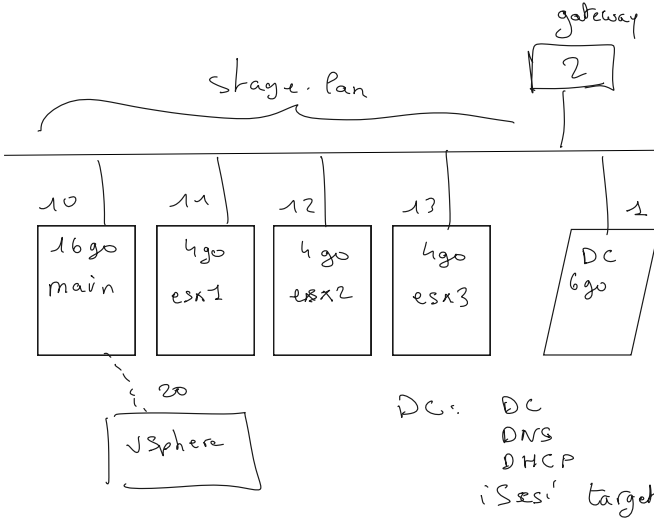
Bonjour tout le monde

https://master.discimus.fr:59890/sharing/nhfw8l3M2

esx000000.francecentral.cloudapp.azure.com

https://master.discimus.fr:59890/sharing/YyoQ8CQLb

lien vers la VM Windows :
https://master.discimus.fr:59890/sharing/CQDJzis8J



Public Key Infrastructure

→ infra de clef d'entreprise (certificats) → Rôles

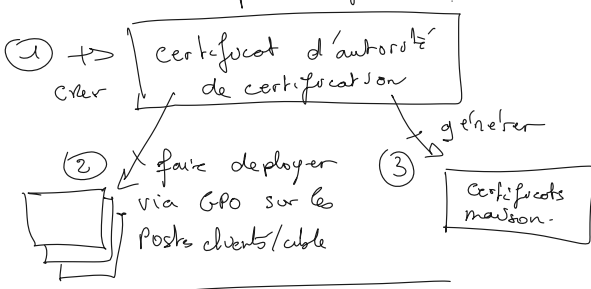
→ Cryptage

→ Authentification

↙ Signés d'une autorité reconnue.

↘ certificats auto signés

Propre infra de certificats



V Center HA

Hashage : obtenir une valeur unique pour une valeur en entrée

f(v1) → v2 non reversible

Authentification par clef

Cryptage → Symétrique (une clef)
→ Asymétrique (2 clefs)

HASH

f(v1) → v2

fonction ? ex CRC Cyclic Redordancy Check

CRC

123 → 6

Collision : 132 → 6

---

fichier → hash → empreinte

ex md5 Collision → prouvé comme possible

sha0 → obsolète

sha1 → " depuis 1 année (128 bits)

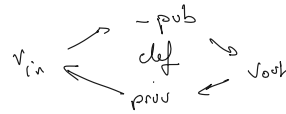
sha2 (224, 256, 512, 1024 ou 2kbits)

Cryptage

Symétrique

V_{in} → clef → V_{out}
(mdp)

Asymétrique



~~DES~~ → obsolète

3DES — DES 3 passes avec 3 clefs

2 clefs

- 1 certificat stocke
  - Symétrique
  - Asymétrique
  - Type de cryptage
  - valeurs de clefs -