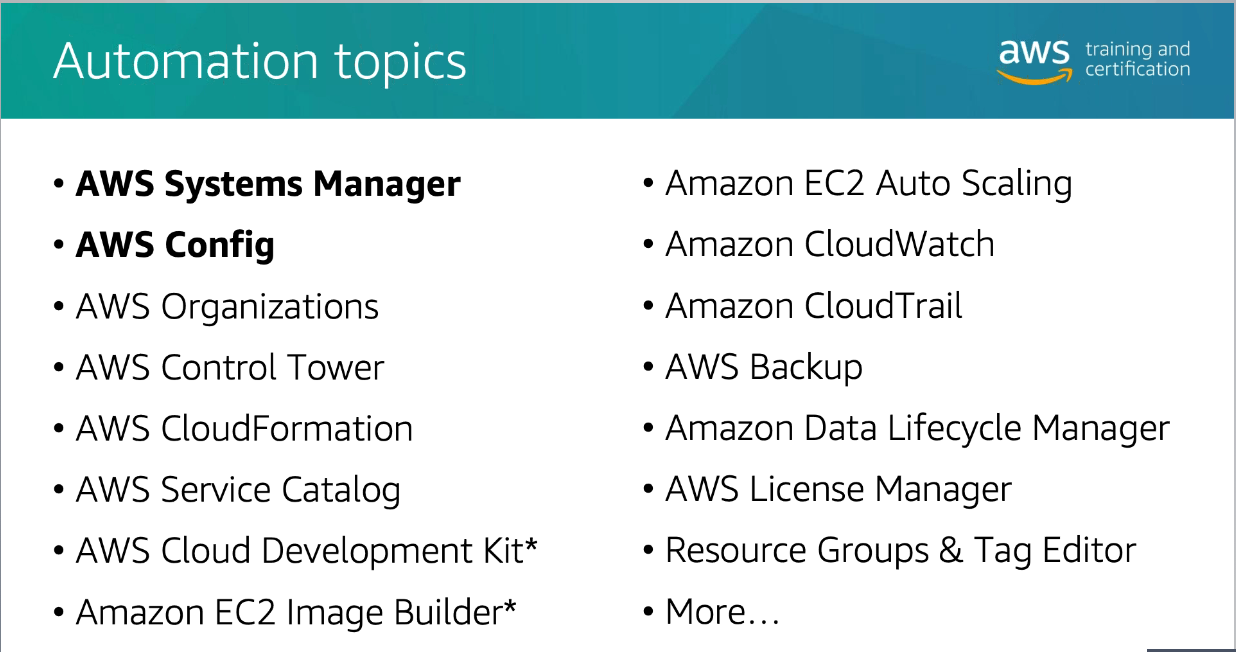
New SysOps details

------------------------------------

**SysOps Goal**

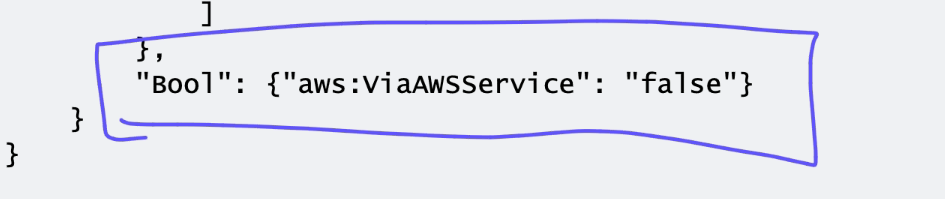
1. Deploy the system
2. Administer the system
3. Monitor the systems
4. Maintain the system
5. Troubleshoot

**Main services to cover**



To do:

* Run a well architected review using the “well-architected tool”
* What is IAM pass role? Example: A user has full ec2 control access. He creates an EC2 instance and assigns full s3 access to the instance. If the user logs into the instance, he will also have access to s3 using the EC2 instance role. With IAM pass role, we can specify what roles the user can pass to the instance thus limiting the user from gaining more access that they should have.
* Create permission templates for groups and roles in AWS
* AWS Config compliance deep dive and demo. Remember AWS config is not real time.
* Learn the “Prepare – Operate - Evolve” process
* What is Permission boundaries?
* IAM policy language AND or OR?
* What is the following? This means you must be an actual person or role to do this.



