

Projet : Document d'Architecture Technique (DAT) Portail d'Accès Zero Trust Access d'une Entreprise

PKI- IAM - Cryptographie

Réalisé par :

Joseline YOUEGO

Table des matières

1 Description du projet	3
1.1 Scénario fonctionnel du projet SecureCorp Zero Trust	3
1.1.1 Objectif général	3
1.1.2 Principes de sécurité appliqués	3
1.1.3 Rôle des machines virtuelles dans le scénario	4
1.1.4 Parcours utilisateur : du navigateur à l'application	5
1.1.5 Lien avec la méthodologie et l'état d'avancement	6
1.2 Déploiement de l'infrastructure virtuelle	7
1.2.1 Lancement des machines avec <code>vagrant up</code>	7
1.2.2 Vérification de l'état des machines avec <code>vagrant status</code>	7
1.2.3 Connexion SSH à la machine <code>sec-core</code>	8
1.3 Phase 1 : Mise en place du coeur de sécurité sur <code>srv-sec-core</code>	8
1.3.1 Installation de HashiCorp Vault	8
1.3.2 Configuration de Vault en service <code>systemd</code>	9
1.3.3 Préparation de l'environnement et installation de <code>jq</code>	10
1.3.4 Mise en place de la PKI à deux niveaux	11
1.3.5 Bilan de la phase 1	14
1.4 Phase 2 : Mise en place de l'Identity Provider (Keycloak) intégré à Vault .	15
1.4.1 Préparation de l'environnement : Java 17 et PostgreSQL	15
1.4.2 Configuration de Vault comme gestionnaire d'identifiants PostgreSQL	16
1.4.3 Installation de Keycloak en mode binaire	18
1.4.4 Script de démarrage intégré à Vault	19
1.4.5 Intégration dans <code>systemd</code> : service Keycloak	21
1.4.6 Incident : erreur interne Keycloak et diagnostic	21
1.4.7 Accès local requis et mise en place d'un tunnel SSH	23
1.4.8 Vérification côté PostgreSQL : création automatique des rôles . .	26
1.4.9 Bilan de la phase 2	26
1.4.10 Résolution critique : Droits PostgreSQL et redémarrage propre . .	26
1.5 Phase 3 : Exposition via la Gateway et résolution des erreurs 502	27
1.5.1 Incident : Erreur 502 Bad Gateway persistante	27
1.6 Phase 4 : Intégration OIDC et Finalisation	29
1.6.1 Correction de l'URI de redirection	29
1.6.2 Stabilisation de la session et succès final	29
1.6.3 Résultat	29

2 Activation du MFA	31
2.1 Configuration de la politique d'accès	31
2.1.1 Accès sécurisé à la console d'administration et activation du MFA .	31
2.1.2 Activation de l'OTP dans le realm SecureCorp	33
2.2 Expérience utilisateur et enrôlement	36
3 Annexes - scripts	38
3.1 VagrantFile pour l'installation de l'infrastructure	38
3.1.1 Script de provisioning commun	40
3.1.2 Définition des machines virtuelles	40
3.2 Script de l'application Flask (Portail SecureCorp)	41
3.3 Configuration Nginx	43
3.4 Script de démarrage Keycloak avec secrets Vault	45
3.5 Extrait de configuration PostgreSQL (<code>pg_hba.conf</code>)	46
3.6 Script de démarrage Keycloak (<code>start_with_vault.sh</code>)	47

1 Description du projet

1.1 Scénario fonctionnel du projet SecureCorp Zero Trust

1.1.1 Objectif général

L'objectif de ce projet est de construire une preuve de concept (*Proof of Concept*, POC) démontrant la maîtrise d'une architecture de sécurité moderne dite Zero Trust. Il ne s'agit pas uniquement d'installer des composants techniques (Vault, Keycloak, Nginx), mais de montrer leur intégration cohérente dans une chaîne de confiance complète, automatisée et documentée.

Le projet se déroule dans un contexte fictif : l'entreprise **SecureCorp**. Cette entreprise dispose d'une application interne sensible (un portail employé), utilisée aussi bien au bureau qu'en télétravail.

Problématique de départ. Historiquement, l'application était accessible uniquement sur le réseau interne, avec une gestion locale des comptes utilisateurs et des mots de passe, sans chiffrement systématique des communications. Cette situation n'est plus acceptable au regard des exigences de sécurité actuelles.

En tant qu'ingénieur sécurité de SecureCorp, la mission est la suivante :

- permettre aux employés d'accéder au portail depuis l'extérieur (télétravail, mobilité);
- supprimer les logins locaux dans l'application au profit d'une authentification centralisée;
- chiffrer l'ensemble des communications;
- appliquer le principe du moindre privilège pour la gestion des secrets (notamment les accès à la base de données).

1.1.2 Principes de sécurité appliqués

Trois règles d'or structurent l'architecture cible :

1. **Nul ne passe sans identité (IAM).** L'application métier ne gère plus directement les mots de passe. Toute authentification passe par un fournisseur d'identité

centralisé (Keycloak), via un protocole standard (OIDC / OAuth2). L'application délègue la vérification de l'identité et ne reçoit que des jetons.

2. Chiffrement partout (PKI). Les communications entre les différents composants sont systématiquement chiffrées. Une PKI interne basée sur Vault émet les certificats utilisés pour :

- l'exposition HTTPS du portail via la passerelle (Nginx) ;
- les échanges internes entre services, à terme en *mutual TLS* (mTLS).

3. Moindre privilège et secrets dynamiques. Les secrets sensibles (en particulier les identifiants de base de données de Keycloak) ne sont pas stockés en clair dans des fichiers de configuration. Ils sont générés à la demande par Vault (moteur **database**), avec un TTL limité. Keycloak ne connaît donc ses identifiants que lors du démarrage, et ceux-ci expirent automatiquement.

1.1.3 Rôle des machines virtuelles dans le scénario

L'architecture réseau décrite par la figure suivante

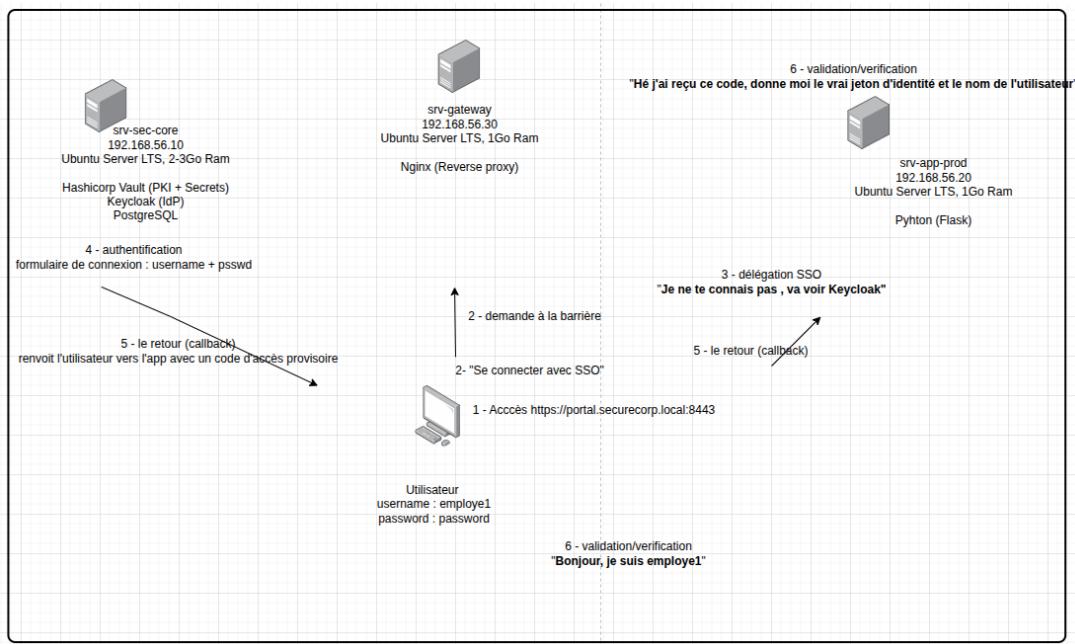


Figure 1.1: Architecture de l'infrastructure

est complétée par un scénario fonctionnel réparti sur trois machines virtuelles principales :

1. **srv-sec-core – le coffre-fort de SecureCorp (192.168.56.10).**

- HashiCorp Vault :

- joue le rôle d’Autorité de Certification (Root CA et Intermediate CA) pour l’émission de certificats internes ;
- fournit des secrets dynamiques pour PostgreSQL via le moteur **database** (création d’utilisateurs temporaires pour Keycloak).

- **Keycloak :**

- centralise la gestion des identités et des rôles ;
- authentifie les utilisateurs du portail et fournit des jetons OIDC à l’application.

2. srv-gateway – la forteresse exposée (192.168.56.30). Il Héberge un reverse proxy **Nginx** qui constitue l’unique point d’entrée depuis l’extérieur; il termine également les connexions HTTPS (certificats internes émis par la PKI Vault) et enfin redirige les requêtes vers les services internes :

- le portail applicatif sur **srv-app-prod** ;
- l’interface Keycloak sur **srv-sec-core**.

3. srv-app-prod – l’application métier (192.168.56.20).

Il héberge le **portail employé** (application Python (flask) / Gunicorn) et ne gère pas directement l’authentification :

- lorsqu’un utilisateur souhaite se connecter, l’application le redirige vers Keycloak ;
- après authentification réussie, l’application reçoit un code d’autorisation puis un jeton, qu’elle valide avant d’ouvrir une session.

1.1.4 Parcours utilisateur : du navigateur à l’application

Le scénario utilisateur complet peut être résumé ainsi :

1. Accès initial au portail. Depuis son poste, un employé saisit l’URL du portail interne dans son navigateur :

`https://portal.securecorp.local`

La requête atteint la passerelle **srv-gateway**, qui présente un certificat interne émis par la PKI. Le navigateur affiche éventuellement un avertissement de certificat autosigné, normal dans le cadre du laboratoire.

2. Demande de connexion. Sur la page d’accueil du portail, l’utilisateur clique sur un bouton Se connecter via SSO. L’application ne lui demande pas de mot de passe local ; elle déclenche un flux OIDC.

3. **Redirection vers l'Identity Provider.** Le reverse proxy redirige l'utilisateur vers Keycloak sur `srv-sec-core`. Le navigateur affiche alors la page de login fournie par Keycloak (realm SecureCorp).
4. **Authentification centralisée.** L'utilisateur saisit ses identifiants sur l'interface Keycloak. Keycloak vérifie ces informations, éventuellement avec un second facteur (MFA) dans une extension future du projet.
5. **Retour vers le portail avec un code.** En cas de succès, Keycloak redirige le navigateur vers le portail avec un *code d'autorisation* (flux OAuth2 / OIDC de type authorization code).
6. **Échange de code contre un jeton.** De manière transparente pour l'utilisateur, le portail contacte ensuite Keycloak en arrière-plan pour échanger ce code contre :
 - un *ID Token* (identité de l'utilisateur) ;
 - un *Access Token* éventuellement utilisé pour des appels API.

L'application vérifie la signature et les informations du jeton (audience, date d'expiration, rôles).

7. **Ouverture de session applicative.** Si le jeton est valide, l'application considère l'utilisateur comme authentifié et ouvre une session. Les pages protégées du portail sont alors accessibles, avec un affichage conditionnel en fonction des rôles (par exemple `ROLE_USER` vs `ROLE_ADMIN`).

1.1.5 Lien avec la méthodologie et l'état d'avancement

La section *Méthodologie utilisée* décrit comment cette infrastructure a été mise en place de manière reproductible à l'aide de Vagrant et d'Ansible (Infrastructure as Code). Ce scénario fonctionnel sert de fil conducteur aux différentes phases techniques décrites dans le mémoire :

- Phase 1 : mise en place du cœur de sécurité (`srv-sec-core`) avec Vault en tant que PKI et gestionnaire de secrets dynamiques ;
- Phase 2 : installation et intégration de Keycloak avec Vault et PostgreSQL ;
- Phases suivantes : configuration de la passerelle `srv-gateway`, sécurisation des flux en HTTPS et intégration OIDC dans l'application sur `srv-app-prod`.

Certaines étapes, comme l'échange final du code d'autorisation contre un jeton (et les erreurs 502 éventuellement rencontrées dans les premières intégrations), sont précisément le reflet de la complexité réelle de ce type d'architecture. Elles sont documentées dans les chapitres techniques et, le cas échéant, dans un *post-mortem* détaillé, afin de montrer la démarche de diagnostic et de correction adoptée.

1.2 Déploiement de l'infrastructure virtuelle

1.2.1 Lancement des machines avec vagrant up

Après avoir placé le fichier `Vagrantfile` à la racine du projet, nous lançons l'infrastructure avec la commande suivante :

```
vagrant up
```

La figure 1.2 montre la sortie de cette commande, avec le téléchargement de l'image Ubuntu et la création des trois machines virtuelles.

```
joseline@joseline-Precision-3581:~/Documents/stage_iliadata/code/projet_pki_iam_crypto/iac$ vagrant up
Bringing machine 'sec-core' up with 'virtualbox' provider...
Bringing machine 'app-prod' up with 'virtualbox' provider...
Bringing machine 'gateway' up with 'virtualbox' provider...
=> sec-core: Box 'bento/ubuntu-22.04' could not be found. Attempting to find and install...
    sec-core: Box Provider: virtualbox
    sec-core: Box Version: >= 0
=> sec-core: Loading metadata for box 'bento/ubuntu-22.04'
    sec-core: Adding box 'bento/ubuntu-22.04' (v202510.26.0) for provider: virtualbox (amd64)
      sec-core: Downloading: https://vagrantcloud.com/bento/boxes/ubuntu-22.04/versions/202510.26.0/providers/virtualbox/amd64/vagrant.box
Progress: 12% (Rate: 33.1M/s, Estimated time remaining: 0:00:32)Progress: 20% (Rate: 31.7M/s, Estimated time remaining: 0:00:32)Progress: 20% (Rate: 31.7M/s, Estimated time remaining: 0:00:32)Progress: 20% (Rate: 31.7M/s, Estimated time remaining: 0:00:32)Progress: 22% (Rate: 28.6M/s, Estimated time remaining: 0:00:28)Progress: 25% (Rate: 26.7M/s, Estimated time remaining: 0:00:27)Progress: 29% (Rate: 26.8M/s, Estimated time remaining: 0:00:25)Progress: 32% (Rate: 25.9M/s, Estimated time remaining: 0:00:23)Progress: 35% (Rate: 24.6M/s, Estimated time remaining: 0:00:22)Progress: 39% (Rate: 26.8M/s, Estimated time remaining: 0:00:20)Progress: 42% (Rate: 26.9M/s, Estimated time remaining: 0:00:19)Progress: 46% (Rate: 26.7M/s, Estimated time remaining: 0:00:18)Progress: 49% (Rate: 27.2M/s, Estimated time remaining: 0:00:16)Progress: 53% (Rate: 29.8M/s, Estimated time remaining: 0:00:15)Progress: 57% (Rate: 28.9M/s, Estimated time remaining: 0:00:14)Progress: 61% (Rate: 29.4M/s, Estimated time remaining: 0:00:12)Progress: 68% (Rate: 29.6M/s, Estimated time remaining: 0:00:10)Progress: 71% (Rate: 28.7M/s, Estimated time remaining: 0:00:09)Progress: 75% (Rate: 29.2M/s, Estimated time remaining: 0:00:07)Progress: 79% (Rate: 29.2M/s, Estimated time remaining: 0:00:06)Progress: 83% (Rate: 31.8M/s, Estimated time remaining: 0:00:05)Progress: 87% (Rate: 30.6M/s, Estimated time remaining: 0:00:04)Progress: 91% (Rate: 30.5M/s, Estimated time remaining: 0:00:02)Progress: 94% (Rate: 30.2M/s, Estimated time remaining: 0:00:01)Progress: 98% (Rate: 30.4M/s, Estimated time remaining: 0:-:-=> sec-core: Successfully added box 'bento/ubuntu-22.04' (v202510.26.0) for 'virtualbox' (amd64)
=> sec-core: Importing base box 'bento/ubuntu-22.04'...
=> sec-core: Matching MAC address for NAT networking...
=> sec-core: Checking if box 'bento/ubuntu-22.04' version '202510.26.0' is up to date...
=> sec-core: Setting the name of the VM: SecureCorp-Sec-Core
=> sec-core: Clearing any previously set network interfaces...
=> sec-core: Preparing network interfaces based on configuration...
    sec-core: Adapter 1: nat
    sec-core: Adapter 2: hostonly
=> sec-core: Forwarding ports...
    sec-core: 22 (guest) => 2222 (host) (adapter 1)
=> sec-core: Running 'pre-boot' VM customizations...
=> sec-core: Booting VM...
=> sec-core: Waiting for machine to boot. This may take a few minutes...
```

Figure 1.2: Exécution de la commande `vagrant up` et création des VMs.

