Kapitel 1

Verschlüsselung mit Vault

Siehe auch unter : http://docs.ansible.com/ansible/playbooks_vault.html

1.1 Ansible-Vault

Vault (en) = Tresorraum, Gruft (de)

Ansible-Vault erstellt verschlüsselte Dateien und stellt diese entschlüsselt im Editor dar.

Die Ver- bzw. Entschlüsselung nach AES (Advanced Encryption Standard) erfordert ein Passwort (shered secret). Die Verschlüsselten Dateien können in einem VCS (Versions Controll System) aufgenommen werden.

Hinweis: Ein git diff (o.ä) funktioniert mit verschlüsselte Dateien nicht.

Das Passwort kann mit der Option `--aks-vault-pass` oder mit `--vault-password-file` abgefragt bzw. eingegeben werden.

AES

Wird hier als symetrischer 256-Bit großer Schlüssel verwendet.

1.2 Was kann Vault verschlüssen

- Variablen Dateien (z. B. `vars` und `defaults`)
- Inventory Variablen (`host_vars` und `group_vars`)
- Inkludierte Variablen (`include_vars` und `vars_files`)
- Variablen Dateien über die Kommandokonzole (-e @vars.yml oder -e @vars.json)

- Da `tasks` und `handlers` auch JSON-Daten sind könnten diese auch verschlüsselt werden

Was nicht geht: * Es kann nur die komplette Datei verschlüsselt werden, nicht Teilabschnitte aus aus einer Datei * Dateien und Vorlagen die keine JSON-Daten sind, können nicht verschlüsselt werden.

Gute Kandidaten sind: * Zugangsberechtigungen * API-Schlüssel (AWS, Azure usw.) * SSL Schlüssel * Private SSH Schlüssel

1.3 Ansible-Vault verwenden

`ansible-vault` hat Unterkommandos:

```
create      Erstellt eine verschlüsselte Datei mit Hilfe des Editors
edit        Editiert (im Klartext) eine verschlüsselte Datei
encrypt     Verschlüsselt eine existierende Datei
decrypt     Entschlüsselt eine versclüsselte Datei
rekey       Erstellt einen neuen Schlüssel
```

1.4 Verschlüsseln

```
# setting up vi as editor
$ export EDITOR=vi
# Generate a encrypted file
$ ansible-vault create aws_creds.yml
Vault password:
Confirm Vault password:
```

Der Editor vi wird geöffnet. Die Datei aws_creds.yml kann erstellt werden. Nach dem Speichern wird diese verschlüsselt.

1.5 Arbeiten mit verschlüsselten Dateien

```
$ ansible-vault edit aws_creds.yml
Vault password:
```

Die Datei kann entschlüsselt bearbeitet werden. Nach dem Speichern liegt diese wieder verschlüsselt vor.

```
$ ansible-vault decrypt aws_creds.yml
Vault password:
Decryption successful
```

