DuckCorp Infrastructure - Review #687

encrypt ansible vault password (locally)

2020-03-10 16:53 - Pierre-Louis Bonicoli

Status:	Resolved	**Start date:**	2020-03-10
Priority:	Normal		
Assignee:	Pierre-Louis Bonicoli		
Category:			
Target version:			
Branch:	duckcorp/admin:encrypt_vault_password and duckcorp/duckcorp-infra:decrypt_vault_password		

Description

1. duckcorp/admin:encrypt_vault_password branch: encrypt Ansible Vault password
2. duckcorp/duckcorp-infra:decrypt_vault_password branch: decrypt Ansible Vault password when needed

History

#1 - 2020-03-10 16:54 - Pierre-Louis Bonicoli

- Description updated

- Status changed from New to In Progress

#2 - 2020-03-12 17:19 - Marc Dequènes

Quack,

I tested the use of ansible-playbook and it work fine. The setup too is very easy. Nevertheless I cannot anymor do any git show/diff/grep with automatic decryption. I suppose that the operation changes the workdir because setting ANSIBLE_VAULT_PASSWORD_FILE with the absolute path of the script solves all these problems. Thus I would be in favor of documenting this too (the setting in ansible.cfg can be kept of not, your choice).

#3 - 2020-03-21 03:00 - Pierre-Louis Bonicoli

Marc Dequènes wrote:

> Nevertheless I cannot anymor do any git show/diff/grep with automatic decryption. I suppose that the operation changes the workdir because setting ANSIBLE_VAULT_PASSWORD_FILE with the absolute path of the script solves all these problems. Thus I would be in favor of documenting this too (the setting in ansible.cfg can be kept of not, your choice).

Does that work with the Git configuration below ?

```
[diff "ansible-vault"]
    textconv = ANSIBLE_VAULT_PASSWORD_FILE=ansible/decrypt-vault-password.sh ansible-vault view
    cachetextconv = false
```

What do you prefer:
- to define ANSIBLE_VAULT_PASSWORD_FILE environment variable
- or to use the configuration above - in this case, should this configuration be commited in $GIT_DIR/config ?

#4 - 2020-03-23 08:27 - Marc Dequènes

- Assignee changed from Marc Dequènes to Pierre-Louis Bonicoli

It works.

I would like things that are mechanism and not really settings to be centralized in my ~/.gitconfig, so I prefer to set ANSIBLE_VAULT_PASSWORD_FILE (as before but different value).

The config in ansible.cfg may stay but since we have encrypted files outside ansible/ that may not be very practical in the end. If you use it yourself and are fine with it, then you can keep it.

#5 - 2020-04-08 05:46 - Marc Dequènes

Any news?
Since this is almost done, it would be nice to have it merged.

#6 - 2020-04-15 06:04 - Pierre-Louis Bonicoli

Pierre-Louis Bonicoli wrote:

> - or to use the configuration above - in this case, should this configuration be commited in $GIT_DIR/config ?

This isn't a valid option: $GIT_DIR/config is only local :)

Marc Dequènes wrote:

> I would like things that are mechanism and not really settings to be centralized in my ~/.gitconfig, so I prefer to set ANSIBLE_VAULT_PASSWORD_FILE (as before but different value).

How do you manage multiple repositories with their own Ansible vault password file ?

> The config in ansible.cfg may stay but since we have encrypted files outside ansible/ that may not be very practical in the end. If you use it yourself and are fine with it, then you can keep it.

- either ansible-vault should be called from the directory containing ansible.cfg
- or ANSIBLE_CONFIG must be defined

You could:

- define ANSIBLE_CONFIG instead of ANSIBLE_VAULT_PASSWORD_FILE
- keep your centralized configuration in ~/.gitconfig unchanged (without ANSIBLE_CONFIG nor ANSIBLE_VAULT_PASSWORD_FILE)
  What do you think ?

Commit has been updated with this change:

```
diff --git a/README.md b/README.md
index dbc4e03..32b585e 100644
--- a/README.md
+++ b/README.md
@@ -59,8 +59,12 @@ Your configuration needs to be enhanced to tel git how to handle these files. Th

 : https://github.com/building5/ansible-vault-tools

+Because `ansible-vault` is called at the top level directory of the repository, this setup requires to define either `ANSIBLE_VAULT_PASSWORD_FILE` or `ANSIBLE_CONFIG` environment variable (otherwise `ansible-vault` would not know the path of the ansible vault password file).
+
 #### Ansible Vault Password

+The Ansible Vault Password is encrypted with GPG.
+
 The path of the Ansible Vault Password is stored in Git configuration and must be defined using the following
 command:

     git config --local --add --path duckcorp.encrypted-vault-password /path/to/encrypted/ansible/vault/password.asc
```

#7 - 2020-04-17 09:29 - Marc Dequènes

- Status changed from In Progress to Resolved

Pierre-Louis Bonicoli wrote:

> How do you manage multiple repositories with their own Ansible vault password file ?

I had to manually set ANSIBLE_VAULT_PASSWORD_FILE for each one specifically, but I kept them closeby so I could use the history and adapt quickly. Then I keep the term dedicated to a specific repo. Not the best but not too complicated either.

> You could:
>
> - define ANSIBLE_CONFIG instead of ANSIBLE_VAULT_PASSWORD_FILE
> - keep your centralized configuration in ~/.gitconfig unchanged (without ANSIBLE_CONFIG nor ANSIBLE_VAULT_PASSWORD_FILE)
>   What do you think ?

I just tested setting ANSIBLE_CONFIG instead of ANSIBLE_VAULT_PASSWORD_FILE and tested the magic in my ~/.gitconfig and it worked fine. The good thing is it is trivial to set and the same for all repos, so very convenient.

> Commit has been updated with this change:

All fine.

Merged.