1.2.2 Vérification de l'état des machines avec vagrant status

Une fois le déploiement terminé, nous vérifions l'état des machines avec :

```
vagrant status
```

La figure 1.3 confirme que les trois machines `sec-core`, `app-prod` et `gateway` sont en état `running`.

```
vagrant@srv-sec-core:~$ exit
logout
joseline@joseline-Precision-3581:~/Documents/stage_iliadata/code/projet_pki_iam_crypto/iac$ vagrant status
Current machine states:

  sec-core           running (virtualbox)
  app-prod          running (virtualbox)
  gateway           running (virtualbox)

This environment represents multiple VMs. The VMs are all listed
above with their current state. For more information about a specific
joseline@joseline-Precision-3581:~/Documents/stage_iliadata/code/projet_pki_iam_crypto/iac$ 
```

Figure 1.3: Vérification de l'état des VMs avec `vagrant status`.

1.2.3 Connexion SSH à la machine sec-core

Pour vérifier la connectivité et la configuration réseau, nous nous connectons à la machine **sec-core** :

```
vagrant ssh sec-core
```

Puis nous testons la résolution de noms avec un ping vers la gateway :

```
ping srv-gateway
```

La figure 1.4 illustre la session SSH et le succès du ping vers **srv-gateway**, preuve que le DNS local (`/etc/hosts`) est correctement configuré.

```
vagrant@srv-sec-core:~$ ping srv-gateway
PING srv-gateway.securecorp.local (192.168.56.30) 56(84) bytes of data.
64 bytes from srv-gateway.securecorp.local (192.168.56.30): icmp_seq=1 ttl=64 time=1.88 ms
64 bytes from srv-gateway.securecorp.local (192.168.56.30): icmp_seq=2 ttl=64 time=1.69 ms
64 bytes from srv-gateway.securecorp.local (192.168.56.30): icmp_seq=3 ttl=64 time=1.74 ms
64 bytes from srv-gateway.securecorp.local (192.168.56.30): icmp_seq=4 ttl=64 time=1.82 ms
^C
--- srv-gateway.securecorp.local ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.690/1.782/1.883/0.073 ms
vagrant@srv-sec-core:~$ exit
logout
```

Figure 1.4: Connexion SSH à **sec-core** et test de connectivité vers **srv-gateway**.

1.3 Phase 1 : Mise en place du cœur de sécurité sur **srv-sec-core**

L’objectif de cette première phase est de transformer la machine virtuelle **srv-sec-core** en véritable cœur de sécurité du laboratoire SecureCorp. Cette VM héberge à la fois le gestionnaire de secrets HashiCorp Vault et l’infrastructure de gestion des certificats (PKI) à deux niveaux (Autorité Racine et Autorité Intermédiaire).

1.3.1 Installation de HashiCorp Vault

Après connexion à la VM via Vagrant :

```
vagrant ssh sec-core
```

nous procédons à l’installation de Vault en utilisant le dépôt officiel HashiCorp. L’utilisation de ce dépôt, plutôt que des paquets Ubuntu par défaut, permet de disposer d’une version à jour, conforme aux environnements de production.

Les étapes sont les suivantes :

- Installation des prérequis et de la clé GPG HashiCorp ;
- Ajout du dépôt `apt.releases.hashicorp.com` au système ;

- Installation du paquet `vault` via `apt-get`.

La figure 1.5 illustre l'installation réussie de Vault sur la machine `srv-sec-core`.

Figure 1.5: Installation de HashiCorp Vault depuis le dépôt officiel HashiCorp.

1.3.2 Configuration de Vault en service systemd

Afin de se rapprocher des pratiques de gestion de services en entreprise, Vault n'est pas lancé manuellement en ligne de commande, mais configuré comme service `systemd`. Un fichier d'unité `/etc/systemd/system/vault.service` est créé avec, notamment, la directive `ExecStart` suivante :

```
/usr/bin/vault server -dev \
    -dev-listen-address="0.0.0.0:8200" \
    -dev-root-token-id="root"
```

Dans le cadre de ce laboratoire, Vault est démarré en mode *dev* et écoute sur toutes les interfaces réseau (0.0.0.0:8200) afin de permettre les échanges avec les autres VMs. Un token racine fixe (**root**) est utilisé pour simplifier les manipulations ; il s'agit évidemment d'un compromis pédagogique et non d'une configuration acceptable en production.

Le service est ensuite activé et démarré via :

```
sudo systemctl enable vault
sudo systemctl start vault
sudo systemctl status vault
```

Lors de l'exécution de `systemctl status`, la sortie est affichée à travers un *pager* (généralement `less`), ce qui est indiqué par la mention lines 1–12 (END) en bas de l'écran. Pour revenir au shell, il suffit d'appuyer sur la touche `q`. La figure 1.6 montre l'état active (running) du service Vault, confirmant son bon fonctionnement.

```
vagrant@srv-sec-core:~$ sudo systemctl status vault
● vault.service - Vault secrets engine
   Loaded: loaded (/etc/systemd/system/vault.service)
   Active: active (running) since Fri 2018-01-12 14:18:11 UTC
     Docs: https://www.vaultproject.io/docs/commands/vault.html
           https://www.vaultproject.io/docs/commands/vault.html
  Process: 1144 ExecStart=/usr/bin/vault start -config /etc/vault/vault.hcl (code=exited, status=0)
 Main PID: 1144 (vault)
    CGroup: /system.slice/vault.service
            └─1144 /usr/bin/vault start -config /etc/vault/vault.hcl

vagrant@srv-sec-core:~$ vault secrets enable database
Success! Enabled the database secrets engine at: database/
vagrant@srv-sec-core:~$ vault write database/config/postgresql \
  plugin_name=postgresql-database-plugin \
  allowed_roles="keycloak-role" \
  connection_url="postgresql://{{username}}:{{password}}@localhost:5432/keycloak" \
  username="vault" \
  password="vault-root-password"
Success! Data written to: database/config/postgresql
vagrant@srv-sec-core:~$ vault write database/roles/keycloak-role \
  db_name=postgresql \
  creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}'; GRANT ALL PRIVILEGES ON DATABASE keycloak TO \"{{name}}\"; GRANT ALL ON SCHEMA public TO \"{{name}}\";" \
  default_ttl="1h" \
  max_ttl="24h"
Success! Data written to: database/roles/keycloak-role
vagrant@srv-sec-core:~$ vault read database/creds/keycloak-role
Key          Value
---          -----
lease_id      database/creds/keycloak-role/mo6dK3ZJnU3kEaFYdyPhJJ7a
lease_duration 1h
lease_renewable true
password      jb0d--8Jgo1wWYm6ZKis
username      v-token-keycloak-vQDmhBe5MPOG1lNsfkM2-1763773701
vagrant@srv-sec-core:~$ [REDACTED]
```

Figure 1.6: Service vault géré par systemd et en état active (running).

1.3.3 Préparation de l'environnement et installation de jq

Pour pouvoir interagir confortablement avec Vault, deux variables d'environnement sont définies de manière persistante dans le fichier `~/.bashrc` :

- `VAULT_ADDR` : URL du serveur Vault (`http://127.0.0.1:8200`) ;
- `VAULT_TOKEN` : token d'authentification utilisé (`root` dans ce laboratoire).

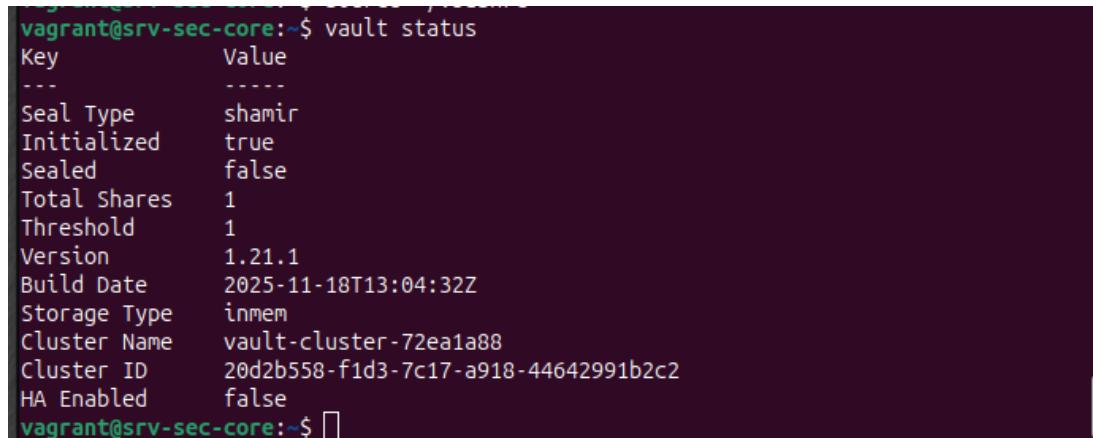
Après mise à jour du fichier de configuration et rechargement avec `source ~/.bashrc`, la commande suivante permet de vérifier l'état du serveur :

```
vault status
```

Par ailleurs, la construction de la PKI repose sur l'utilisation de l'outil `jq`, qui permet d'extraire proprement les champs renvoyés au format JSON par Vault (par exemple les CSR et certificats). Cet outil n'étant pas installé par défaut, il est ajouté via :

```
sudo apt-get install -y jq
```

La figure 1.7 présente la sortie de la commande `vault status`, indiquant un serveur non scellé (Sealed: false) et prêt à émettre des certificats.



```
vagrant@srv-sec-core:~$ vault status
Key          Value
...
Seal Type    shamir
Initialized   true
Sealed       false
Total Shares 1
Threshold    1
Version      1.21.1
Build Date   2025-11-18T13:04:32Z
Storage Type inmem
Cluster Name vault-cluster-72ea1a88
Cluster ID   20d2b558-f1d3-7c17-a918-44642991b2c2
HA Enabled   false
vagrant@srv-sec-core:~$
```

Figure 1.7: Vérification de l'état de Vault avec la commande `vault status`.

1.3.4 Mise en place de la PKI à deux niveaux

Une fois Vault opérationnel, nous configurons une infrastructure de gestion de certificats (PKI) à deux niveaux, composée d'une Autorité Racine (Root CA) et d'une Autorité Intermédiaire (Intermediate CA). Cette architecture est conforme aux bonnes pratiques de sécurité : la racine est très peu utilisée et peut rester hors ligne, tandis que l'intermédiaire signe les certificats utilisés au quotidien et peut être révoquée si nécessaire.

1.3.4.1 Cration de l'Autorite Racine

Nous activons tout d'abord un moteur de secrets de type PKI monté sur le chemin `pki`, puis nous ajustons le TTL maximal à 10 ans :

```
vault secrets enable pki
vault secrets tune -max-lease-ttl=87600h pki
```

Un certificat racine interne est ensuite genr avec le nom commun `SecureCorp Root CA` et export dans un fichier `root_ca.crt`. Enfin, les URLs de publication des certificats et des listes de revocation (CRL) sont configures pour permettre aux clients d'aller verifier la validite des certificats emis.

```

vagrant@srv-sec-core:~$ vault secrets enable pki
Success! Enabled the pki secrets engine at: pki/
vagrant@srv-sec-core:~$ vault secrets tune -max-lease-ttl=87600h pki
Success! Tuned the secrets engine at: pki/
vagrant@srv-sec-core:~$ vault write -field=certificate pki/root/generate/internal \
    common_name="SecureCorp Root CA" \
    ttl=87600h > root_ca.crt
vagrant@srv-sec-core:~$ vault write pki/config/urls \
    issuing_certificates="$VAULT_ADDR/v1/pki/ca" \
    crl_distribution_points="$VAULT_ADDR/v1/pki/crl"
Key          Value
---          -----
crl_distribution_points [http://127.0.0.1:8200/v1/pki/crl]
delta_crl_distribution_points []
enable_templateing false
issuing_certificates [http://127.0.0.1:8200/v1/pki/ca]
ocsp_servers []
vagrant@srv-sec-core:~$ 

```

Figure 1.8: Création de la Root CA dans Vault (pki) .