Kapitel 2

Diff

```
Binärdateien ../B03800_07_code/Cluster.md.pdf und ./Cluster.md.pdf sind
   verschieden.
diff -uNr -X diffignore ../B03800_07_code/projects/aws_creds.yml ./
   projects/aws_creds.yml
--- ../B03800_07_code/projects/aws_creds.yml    1970-01-01
   01:00:00.000000000 +0100
+++ ./projects/aws_creds.yml    2016-04-11 20:47:33.208187856 +0200
@@ -0,0 +1,10 @@
+$ANSIBLE_VAULT;1.1;AES256
+30346239616537373261633165373666386264613239643064656434333643532386435326662380

+30346232643336313364306339656566376633656639376330
   a353463326261653031613661653636
+32386266613733303936623861613731386162316435386533363633643061663730323635313630

+6166386661653434310
   a333539356139633433613532303033656430636235343932613230643765
+33356130356666663661636538306631633436366265386363373130323836316637616663303437

+35363438393862343736303734643433623432323132343566316366386561393861336562636263

+64336539393637303262643036363931356631653430663133366632653433386335616539353232

+64393166356162633732353362343263623630366337396165343135383535326230356532613463

+64613836306433633762353635616536346636646538326363376565383163666335
diff -uNr -X diffignore ../B03800_07_code/projects/group_vars/www ./
   projects/group_vars/www
--- ../B03800_07_code/projects/group_vars/www   1970-01-01
   01:00:00.000000000 +0100
+++ ./projects/group_vars/www   2016-04-11 20:47:33.208187856 +0200
@@ -0,0 +1,52 @@
+#filename : group_vars/www
+nginx_ssl_cert_content: |
+    -----BEGIN CERTIFICATE-----
```

```
+    MIIDXTCCAkWgAwIBAgIJAIMXFV1Fn3m0MA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
+    BAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
+    aWRnaXRzIFB0eSBMdGQwHhcNMTUwNTI1MTI1NzQ0WhcNMTUwNjI0MTI1NzQ0WjBF
+    MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
+    ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
+    CgKCAQEAtajLFANI/GVEkya06G6QYYFbtWG+qCV3vexV947raomNk1ee6iHktz62
+    gBv6Y8bus7l/8RPec/75cbw1PP2VyxzX7Vj4wGEU5QNvs6c3Z9tpyGyN2vqYYqPW
+    9jIlRctdGKiiASlzBoI9hK+K1L6Y0KvlmLL4z99NVI9iL9vx3mEWKZg4yuugO97a
+    498DupNN9IpvBqH/2WcZLoOZgaXq3Nk0MwiDiV4F3ZgFJGHSo0SoNllj/33Sg0Sw
+    Uxh+ysefOWg3WB3WwdeeoLGfZbC14zSM9ddFZgWamrajfN9bICYnk5Hm/jvzAiV+
+    xyaWLgR5pBHA8CIej4tfrztD3DU0kQIDAQABo1AwTjAdBgNVHQ4EFgQUgaE1tMCr
+    5XTrGsS4+awLEwQZAt8wHwYDVR0jBBgwFoAUgaE1tMCr5XTrGsS4+awLEwQZAt8w
+    DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAf8oyp2zG9qp5CB9etqsb
+    /sh1pCUvxie8ZCK2CJDC/wWacY79YSpDGP4FACYSsXkjxwUOfIzebX3lGeVuvuSp
+    cIgJrKi05xIBTgf4j/rz24+1d1S7SqqlAsCiAUXm+8Rp5xK12w9Ih/IcQtwy46Rq
+    S+4U/Bvja94Mqc8FxoMZKofsPEPn8lqfdTfwfSnOjlLR7Wx1QPCQg8OxW1yHnFG6
+    Jgc+Dt3mr0dh0TJqqIaRKd+TXgXzaMQvRj9nbfhJDE2cdObO6Ld3YKneicpcmv2S
+    r8I3DM3fhm2/4r4hvLKwPLrTeIITh1dTEvxVv5Pk488E7lFIIj2qoLbE8AIIh0hb
+    yw==
+    -----END CERTIFICATE-----
