

- Secret management tools
- Secret management tools with Terraform

Secret Management Basics

The first rule of secrets management is:

Do not store secrets in plain text.

The second rule of secrets management is:

DO NOT STORE SECRETS IN PLAIN TEXT.

Seriously, don't do it. For example, do *not* hardcode your database credentials directly in your Terraform code and check it into version control:

```
resource "aws_db_instance" "example" {
  identifier_prefix      = "terraform-up-and-running"
  engine                 = "mysql"
  allocated_storage       = 10
  instance_class          = "db.t2.micro"
  skip_final_snapshot     = true
  db_name                = var.db_name

  # DO NOT DO THIS!!!
  username = "admin"
  password = "password"
  # DO NOT DO THIS!!!
}
```

Storing secrets in plain text in version control is a *bad idea*. Here are just a few of the reasons why:

Anyone who has access to the version control system has access to that secret.

In the preceding example, every single developer at your company who can access that Terraform code will have access to the master credentials for your database.

Every computer that has access to the version control system keeps a copy of that secret.

Every single computer that has ever checked out that repo may still have a copy of that secret on its local hard drive. That includes the computer of every developer on your team, every computer involved in CI (e.g., Jenkins, CircleCI, GitLab, etc.), every computer involved in version control (e.g., GitHub, GitLab, BitBucket), every computer involved in deployment (e.g., all your pre-prod and prod environments), every computer involved in backup (e.g., CrashPlan, Time Machine, etc.), and so on.

Every piece of software you run has access to that secret.

Because the secrets are sitting in plain text on so many hard drives, every single piece of software running on any of those computers can potentially read that secret.

There's no way to audit or revoke access to that secret.

When secrets are sitting on hundreds of hard drives in plain text, you have no way to know who accessed them (there's no audit log) and no easy way to revoke access.

In short, if you store secrets in plain text, you are giving malicious actors (e.g., hackers, competitors, disgruntled former employees) countless ways to access your company's most sensitive data—e.g., by compromising the version control system, or by compromising any of the computers you use, or by compromising any piece of software on any of those computers—and you'll have no idea if you were compromised or have any easy way to fix things if you were.

Therefore, it's essential that you use a proper *secret management tool* to store your secrets.