INSTITUT DU
DÉVELOPPEMENT ET DES
RESSOURCES EN
INFORMATIQUE
SCIENTIFIQUE

www.idris.fr

SSH Access Management

IDRIS : Jean Zay et SSH

(*) Moyenne T2 2021

Authentification SSH
une affaire de compromis~~sion~~

Le champion : Le mot de passe

- Cycle de vie maitrisé, complexité maitrisée, historisation, gestion centralisée, traçabilité, politique de sécurité
- Réutilisabilité, cassable, facteur simple (*ce que je sais*)

Usage interactif uniquement

Le performeur : La bi-clé SSH

- Incassable (algo/taille), 2ème facteur (*passphrase* - recommandation)
- Cycle de vie non maitrisé, complexité non maitrisée, réutilisabilité, facteur simple (*ce que je possède*), volable, gestion non centralisée, pas de traçabilité

Usage interactif / non interactif

Authentification SSH
une affaire de compromis~~sion~~

Le challenger : Le certificat SSH

- Introduit en 2010 dans le standard OpenSSH
- 2 types : certificat utilisateur et certificat machine
- Pas X.509 (autorité intermédiaire et non standard)
- Bi-clé signée avec une validité, des extensions …. et révocable via une *Key Revocation List* (KRL, analogie à la CRL)
- Technologie utilisées par de nombreuses « grosses » entreprises dans la gestion des droits d'accès
- Evite le TOFU (*Trust On First Use*) lors d'utilisation de certificats machines

Authentification SSH
une affaire de compromis~~sion~~

Anatomie

```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d6"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Données d'identification du certificat

Authentification SSH
une affaire de compromis~~sion~~

Anatomie

```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d6"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Validité

Authentification SSH
une affaire de compromis~~sion~~

Anatomie

```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d6"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Me connecte en tant que bob ou zone-admin

Le principal peut être un nom d'utilisateur et/ou une « zone »

```
echo "zone-admin" > /etc/ssh/auth_principals/alice
```

Authentification SSH
une affaire de compromission

Anatomie


```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Me connecte en tant que bob ou zone-admin

Le principal peut être un nom d'utilisateur et/ou une « zone »

```
echo "zone-admin" > /etc/ssh/auth_principals/alice
```

principal **root** ou zone **root**

Authentification SSH
une affaire de compromis~~sion~~

Anatomie

```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d6"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Directive côté serveur qui n'autorise que
- L'utilisation de la commande script.sh
- Les connexions depuis les IPs 192.168.0.0/24

Authentification SSH
une affaire de compromis~~sion~~

Anatomie