+nginx_ssl_key_content: |
+    -----BEGIN PRIVATE KEY-----
+    MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC1qMsUA0j8ZUST
+    JrTobpBhgVu1Yb6oJXe97FX3jutqiY2TV57qIeS3PraAG/pjxu6zuX/xE95z/vlx
+    vDU8/ZXLHNftWPjAYRTlA2+zpzdn22nIbI3a+phio9b2MiVFy10YqKIBKXMGgj2E
+    r4rUvpjQq+WYsvjP301Uj2Iv2/HeYRYpmDjK66A73trj3wO6k030im8Gof/ZZxku
+    g5mBperc2TQzCIOJXgXdmAUkYdKjRKg2WWP/fdKDRLBTGH7Kx585aDdYHdbB156g
+    sZ9lsLXjNIz110VmBZqatqN831sgJieTkeb+O/MCJX7HJpYuBHmkEcDwIh6Pi1+v
+    O0PcNQ6RAgMBAAECggEBAK16ENz+uh9VseP4jcB9fWGv/906B7FZfn0fiYUMteIa
+    k9nGThr23QzlVbEHhtjr6540Imsdd008jAfCHPEulXLPC6E8WuiUjTiaTHy6zh1f
+    GijtCZa5wvZH0gtwHcoGB9R5jaQgahkoHQlt/d1mWlbEIVDucM9KRvXeq3xaxSJ/
+    5bqMpg3ZOm8GHXyxQeFKxrKfOMUFRhaql18RDKzzgJxf8roIFpidw9yM6ykLisrB
+    +3XPPt5Bosby3N9gs8yIk9Zw6obiD3HdU2PxmzV0/BKXXm8ffdWdi9Mw6OopU8f8
+    KXPF0+OUv6Idzd45kQjPh/GX6w7Dmen9JWIfVKw4SRUCgYEA5m4FIrrUpC39z1CC
+    7YFgeELT2TycYwnF4lm08nSZrZtfyfLEje9uiZLDYfUzA2KPSCsqYTKl/hqTxI61
+    3KI6kt1Eeh4vz/ZCroMcUvYIadNmeAfNhCodytqS1Fj2Gvg5pQS4C5X6Vu+B9doX
+    f6lQer6VDmQS6Go1VZ973w8REeMCgYEAydFRWbNFxAjewa7DOY734A7HeAWk2lG3
+    EsV5fJJf992379x0mayNvhkUXATfYdQI4WvEq0iAzB+Ysax7heR8DAIQqmQBdoSF
+    Aj07HbgR0vp1lLmwYg6p6cmJZQvbvoVCeyNiyjeyM8A4A4ITbDpUFpVpzAYN03+a
+    hiK5bkS4d/sCgYEAiWOBtmJU1IsDcK9dUQS5oxqdO0ITME2sabf41jLFSiiApWUU
+    4lemvWn/CpHq15LVQT9TZl6PcAEip6g7MJCdgeFhqboD4ee/fFN5+NDu1UIRL3Hf
+    jHScDM3ji657Fjt4CzbUETxb5aeqAg8Fwb0O2hB1yP3L9D0XDbUoYyeVkucCgYAb
+    ZQ5l3q/ZrFqQb+iQJ5f+EgOBh0KZX/45zhRvlG7ydmZBaOtq8MFMzJq24vJvlRif
+    gMFxfqX9D0zq0T7zLdCo0J7ygiCwtcxYQXeE0TeaK+VKCuqmZNcrpO/Bh5qMggpE
+    LMl8KZNG8xCnaUC5sDE5344845V84BVZn90L2sgvgQKBgBitO1pSdH9ioeeD65Jp
+    1ER4zZkBzGpRXEmAo50DVes/na6hk1jMAH4xlDLgN8eXsCGwEFPxwT9QAiI77aJF
+    BDSO4X6GfCO2kq3LQSoTLCTp/8SbOYU4yBJmzAaqHX4TD+ZtuwiOeU9oEu18KScE
+    jzIlLZXpcVhv5QIzKDH30jTU
+    -----END PRIVATE KEY-----
\ Kein Zeilenumbruch am Dateiende.
```

```
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/defaults/
   main.yaml ./projects/roles/nginx/defaults/main.yaml
--- ../B03800_07_code/projects/roles/nginx/defaults/main.yaml
   2016-04-11 20:47:33.212187857 +0200
+++ ./projects/roles/nginx/defaults/main.yaml   2016-04-11
   20:47:33.204187856 +0200
@@ -3,3 +3,8 @@
 nginx_port: 80
 nginx_root: /usr/share/nginx/html
 nginx_index: index.html
+nginx_ssl: true
+nginx_port_ssl: 443
+nginx_ssl_path: /etc/nginx/ssl
+nginx_ssl_cert_file: nginx.crt
+nginx_ssl_key_file: nginx.key
\ Kein Zeilenumbruch am Dateiende.
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/tasks/
   configure_ssl.yml ./projects/roles/nginx/tasks/configure_ssl.yml
--- ../B03800_07_code/projects/roles/nginx/tasks/configure_ssl.yml
   1970-01-01 01:00:00.000000000 +0100
+++ ./projects/roles/nginx/tasks/configure_ssl.yml  2016-04-11
   20:47:33.200187856 +0200
@@ -0,0 +1,15 @@