1.3.4.2 Création de l’Autorité Intermédiaire

Une seconde instance du moteur PKI est activée sur le chemin `pki_int` pour héberger l’Autorité Intermédiaire. Après avoir ajusté son TTL maximal à un an, une requête de signature de certificat (CSR) est générée :

```

vault write -format=json pki_int/intermediate/generate/internal \
    common_name="SecureCorp Intermediate CA" | \
    jq -r '.data.csr' > pki_intermediate.csr

```

Cette CSR est signée par l’Autorité Racine via la commande `pki/root/sign-intermediate`, puis le certificat intermédiaire obtenu est importé dans le moteur `pki_int`. La figure 1.9 illustre les principales étapes de création et d’enregistrement des autorités racine et intermédiaire dans Vault.

```

vagrant@srv-sec-core:~$ vault secrets enable -path=pki_int pki
Success! Enabled the pki secrets engine at: pki_int/
vagrant@srv-sec-core:~$ vault secrets tune -max-lease-ttl=43800h pki_int
Success! Tuned the secrets engine at: pki_int/
vagrant@srv-sec-core:~$ vault write -format=json pki_int/intermediate/generate/internal \
    common_name="SecureCorp Intermediate CA" \
    | jq -r '.data.csr' > pki_intermediate.csr
vagrant@srv-sec-core:~$ vault write -format=json pki/root/sign-intermediate \
    csr=@pki_intermediate.csr \
    format=pem_bundle ttl=43800h \
    | jq -r '.data.certificate' > intermediate.cert.pem
vagrant@srv-sec-core:~$ vault write pki_int/intermediate/set-signed certificate=@intermediate.cert.pem
WARNING! The following warnings were returned from Vault:

* This mount hasn't configured any authority information access (AIA) fields; this may make it harder for systems to find missing certificates in the chain or to validate revocation status of certificates. Consider updating /config/urls or the newly generated issuer with this information.

Key          Value
---          -----
existing_issuers   <nil>
existing_keys      <nil>
imported_issuers  [14166cec-8999-4e5d-37ea-a61f62d15854 c9e233f4-174c-7b2d-1018-daf5a4679ad3]
imported_keys      <nil>
mapping           map[14166cec-8999-4e5d-37ea-a61f62d15854:6ec5eff0-456a-0fd2-7e66-5744fd55e931 c9e233f4-174c-7b2d-1018-daf5a4679ad3:]
vagrant@srv-sec-core:~$ 

```

Figure 1.9: Création de l’Intermediate CA dans Vault (pki_int).

1.3.4.3 Définition des rôles et émission de certificats serveur

Pour structurer l’émission des certificats, un rôle dédié aux serveurs de domaine `securecorp.local` est créé :

```

vault write pki_int/roles/securecorp-dot-local \
    allowed_domains="securecorp.local" \
    allow_subdomains=true \
    max_ttl="72h"

```

Ce rôle autorise la génération de certificats pour le domaine racine `securecorp.local` ainsi que pour tous ses sous-domaines (par exemple `portal.securecorp.local` ou `idp.securecorp.local`), avec une durée de vie maximale de 72 heures.

Un premier test d’émission de certificat est réalisé avec :

```

vault write pki_int/issue/securecorp-dot-local \
    common_name="test.securecorp.local" ttl="24h"

```

La réponse renvoyée contient le certificat X.509, la clé privée associée et la chaîne de certification complète. Ce test valide la bonne configuration de la PKI basée sur Vault. La figure 1.10 montre le succès de cette opération d’émission de certificat pour le sous-domaine `test.securecorp.local`.

```
vagrant@srv-sec-core:~$ vault write pki_int/issue/securecorp-dot-local common_name="test.securecorp.local" ttl="24h"
Key          Value
...
authority_key_id 2e:22:b4:ad:30:4b:9a:fd:33:06:3c:04:19:a6:de:79:32:03:bd:94
ca_chain        [-----BEGIN CERTIFICATE-----]
MIIDpTCCAO2gAwIBAgIUBWPFPtJEOMQpcHVM+6wk7oT//WAwDQYJKoZIhvNAQEL
BQAwhTEbMBkGA1UEAxMSU2VjdxJlQ29ycCBSb290IENBMB4XDIT1MTEyMjAwMzUx
Ov0XDTMwMTEyMTAwMzU0VowJTEjMCEGA1UEAxMaU2VjdXJlQ29ycCBjbnRlcml1
ZGhdcUQ040EwgElMA0GCSqGSIb3DQEBAQUA4IBDwAwggEKAoIBAQCbTMwmIZfq
wWRJb/fJco1sXGt2HpaXKtUzjZmwjLc1l59r561bggwiaSF+i7hnYqVNx+kEpl
xLI61jrF1PymrxFph5moyekiuUKMMAnyN8T0TQbAN1l/gopzplwv2bPRU3kIot
h9WF5Y6NAOfVc3yIu642X820jiucQmRrv6Fzula8X5BZastOqi/67s0RxCKiCY
cqCo42Pv7vSSQdsWINEf5KLxx+S3nmjbimRCSoVxSNdPL+bazDwsL2/xmcjexlH
oUVxuLwjHIMipqlMddGe0cxkuJaCl4CvpQAr1a8a0dsFGFxcL3h70gi0/eVxRug
dRQxuLuwun5AgMBAAGjgdwgdEDVr6PAQH/BAODAgEgMA8GA1udEwEB/wQF
MAMBAF8wHQYDVR00BYEFCAitk0wS5r9MWY8BBmm3nkyATZUMB8GA1udIwQYMBAA
FLbKJHjLB212VmR6GvhPdEc75b0MsGCCsGAQFBwEBBC8wLTarBgrBgeFBQcw
AoYfaHR0cDovLzEyNy4wLjaUMt04MjAwL3YxL3Bras9jYTAXBgNVHR8EKjAoMCag
JKAhiBodHRwO18vMTI3LjaUMC4x0jgyMDAvdjEvCtP12nybDANBkgkhk1G9w0B
AQsFAAACQAQEAyTjb61YmgX4gKCX/biE/QbxpQ8gj7NrjXK+RjCOGW5vjrnDdbK
mUGxGzCvMrX001NE3AVK5UTgnsMaSp17ntjSYLjxMeCDsGm@05SY+yKUKFvJB0
+ecIIzew/+OPgJHOMy13wqmzXfOB2LtDUVRNxYzV3oZKz0uRxVVA8sWTngmHJr
Y15c/BeqQxDtvTrA779/70+p0U50e9HxsLsqoRtk0QisCnbXUH94YAhia01h5e6
nduyorllazMqTxp04NwecpJx06/HDUtBjMfUB+PIZMiP70y8QMRyjZ0Tum0oYwg0
ZhVwK5x3p+bfyAoV96JVBZthIwqM/FF4og==
-----END CERTIFICATE-----[-----BEGIN CERTIFICATE-----]
MIIDkzCCA0gAwIBAgIUPh1JvxBNT99wiicWQjG598ZRxIgwDQYJKoZIhvNAQEL
BQAwhTEbMBkGA1UEAxMSU2VjdxJlQ29ycCBSb290IENBMB4XDIT1MTEyMjAwMzIx
MloXTD1MTEyMDAwMzI0MvowHTEbMBkGA1UEAxMSU2VjdxJlQ29ycCBSb290IENB
MIIBijANBgqhkicG9w0BAQEFAAOCQAQ8AMIIbCgKCAQEAs/2UBZKsrba43i9KpkOYe
awiud8lzo75sk1KEEpb33sp1Mqy565P7LUa0Z42Sw14t5uUDL71uBnx6YscCTU
WMBYyb/fod17EfqwrZLN82pjy4crw2jaCbjAUofmjIgj9YqcyoR0Dn1P5X2CV
YD8KYwUdiJjuReiXu6kXerqwlJg8ucp2kuT4vHm1pxm3Hb1g93z4Jle9JK9
9zb1QhbATK8WYxfY3SFri1834lfj1Hh+7AJlQdb/Ev5dyguYnexPlWKC2svGlzz6
XT71A7MR1hpItby0Md00fe1zE96z011SECs4NHA910712nspb665s4c165h8M
3QIDAQABo2MwTYA0BgNVHQ8BAfEBAMCAQyWdYDVr0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQUtsokeOIHaLZhZHoae8E960LvlvQwHwYDVr0JBgwFoAUtsokeOIHaLZW
ZHoae8E90QlvLqvWQDQYJKoZIhvNAQELBQA0DggEBAA9awr0IlkqCOL35fAbhAcu
WuBkZd82PA1NBhEImsfB1rokSrr9aydJNDkqkdztFxlvTVanHAT557hcT6G3TN
vL//sDvb2BXlzSiLAMGGW3DMKySK/p6ydg/yZuad0Thjzs0xkatDjTlp34+qFw8
reqPuuKw40/5yw9sybcr35m4pkXeLwJ/dbZxm6jkQs0+Xn4GtzirNdV7RtarXGK8
hpgE6ugqgtoxGgDPigqodBajjDBzLI2f3kxu/WFiYpIzGNvnl2phOLA7PgZ/m6G
F+g9YRwjEwyPBjst9TFS8mvzBelZVklnj3Rd4CMcP4oZG/qC51neYv/ei2wPy3k=
-----END CERTIFICATE-----]
certificate      -----BEGIN CERTIFICATE-----[-----BEGIN CERTIFICATE-----]
MIIDaDCCalCgAwIBAgIUGwnPrWzZYNBv8n0zE25o5WAx3uowDQYJKoZIhvNAQEL
BQAwhTEjMCEGA1UEAxMaU2VjdxJlQ29ycCBSb290IENBMB4XDIT1MTEyMjAwMzUx
MTIyMDAzOTI5WhcnmjUxMTIzMDA2OTU5WjAgMR4wHAYDVQDExV0ZXN0Lnly3Vy
ZnWnvnAubG9jYlwggE1MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQc9UnP+
xMHeSf3s8BuF2j6DwJiFsp5tELVit/+2J/nP0/h6pEbd98zd0pz9GGCWKjrGR/+_
Xt/mKzq8MuC5DhpNXCfrvNHsSEAE0k7XclBjzhavNTH8Wgnf6CspKuwPrCHL
Jtxo/P2Ex3BsdiSM8uOCYUViikMhbhaj0TE25x09ZnAmE0G+IihfTC54nK9Vv
+0MSS+Up52BRKafBbFPdj12kHfithwjeITjgj/38sp5szF/yEb2deisH62lsA1LE
74g+10i7RhriQLq6qgbGgZls/nVCZv9a7pv1+wdZntKe5KFHF6pdpyubEwwJaLn8
PjR0N345yr4E37r5AgMBAAGjgZQwqZEWdGyDVR0PAQH/BAODAg0OMB0GA1udjQ0W
MBGCCsGAQUFBwMBBggRgEFBQcDAjBgNVHQ4EFgQUcrMHKhowaMy/oYJkr7Y
XApcj0WhwYDVr0jBbwFoAULk0rTBLmvbzjwEGabeyTDVzQwIAYDVr0RBbkw
F4IVDgvzdC5zzWN1cmVjb3JwLmxvY2FsmA0GCSqGSIb3DQEBCwUA4IBAQ0DAyH
YQG06uKyZknmEnKfTR2avhulg7hiY9bVR2KZcn9d/Cdu4veRlnCbosjv/AQvqTO
tdtzQ1aX4rhclZIHrkxDcmSpqYi1IoK31gdyUM9j1K0iTVAt7v+9rA4ABrszjWKg
fkMg2/02RLE0AmUdoYwhRw0aHJQrwgOSWSRm371H3G7zMK0xt+wYfWfbCtnDEN
0RIVGiHmRgWte0XEHCpoTHBN4CaFwRbyggArLfBx4I/gacF5bSZK3Ha4TyhGTx2
dLx3a43Dn/aTYS/b2+Mb7vLcoxy0V5z7o9KcA1kgpBp0hewF89NmYvV2TIVyph

```

Figure 1.10: Émission d'un certificat pour `test.securecorp.local` via l'Autorité Intermédiaire.

1.3.5 Bilan de la phase 1

À l'issue de cette phase, la VM `srv-sec-core` joue pleinement son rôle de cœur de sécurité :

- Vault est déployé comme service `systemd` et accessible sur le réseau interne du laboratoire.
- Une hiérarchie PKI à deux niveaux (Root CA + Intermediate CA) est opéra-

tionnelle.

- L'émission de certificats pour le domaine `securecorp.local` est fonctionnelle et pilotée par des rôles dédiés.

Cette base sera utilisée dans les phases suivantes pour sécuriser les communications (HTTPS et mTLS) entre la passerelle, le serveur d'application et, plus tard, l'Identity Provider.

1.4 Phase 2 : Mise en place de l'Identity Provider (Keycloak) intégré à Vault

Après avoir mis en place le coeur PKI avec Vault, l'étape suivante consiste à déployer un fournisseur d'identité (Identity Provider, IdP) moderne : Keycloak. L'objectif n'est pas seulement de lancer Keycloak, mais de l'intégrer dans une approche Zero Trust en déléguant à Vault la gestion des identifiants de base de données. Ainsi, Keycloak n'utilise pas un mot de passe statique, mais des identifiants éphémères générés à la demande par Vault.

1.4.1 Préparation de l'environnement : Java 17 et PostgreSQL

Keycloak repose sur la JVM et nécessite une base de données relationnelle pour persister sa configuration et ses comptes. Sur la machine `srv-sec-core`, nous installons donc Java 17 et PostgreSQL, puis créons une base dédiée à Keycloak.

```
sudo apt-get update
sudo apt-get install -y openjdk-17-jdk postgresql postgresql-contrib

sudo -u postgres psql -c "CREATE DATABASE keycloak;" 
sudo -u postgres psql -c \
"CREATE USER vault WITH SUPERUSER ENCRYPTED PASSWORD 'vault-root-password';"
```

Le compte PostgreSQL `vault` joue un rôle particulier : il dispose de droits étendus (`SUPERUSER`) et sert de compte d'administration pour Vault, qui l'utilisera pour créer et révoquer dynamiquement des utilisateurs destinés à Keycloak.

La figure 1.11 illustre l'installation de Java 17 et de PostgreSQL, ainsi que la création de la base `keycloak` et de l'utilisateur `vault`.

List of roles			
Role name	Attributes	Member of	
postgres	Superuser, Create role, Create DB, Replication, Bypass RLS	{}	{}
v-token-keycloak-D9Ny9rPETGoxUnZ11DlE-1763775541	{}	{}	{}
v-token-keycloak-vQDmhbe5MPOG1lNsfkM2-1763773701	{}	{}	{}
vault	Superuser	{}	{}
~			
~			
~			

Figure 1.11: Installation de Java 17 et PostgreSQL, création de la base `keycloak` et de l'utilisateur `vault`.

1.4.2 Configuration de Vault comme gestionnaire d'identifiants PostgreSQL

Afin d'éviter d'avoir un mot de passe de base de données écrit en dur dans un fichier de configuration, Vault est configuré pour jouer le rôle de maître des clés pour PostgreSQL. Pour cela, nous activons le moteur de secrets `database` et lui apprenons comment se connecter à la base `keycloak` avec le compte `vault` :

```
vault secrets enable database

vault write database/config/postgresql \
  plugin_name=postgresql-database-plugin \
  allowed_roles="keycloak-role" \
  connection_url="postgresql://{{username}}:{{password}}@localhost:5432/keycloak" \
  username="vault" \
  password="vault-root-password"
```

La directive `allowed_roles="keycloak-role"` restreint les rôles que Vault est autorisé à servir via cette configuration. Nous définissons ensuite le rôle `keycloak-role`, qui décrit la manière dont doivent être créés les utilisateurs SQL éphémères pour Keycloak :

```
vault write database/roles/keycloak-role \
  db_name=postgresql \
  creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}' \
    GRANT ALL PRIVILEGES ON DATABASE keycloak TO \"{{name}}\"; \
    GRANT ALL ON SCHEMA public TO \"{{name}}\";" \
  default_ttl="1h" \
  max_ttl="24h"
```

Ce rôle indique à Vault :

- comment créer un nouveau rôle PostgreSQL (`CREATE ROLE`) avec un mot de passe aléatoire ;
- quels droits lui accorder sur la base `keycloak` et son schéma `public` ;
- quelle durée de vie par défaut attribuer aux identifiants générés (1 heure), avec un maximum de 24 heures.

