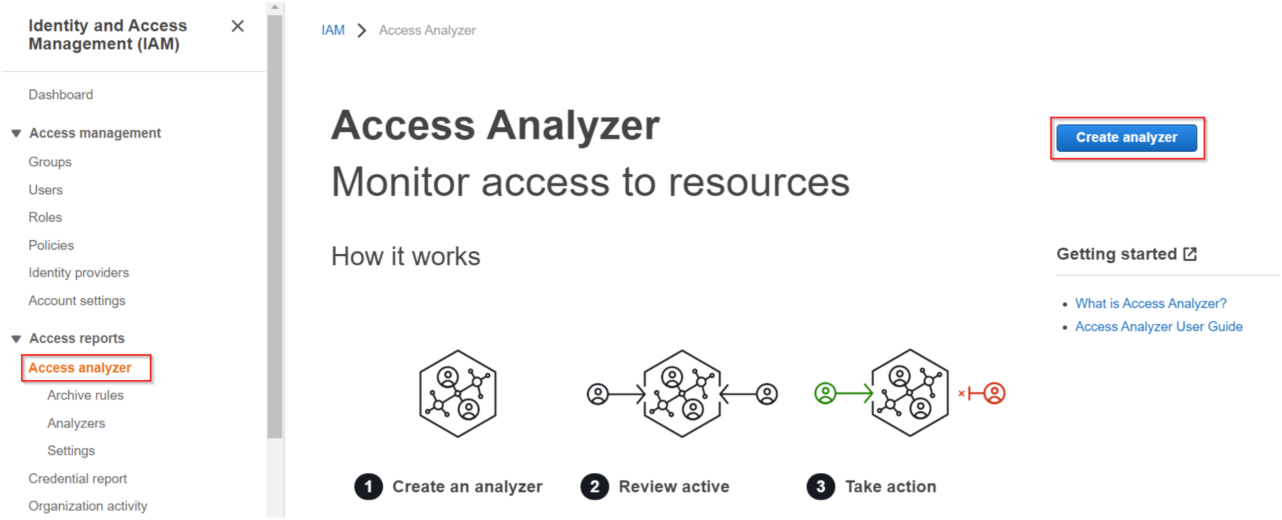
Module 8: Hands-On: IAM Access Analyzer

Step 1: Open the IAM console. Under Access reports, you can find **Access analyzer**, and once you choose it, click on **Create analyzer**

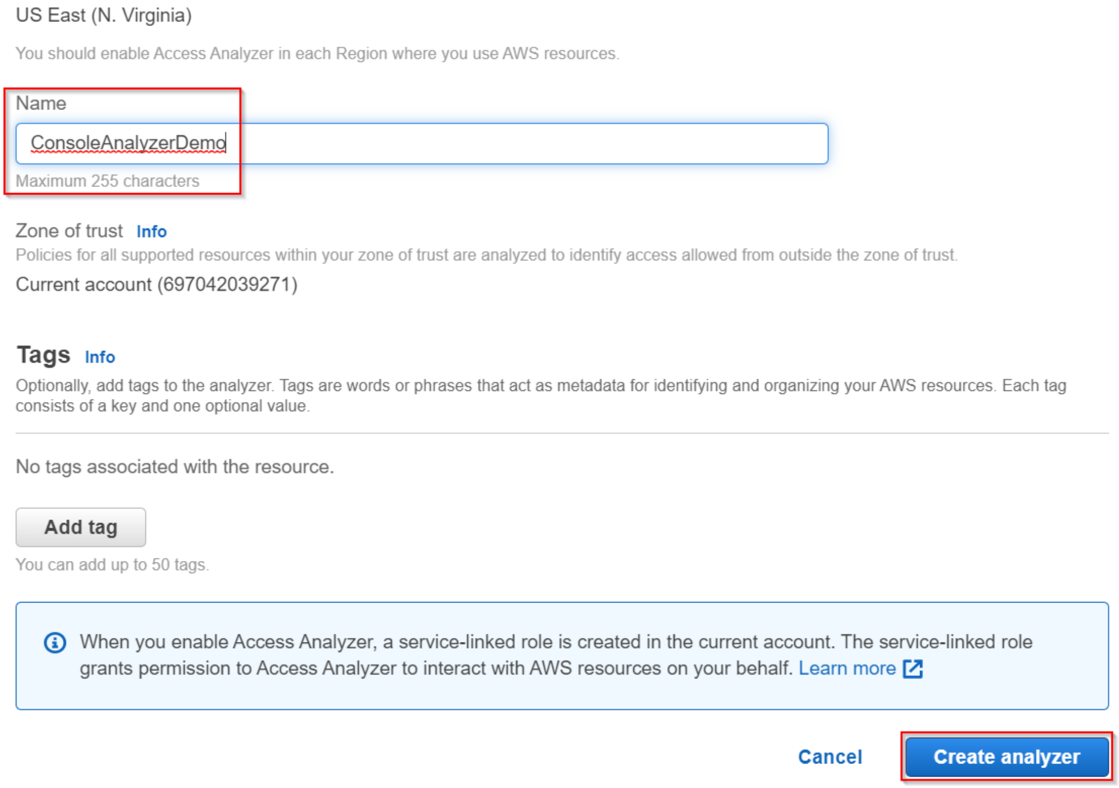


Access Analyzer

Monitor access to resources

How it works

Step 2: Provide a name for your analyzer, and click on **Create analyzer**



US East (N. Virginia)

You should enable Access Analyzer in each Region where you use AWS resources.