+---
+# filename: roles/nginx/tasks/configure_ssl.yml
+ - name: create ssl directory
+   file: path="{{ nginx_ssl_path }}" state=directory owner=root group=
   root
+
+ - name: add ssl key
+   template: src=nginx.key.j2 dest="{{ nginx_ssl_path }}/nginx.key"
   mode=0644
+
+ - name: add ssl cert
+   template: src=nginx.crt.j2 dest="{{ nginx_ssl_path }}/nginx.crt"
   mode=0644
+
+ - name: create ssl site configurations
+   template: src=default_ssl.conf.j2 dest=/etc/nginx/conf.d/default_ssl
   .conf mode=0644
+   notify:
+    - restart nginx service
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/tasks/
   main.yml ./projects/roles/nginx/tasks/main.yml
--- ../B03800_07_code/projects/roles/nginx/tasks/main.yml   2016-04-11
   20:47:33.212187857 +0200
+++ ./projects/roles/nginx/tasks/main.yml   2016-04-11
   20:47:33.200187856 +0200
@@ -2,4 +2,6 @@
 # This is main tasks file for nginx role
  - include: install.yml
```

```
  - include: configure.yml
+ - include: configure_ssl.yml
+   when: nginx_ssl
  - include: service.yml
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/templates
   /default_ssl.conf.j2 ./projects/roles/nginx/templates/default_ssl.
   conf.j2
--- ../B03800_07_code/projects/roles/nginx/templates/default_ssl.conf.j2
      1970-01-01 01:00:00.000000000 +0100
+++ ./projects/roles/nginx/templates/default_ssl.conf.j2    2016-04-11
   20:47:33.200187856 +0200
@@ -0,0 +1,12 @@
+server {
+    listen       {{ nginx_port_ssl }};
+    server_name  {{ ansible_hostname }};
+    ssl    on;
+    ssl_certificate      {{ nginx_ssl_path }}/{{ nginx_ssl_cert_file
   }};
+    ssl_certificate_key  {{ nginx_ssl_path }}/{{ nginx_ssl_key_file }};
+
+    location / {
+        root   {{ nginx_root }};
+        index  {{ nginx_index }};
+    }
+}
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/templates
   /nginx.crt.j2 ./projects/roles/nginx/templates/nginx.crt.j2
--- ../B03800_07_code/projects/roles/nginx/templates/nginx.crt.j2
   1970-01-01 01:00:00.000000000 +0100
+++ ./projects/roles/nginx/templates/nginx.crt.j2   2016-04-11
   20:47:33.200187856 +0200
@@ -0,0 +1 @@
+{{ nginx_ssl_cert_content }}
diff -uNr -X diffignore ../B03800_07_code/projects/roles/nginx/templates
   /nginx.key.j2 ./projects/roles/nginx/templates/nginx.key.j2
--- ../B03800_07_code/projects/roles/nginx/templates/nginx.key.j2
   1970-01-01 01:00:00.000000000 +0100
+++ ./projects/roles/nginx/templates/nginx.key.j2   2016-04-11
   20:47:33.200187856 +0200
@@ -0,0 +1 @@
+{{ nginx_ssl_key_content }}
diff -uNr -X diffignore ../B03800_07_code/projects/test/vars.yml ./
   projects/test/vars.yml
--- ../B03800_07_code/projects/test/vars.yml    1970-01-01
   01:00:00.000000000 +0100
+++ ./projects/test/vars.yml    2016-04-11 20:47:33.196187856 +0200
@@ -0,0 +1,4 @@
+---
+demo:
+  pass: supersecret
+
```