La figure 1.12 montre la configuration du moteur `database` et la création du rôle `keycloak-role`.

```

GNU nano 6.2          /opt/keycloak/start_with_vault.sh *
#!/bin/bash

# 1. On s'authentifie à Vault (Ici le fait avec le root token pour le lab, en vrai on utiliserait 'AppRole' ou 'Kubernetes Auth')
# export VAULT_ADDR='http://127.0.0.1:8200'
# export VAULT_TOKEN='root'

echo ">>> Demande de credentials DB à Vault..."
SECRET_JSON=$(vault read -format=json database/creds/keycloak-role)

# 2. On extrait user/pass avec jq
DB_USER=$(echo $SECRET_JSON | jq -r .data.username)
DB_PASS=$(echo $SECRET_JSON | jq -r .data.password)

echo ">>> Credentials obtenus ! User: $DB_USER"

# 3. On injecte les variables d'environnement pour Keycloak
export KC_DB=postgres
export KC_DB_URL=jdbc:postgresql://localhost:5432/keycloak
export KC_DB_USERNAME=$DB_USER
export KC_DB_PASSWORD=$DB_PASS

# Variables Admin initiales (A supprimer après le 1er boot en prod)
export KC_BOOTSTRAP_ADMIN_USERNAME=admin
export KC_BOOTSTRAP_ADMIN_PASSWORD=admin

# 4. On lance Keycloak
# proxy=edge car on aura Nginx devant plus tard
exec /opt/keycloak/bin/kc.sh start --proxy=edge --hostname=portal.securecorp.local --http-port=8080

```

Figure 1.12: Configuration du moteur database de Vault pour PostgreSQL et définition du rôle keycloak-role.

1.4.2.1 Test de génération d'identifiants éphémères

Pour valider la configuration, nous demandons à Vault de générer une paire identifiant/-mot de passe pour le rôle keycloak-role :

```
vault read database/creds/keycloak-role
```

Vault renvoie un document JSON contenant notamment un champ `username` (de la forme `v-root-keycloak-role-xxxxx`) et un `password` aléatoire, ainsi qu'un TTL indiquant la durée de validité des identifiants. Ceci confirme que Vault est capable de créer à la demande des comptes PostgreSQL éphémères pour Keycloak.

La figure 1.13 présente un exemple de sortie de la commande `vault read database/creds/keycloak-role`.

```

vagrant@srv-sec-core:~$ vault secrets enable database
Success! Enabled the database secrets engine at: database/
vagrant@srv-sec-core:~$ vault write database/config/postgresql \
    plugin_name=postgresql-database-plugin \
    allowed_roles="keycloak-role" \
    connection_url="postgresql://{{username}}:{{password}}@localhost:5432/keycloak" \
    username="vault" \
    password="vault-root-password"
Success! Data written to: database/config/postgresql
vagrant@srv-sec-core:~$ vault write database/roles/keycloak-role \
    db_name=postgresql \
    creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}'; GRANT ALL PRIVILEGES ON DATABASE keycloak TO \"{{name}}\"; GRANT ALL ON SCHEMA public TO \"{{name}}\";" \
    default_ttl="1h" \
    max_ttl="24h"
Success! Data written to: database/roles/keycloak-role
vagrant@srv-sec-core:~$ vault read database/creds/keycloak-role
Key          Value
---          -----
lease_id      database/creds/keycloak-role/mo6dK3ZJnU3kEaFYdyPhJJ7a
lease_duration 1h
lease_renewable true
password      jb0d--8Jgo1wWYm6ZKis
username       v-token-keycloak-vQDmhBe5MPOG1lNsfkM2-1763773701
vagrant@srv-sec-core:~$ 

```

Figure 1.13: Génération d’identifiants PostgreSQL éphémères pour Keycloak via Vault (database/creds/keycloak-role).

1.4.3 Installation de Keycloak en mode binaire

Keycloak est installé sous forme d’archive binaire dans le répertoire /opt. Nous utilisons une version moderne basée sur Quarkus, et préparons Keycloak pour une utilisation avec PostgreSQL :

```

cd /opt
sudo wget https://github.com/keycloak/keycloak/releases/download/24.0.1/keycloak-24.0.1.tar.gz
sudo tar -xvzf keycloak-24.0.1.tar.gz
sudo mv keycloak-24.0.1 keycloak
sudo chown -R root:root /opt/keycloak
sudo chmod -R o+rwx /opt/keycloak/

cd /opt/keycloak
bin/kc.sh build --db=postgres

```

La commande `kc.sh build -db=postgres` permet de préconfigurer et optimiser Keycloak pour une base de données PostgreSQL. La figure 1.14 illustre le processus de build de Keycloak.

```

vagrant@srv-gateway:~$ sudo mkdir -p /etc/nginx/certs
vagrant@srv-gateway:~$ sudo nano /usr/local/bin/renew_certs.sh
vagrant@srv-gateway:~$ sudo nano /usr/local/bin/renew_certs.sh
vagrant@srv-gateway:~$ sudo chmod +x /usr/local/bin/renew_certs.sh
sudo /usr/local/bin/renew_certs.sh
>>> [Mon Nov 24 02:17:27 PM UTC 2025] Demande de nouveau certificat à Vault...
>>> Certificats générés.
>>> Nginx recharge avec succès.
vagrant@srv-gateway:~$ ls -l /etc/nginx/certs
total 16
-rw-r--r-- 1 root root 1326 Nov 24 14:17 ca_chain.crt
-rw-r--r-- 1 root root 2575 Nov 24 14:17 fullchain.crt
-rw-r--r-- 1 root root 1249 Nov 24 14:17 server.crt
-rw-r--r-- 1 root root 1679 Nov 24 14:17 server.key
vagrant@srv-gateway:~$ 

```

Figure 1.14: Installation et build de Keycloak pour une utilisation avec PostgreSQL.

1.4.4 Script de démarrage intégré à Vault

Keycloak ne gère pas nativement la récupération de ses identifiants de base de données depuis Vault. Pour implémenter ce comportement de manière propre, nous créons un script wrapper `/opt/keycloak/start_with_vault.sh` qui :

1. s'authentifie à Vault ;
2. demande des identifiants PostgreSQL pour le rôle `keycloak-role` ;
3. extrait le nom d'utilisateur et le mot de passe à l'aide de `jq` ;
4. injecte ces informations dans les variables d'environnement attendues par Keycloak ;
5. lance finalement Keycloak.

Le script est le suivant :

```

#!/bin/bash

export VAULT_ADDR='http://127.0.0.1:8200'
export VAULT_TOKEN='root'

echo ">>> Demande de credentials DB à Vault..."
SECRET_JSON=$(vault read -format=json database/creds/keycloak-role)

DB_USER=$(echo $SECRET_JSON | jq -r .data.username)
DB_PASS=$(echo $SECRET_JSON | jq -r .data.password)

echo ">>> Credentials obtenus ! User: $DB_USER"

export KC_DB=postgres
export KC_DB_URL=jdbc:postgresql://localhost:5432/keycloak
export KC_DB_USERNAME=$DB_USER

```

```

export KC_DB_PASSWORD=$DB_PASS

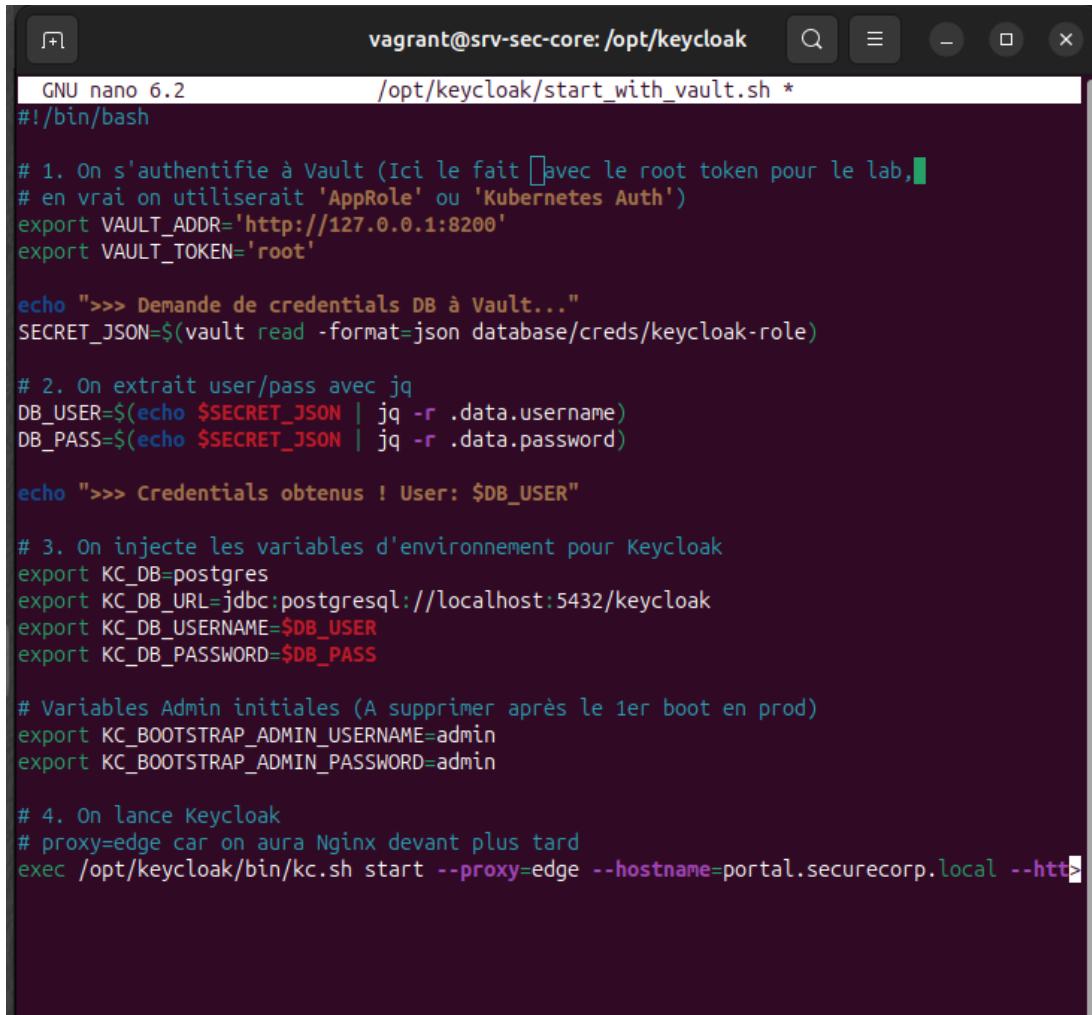
export KC_BOOTSTRAP_ADMIN_USERNAME=admin
export KC_BOOTSTRAP_ADMIN_PASSWORD=admin

exec /opt/keycloak/bin/kc.sh start \
--proxy=edge \
--hostname=portal.securecorp.local \
--http-enabled=true

```

Dans un contexte de production, l'authentification à Vault utiliserait un mécanisme plus robuste (par exemple *AppRole* ou un backend d'authentification Kubernetes), et les identifiants d'administration de Keycloak ne seraient pas fixés dans le script. Pour ce laboratoire, ces simplifications sont assumées et documentées.

La figure 1.15 montre la création et l'exécution du script `start_with_vault.sh`.



```

vagrant@srv-sec-core: /opt/keycloak
GNU nano 6.2          /opt/keycloak/start_with_vault.sh *
#!/bin/bash

# 1. On s'authentifie à Vault (Ici le fait avec le root token pour le lab, en vrai on utiliserait 'AppRole' ou 'Kubernetes Auth')
export VAULT_ADDR='http://127.0.0.1:8200'
export VAULT_TOKEN='root'

echo ">>> Demande de credentials DB à Vault..."
SECRET_JSON=$(vault read -format=json database/creds/keycloak-role)

# 2. On extrait user/pass avec jq
DB_USER=$(echo $SECRET_JSON | jq -r .data.username)
DB_PASS=$(echo $SECRET_JSON | jq -r .data.password)

echo ">>> Credentials obtenus ! User: $DB_USER"

# 3. On injecte les variables d'environnement pour Keycloak
export KC_DB=postgres
export KC_DB_URL=jdbc:postgresql://localhost:5432/keycloak
export KC_DB_USERNAME=$DB_USER
export KC_DB_PASSWORD=$DB_PASS

# Variables Admin initiales (A supprimer après le 1er boot en prod)
export KC_BOOTSTRAP_ADMIN_USERNAME=admin
export KC_BOOTSTRAP_ADMIN_PASSWORD=admin

# 4. On lance Keycloak
# proxy=edge car on aura Nginx devant plus tard
exec /opt/keycloak/bin/kc.sh start --proxy=edge --hostname=portal.securecorp.local --htt

```

Figure 1.15: Script de démarrage de Keycloak intégrant une récupération des identifiants DB depuis Vault.

1.4.5 Intégration dans systemd : service Keycloak

Dans la continuité de la Phase 1, Keycloak est également géré comme un service `systemd`. Un fichier d'unité `/etc/systemd/system/keycloak.service` est créé :

```
[Unit]
Description=Keycloak IAM with Vault Secrets
After=network.target vault.service postgresql.service
Requires=vault.service postgresql.service

[Service]
User=root
ExecStart=/opt/keycloak/start_with_vault.sh
Restart=always

[Install]
WantedBy=multi-user.target
```

Les directives `After` et `Requires` garantissent que Vault et PostgreSQL sont démarrés avant Keycloak. Le service est ensuite rechargé, activé et démarré :

```
sudo systemctl daemon-reload
sudo systemctl enable keycloak
sudo systemctl start keycloak
```

La commande suivante permet de suivre les logs en temps réel :

```
journalctl -u keycloak -f
```

Après un certain temps (le premier démarrage initialisant le schéma de base de données), Keycloak indique qu'il écoute sur le port HTTP 8080. À ce stade, le service est fonctionnel du point de vue système, mais plusieurs incidents applicatifs sont apparus lors des premiers tests, comme décrit dans la section suivante.

1.4.6 Incident : erreur interne Keycloak et diagnostic

Lors du premier test d'accès via le navigateur, en passant par la passerelle et le reverse proxy, l'URL exposée renvoie une page d'erreur rouge Internal Server Error de Keycloak (et non une erreur Nginx de type 502 Bad Gateway).

