# &
# Automation

# Why?

- Old days
- API keys/Tokens
- Secrets and developers
  - Developers tend to deal with secrets loosely
  - Lastpass story
- Code repos
  - Check in code to repos with secrets in it, mostly by mistake
  - Never embed secrets directly into scripts/programs as a best practice

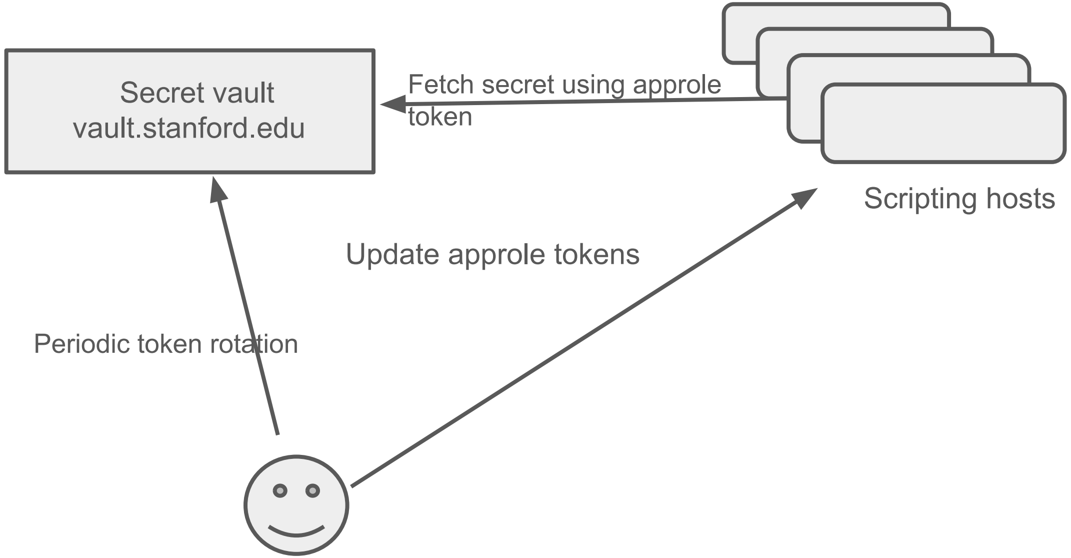
# Provisioning Secrets - Best Practices

- When creating api tokens use the minimum privileges needed
  - Use proper scopes and roles
- When there are many programs/scripts accessing resources, provision a key for each program/script with just the access needed for that application
- Lifecycle management
  - You can setup auto-expiration, but this might be problematic
  - In cases like JWT the primary token is used to issue a time-bound temp. Token
- Document and educate your team

# Secret Store

- Security! **Security!**
  - It is similar to putting all your keys in one lockbox
- Able to add and update secrets easily and securely
- Able to fetch secrets easily and securely
- Conducive to automation
- Able to enforce policies

# Security Operations’ Previous Architecture



Secret vault
vault.stanford.edu

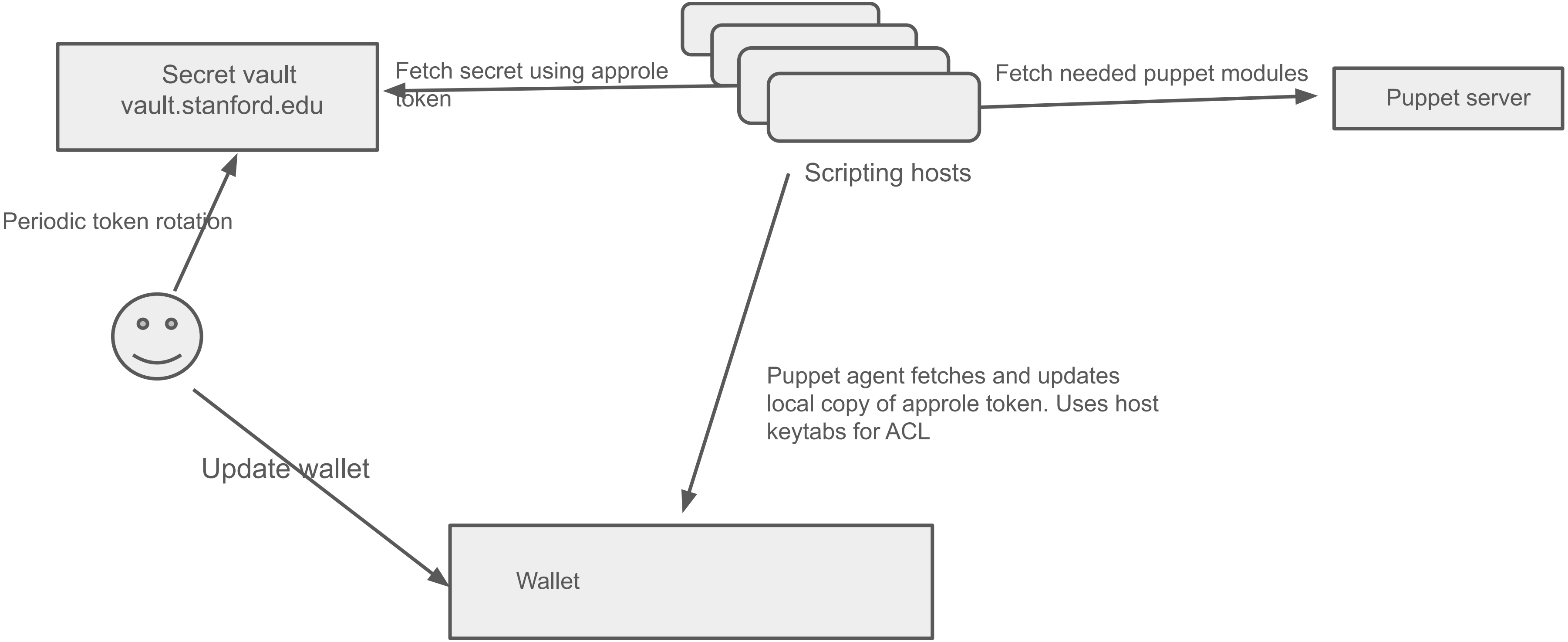
Fetch secret using approle token

Scripting hosts

Update approle tokens

Periodic token rotation

# Security Operations’ Current Architecture



Secret vault
vault.stanford.edu

Fetch secret using approle token

Scripting hosts

Fetch needed puppet modules

Puppet server

Periodic token rotation

Puppet agent fetches and updates local copy of approle token. Uses host keytabs for ACL

Update wallet

Wallet

# Security Operations - Next Steps

- Additional access control restrictions for AppRole
  - Use IP block and/or PKI for AppRole access control