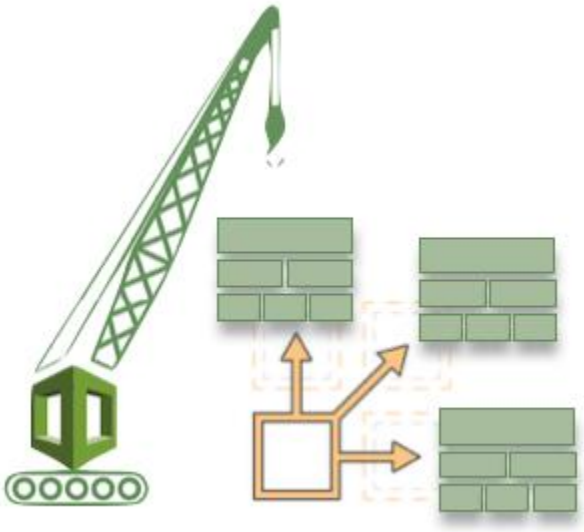
CloudFormation Drift Detection

AWS CloudFormation supports you in your efforts to implement Infrastructure as Code (IaC). You can use a template to define the desired AWS resource configuration, and then use it to launch a CloudFormation stack. The stack contains the set of resources defined in the template, configured as specified. When you need to make a change to the configuration, you update the template and use a CloudFormation Change Set to apply the change. Your template completely and precisely specifies your infrastructure and you can rest assured that you can use it to create a fresh set of resources at any time.

That's the ideal case! In reality, many organizations are still working to fully implement IaC. They are educating their staff and adjusting their processes, both of which take some time. During this transition period, they sometimes end up making direct changes to the AWS resources (and their properties) without updating the template. They might make a quick out-of-band fix to change an EC2 instance type, fix an Auto Scaling parameter, or update an IAM permission. These unmanaged configuration changes become problematic when it comes time to start fresh. The configuration of the running stack has drifted away from the template and is no longer properly described by it. In severe cases, the change can even thwart attempts to update or delete the stack.



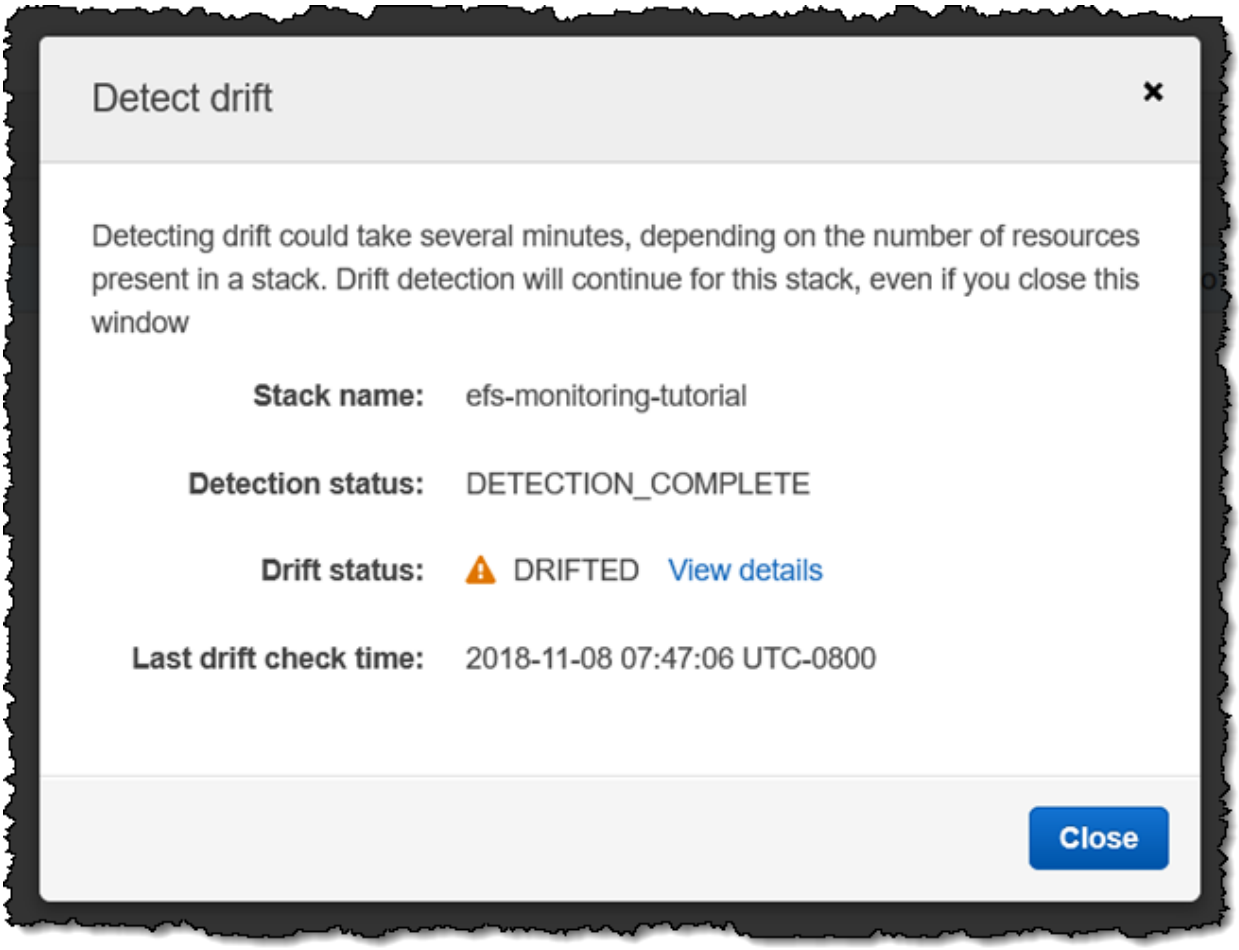
After you create a stack from a template, you can detect drift from the Console, CLI, or from your own code. You can detect drift on an entire stack or on a particular resource, and see the results in just a few minutes. You then have the information necessary to update the template or to bring the resource back into compliance, as appropriate.