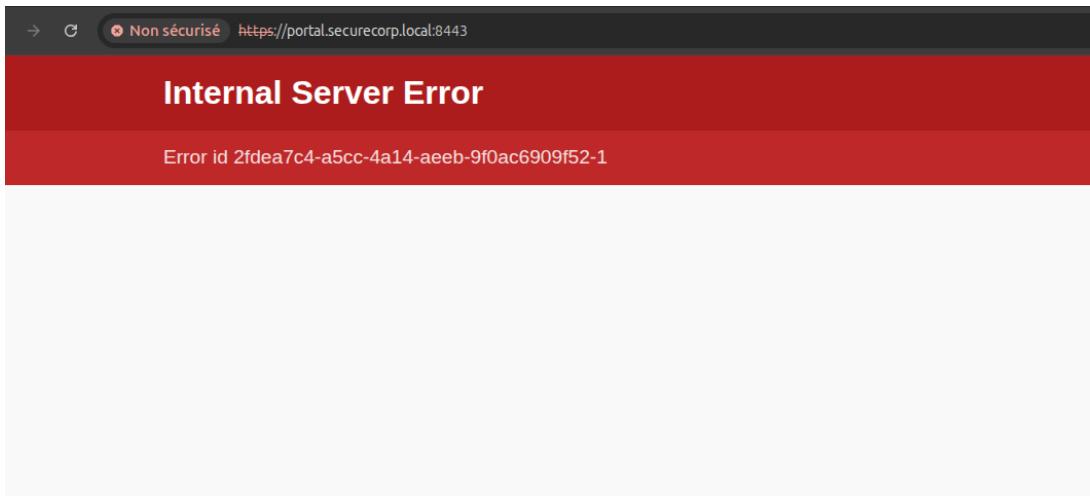


Figure 1.16: Erreur interne keycloak.

Cette observation est importante car elle montre que :

- la résolution DNS et le routage fonctionnent (le navigateur atteint bien la VM Gateway) ;
- la couche TLS fonctionne (la connexion HTTPS est établie, malgré l'avertissement attendu sur le certificat interne) ;
- le reverse proxy transmet correctement la requête jusqu'à Keycloak.

L'erreur ne provient donc pas du réseau, mais bien de Keycloak lui-même. Le réflexe adopté a été d'analyser les journaux du service :

```
vagrant ssh sec-core
journalctl -u keycloak -n 200 -e
```

Dans ces logs, une erreur explicite apparaît côté PostgreSQL :

```
org.postgresql.util.PSQLException:
    ERROR: permission denied for table realm_attribute
```

Cette erreur met en évidence un problème subtil lié à l'utilisation de secrets dynamiques pour la base de données .

Au premier démarrage, Vault a généré un premier utilisateur PostgreSQL (par exemple `v-root-keycloak-role-...`) pour Keycloak, qui a ensuite créé les tables et en est devenu propriétaire. Après un redémarrage, ce premier utilisateur a expiré ou a été abandonné. Vault a alors généré un nouvel utilisateur (par exemple `v-root-keycloak-role-...2`), avec accès à la base `keycloak`, mais sans être propriétaire des tables existantes. Lorsque Keycloak, exécuté sous ce nouvel utilisateur, tente de lire ou modifier la table `realm_attribute`, PostgreSQL refuse l'accès, d'où le permission denied.

Ce comportement illustre une limite classique des secrets dynamiques si les droits sur les objets (tables, séquences) ne sont pas correctement anticipés.

1.4.6.1 Ajustement des droits via Vault

Dans un premier temps, une réinitialisation complète de la base `keycloak` a été envisagée via :

```
sudo -u postgres psql -c "DROP DATABASE keycloak;"
```

Cependant, PostgreSQL a refusé l'opération car plusieurs services utilisaient déjà cette base (connexions actives). Plutôt que de forcer le drop, l'approche retenue a été de corriger la recette SQL utilisée par Vault lors de la création des comptes dynamiques.

Le rôle `keycloak-role` de Vault a donc été mis à jour pour inclure explicitement des droits sur l'ensemble des tables et séquences du schéma `public` :

```
vault write database/roles/keycloak-role \
  db_name=postgresql \
  creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}';
    GRANT ALL PRIVILEGES ON DATABASE keycloak TO \"{{name}}\";
    GRANT ALL ON SCHEMA public TO \"{{name}}\";
    GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO \"{{name}}\";
    GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA public TO \"{{name}}\"";
  default_ttl="1h" \
  max_ttl="24h"
```

Après cette modification, le service Keycloak a été redémarré :

```
sudo systemctl restart keycloak
```

Les nouvelles instances d'utilisateurs dynamiques générées par Vault disposent ainsi de droits complets sur les objets de la base `keycloak`, ce qui corrige l'erreur permission denied for table `realm_attribute`.

1.4.7 Accès local requis et mise en place d'un tunnel SSH

Une fois l'erreur de droits corrigée, le message renvoyé par Keycloak lors de l'accès à l'interface d'administration a évolué : au lieu d'une erreur interne, Keycloak affichait la page Local access required. Ce comportement correspond à la politique de sécurité par défaut de Keycloak : tant qu'aucun compte administrateur n'a été créé, l'interface de création de l'utilisateur admin n'est accessible qu'en local (<http://localhost:8080/>) et non via un reverse proxy distant.

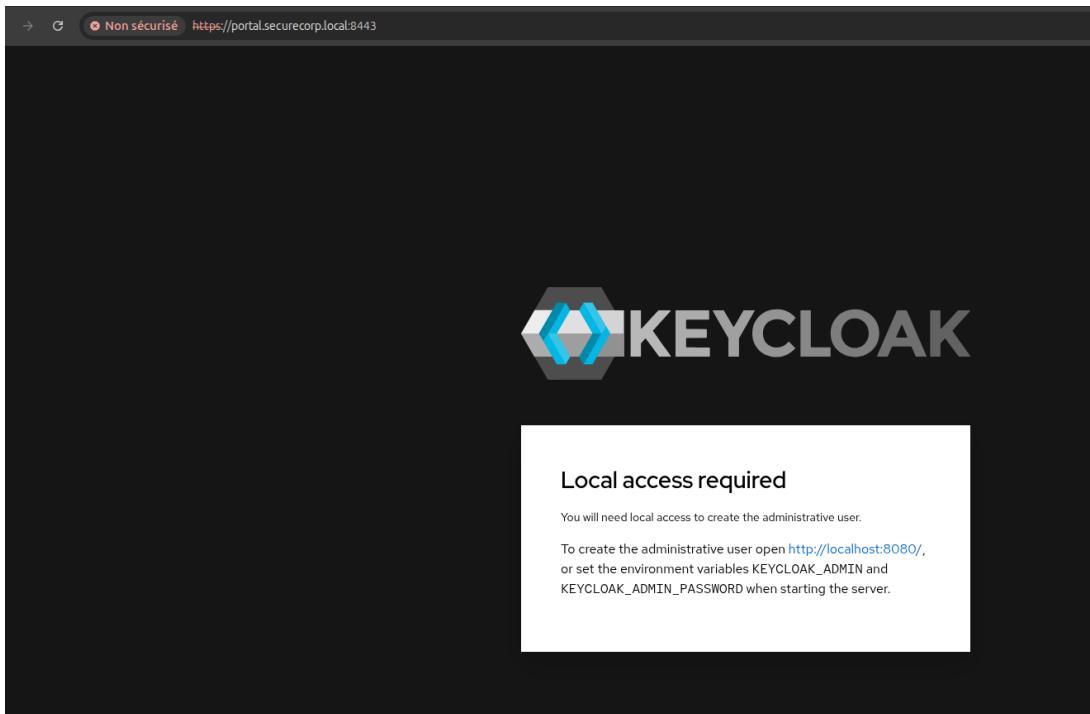


Figure 1.17: Premier accès à keycloak

Pour respecter cette contrainte tout en travaillant depuis le poste de développement, un tunnel SSH a été mis en place depuis la machine hôte vers la VM **srv-sec-core** :

```
vagrant ssh sec-core -- -L 8888:localhost:8080
```

Cette commande établit un tunnel chiffré entre le port 8888 de la machine locale et le port 8080 de la VM, de sorte que l'URL suivante dans le navigateur du poste ressemble, du point de vue de Keycloak, à un accès local :

```
http://localhost:8888
```

En utilisant ce tunnel, l'interface de création du premier utilisateur administrateur apparaît correctement.

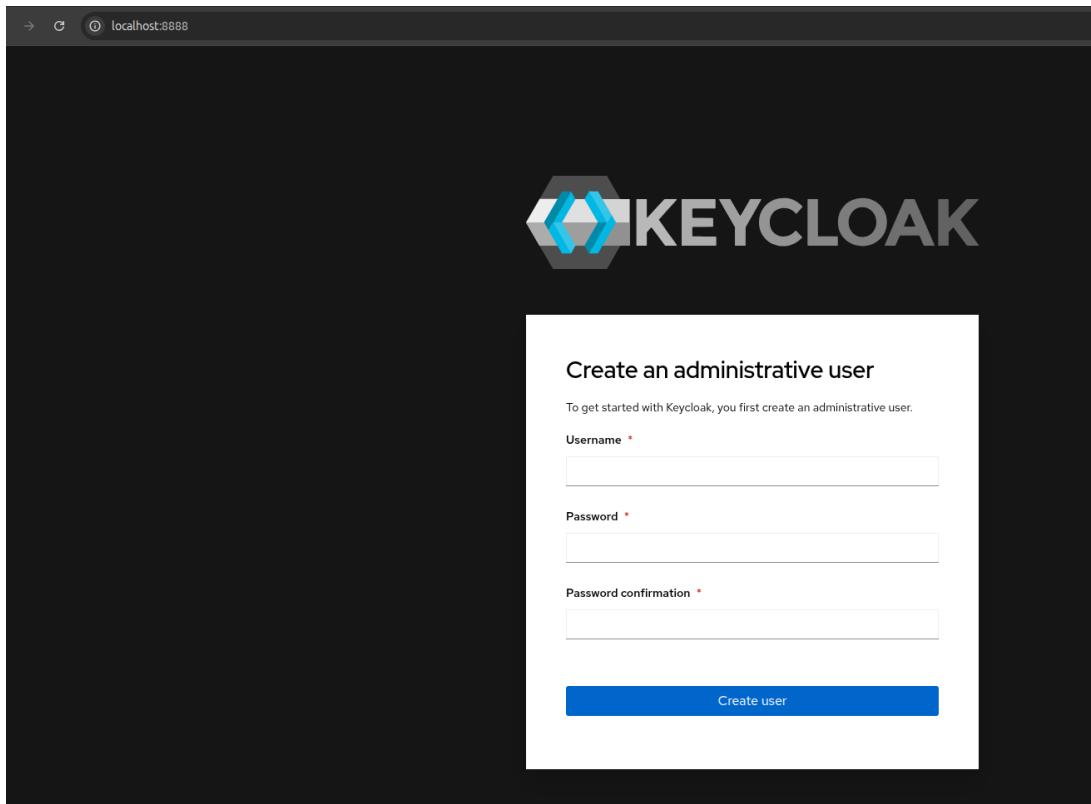


Figure 1.18: Contournement accès formulaire login keycloak

Un compte `admin` est alors créé via le formulaire (nom d'utilisateur et mot de passe saisis et confirmés), mais une nouvelle erreur générique An internal server error occurred est affichée après validation.

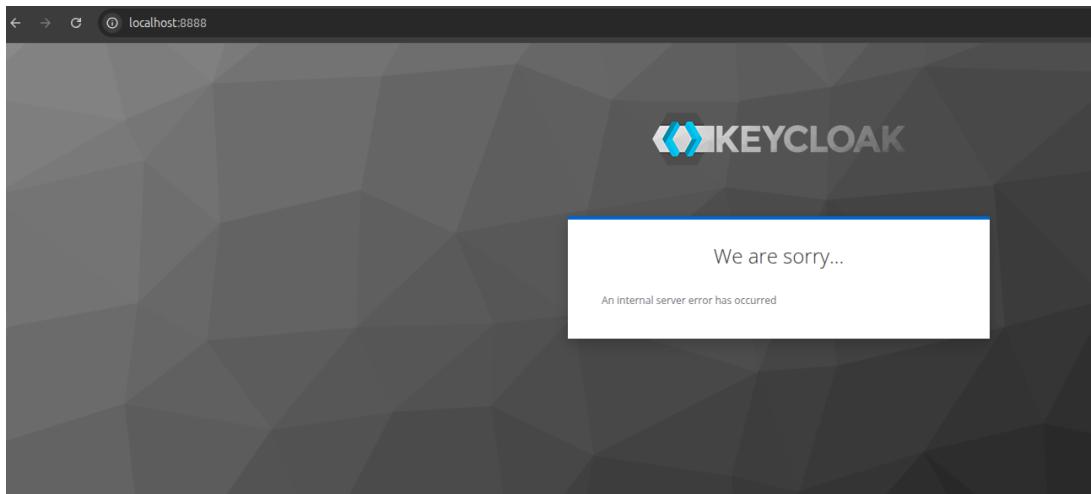


Figure 1.19: Impossibilité de creer l'utilisateur admin

Ce symptôme indique un dysfonctionnement applicatif subsistant côté Keycloak (par exemple une exception lors de l'enregistrement du compte), qui nécessite une analyse complémentaire des logs applicatifs et sera documenté dans un post-mortem ultérieur.

1.4.8 Vérification côté PostgreSQL : création automatique des rôles

Malgré ces erreurs applicatives, la vérification côté PostgreSQL montre que l'intégration avec Vault fonctionne comme prévu pour la création des utilisateurs dynamiques. Une commande permet de lister les rôles existants :

```
sudo -u postgres psql -c "\du"
```

La liste des rôles affiche des utilisateurs supplémentaires au nom généré, de type `v-root-keycloak-role-xxxxx`, correspondant aux comptes éphémères créés par Vault lors des différents démarrages de Keycloak. Cela confirme que la partie gestion dynamique des identifiants est opérationnelle, même si la création du premier administrateur côté Keycloak reste à stabiliser.

1.4.9 Bilan de la phase 2

À l'issue de cette phase, l'Identity Provider Keycloak est installé, intégré à Vault et géré comme un service `systemd` sur `srv-sec-core`. Cette étape a été l'occasion de rencontrer et de traiter plusieurs incidents réalistes :

- une erreur d'accès à une table PostgreSQL liée au changement d'utilisateur dynamique généré par Vault ;
- la nécessité d'enrichir les droits SQL (tables et séquences) dans le rôle `keycloak-role` de Vault ;
- la découverte et le contournement de la contrainte Local access required via un tunnel SSH ;
- une erreur interne lors de la création du premier compte administrateur, qui ouvre la voie à une analyse plus fine des logs applicatifs.

