Sécurité dans les environnements infonuagiques

Module 1 : Introduction à l'infonuagique (Partie 1)

Armstrong Foundjem, Ph.D

Polytechnique Montréal

Automne 2022

Plan du module

Sondage ☺: `https://www.wooclap.com/BNTAML`.

wooclap

Qu'es ce que l'infonuagique ?

L'infonuagique permet

1. l'accès distant
2. à la demande
3. des ressources
   1. calcul
   2. stockage
   3. reseau
4. la reduction des coûts
   1. matériels on-premise et off-premise
   2. de gestion/maintenance
   3. en temps
   4. de passage à l'échelle
5. mutualisation (pooling)

Quels sont les types de nuage ?

Cloud Public

- Paiement à l'utilisation
- Stockage illimité
- Reduction des coûts
- Evolutif
- Exposition aux risques de sécurité

Cloud Privé

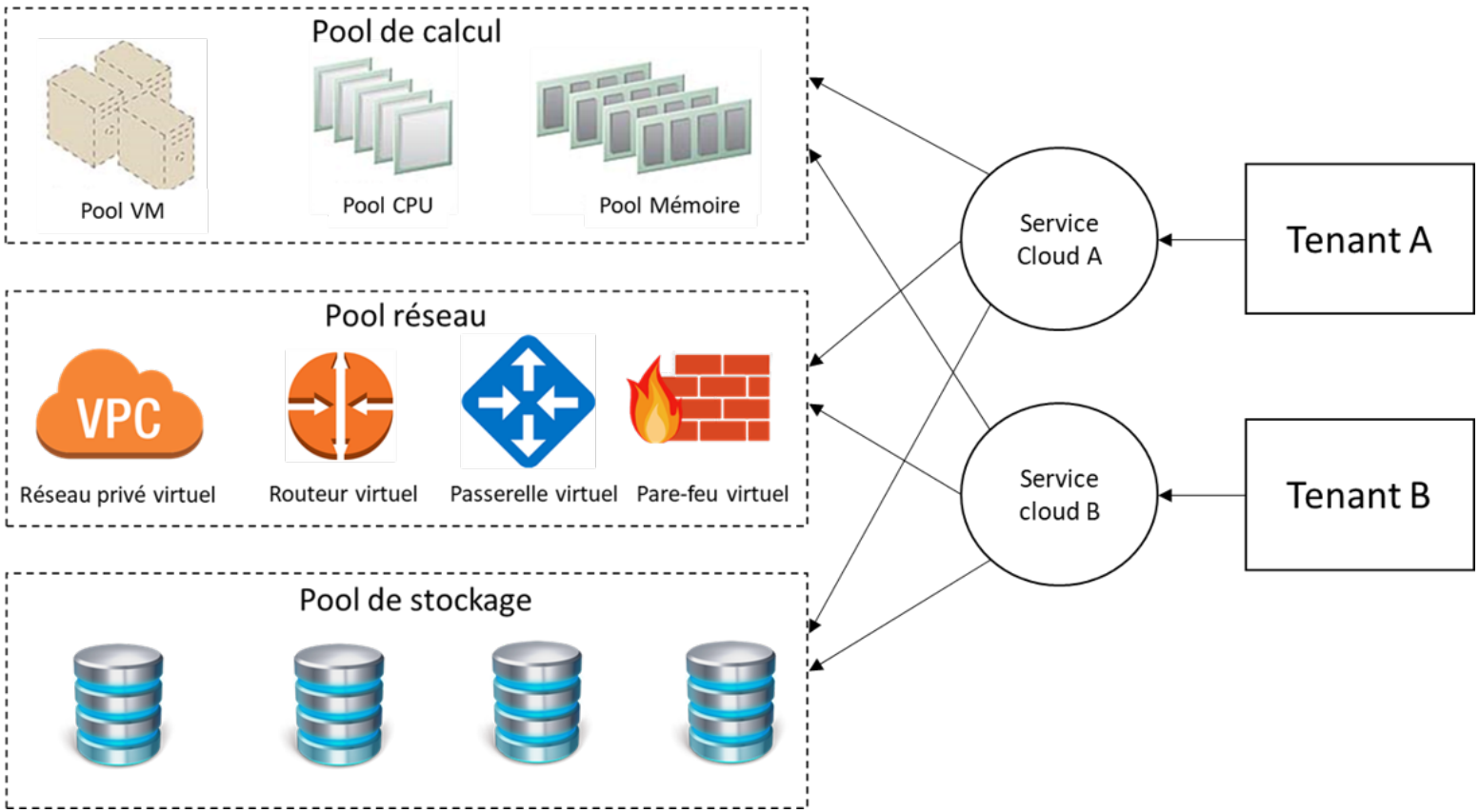
- Plus sécurisé
- Utilisateur restreint
- Flexible : adaptation au besoin
- Coûts entièrement géré par le fournisseur

