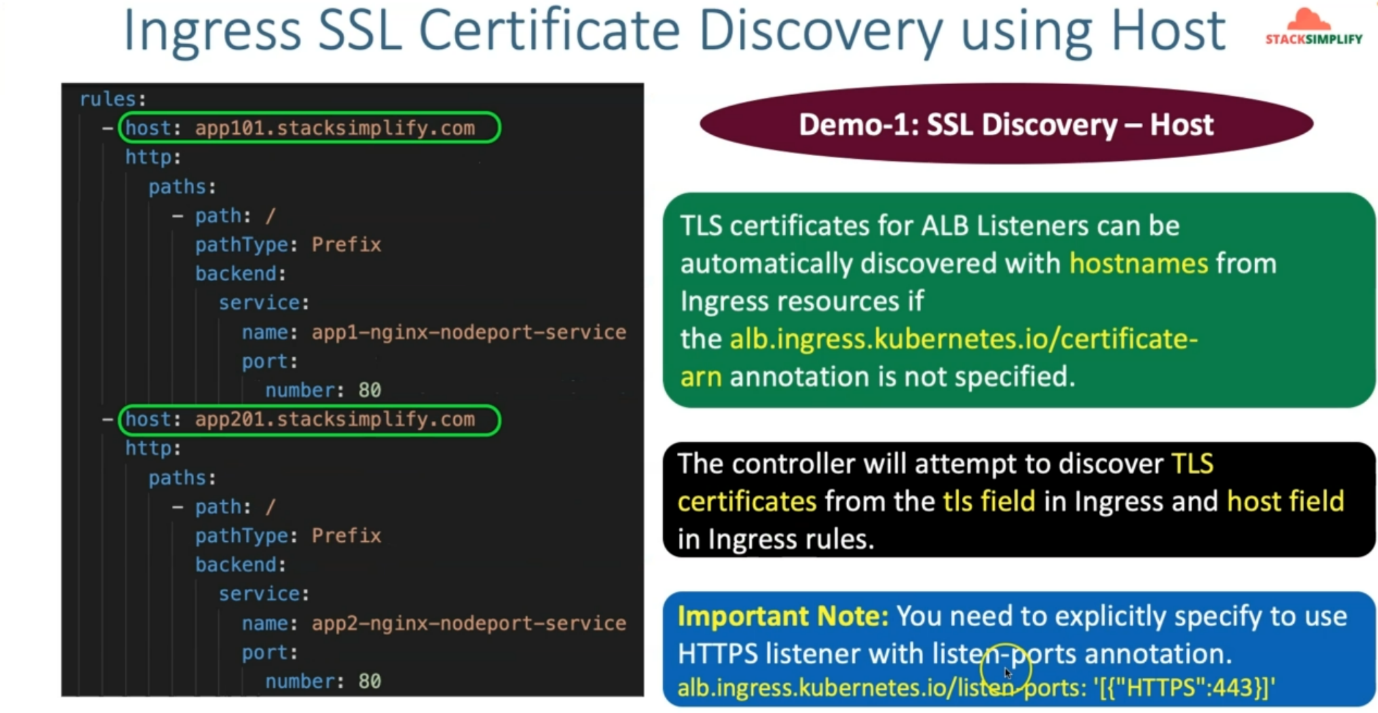
**1. Introduction to Ingress SSL Discovery**

--- in this section, we are going to learn about the Kubernetes ingress concept SSL discovery with Host & TLS. So, we are going to implement 2 demos as part of this concept.

--- So now let's go and understand what exactly is this SSL certificate discovery?

**Demo -1**



--- if you see here, this is SSL certificate discovery using host. So, if you see in the rules, earlier, we have already implemented the host header-based routing. Where we have seen the **app101.stacksimplify.com** and **app201.stacksimplify.com** were specified in the ingress rules with the host as the argument.

--- here the **TLS** certificates for **alb** listeners can be automatically discovered with host names from

ingress resources. if the alb ingress related certificate arn is not specified, in simple terms when you are using this host header-based routing, from these host values, you are given that the DNS name very clearly. **app101.stacksimplify.com**.

--- which means you really don't need to provide this certificate **arn** related annotation and provided the arn off your SSL certificate from your certificate manager. So, by default, Ingress can directly take the available certificate for these names, which means if the name matches **\*.stacksimplify.com**.