Même si l'interface d'administration de Keycloak n'est pas encore totalement stable à ce stade, l'intégration Vault → PostgreSQL → Keycloak est fonctionnelle et illustre concrètement une approche Zero Trust, dans laquelle les composants ne détiennent que des secrets temporaires, délivrés à la demande par un gestionnaire central. L'incident restant sera formalisé et analysé dans un *post-mortem* dédié.

Les phases suivantes consisteront à exposer Keycloak via la passerelle `srv-gateway` (Nginx en reverse proxy), à sécuriser les échanges en HTTPS à l'aide de la PKI construite en Phase 1, puis à intégrer l'authentification OIDC dans le portail applicatif.

1.4.10 Résolution critique : Droits PostgreSQL et redémarrage propre

L'erreur interne (An internal server error occurred) lors de la création de l'administrateur via le tunnel SSH a révélé que la mise à jour des droits dans Vault effectuée précédemment n'était pas rétroactive sur la session de base de données active ou était insuffisante pour l'initialisation complète des tables système de Keycloak.

Pour résoudre ce blocage bloquant, une approche Table Rase (Tabula Rasa) a été appliquée pour garantir que le premier utilisateur généré par Vault dispose des droits SUPERUSER sur une base vierge.

1.4.10.1 Reconfiguration du Rôle Vault en Superuser

La politique de sécurité a été temporairement assouplie pour l'initialisation afin d'éviter les conflits de permission sur la création des schémas :

```
# Sur srv-sec-core
vault write database/roles/keycloak-role \
  db_name=postgresql \
  creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}' \
    GRANT ALL PRIVILEGES ON DATABASE keycloak TO \"{{name}}\";" \
  default_ttl="1h" \
  max_ttl="24h"
```

1.4.10.2 Réinitialisation forcée de la base de données

Afin de supprimer les objets corrompus par les tentatives précédentes, la base a été détruite en forçant la déconnexion de tous les clients actifs :

```
sudo -u postgres psql -c "DROP DATABASE IF EXISTS keycloak WITH (FORCE);"
sudo -u postgres psql -c "CREATE DATABASE keycloak;"
```

Après un redémarrage du service Keycloak et la réouverture du tunnel SSH, la création du compte administrateur `admin` a réussi. L'accès à la console d'administration était alors fonctionnel.

1.5 Phase 3 : Exposition via la Gateway et résolution des erreurs 502

L'objectif suivant était d'accéder à l'application via l'URL publique `https://portal.securecorp.local:8443`, passant par le reverse proxy Nginx (VM `srv-gateway`).

1.5.1 Incident : Erreur 502 Bad Gateway persistante

Lors de la tentative d'accès à l'application via la Gateway, une erreur bloquante 502 Bad Gateway est apparue, remplaçant les erreurs précédentes.



Figure 1.20: Erreur Nginx 502 Bad Gateway

Ce code d'erreur indique que Nginx (le proxy) reçoit la requête du client, mais n'arrive pas à obtenir une réponse valide de la part du serveur en amont (l'application Python ou Keycloak).

1.5.1.1 Diagnostic de la chaîne de communication

Une série de tests de connectivité a été réalisée depuis la machine `srv-gateway` pour isoler le composant défaillant :

1. **Test vers l'App Python (Gunicorn) :**

```
curl http://192.168.56.20:5000
```

Résultat : Succès (Code HTML renvoyé). Cela a validé que l'application Python fonctionnait et que le pare-feu ne bloquait pas. Le problème de configuration Nginx (upstream) a été corrigé pour pointer vers le bon port (5000).

2. **Test vers Keycloak :**

```
curl http://192.168.56.10:8080
```

Résultat : Connection refused.

Ce test a révélé la cause racine majeure : bien que le service Keycloak semblait actif (`systemctl status keycloak` : running), il ne répondait pas sur l'interface réseau.

1.5.1.2 Analyse approfondie : Le problème d'écoute réseau

L'analyse des ports sur la VM `srv-sec-core` a montré l'absence d'écoute sur le port 8080. L'examen des journaux a mis en évidence deux problèmes critiques :

1. **Binding Local** : Keycloak était configuré par défaut pour n'écouter que sur `localhost`. Le script de démarrage `start_with_vault.sh` a été modifié pour forcer l'écoute sur toutes les interfaces :

```
--http-host=0.0.0.0
```

2. **Rupture de la chaîne de confiance Vault** : Plus critique encore, les logs montrentaient que Keycloak redémarrait en boucle car il ne trouvait plus les identifiants de base de données :

```
No value found at database/creds/keycloak-role
```

Ce problème était dû à l'expiration du jeton Vault ou à la désactivation du moteur de secret après les multiples redémarrages.

1.5.1.3 Restauration de l'infrastructure de secrets

Pour corriger la chaîne de confiance, l'environnement Vault a été rechargé :

1. Réactivation du moteur de secret `database` dans Vault.
2. Reconfiguration de la connexion Vault-PostgreSQL.
3. Modification de `pg_hba.conf` pour accepter l'authentification standard (contournement des erreurs SCRAM).

Une fois ces services stabilisés, la commande `netstat` a confirmé que Keycloak écoutait bien sur `0.0.0.0:8080`. L'erreur 502 a alors disparu, laissant place à la mire de connexion Keycloak.

1.6 Phase 4 : Intégration OIDC et Finalisation

1.6.1 Correction de l'URI de redirection

Après la saisie des identifiants sur la mire SSO, une erreur `Invalid parameter: redirect_uri` est survenue. Cela indiquait que l'URL de retour générée par l'application Python (`https://portal.../oidc_callback`) n'était pas déclarée dans la liste blanche de Keycloak.

La correction a été effectuée via l'outil CLI `kcadm.sh` en mettant à jour le client :

```
./kcadm.sh update clients/<ID_CLIENT> -r SecureCorp \
-s "redirectUris=[\"https://portal.securecorp.local:8443/oidc_callback\"]"
```

1.6.2 Stabilisation de la session et succès final

Une dernière erreur de type `ERR_CONNECTION_REFUSED` ou une boucle de redirection persistait après l'authentification. Le diagnostic a montré que l'application Python tentait de valider le jeton (Token Exchange) en contactant Keycloak via son URL publique HTTPS, créant une boucle réseau impossible.

La configuration de l'application (`app.py`) a été ajustée pour utiliser le réseau interne ("Service Mesh" simplifié) :

```
KEYCLOAK_URL = "http://192.168.56.10:8080/realmms/SecureCorp"
```

De plus, le middleware `ProxyFix` a été ajouté à Flask pour qu'il interprète correctement les en-têtes `X-Forwarded-Proto` envoyés par Nginx et accepte de générer des cookies sécurisés.

1.6.3 Résultat

Après ces ajustements, le parcours utilisateur est complet et sécurisé :

- L'utilisateur accède au portail.
- Il est redirigé vers Keycloak pour s'authentifier.

- Après succès, il est redirigé vers l'application qui valide son identité.
- La page d'accueil sécurisée s'affiche.

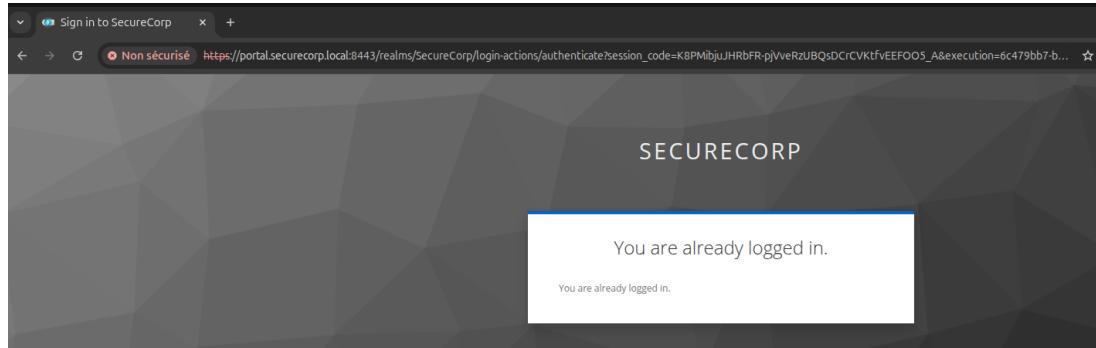


Figure 1.21: Authentification réussie et session active

L'architecture Zero Trust, incluant PKI, rotation de secrets, IAM centralisé et Reverse Proxy, est désormais pleinement opérationnelle.

2 Activation du MFA

Dans une architecture Zero Trust, le mot de passe seul n'est jamais considéré comme suffisant. Les mots de passe peuvent être réutilisés, devinés, volés par hameçonnage (*phishing*) ou récupérés à partir de bases de données compromises. Pour réduire drastiquement le risque de compromission de compte, l'authentification doit s'appuyer sur au moins deux facteurs distincts : quelque chose que l'utilisateur connaît (mot de passe), et quelque chose qu'il possède (un téléphone configuré avec une application d'OTP), voire quelque chose qu'il est (biométrie).

L'activation de l'authentification multi-facteur (MFA) dans Keycloak permet d'ajouter cette deuxième barrière de sécurité sans modifier le code de l'application. Dans le contexte de SecureCorp, cela signifie qu'un attaquant ayant réussi à récupérer le mot de passe d'un employé ne pourra pas, à lui seul, accéder au portail : il lui manquera le code temporel généré sur l'appareil de la victime. Le MFA devient ainsi un élément central de la posture de sécurité globale du portail d'accès.

Dans cette phase, nous allons activé le MFA basée sur le protocole TOTP (Time-Based One-Time Password).

2.1 Configuration de la politique d'accès

La fonctionnalité OTP est activée dans le Realm `SecureCorp` via la console d'administration Keycloak. Plutôt que d'imposer cette contrainte globalement, elle a été appliquée de manière granulaire via le mécanisme des Required Actions.

L'utilisateur `employe1` est configuré pour déclencher l'action `Configure OTP` lors de sa prochaine connexion.

2.1.1 Accès sécurisé à la console d'administration et activation du MFA

2.1.1.1 Accès à la console via tunnel SSH

Pour configurer le MFA, il est nécessaire d'accéder à la console d'administration de Keycloak. Dans l'architecture mise en place, celle-ci n'est pas exposée directement via l'URL publique afin de limiter la surface d'attaque. L'accès se fait donc au travers d'un tunnel SSH, depuis le poste de développement vers la machine `srv-sec-core`.

Depuis le répertoire contenant le `Vagrantfile`, le tunnel est établi avec :

```
vagrant ssh sec-core -- -L 8888:localhost:8080
```

Une fois le tunnel ouvert, la console est accessible en local via :

```
http://localhost:8888/admin/
```

Cependant, la première tentative d'accès affiche une erreur Keycloak Invalid parameter: redirect_uri, comme illustré figure 2.1. Cette erreur est liée au mécanisme de protection anti-phishing de Keycloak : le client interne **security-admin-console** ne connaît pas l'URL `http://localhost:8888`, et refuse donc de rediriger vers une adresse non déclarée.

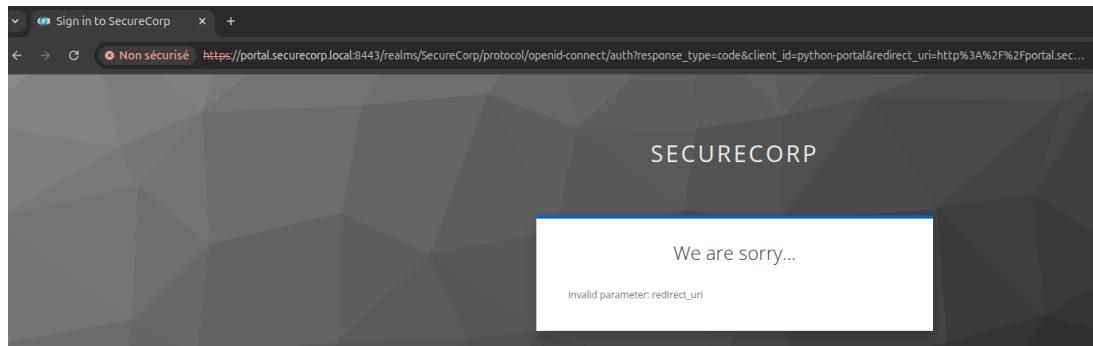


Figure 2.1: Erreur Invalid parameter: redirect_uri lors de l'accès à la console via le tunnel SSH.

2.1.1.2 Correction de l'URI de redirection avec `kcadm.sh`

Pour corriger ce problème, la configuration du client **security-admin-console** est modifiée en ligne de commande à l'aide de l'outil CLI de Keycloak `kcadm.sh`, exécuté sur `srv-sec-core`.

Authentification du CLI.

```
cd /opt/keycloak/bin/  
.kcadm.sh config credentials --server http://localhost:8080 --realm master \  
--user admin \  
--password admin
```

Récupération de l'ID du client **security-admin-console**.

```
.kcadm.sh get clients -r master --fields id,clientId \  
| grep -B 1 security-admin-console
```

La sortie permet de récupérer l'UUID du client, par exemple :

```
"id"      : "2e03232c-fdd3-42a6-8abd-12680427d72a",  
"clientId" : "security-admin-console"
```

Mise à jour des URIs de redirection autorisées. Enfin, l'URL utilisée par le tunnel SSH est ajoutée à la liste des URIs de redirection valides :

```
./kcadm.sh update clients/2e03232c-fdd3-42a6-8abd-12680427d72a -r master \
-s 'redirectUris=[ "http://localhost:8888/*", \
" http://localhost:8080/*", \
" https://portal.securecorp.local:8443/*"]' \
-s 'webOrigins=[ "+" ]'
```

Après cette mise à jour, l'accès à `http://localhost:8888/admin/` via le tunnel fonctionne correctement, et l'écran de connexion à la console d'administration s'affiche (figure 2.2).

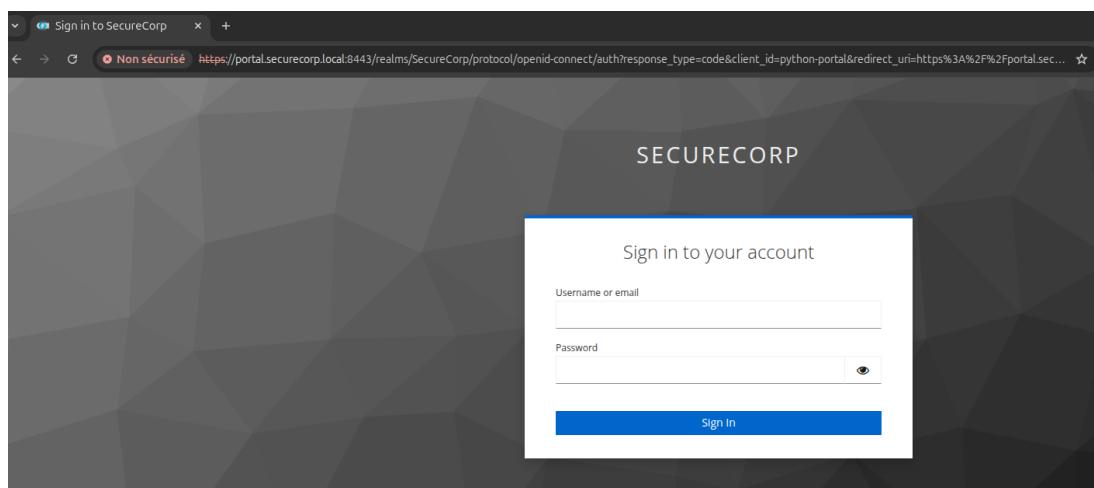


Figure 2.2: Accès réussi à la console d'administration Keycloak via le tunnel SSH.