* Show how roles work for cross account access and trusts
* We can enable multi factor authentication through “cli, gui and api” for normal users but for root user you can only use gui.
* Software MFA can be used on multiple devices and is useful specifically for the root user but a hardware mfa is limited to only one user. So it’s better to use virtual or software mfa when it comes to root.
* Rotating keys is super helpful specifically if a key is compromised. AWS config can be used for automatic key rotation.
* What is policy simulator? It’s testing your policies. It doesn’t harm your AWS environment.
* What is cloud shell
* Know how to setup AWS organizations
* Know how to use SCP inside organizations.
* If we login using the session manager, it’s already using a role and we don’t need to use “AWS configure”. We have to if we need a different level of access.
* What is aws console recorder?
* Learn AWS cli builder
* Ssm port forwarding should be tested.
* AWS config inventory
* Aws config remediation
* Aws config discovery
* AWS config capture changes
* AWS config compliance
* Aws config conformance packs? It’s a package including the config rules and remediation rules to identify and automatically remediate. Learn more. Use it between multiple accounts and regions.
* System manager quick setup will quickly add your current instances to system manager and deploy the agent, add the role and automatically update the instances. It also checks for software inventory every 30 minutes.
* You must know control tower in and out
* What is conformity monkey
* We can use AWS Organizations for organization wide tagging
* We have a service called cost explorer. We can use cost allocation tags to assist with cost analysis
* Tools like IAM and AWS Organizations can force tagging
* We can use Cloud formation and … for automating tagging
* Resource groups are also part of tagging
* Demo ec2 image builder
* Know how control tower and AWS organizations and landing zones work.
* Also control tower guard rails
* Cloud former2 can build template from current environment. <https://former2.com/>
* Know how to create a cloud formation template
* Helper script vs functions in cloud formation templates
* Cloud-init details .

<https://cloudinit.readthedocs.io/en/latest/>

<https://aws.amazon.com/blogs/devops/view-cloudformation-logs-in-the-console/>

* Use ssm secrets manager for cloud formation to access their credentials
* Build service catalog using CF templates
* Test driven development study.
* What is an OpsItem? You can create one using a cloud watch event.
* Know how to use AppConfig
* Practice Parameter store and secrets manager
* Parameter Store tutorials: <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-paramstore-walk.html>
* OpsItems: <https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter-working-with-OpsItems.html>
* Patch management and patch groups
* Patch Groups - How they work: <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-patchgroups.html>
* Check Spot block details

<https://aws.amazon.com/blogs/aws/new-ec2-spot-blocks-for-defined-duration-workloads/>

* Spot fleets study

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html>

* Review License Manager. It can manage licenses and it can also setup instances.
* What is log shipping?
* You can save logs in s3 and use Athena to query. You can also stream your logs to Cloud watch logs, you can use logs insights to query information
* If we want to use ELK stack, we can have our services stream logs to cloud watch logs and have Kibana use ES to view logs
* Install sample apps to use xray. You can use elastic bean stalk with java that supports xray.
* IAM access analyzer should be reviewed.
* What’s a permissions boundary? Set one up. For example one role might have admin access in one region and lower access in another region.
* What is a route 53 resolver? Can we use other options
* How to setup a cloud front distribution?
* Know what firewall manager is.
* Use AWS Certificate manager and build your own CA’s (ACM private CA)
* Hadoop uses high performance computing (HPC). They use the Lustre file system.
* Ssm create a command document
* How to automate resource deployment using a service catalog?

**Control Tower**

[**https://www.youtube.com/watch?v=Zxrs6YXMidk**](https://www.youtube.com/watch?v=Zxrs6YXMidk)