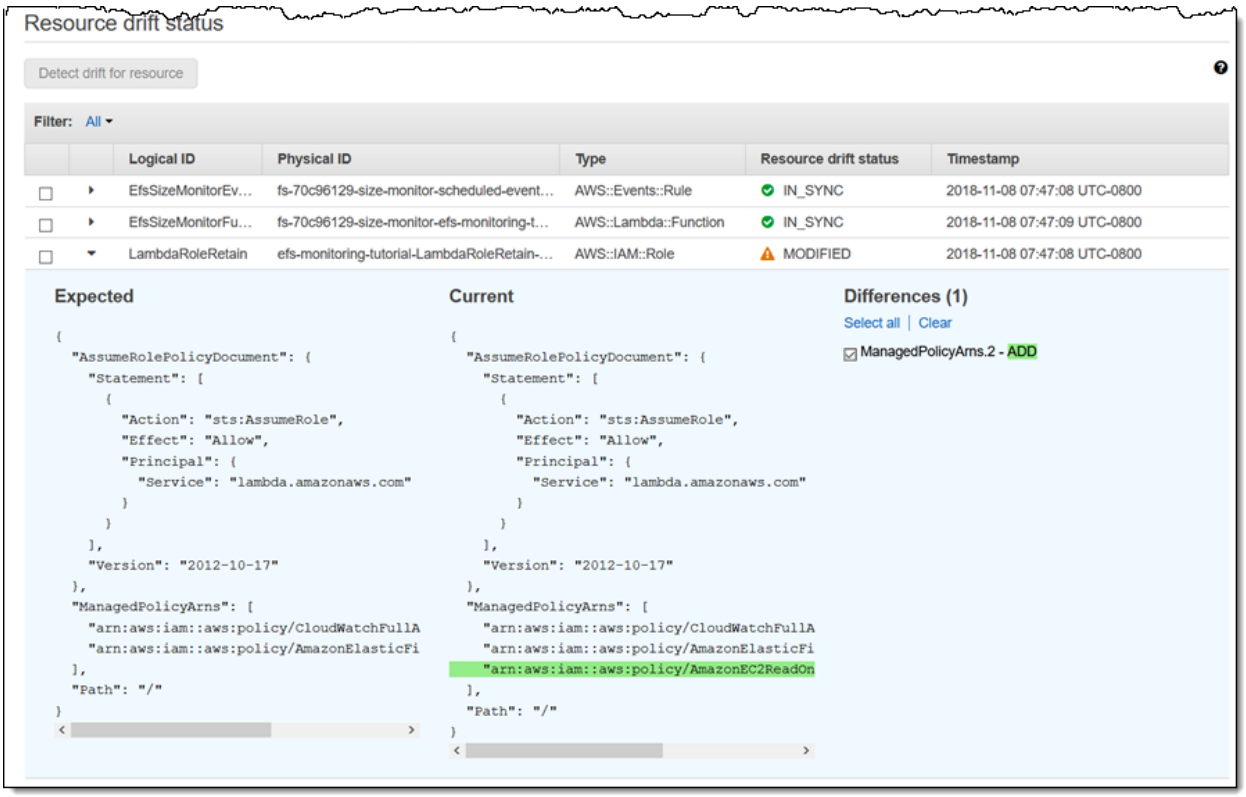
When you initiate a check for drift detection, CloudFormation compares the current stack configuration to the one specified in the template that was used to create or update the stack and reports on any differences, providing you with detailed information on each one.

