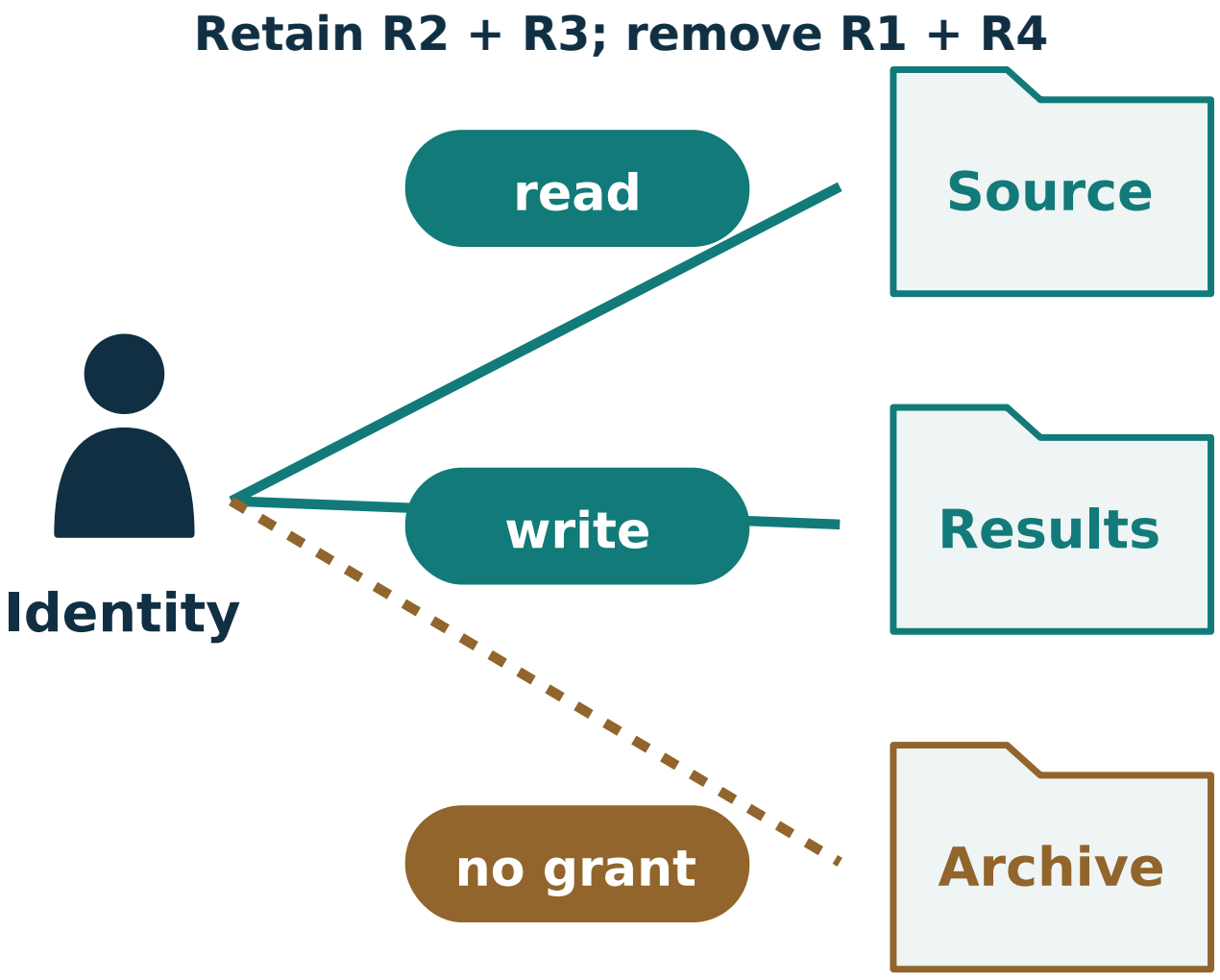
AZ-U09 / SEE THE CONCEPT

A valid session. Three security jobs still remain.

Read the visual model, then test the reasoning.



Verify context, narrow the grant union and observe allowed misuse.

A fictional identity should read Source and write Results only. Its complete grants are R1: read Source/Results/Archive; R2: read Source; R3: write Results; R4: write Archive. A valid session reads Source unusually often.

AZ-U09 / WORK THE CASE

A valid session. Three security jobs still remain.

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

VERIFY	LIMIT	OBSERVE
Identity / device / request	Approved actions and scope	Misuse of successful actions

BEFORE / R1 + R2 + R3 + R4	AFTER / KEEP R2 + R3
READ: Source, Results, Archive	READ: Source
WRITE: Results, Archive	WRITE: Results

1 VERIFY EXPLICITLY

Evaluate relevant identity, device and request context. A private address or successful earlier sign-in does not certify every later action.

2 KEEP THE NARROW UNION

Through the authorized process, remove surplus R1/R4 and retain R2/R3. Adding another narrow role does not cancel an existing broad grant.

3 OBSERVE ALLOWED MISUSE

Denial-only logs miss unusually frequent successful reads. Collect scoped successful data-operation evidence and assess the defined behavior condition.

TEST YOUR REASONING

Does successful sign-in show the frequency of later document reads?

No. Session verification and data-operation behavior answer different evidence questions. Test both permitted and prohibited operations after correction.

No other grants or denies apply in this closed teaching model. These custom sets are not Azure built-in role definitions. No tenant access or alert is configured.