--- So, if you have something called **\*.stacksimplify.com**. so that matches these domain names

**app101.stacksimplify.com** and **app201.stacksimplify.com** so automatically it will take that and then associate with your ingress service. So, it is nothing but it will associate with your application load balancer.

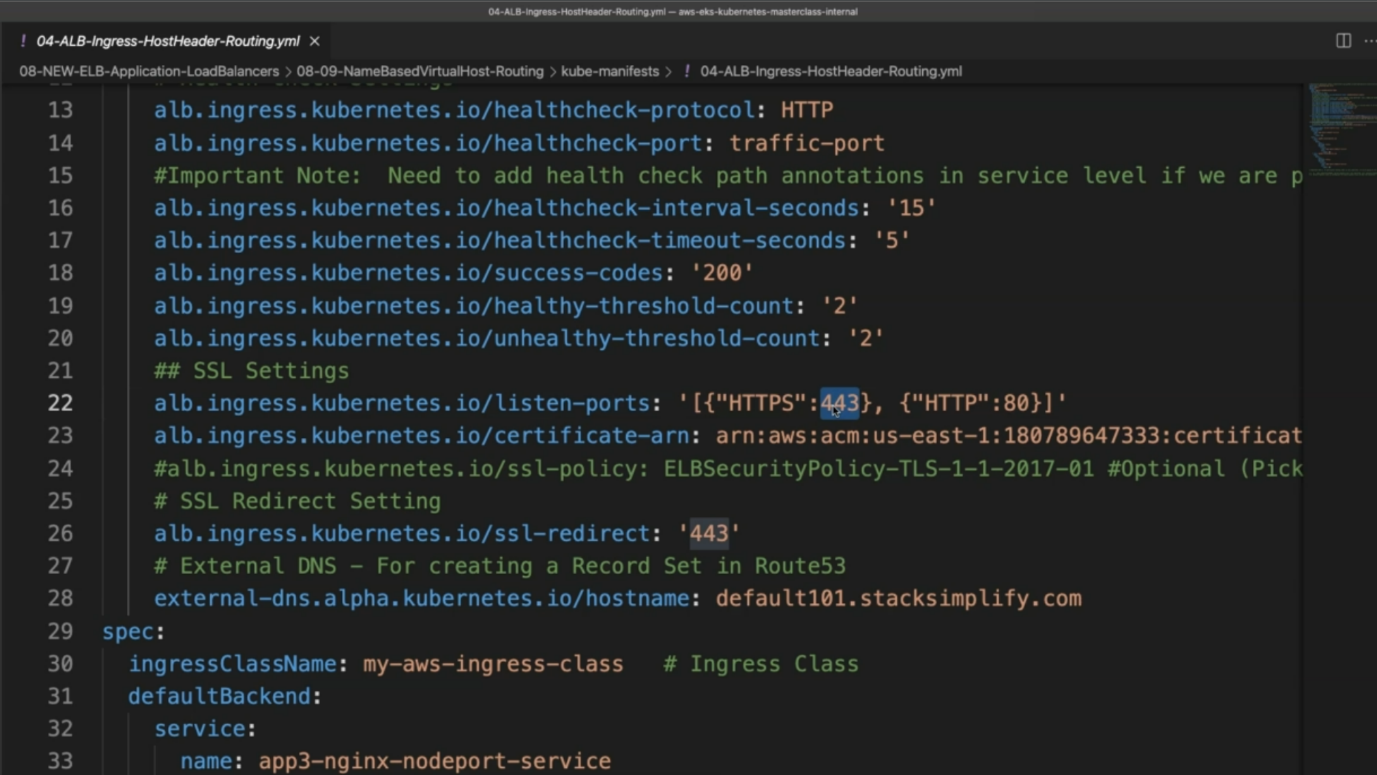
--- We explicitly don't need to define this certificate and add an annotation. which means which is a very good thing that we don't need to go to our certificate manager and go to that respective certificate and get the arn and hard code that arn in the ingress service.

--- We don't need to do all those. It is going to take it with this SSL discovery with host option whenever you are using the host basic rules.

--- In addition to that, any other rules, not the host base rules, you are doing the context-based routing. So, at that point of time or you are using only a default backend for something. So, at that point of time. it can also use something called a peerless field.