Cloud Hybride

- Stockage illimité
- Evolutivité
- Flexible : adaptation au besoin

Mutualisation (resource pooling)

- Tenant A accède au service A
- Allocation dynamique des resources au service A
- Liberation des ressources après utilisation

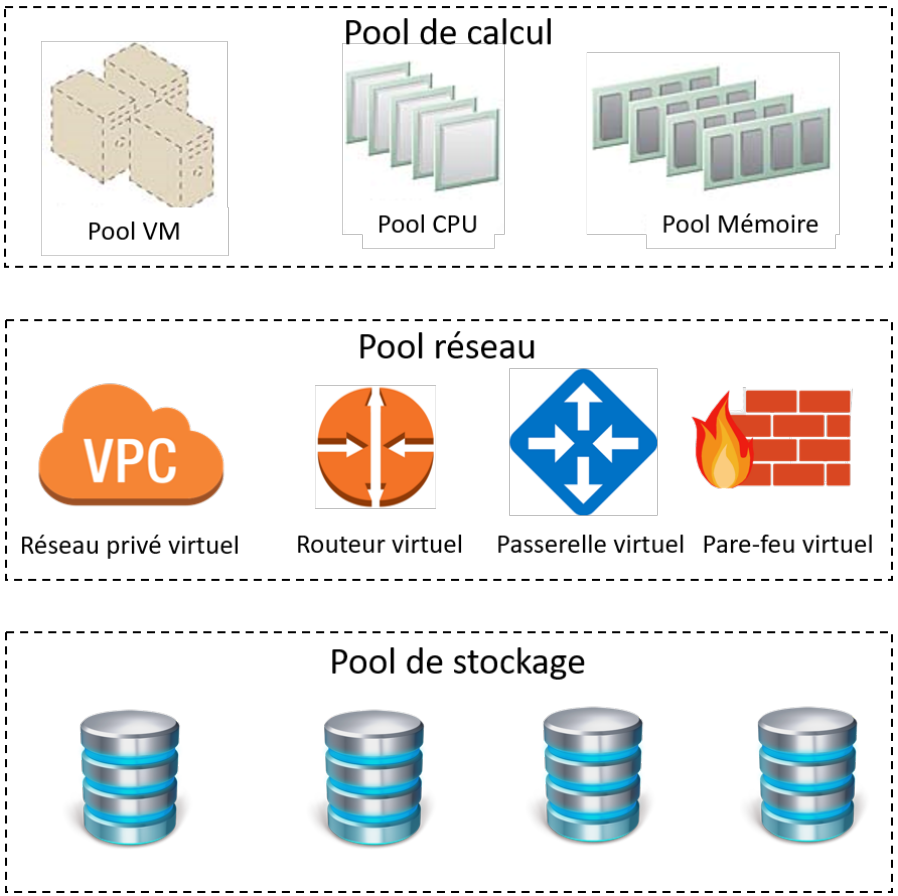


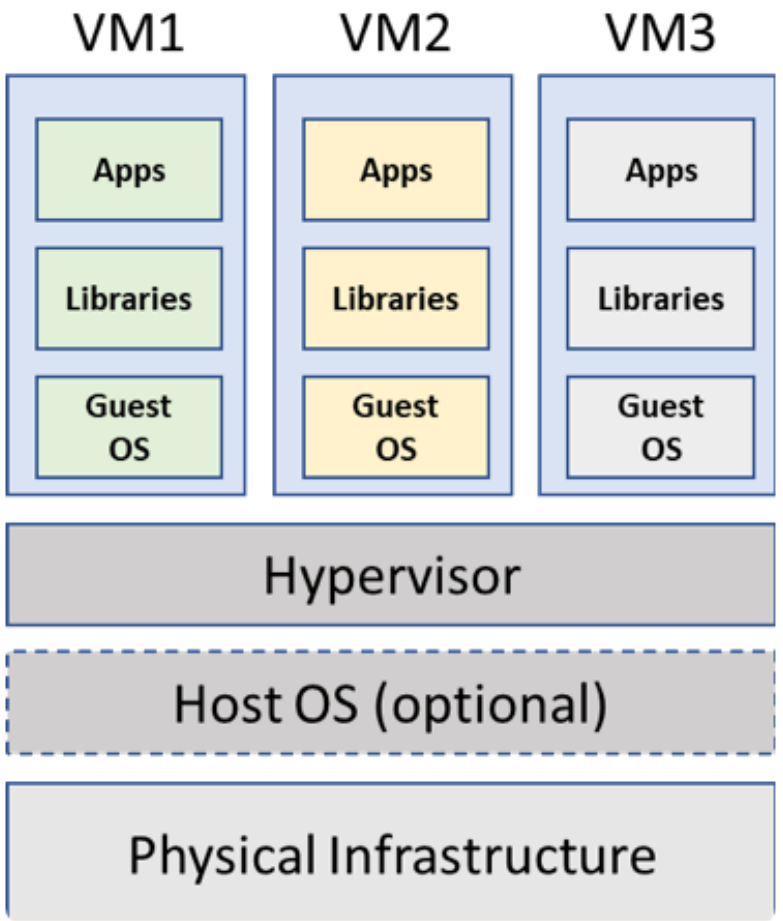
Mutualisation (resource pooling)

