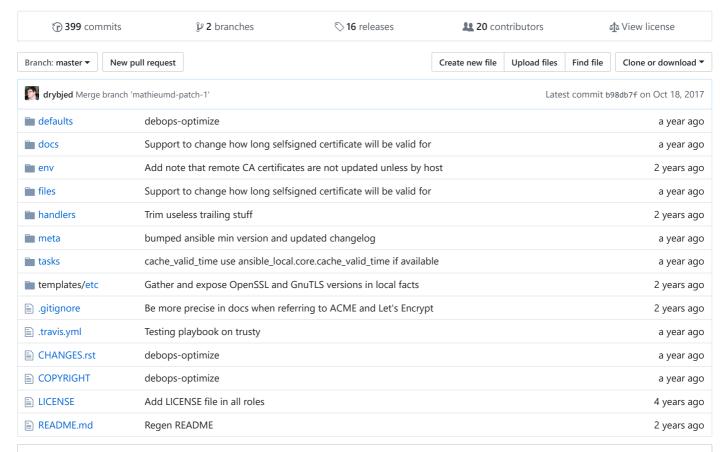
#### 📮 debops / ansible-pki

Bootstrap and manage internal PKI, Certificate Authorities and OpenSSL/GnuTLS certificates



## III README.md



# pki



The debops.pki role provides a standardized management of the X.509 certificates on hosts controlled by Ansible. Other Ansible roles can utilize the environment created by debops.pki to automatically enable TLS/SSL encrypted connections.

Using this role, you can bootstrap a Public Key Infrastructure in your environment using an internal Certificate Authority, easily switch the active set of certificates between internal and external Certificate Authorities, or use the ACME protocol to automatically obtain certificates from CA that support it (currently, Let's Encrypt).

### Installation

This role requires at least Ansible v2.0.0. To install it, run:

ansible-galaxy install debops.pki

#### **Documentation**

More information about debops.pki can be found in the official debops.pki documentation.

## Role dependencies

debops.secret

# Are you using this as a standalone role without DebOps?

You may need to include missing roles from the DebOps common playbook into your playbook.

Try DebOps now for a complete solution to run your Debian-based infrastructure.

# Authors and license

- Maciej Delmanowski (maintainer) | e-mail | Twitter | GitHub
- Robin Schneider | e-mail | Twitter | GitHub

License: GPL-3.0

This role is part of DebOps. README generated by ansigenome.