We are launching with support for a core set of services, resources, and properties, with plans to add more over time. The initial list of resources spans API Gateway, Auto Scaling, CloudTrail,

CloudWatch Events, CloudWatch Logs, DynamoDB, Amazon EC2, Elastic Load Balancing, IAM, AWS IoT, Lambda, Amazon RDS, Route 53, Amazon S3, Amazon SNS, Amazon SQS, and more.

You can perform drift detection on stacks that are in the CREATE_COMPLETE, UPDATE_COMPLETE, UPDATE_ROLLBACK_COMPLETE, and UPDATE_ROLLBACK_FAILED states. The drift detection does not apply to other stacks that are nested within the one you check; you can do these checks yourself instead.





Amazon Machine Images (AMI)

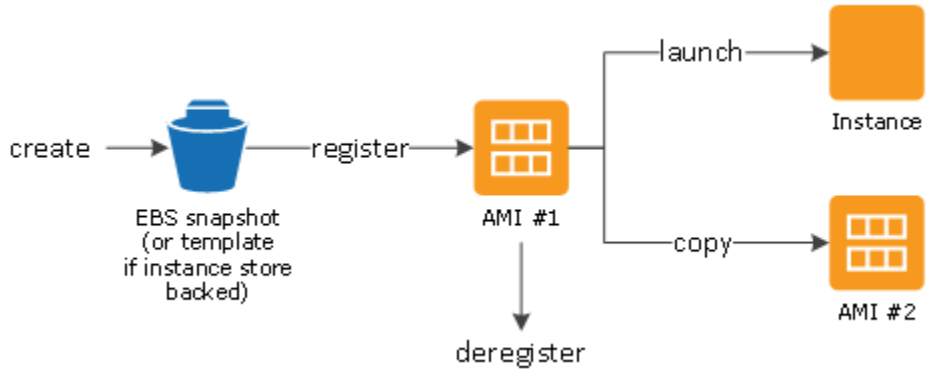
An Amazon Machine Image (AMI) is a supported and maintained image provided by AWS that provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you require multiple instances with the same configuration. You can use different AMIs to launch instances when you require instances with different configurations.

An AMI includes the following:

- One or more Amazon Elastic Block Store (Amazon EBS) snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched.

Use an AMI

The following diagram summarizes the AMI lifecycle. After you create and register an AMI, you can use it to launch new instances. (You can also launch instances from an AMI if the AMI owner grants you launch permissions.) You can copy an AMI within the same AWS Region or to different AWS Regions. When you no longer require an AMI, you can deregister it.



Create your own AMI

You can launch an instance from an existing AMI, customize the instance (for example, install software on the instance), and then save this updated configuration as a custom AMI. Instances launched from this new custom AMI include the customizations that you made when you created the AMI.

The root storage device of the instance determines the process you follow to create an AMI. The root volume of an instance is either an Amazon Elastic Block Store (Amazon EBS) volume or an instance store volume. For more information about the root device volume, see Amazon EC2 instance root device volume.

- To create an Amazon EBS-backed AMI, see Create an Amazon EBS-backed Linux AMI.
- To create an instance store-backed AMI, see Create an instance store-backed Linux AMI.

Buy, share, and sell AMIs

After you create an AMI, you can keep it private so that only you can use it, or you can share it with a specified list of AWS accounts. You can also make your custom AMI public so that the community can use it. Building a safe, secure, usable AMI for public consumption is a fairly straightforward process,

Deregister your AMI

You can deregister an AMI when you have finished with it. After you deregister an AMI, it can't be used to launch new instances. Existing instances launched from the AMI are not affected.

An *Amazon Machine Image (AMI)* is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, you launch an *instance*, which is a copy of the AMI running as a virtual server in the cloud. You can launch multiple instances of an AMI,