- La mutualisation exploite les concepts de
  1. Pool de calcul
     1. Virtualization
     2. Conteneurisation
     3. Fonction sans serveur (serverless)
  2. Pool réseau
     1. Virtualisation des fonctions réseau (NFV)
     2. Réseau défini par logiciel (SDN)
  3. Pool de stockage
     1. Stockage de collection d'objets (buckets)
     2. Réseau de zones de stockage

Infonuagique vs Virtualisation

- Quel est la différence entre l'infonuagique et la virtualisation ?





credit: Blue Sentry

Infonuagique vs Virtualisation

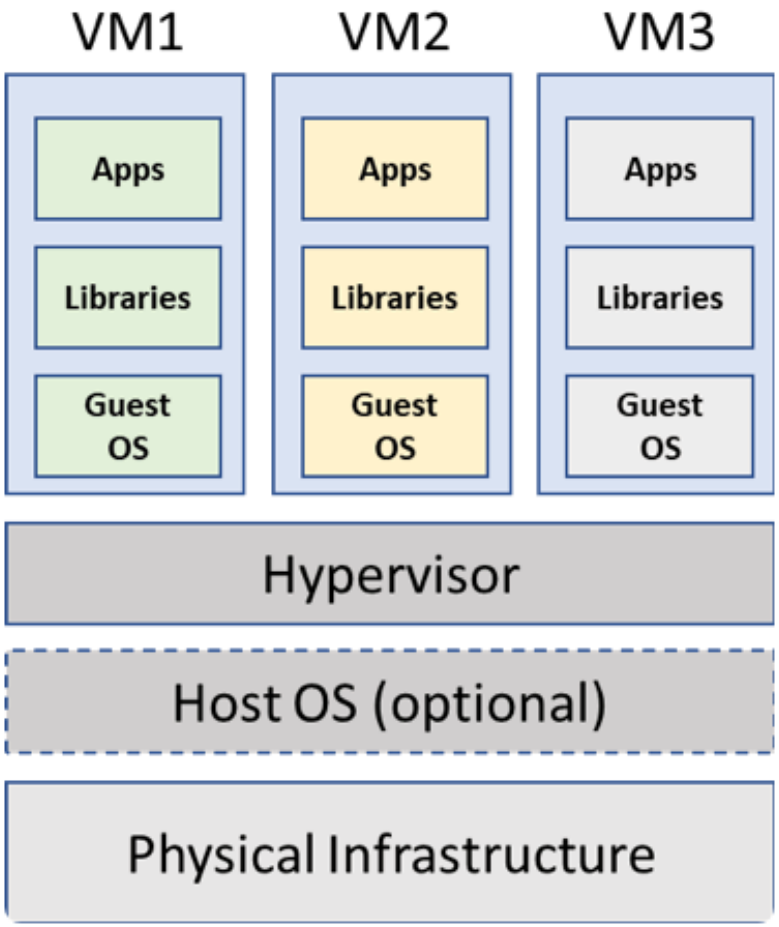
- **Infonuagique**
  1. pratique permettant l'accès réseau omniprésent et
  2. à la demande via un pool partagé de ressources
  3. pouvant être rapidement provisionnés et libérés avec un minimum d'effort de gestion
- **Virtualisation**
  1. creation et exécution de plusieurs *environnements isolés possédant leur propre OS*
  2. sur une seule machine physique
  3. à l'aide d'un hyperviseur qui en assure leur gestion
- **Hyperviseur bare-metal vs hébergé**
  1. L'hyperviseur bare-metal ou de type 1 est installé directement sur le materiel et dispose d'un micro-kernel pour s'exécuter (ex. VMware ESXi, Hyper-V)
  2. L'hyperviseur hébergé ou de type 2 est installé au niveau de l'OS comme une application (ex. Virtual Box, VMware Fusion)

Sondage ☺: `https://www.wooclap.com/EUBPPX`.