Name: ConsoleAnalyzerDemo

Maximum 255 characters

Zone of trust Info

Policies for all supported resources within your zone of trust are analyzed to identify access allowed from outside the zone of trust.

Current account (697042039271)

Tags Info

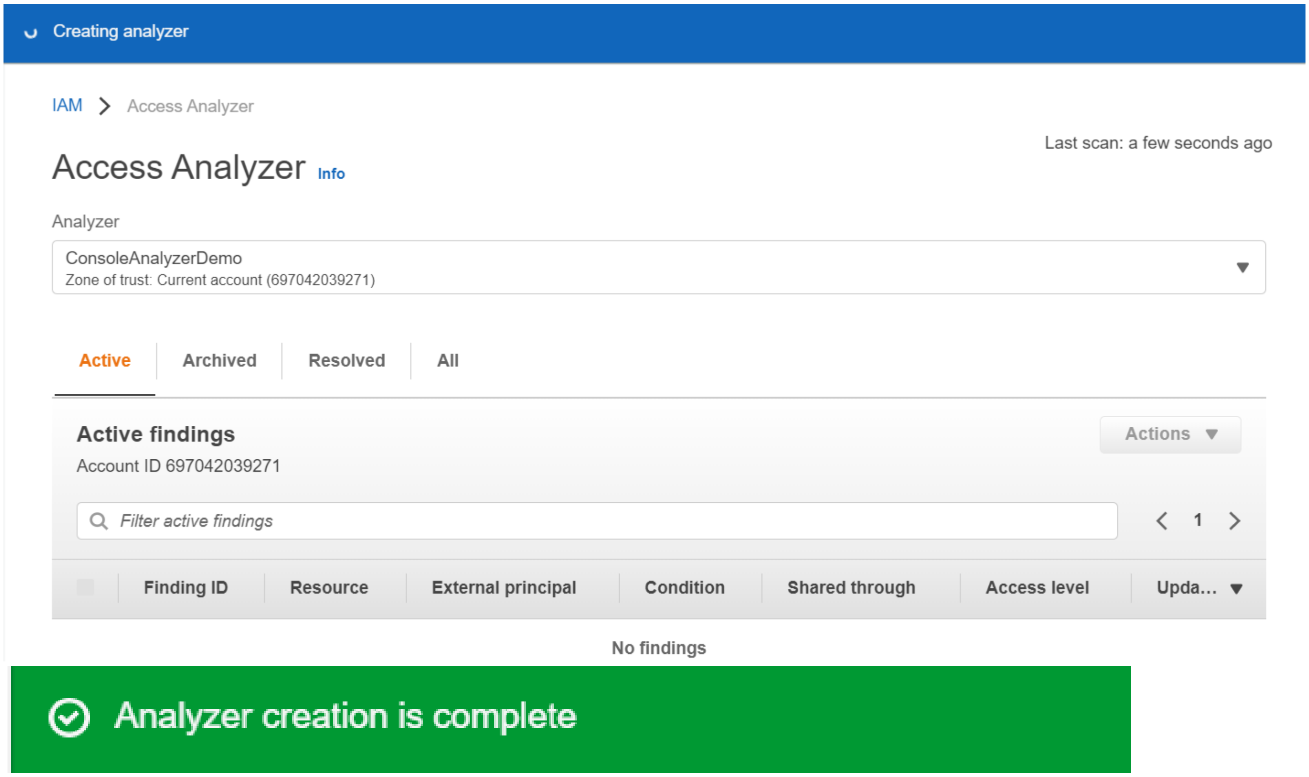
Optionally, add tags to the analyzer. Tags are words or phrases that act as metadata for identifying and organizing your AWS resources. Each tag consists of a key and one optional value.

No tags associated with the resource.

You can add up to 50 tags.

When you enable Access Analyzer, a service-linked role is created in the current account. The service-linked role grants permission to Access Analyzer to interact with AWS resources on your behalf. Learn more

Step 3: That’s it. The analyzer will be created, and then it starts scanning automatically



Creating analyzer

IAM > Access Analyzer

Last scan: a few seconds ago

Access Analyzer Info

Analyzer

ConsoleAnalyzerDemo
Zone of trust: Current account (697042039271)

Active findings
Account ID 697042039271

□	Finding ID	Resource	External principal	Condition	Shared through	Access level	Upda…

No findings

Analyzer creation is complete