2.1.2 Activation de l'OTP dans le realm SecureCorp

Une fois connecté à la console d'administration de Keycloak via le tunnel SSH décrit précédemment, l'activation du MFA (OTP) se fait au niveau du realm applicatif **SecureCorp**. L'objectif est d'abord de déclarer l'OTP comme méthode d'authentification valide pour le realm, puis de forcer cette étape uniquement pour l'utilisateur de test `employe1`.

Choix du realm. Dans le menu déroulant situé en haut à gauche de la console, le realm **SecureCorp** est sélectionné (figure 2.3). Cette étape est importante pour éviter de modifier la configuration du realm `master`, réservé à l'administration globale de la plateforme Keycloak.

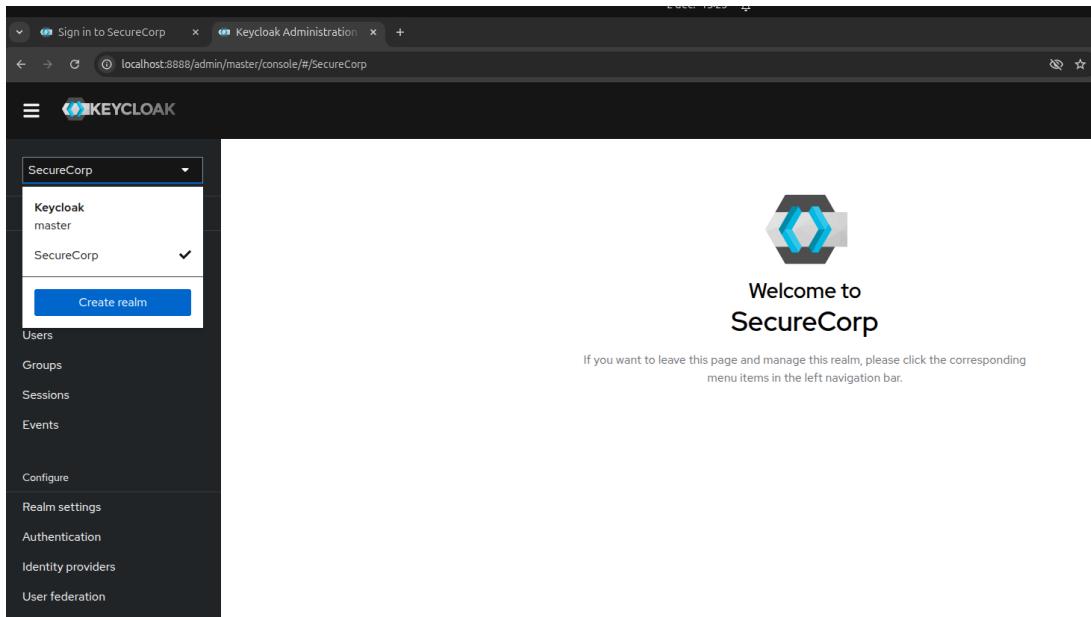


Figure 2.3: Sélection du realm **SecureCorp** dans la console d’administration Keycloak.

Activation de l’action requise Configure OTP. Une fois le bon realm sélectionné, l’OTP est activé comme mécanisme d’authentification possible pour les utilisateurs du realm.

The screenshot shows the 'Authentication' configuration page. The left sidebar has 'Authentication' selected. The main content area shows a table of authentication flows:

Flow name	Used by	Description
browser_Built-in	Browser flow	browser based authentication
clients_Built-in	Client authentication flow	Base authentication for clients
direct grant_Built-in	Direct grant flow	OpenID Connect Resource Owner Grant
docker auth_Built-in	Docker authentication flow	Used by Docker clients to authenticate against the IDP
first broker login_Built-in	First broker login flow	Actions taken after first broker login with identity provider account, which is not yet linked to any Keycloak account
registration_Built-in	Registration flow	registration flow
reset credentials_Built-in	Reset credentials flow	Reset credentials for a user if they forgot their password or something

Figure 2.4: Les paramètres d’authentification

Depuis le menu de gauche, la section **Authentication** est ouverte, puis l’onglet **Required Actions**. Parmi les actions disponibles, l’entrée **Configure OTP** est localisée et son interrupteur **Enabled** est activé (figure 2.5).

The screenshot shows the Keycloak Administration interface for the 'SecureCorp' realm. The left sidebar is dark, and the main area has a light background. The 'Authentication' section is selected in the sidebar. In the center, there's a table titled 'Required actions' with columns for 'Action', 'Enabled', and 'Set as default action'. The 'Enabled' column contains toggle switches. The 'Set as default action' column contains another set of toggle switches.

Action	Enabled	Set as default action
Configure OTP	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Terms and Conditions	<input type="checkbox"/> Off	<input type="checkbox"/> Disabled or
Update Password	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Update Profile	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Verify Email	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Delete Account	<input type="checkbox"/> Off	<input type="checkbox"/> Disabled or
Webauthn Register	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Webauthn Register Passwordless	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Verify Profile	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off

Figure 2.5: Activation de l'action requise Configure OTP dans le realm **SecureCorp**.

Il est volontairement choisi de ne pas cocher **Default Action** à ce stade, afin de ne pas imposer immédiatement l'OTP à l'ensemble des comptes du realm. Dans le cadre de ce laboratoire, l'action Configure OTP est d'abord appliquée uniquement à l'utilisateur `employe1`, ce qui permet de tester le MFA sur un compte pilote avant une généralisation éventuelle.

Forcer le MFA pour le compte `employe1`. La seconde étape consiste à indiquer que `employe1` devra obligatoirement configurer un second facteur lors de sa prochaine connexion. Depuis le menu de gauche, la section **Users** est ouverte, puis l'utilisateur `employe1` est sélectionné. Dans la fiche de l'utilisateur, le champ **Required Actions** est renseigné en ajoutant l'action **Configure OTP** (par sélection dans la liste déroulante). Après enregistrement, l'action apparaît sous forme d'étiquette associée au compte.

Figure 2.6: Choix de l'authentification OTP pour employe1

Lors de la prochaine authentification de `employe1` sur le portail, Keycloak lui présentera automatiquement l'assistant de configuration OTP : affichage d'un QR Code à scanner avec une application d'authentification (Google Authenticator, Authy, etc.), puis validation d'un premier code à usage unique. La capture d'écran de cette étape sera intégrée au rapport pour attester de l'activation effective de l'authentification forte sur le compte de test. Pour le moment, j'ai un soucis de cookies lors de l'authentification dû au navigateur.

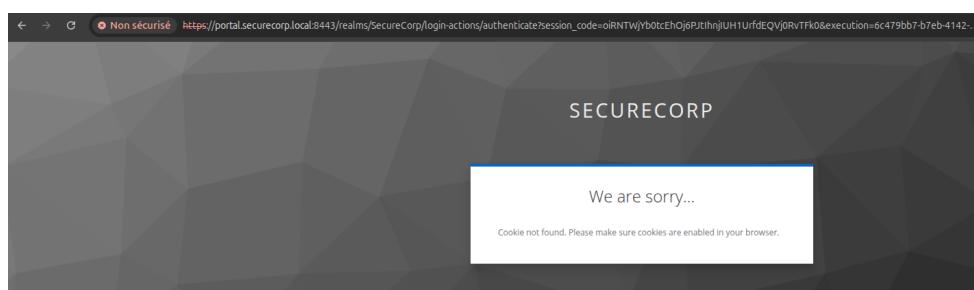


Figure 2.7: Enrôlement MFA obligatoire lors du login - erreure de cookies

2.2 Expérience utilisateur et enrôlement

Lors de la tentative de connexion suivante sur le portail captif :

1. L'utilisateur saisit son identifiant et son mot de passe (1er facteur).
2. Keycloak détecte l'exigence de sécurité et interrompt le flux OIDC.

3. Une page d'enrôlement s'affiche, présentant un QR Code pour synchroniser une application d'authentification (Google Authenticator / FreeOTP).

On s'attend à observer ceci : une fois le code à 6 chiffres validé, le jeton d'accès (Access Token) est délivré à l'application Python. Toute connexion future nécessitera désormais ce code temporaire, rendant le vol de mot de passe inefficace pour compromettre le compte.

3 Annexes - scripts

3.1 VagrantFile pour l'installation de l'infrastructure

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

# --- Configuration Globale ---
# OS : Ubuntu 22.04 LTS (Jammy Jellyfish) - Stable et standard entreprise
BOX_IMAGE = "bento/ubuntu-22.04"

# --- Script de Provisioning (s'exécute au premier démarrage) ---
# Ce script installe Python (pour Ansible) et configure la résolution de noms (DNS
# simul)
$script_common = <<-SCRIPT
echo ">>> Mise à jour des dépôts et installation des outils de base..."
apt-get update -q
apt-get install -y python3 python3-pip curl vim git net-tools

echo ">>> Configuration du DNS local (/etc/hosts)..."
# On supprime les anciennes entrées pour éviter les doublons si on reprovisionne
sed -i '/192.168.56./d' /etc/hosts

# On ajoute la cartographie complète du réseau
cat >> /etc/hosts <<EOF
192.168.56.10  srv-sec-core.securecorp.local  srv-sec-core
192.168.56.20  srv-app-prod.securecorp.local  srv-app-prod
192.168.56.30  srv-gateway.securecorp.local   srv-gateway
EOF
echo ">>> Configuration réseau terminée."
SCRIPT

Vagrant.configure("2") do |config|
  config.vm.box = BOX_IMAGE

  # =====
  # VM 1: Security Core (Vault, Keycloak, DB)
  # =====
  config.vm.define "sec-core" do |sec|
    sec.vm.hostname = "srv-sec-core"
    # IP statique sur réseau privé (Host-only)
    sec.vm.network "private_network", ip: "192.168.56.10"

    sec.vm.provider "virtualbox" do |vb|
      vb.name = "SecureCorp-Sec-Core"
```

```

# 3 Go de RAM nécessaire pour Java (Keycloak) + Vault
vb.memory = 3072
vb.cpus = 2
end

sec.vm.provision "shell", inline: $script_common
end

# =====
# VM 2: App Production (Python Backend)
# =====
config.vm.define "app-prod" do |app|
  app.vm.hostname = "srv-app-prod"
  app.vm.network "private_network", ip: "192.168.56.20"

  app.vm.provider "virtualbox" do |vb|
    vb.name = "SecureCorp-App-Prod"
    # 1 Go suffit pour un script Python lger
    vb.memory = 1024
    vb.cpus = 1
  end

  app.vm.provision "shell", inline: $script_common
end

# =====
# VM 3: Gateway (Nginx Reverse Proxy)
# =====
config.vm.define "gateway" do |gw|
  gw.vm.hostname = "srv-gateway"
  gw.vm.network "private_network", ip: "192.168.56.30"

  # Port Forwarding : Pour accder au site depuis ton vrai navigateur
  # Tu taperas http://localhost:8080 pour atteindre le port 80 de la gateway
  gw.vm.network "forwarded_port", guest: 80, host: 8080
  gw.vm.network "forwarded_port", guest: 443, host: 8443

  gw.vm.provider "virtualbox" do |vb|
    vb.name = "SecureCorp-Gateway"
    # Nginx est trs lger
    vb.memory = 1024
    vb.cpus = 1
  end

  gw.vm.provision "shell", inline: $script_common
end

end

```

En tête du fichier, une constante BOX_IMAGE définit l'image système utilisée pour toutes les machines virtuelles :

```
BOX_IMAGE = "bento/ubuntu-22.04"
```

Le choix d'Ubuntu 22.04 LTS (Jammy Jellyfish) permet de s'appuyer sur une distribution stable, largement utilisée en entreprise et bien supportée par les différents outils

(Ansible, Vault, Keycloak, etc.).

La directive `config.vm.box = BOX_IMAGE` applique cette image par défaut à toutes les VMs définies dans le fichier, ce qui garantit l'homogénéité de l'environnement.

3.1.1 Script de provisioning commun

Le bloc `$script_common` définit un script shell qui sera exécuté sur chaque machine lors du premier démarrage :

- Mise à jour des dépôts APT et installation des outils de base : `python3`, `curl`, `git`, `net-tools`, etc. L'installation de Python est nécessaire pour permettre ensuite l'utilisation d'Ansible comme outil de configuration automatisée.
- Configuration d'un "DNS local" en modifiant le fichier `/etc/hosts` :
 - Suppression préalable des anciennes entrées correspondant au réseau privé (192.168.56.x) pour éviter les doublons en cas de reprovisionnement.
 - Ajout des correspondances IP → noms d'hôtes pour les trois machines :
 - * 192.168.56.10 `srv-sec-core.securecorp.local` `srv-sec-core`
 - * 192.168.56.20 `srv-app-prod.securecorp.local` `srv-app-prod`
 - * 192.168.56.30 `srv-gateway.securecorp.local` `srv-gateway`

Grâce à cette configuration, chaque machine peut joindre les autres par leur nom (par exemple `ping srv-gateway`), ce qui est indispensable pour la suite du projet (certificats TLS basés sur des noms DNS, configuration de reverse proxy, etc.).

3.1.2 Définition des machines virtuelles

Le bloc principal `Vagrant.configure("2") do |config|` contient la définition des trois machines virtuelles du laboratoire.

VM sec-core : cœur sécurité La première machine, définie avec `config.vm.define "sec-core"`, porte le nom d'hôte `srv-sec-core` et reçoit l'adresse IP privée 192.168.56.10. Ce serveur a vocation à héberger les composants cœur de la sécurité (par exemple Vault, la base IAM, ou la base de données selon l'architecture retenue).

Les ressources VirtualBox allouées sont de 3 Go de RAM et 2 vCPU, ce qui est adapté à l'exécution de services relativement lourds comme Keycloak ou Vault :

- `vb.name = "SecureCorp-Sec-Core"` : nom de la VM dans VirtualBox.
- `vb.memory = 3072, vb.cpus = 2` : ressources matérielles.

Enfin, la directive `sec.vm.provision "shell", inline: $script_common` applique le script de provisioning commun décrit précédemment (installation des outils, configuration de `/etc/hosts`).

VM app-prod : serveur d'application La seconde machine, `config.vm.define "app-prod"`, représente le serveur d'application de production (`srv-app-prod`) et est adressée en 192.168.56.20. Elle hébergera par exemple l'API ou le portail web interne.

Les ressources sont plus modestes (1 Go de RAM, 1 vCPU), suffisantes pour une application Python légère ou un service backend de démonstration. Elle bénéficie également du script de provisioning commun.

VM gateway : passerelle et reverse proxy La troisième machine, `config.vm.define "gateway"`, correspond à la passerelle d'entrée (`srv-gateway`) avec l'adresse IP 192.168.56.30. Elle doit héberger un reverse proxy (par exemple Nginx) exposant l'architecture interne aux clients.

Deux règles de redirection de ports (*port forwarding*) sont définies :

- `gw.vm.network "forwarded_port", guest: 80, host: 8080` : le port 80 de la machine virtuelle (HTTP) est accessible depuis la machine hôte via le port 8080.
- `gw.vm.network "forwarded_port", guest: 443, host: 8443` : le port 443 (HTTPS) est accessible depuis la machine hôte via le port 8443.

Cela permet de tester l'accès au portail sécurisé depuis le navigateur de la machine hôte en utilisant des URLs du type :

