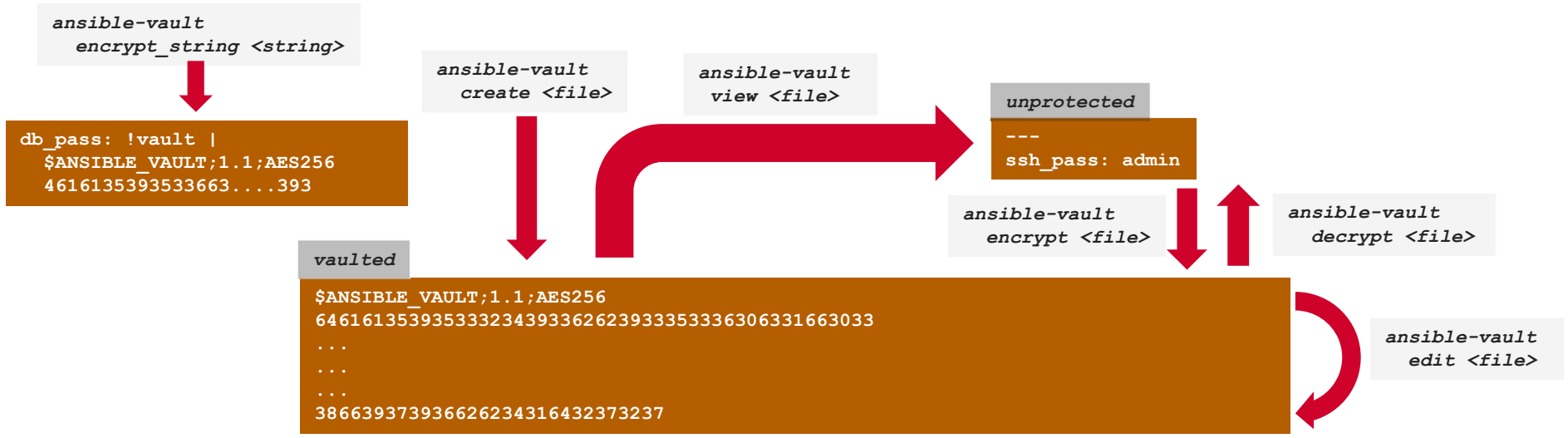
ANSIBLE VAULT
PRESENTATION

- Les vaults (coffres-forts) sont des fichiers chiffrés de variables protégés par un mot de passe
- Ils permettent de stocker des informations sensibles
  - Mots de passe
  - Clés privées
  - Tokens
- Ils sont manipulés à l'aide des commandes ansible-vault

Si votre playbook utilise plusieurs vaults, utilisez l'option --vault-id



Pour aller plus loin : https://docs.ansible.com/ansible/latest/user_guide/vault.html

ANSIBLE VAULT
VAULT ID

A noter : plusieurs vault id peuvent être utilisés au sein d'un playbook

Code : *fichiers de password des différents vaults*

2 vaults ayant chacun leur password : un pour la bdd et un pour les certificats

```
$ echo -n bdd_vault_password > bdd_vault_password_file
$ echo -n cert_vault_password > cert_vault_password_file
```

Code : *fichier de variables non protégées*

Le password utilisé pour se connecter à la BDD

```
$ echo var_bdd_password: pA$$w0rd > bdd.yml
```

Code : chiffrement du fichier de variable avec le vault id bdd, en utilisant le password du vault contenu dans le fichier bdd_vault_password_file

A noter : si output non renseigné; bdd.yml sera chiffré

```
$ ansible-vault encrypt bdd.yml --vault-id bdd@bdd_vault_password_file --output bdd_vault.yml
```

A noter : @ précise l'emplacement du password

```
$ANSIBLE_VAULT;1.2;AES256;bdd
643236656438306566356232663533303864373464366436313933653461663630326231393065 36
...
363534383938653732356632323762393164353630343539666638393438393863 39
```

si **erreur [WARNING]: Error in vault password file loading …. If this is not a script, remove the executable bit from the file**.
Et que chmod –x ne fonctionne pas,
Remplacer le password du vault par :
#!/bin/bash
echo <password>

Pour aller plus loin : https://docs.ansible.com/ansible/latest/user_guide/vault.html

ANSIBLE VAULT
COMMANDES

- Passer un fichier vault.yml (contenant les valeurs chiffrées) en ligne de commande avec –e et --ask-vault-pass

A noter : @ précise qu'il s'agit d'un fichier

Code : *usage d'un fichier vault.yml à l'exécution d'un playbook*

```
$ ansible-playbook all –i inventories/rec site.yml -e @vault.yml --ask-vault-pass
```

- Passer un fichier vault.yml en ligne de commande avec un fichier contenant le mot de passe

Code : *usage d'un fichier vault.yml à l'exécution d'un playbook*

```
$ ansible-playbook all –i inventories/rec site.yml -e @vault.yml --vault-passworld-file .vault.pass
```

- Passer des vaults Id en ligne de commande avec des fichiers contenant le mot de passe de chaque vault

*A noter : **prompt** demandera la saisie du mot de passe pour le vault id **cert***

Code : *usage de multiples vault (id : bdd, cert) à l'exécution d'un playbook*

```
$ ansible-playbook all –i inventories/rec site.yml -vault-id bdd@rec/bdd.pwd -vault-id cert@prompt
```

*A noter : pour le vault id **bdd,** le mot de passe du vault est défini dans le **fichier rec/bdd.pwd***