**Patching in AWS**

We can set up and monitor system patching in AWS using AWS System Manager using a component called Patch Manager.

After setting up the Patch Policy then patches baseline/updates can be scheduled and automated.

Key metrics are "***Configuration deployment status***" that shows success, failure and pending are important.

Resource compliance is crucial too to ensure baseline security are address

**Monitoring patches**

System Manager Patch Manager provides a dashboard that shows the success, failures and pending of deployed patches.

Patches logs can be configured to push to s3 - and we can make use of AWS lambda to process those logs and push that into SNS for alerting and notifications.

Patch manager also supports Security Hub which provides security overview of resources in AWS.