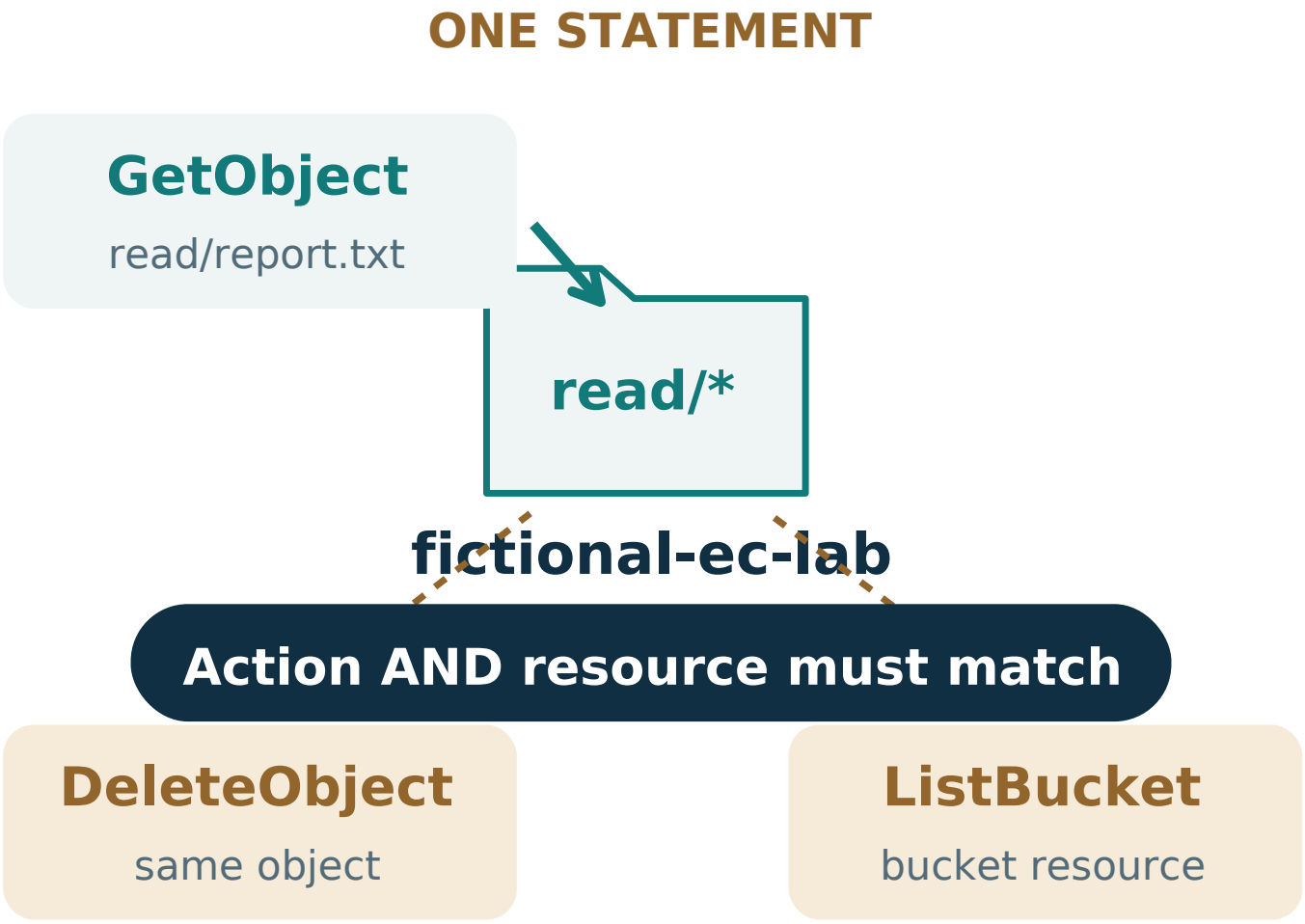
AWS-U02 / SEE THE CONCEPT

Read the policy. Trace the permission boundary.

Read the visual model, then test the reasoning.



An allow matches a specific action and resource together.

Assume this offline teaching statement applies to the requesting identity. Compare reading a matching object, deleting it and listing the bucket. Read the action and resource together.

AWS-U02 / WORK THE CASE

Read the policy. Trace the permission boundary.

Follow the stated conditions. Check the answer against the original case.

```
{ "Effect": "Allow",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::fictional-ec-lab/read/*" }
```

GET OBJECT	DELETE OBJECT	LIST BUCKET
read/report.txt	read/report.txt	Bucket-level scope
Supplies an allow*	Different action	Not supplied here

1 MATCH BOTH FIELDS

GetObject on read/report.txt matches the stated action and object prefix. This statement supplies an allow.

2 KEEP THE BOUNDARY

DeleteObject is another action. ListBucket also uses a bucket-level resource. Neither permission is supplied by this statement.

3 TEST THE REAL CONTEXT

In an authorized environment, use the actual identity and policy context to verify required and forbidden operations. Inspect applicable denies before adding broad access.

TEST YOUR REASONING

Can this one matching allow prove effective permission?

No. Other applicable policy controls and conditions still matter. An applicable explicit deny can override the allow.

Authentication alone is not universal authorization. This illustrative statement is not a complete production policy; the example creates no cloud resources.