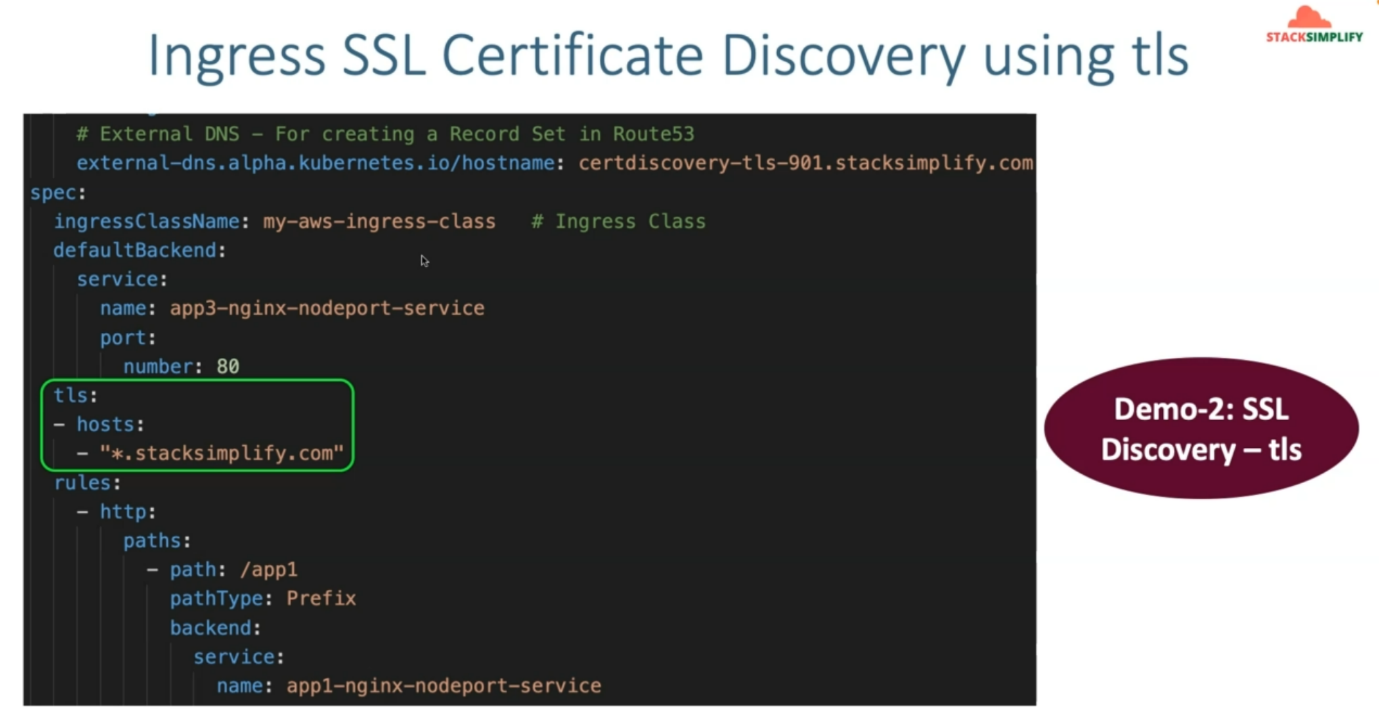
--- So, in the next demo, we are going to see that **tls** field related demo. So, the controller will attempt to discover **tls** certificate from the tls filed in ingress and host filed in ingress rules.

--- **note** - another important note here is you need to explicitly specify https:443 Listeners with Listen ports annotation and anyway, we are going to do that and we have already seen in our ingress resources also.



--- So, you can see we are already specifying the Listen Port 443 for SSL communication.

**Demo - 2**



--- let's come back to this Demo 2, which is SSL discovery with tls.

--- If you see your DNS name, you have provided us **certdiscovery-tls-901.stacksimplify.com**. You have something called your default backend, and here there is no host rules here. this is simple context-based routing related example.

--- So, at that point when you are using other than host and then if you want to use, if you want to auto detect your SSL certificate and associate with you are ingress service, which means it need to associate with your application load balancer.

--- You can also use this **tls** option and provide with TLC hosts and provide your host names. You have \*.stacksimplify.com, so automatically this related certificate will be associated with your ingress resource or service. which means whenever we are implementing these SSL certificate discovering ingress using host or tls options, we really don't need to have this annotation enabled so you can go ahead and then comment this certificate related annotation arn in your both demos.

