Sadie Stokes

SSW-567

1/30/2020

HW 02: Docker and Configuration Management

Docker is a great tool that allows users to create, deploy and run applications within containers that will run on any machine regardless of any settings on the machine. This is great for any size or product a team is creating because this leaves lots of flexibility in terms of allowing the developers to package their entire application with any and all libraries or dependencies in that environment to ensure deploying and testing goes according to plan. When it comes to integration Docker also excels. A common deterrent for most companies when it comes to adopting new technology is because of the cost to integrate. Docker not only drives down the cost of infrastructure because physical machines are no longer a requirement, this not only helps with integrating this into daily practices but also with outside tools or platforms such as TFS, GitHub, etc...

When it comes to testing and deployment standardization and consistency are going to be key. Docker containers keep that consistency across multiple development and release cycles and that provides a repeatable development, build, test and production environments. This is a huge positive because as a customer, you want to ensure you are testing the “latest and greatest” features with little to no defects. In the event that a developer does create a feature that breaks the environment it is very easy to rollback to a previous version which greatly helps with testing, deployment and providing that support to a customer if they run into an issue. Deployment is also another issue that Docker can easily solve. As mentioned earlier, Docker creates a container for every process and does not boot an OS. This drastically reduces the time to deploy to seconds and this is not only very affordable but beneficial to the customer. This also will allow for the team to build, test and release builds that can be deployed across multiple servers.

Security is a hot topic for most because of in the insurgence of internal or external hackers. Docker does a great job at reassuring its users by ensuring applications running on containers are separate and isolated from each other. This is a good thing because if anything is compromised you can easily get rid of or fix that isolated container. In saying that, while security is being taken into account it is still left up to the team to ensure best practices are upheld and each environment is monitored.