Irmin Auwerda

Transport Layer Security (HTTPS) voor jouw applicatie

In de afgelopen jaren heb ik meerdere keren TLS moeten inrichten voor een systeem. Ook nu is dit het geval bij de NS. Hoe moet je dit eigenlijk doen, en wat komt er bij kijken? Hoe werkt TLS eigenlijk en hoe is een certificate-chain opgebouwd? In deze talk neem ik jullie mee door het process van TLS inrichten voor een applicatie. Van het maken van een certificaat, naar het inrichten van een identity- en trust-store tot de inrichting van je load balancer / gateway om de applicatie op meerdere URLs beschikbaar te maken.

Waarom juist dit onderwerp?

Bij het project waar ik aan werk werd HTTP gebruikt, met basic auth. Toen ik de vraag stelde: “Is dat wel veilig?”, werd gesuggereerd dat we misschien TLS zouden moeten gebruiken. De volgende vraag was om uit te zoeken hoe dat precies moest. Bij een ander project was ik hier ook al mee bezig geweest. Als je niks inricht, dan valt je applicatie server terug op een dummy trust store voor de certificaten. Daarmee stel je je potentieel open voor certificaten die niet per definitie te vertrouwen zijn, tot aan de productie omgeving. Het bleek dat niemand hier eigenlijk kaas van had gegeten; niemand had de benodigde basis. Dus ik ging dat uitzoeken en het is bijzonder nuttig om te begrijpen. Uiteindelijk is het allemaal relatief simpel, maar wel heel belangrijk. Als je een nieuwe service wilt ontsluiten, of als je iets toevoegt aan een bestaand cluster, heb je er eigenlijk automatisch ook mee te maken.

Van welke sessie baal je het meest dat deze naast de jouwe staat?

De sessie van Dries. Over front-end testing zou ik als developer zeker iets meer willen weten. Cypress als tool ken ik nog niet.

Waarom moeten mensen komen kijken?

Bij deze sessie ga je iets opsteken van hoe je een identity- en trust store inricht in je applicatie server. We kijken naar hoe je bepaalt welk certificaat je gebruikt voor je identity store en hoe de certificate chain eruit ziet. Dit is toepasbaar voor elke applicatie server, ook al zijn de specifieke commando’s die je nodig hebt anders. Je ziet hoe je m.b.v. de keytool een self-signed certificate maakt en gebruikt en hoe je de trust store beheert als je bv. een beveiligde verbinding moet maken naar een andere partij.

Als je een light saber zou maken, welke kleur zou je dan kiezen?

Donkerpaars: als ode aan Senator Palpatine, een *man met visie*.

mini.CONF Episode SX - Revenge of the Hermit vindt online plaats op 4 maart 2021. Voor alle informatie over het evenement, het programma en de sprekers ga je naar https://miniconf.group9.io

**Tijd om de boel wat beter te beveiligen?
De sessie van Irmin vindt plaats in virtuele kamer *Jedi* om 19:55.**