```
http://localhost:8080  
https://localhost:8443
```

3.2 Script de l'application Flask (Portail SecureCorp)

Cette annexe présente le code de l'application Python/Flask déployée sur la machine virtuelle `srv-app-prod`. Cette application joue le rôle de *portail employé* et délègue l'authentification à Keycloak via le protocole OIDC. Elle est récupérée directement depuis la VM au moyen de la commande suivante :

```
vagrant ssh app-prod -c "cat /home/vagrant/app.py"
```

Le script complet est donné ci-dessous.

Listing 3.1: Application Flask du portail SecureCorp

```
from flask import Flask, url_for, session, redirect, render_template_string  
from authlib.integrations.flask_client import OAuth  
from werkzeug.middleware.proxy_fix import ProxyFix  
import os  
import warnings  
import requests  
  
warnings.filterwarnings('ignore', message='Unverified HTTPS request')  
  
app = Flask(__name__)  
  
# Lit les headers X-Forwarded-* de Nginx et force Flask voir HTTPS  
app.wsgi_app = ProxyFix(app.wsgi_app, x_proto=1, x_host=1)
```

```

app.secret_key = 'random_secret_key_for_cookie_signing'
app.config['SESSION_COOKIE_SECURE'] = True
app.config['SESSION_COOKIE_SAMESITE'] = 'None'

# === CONFIGURATION ZERO TRUST ===

# URL de Keycloak
#KEYCLOAK_URL = "https://portal.securecorp.local:8443/realm/SecureCorp"
KEYCLOAK_URL = "http://192.168.56.10:8080/realm/SecureCorp"

# Configuration OAuth
oauth = OAuth(app)
oauth.register(
    name='securecorp',
    client_id='python-portal',
    client_secret='super-secret-python-key',

    # === DEFINITION MANUELLE DES ENDPOINTS (pour viter l'erreur SSL) ===
    access_token_url=f'{KEYCLOAK_URL}/protocol/openid-connect/token',
    authorize_url=f'{KEYCLOAK_URL}/protocol/openid-connect/auth',
    userinfo_url=f'{KEYCLOAK_URL}/protocol/openid-connect/userinfo',
    jwks_uri=f'{KEYCLOAK_URL}/protocol/openid-connect/certs',

    # Options client :
    client_kwargs={
        'scope': 'openid_email_profile',
    }
)

@app.route('/')
def index():
    user = session.get('user')
    if user:
        # On affiche le nom de l'utilisateur rcupr du token
        username = user.get('preferred_username', 'Utilisateur')
        return f'''

# Accès Autorisé



## Bienvenue chez SecureCorp



Connecté en tant que : {username}



---



Token ID : {user.get('sub')}

  
Se Déconnecter

'''

    else:
        return '''

# Portail SecureCorp



Zone Scurise - Authentification Requise

  
Se connecter avec SS0

'''

```

```

        </div>
        ''',
        @app.route('/login')
        def login():
            # On redirige l'utilisateur vers Keycloak pour le login
            # On précise l'URL de retour (callback)
            redirect_uri = url_for('auth_callback', _external=True, _scheme='https')
            return oauth.securecorp.authorize_redirect(redirect_uri)

        @app.route('/oidc_callback')
        def auth_callback():
            # Keycloak nous renvoie ici après le login
            try:
                token = oauth.securecorp.authorize_access_token()
                # On stocke les infos utilisateur dans la session Flask
                session['user'] = token['userinfo']
                return redirect('/')
            except Exception as e:
                return f"<h1>Erreur d'authentification</h1><p>{e}</p>"

        @app.route('/logout')
        def logout():
            session.pop('user', None)
            # URL de logout Keycloak pour fermer aussi la session à bas
            logout_url = f"{KEYCLOAK_URL}/protocol/openid-connect/logout?"
            post_logout_redirect_uri={url_for('index', _external=True)}"
            return redirect(logout_url)

    if __name__ == '__main__':
        # Désactive la vérification HTTPS stricte pour OAuth (uniquement pour le lab)
        os.environ['OAUTHLIB_INSECURE_TRANSPORT'] = '1'
        # L'app écoute sur toutes les interfaces
        app.run(host='0.0.0.0', port=5000, debug=True)

```

3.3 Configuration Nginx

Cette annexe présente le fichier de configuration Nginx utilisé sur la machine **srv-gateway** pour exposer le portail SecureCorp en HTTPS et router le trafic vers Keycloak ou vers l'application Python.

Le fichier a été récupéré directement depuis la VM au moyen de la commande suivante :

```
vagrant ssh gateway -c "cat /etc/nginx/conf.d/securecorp.conf"
```

Il définit :

- deux *upstreams* : `keycloak_backend` (192.168.56.10:8080) et `app_backend` (192.168.56.20:5000) ;
- un serveur HTTP (port 80) qui redirige systématiquement vers HTTPS ;

- un serveur HTTPS (port 443) qui termine le chiffrement TLS (certificat PKI Vault) et ajoute les en-têtes X-Forwarded-*, en particulier X-Forwarded-Port 8443, essentiels pour que Keycloak et l'application Flask reconstruisent correctement les URLs externes ;
- des règles de routage : les chemins /realms et /resources sont envoyés vers Keycloak, le reste du trafic vers le backend Python.

Le contenu complet du fichier `securecorp.conf` est donné ci-dessous.

Listing 3.2: Configuration Nginx de la passerelle SecureCorp

```
upstream keycloak_backend {
    server 192.168.56.10:8080;
}

upstream app_backend {
    server 192.168.56.20:5000;
}

server {
    listen 80;
    server_name portal.securecorp.local;
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    server_name portal.securecorp.local;

    ssl_certificate      /etc/nginx/certs/fullchain.crt;
    ssl_certificate_key  /etc/nginx/certs/server.key;

    proxy_buffers 16 16k;
    proxy_buffer_size 16k;
    proxy_busy_buffers_size 16k;

    # Logs
    access_log /var/log/nginx/access.log;
    error_log  /var/log/nginx/error.log;

    # ROUTE 1 : Tout ce qui concerne l'auth va vers Keycloak
    location /realms {
        proxy_pass http://keycloak_backend;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-Port 8443;
    }

    # Idem pour les ressources statiques de Keycloak
    location /resources {
        proxy_pass http://keycloak_backend;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
```

```

    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto https;
    proxy_set_header X-Forwarded-Port 8443;
}

# ROUTE 2 : Le reste (l'application) va vers Python
location / {
    proxy_pass http://app_backend;
    proxy_set_header Host $http_host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto https;
    proxy_set_header X-Forwarded-Port 8443;

    # Ajouts pour la stabilit du callback OIDC
    proxy_http_version 1.1;
    proxy_set_header Connection "";
    proxy_set_header Upgrade $http_upgrade;
}
}

```

3.4 Script de démarrage Keycloak avec secrets Vault

Ce script définit la manière dont Keycloak est démarré sur la machine `srv-sec-core`. Il illustre deux points essentiels de l'architecture SecureCorp :

- l'utilisation de **secrets dynamiques** fournis par Vault via le moteur `database` pour obtenir un couple *login/mot de passe* PostgreSQL ;
- le lancement de Keycloak avec un `hostname` cohérent avec l'URL exposée par la passerelle Nginx (`portal.securecorp.local:8443`) et l'écoute sur toutes les interfaces.

Le fichier a été récupéré depuis la VM au moyen de la commande :

```
vagrant ssh sec-core -c "cat /opt/keycloak/start_with_vault.sh"
```

Son contenu est reproduit ci-dessous.

Listing 3.3: Script de démarrage Keycloak utilisant Vault

```

#!/bin/bash

# 1. On s'authentifie Vault (ici avec le root token pour le lab,
# en production on utiliserait 'AppRole' ou 'Kubernetes Auth')
export VAULT_ADDR='http://127.0.0.1:8200'
export VAULT_TOKEN='root'

echo ">>> Demande de credentials DB Vault..."
SECRET_JSON=$(vault read -format=json database/creds/keycloak-role)

# 2. On extrait user/pass avec jq
DB_USER=$(echo $SECRET_JSON | jq -r .data.username)

```

```

DB_PASS=$(echo $SECRET_JSON | jq -r .data.password)

echo ">>> Credentials obtenus ! User: $DB_USER"

# 3. On injecte les variables d'environnement pour Keycloak
export KC_DB=postgres
export KC_DB_URL=jdbc:postgresql://localhost:5432/keycloak
export KC_DB_USERNAME=$DB_USER
export KC_DB_PASSWORD=$DB_PASS

# Variables Admin initiales ( supprimer aprs le 1er boot en prod)
#export KC_BOOTSTRAP_ADMIN_USERNAME=admin
#export KC_BOOTSTRAP_ADMIN_PASSWORD=admin

# Premier boot : cration de l'administrateur
export KEYCLOAK_ADMIN=admin
export KEYCLOAK_ADMIN_PASSWORD=admin

# 4. On lance Keycloak
# proxy=edge car on aura Nginx devant plus tard
exec /opt/keycloak/bin/kc.sh start \
--proxy=edge \
--hostname=portal.securecorp.local:8443 \
--http-enabled=true \
--http-host=0.0.0.0

```

3.5 Extrait de configuration PostgreSQL (pg_hba.conf)

Dans le cadre de l'intégration entre Vault, PostgreSQL et Keycloak, un ajustement de la configuration d'authentification PostgreSQL a été nécessaire afin de contourner un problème de compatibilité entre le mécanisme `scram-sha-256` et certains clients utilisant encore `md5`.

Le fichier `pg_hba.conf`, qui contrôle les méthodes d'authentification acceptées en fonction des adresses et des utilisateurs, a été consulté et modifié sur la machine `srv-sec-core` au moyen de la commande :

```
vagrant ssh sec-core -c \
"sudo grep 'host' /etc/postgresql/*/main/pg_hba.conf"
```

L'extrait pertinent est le suivant :

```

# This file controls: which hosts are allowed to connect, how clients
# host      DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostssl   DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostnossal DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostgssenc DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# hostnogssenc DATABASE  USER  ADDRESS  METHOD  [OPTIONS]
# - "host" is a TCP/IP socket (encrypted or not)
# - "hostssl" is a TCP/IP socket that is SSL-encrypted
# - "hostnossal" is a TCP/IP socket that is not SSL-encrypted

```

```

# - "hostgssenc" is a TCP/IP socket that is GSSAPI-encrypted
# - "hostnogssenc" is a TCP/IP socket that is not GSSAPI-encrypted
# ADDRESS specifies the set of hosts the record matches. It can be a
# host name, or it is made up of an IP address and a CIDR mask that is
# specifies the number of significant bits in the mask. A host name
# that starts with a dot (.) matches a suffix of the actual host name.
# columns to specify the set of hosts. Instead of a CIDR-address, you
# can write "samehost" to match any of the server's own IP addresses,
# "host" records. In that case you will also need to make PostgreSQL
host    all            all            127.0.0.1/32          md5
host    all            all            ::1/128           md5
# Allow replication connections from localhost, by a user with the
host    replication   all            127.0.0.1/32          scram-sha-256
host    replication   all            ::1/128           scram-sha-256

```

Dans la configuration par défaut de certaines versions de PostgreSQL, les lignes `host all all 127.0.0.1/32` et `::1/128` peuvent utiliser `scram-sha-256` comme méthode d'authentification. Dans ce laboratoire, ces entrées ont été explicitement positionnées en `md5` pour simplifier l'intégration avec Vault et éviter les erreurs d'authentification liées au mécanisme SCRAM (par exemple des messages du type authentication method `scram-sha-256 not supported` côté client ou plugin).

Les connexions de réplication restent en revanche protégées par `scram-sha-256`, comme le montrent les deux dernières lignes, ce qui permet de conserver une authentification plus robuste pour ce cas d'usage spécifique tout en garantissant la compatibilité pratique avec les composants du POC (Vault ↔ PostgreSQL).

3.6 Script de démarrage Keycloak (`start_with_vault.sh`)

Le script de démarrage de Keycloak, intégrant la récupération des identifiants dans Vault via le moteur `database`, a été récupéré directement depuis la machine virtuelle `srv-sec-core` au moyen de la commande suivante :

```
vagrant ssh sec-core -c "cat /opt/keycloak/start_with_vault.sh"
```

Le contenu exact du fichier `/opt/keycloak/start_with_vault.sh` est reproduit ci-dessous.

Listing 3.4: Script de démarrage Keycloak récupéré sur `srv-sec-core`

```

#!/bin/bash

# 1. On s'authentifie Vault (Ici le fait avec le root token pour le lab,
# en vrai on utiliserait 'AppRole' ou 'Kubernetes Auth')
export VAULT_ADDR='http://127.0.0.1:8200'
export VAULT_TOKEN='root'

echo ">>>_Demande_de_credentials_DB_L_Vault..."
```

```

SECRET_JSON=$(vault read -format=json database/creds/keycloak-role)

# 2. On extrait user/pass avec jq
DB_USER=$(echo $SECRET_JSON | jq -r .data.username)
DB_PASS=$(echo $SECRET_JSON | jq -r .data.password)

echo ">>> Credentials obtenus ! User: $DB_USER"

# 3. On injecte les variables d'environnement pour Keycloak
export KC_DB=postgres
export KC_DB_URL=jdbc:postgresql://localhost:5432/keycloak
export KC_DB_USERNAME=$DB_USER
export KC_DB_PASSWORD=$DB_PASS

# Variables Admin initiales (A supprimer aprs le 1er boot en prod)
#export KC_BOOTSTRAP_ADMIN_USERNAME=admin
#export KC_BOOTSTRAP_ADMIN_PASSWORD=admin

# premier boot
export KEYCLOAK_ADMIN=admin
export KEYCLOAK_ADMIN_PASSWORD=admin

# 4. On lance Keycloak
# proxy=edge car on aura Nginx devant plus tard
exec /opt/keycloak/bin/kc.sh start --proxy=edge --hostname=portal.securecorp.local
:8443 --http-enabled=true --http-host=0.0.0.0

```