```
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:8bFctQEapc7CLIfVRNusOqbXGVW+hina90LwAnrwRNY
Signing CA: ECDSA SHA256:SX62xT4mcc6XW+bSjHtLLWLXDIuOWaLVTgCcWJNx5iA (using ecdsa-sha2-nistp521)
Key ID: "vault-userpass-bob-f1b15cb5011aa5cec22c87d544dbac3aa6d71955be8629daf742f0027af044d6"
Serial: 17009644117390090909
Valid: from 2021-07-06T16:26:30 to 2021-07-06T16:57:00
Principals:
        bob
        zone-admin
Critical Options:
        force-command /usr/local/bin/script.sh
        source-address 192.168.0.0/24
Extensions:
        permit-pty
        permit-X11-forwarding
```

Permet les
- Sessions interactives
- X11 forwarding

Authentification SSH
une affaire de compromis~~sion~~

Le challenger : Le certificat SSH

Cycle de vie maitrisé, complexité maitrisée, gestion centralisée, traçabilité, 2ème facteur (*passphrase* - recommandation), non réutilisabilité, non cassable, sécurisation au sein du certificat

Facteur simple (*ce que je possède*), pas d'autorité intermédiaire, gestion de « principal », configuration serveur ssh (*AuthorizedKeysFile*..), passage à l'échelle difficile

Usage interactif / non interactif

INTERESSANT MAIS

Nécessite système de gestion ⇨ SSHAM

SSHAM : une IGC/AC de gestion de certificats SSH utilisateurs

OBJECTIFS

- disposer d'une IGC/AC « rapide » à déployer et sécurisée (CONTENEUR/ANSIBLE/…?)
- disposer d'outils de gestion de certificats SSH « utilisateurs » par API REST (création, personnalisation, révocation)
- permettre l'établissement d'une politique de sécurité des certificats SSH analogue et compatible avec une politique de sécurité des mots de passe
- ouvrir le code à la communauté

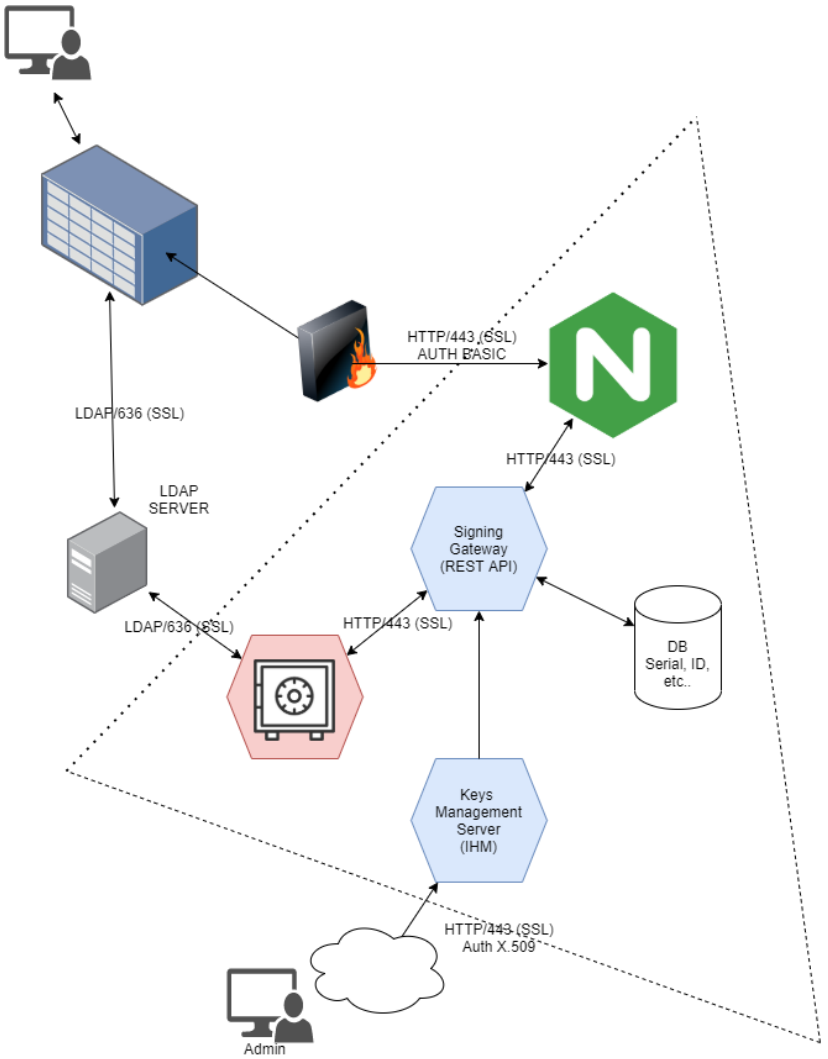
ECOSYSTEME

Plusieurs projets analogues existent : *CASSH*, *SignMyKey*, *Teleport*..
Mais peu adaptés à un usage HPC (délivré par confiance, en général pour un nombre limité de « principal »)

SSHAM : une IGC/AC de gestion de certificats SSH utilisateurs

ARCHITECTURE ET TECHNOLOGIES

- Signature: Hicorp Vault
- Reverse Proxy : nginx
- Signing Gateway : python3
- BDD : SQL compatible
- Key Management Server : *TODO*
- Traçabilité : nginx, SG, Vault, DB



SSHAM : une IGC/AC de gestion de certificats SSH utilisateurs

OBJECTIFS DE SECURITE

- Maitriser la sécurité des authentificateurs (unicité, validité, complexité)
- Traçabilité fine et complète

CAS D'USAGES – exemples de politiques de sécurité

Usage	Nom	Validité	Passphrase	Extensions	Options Critiques
Interactif	pty	365j	OUI	n/a	permit-pty permit-X11-forwarding
Transfert non interactif	rsync	7j	NON	force-command source-address	n/a
Intégration continue	ci	150j	NON	force-command source-address	n/a

SSHAM : une IGC/AC de gestion de certificats SSH utilisateurs

DEMONSTRATION

SSHAM : une IGC/AC de gestion de certificats SSH utilisateurs

QUESTIONS