Terraform from modules to security gate

DevOps & infrastructure | Advanced

Session M4-02 | 2 hours 30 minutes

Agenda

Time	Topic
0:00 to 0:08	Architecture and project model
0:08 to 0:20	Module contracts
0:20 to 0:32	Root composition
0:32 to 0:44	Staged validation
0:44 to 0:54	Security failure
0:54 to 1:00	Bicep comparison and lab handoff

Terraform is required

Use Terraform for the lab:

```
architecture → modules → root composition → format → init → validate → security gate
```

Bicep appears as a prepared comparison. Learners do not build both projects.

Modules define contracts

Module	Consumes	Exposes
Network	CIDR and names	VPC and subnet IDs
Compute	VPC and subnet IDs	Load balancer DNS and app security group
Database	Private subnets and app security group	Database endpoint

Keep secrets in sensitive inputs. Do not copy values between layers.

Prompt from fixed constraints

```
Complete the network, compute, and database module contracts. Pass values through
typed variables and outputs. Keep the database password sensitive. Do not add
credentials, a backend, plan, or apply command.
```

Use the architecture to set the boundaries before Copilot drafts the files.

Validate in stages

```
terraform fmt -check -recursive
terraform init -backend=false
terraform validate
```

Fix the first failure before moving on. Each stage answers a different question.

What local validation does not prove

It does not check:

- the current cloud state;
- organization policy;
- quota or regional availability;
- the effect of an apply.

A reviewed plan needs an approved identity and target environment.

One intentional security failure

```
bash lab/starter/check-security.sh lab/starter/insecure-iac/main.tf
```

The gate must fail. Inspect the cited lines, repair the file, and check that the rerun passes.

Bicep is a comparison

Show:

- module inputs and outputs;
- `@secure()` parameters;
- `az bicep build`;
- the same human review boundary.

Six minutes. No second required build.

Lab

Complete Terraform, validate each stage, and repair the security-gate failure.