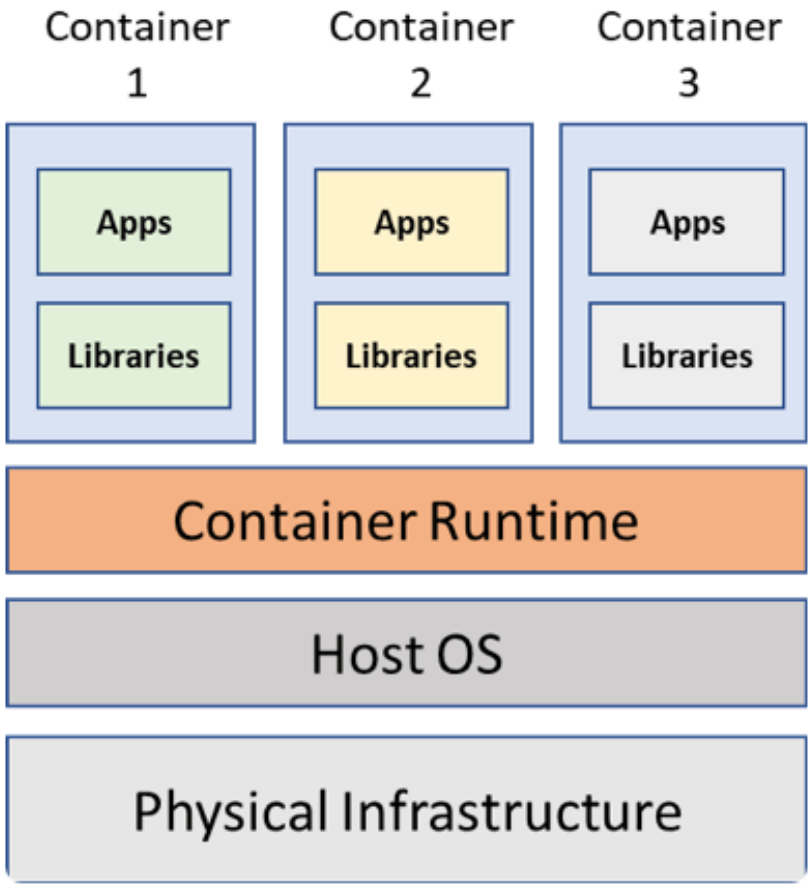
wooclap

Virtualization vs Conteneurisation

- Quel est la différence entre la virtualisation et la conteneurisation ?



credit: Blue Sentry



credit: Blue Sentry

Virtualization vs Conteneurisation

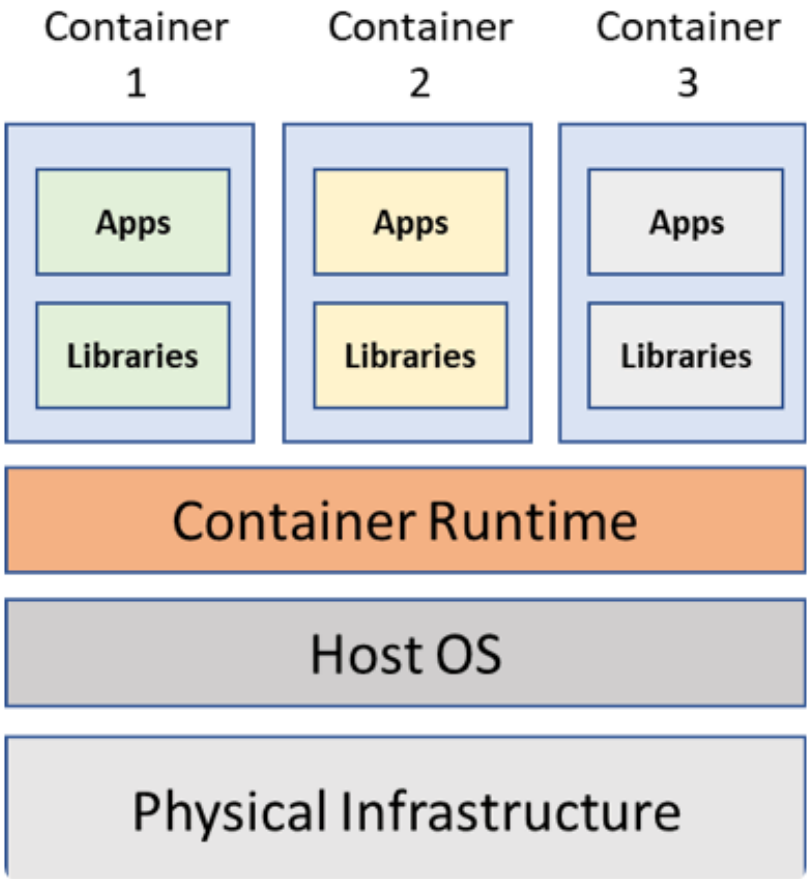
- **Virtualisation**
  1. creation et exécution de plusieurs *environnements isolés possédant leur propre OS*
  2. sur une seule machine physique
  3. à l'aide d'un hyperviseur qui en assure leur gestion
- **Conteneurisation**
  1. creation et exécution de plusieurs *applications isolés possédant leurs propres librairies*
  2. sur un seul OS
  3. à l'aide d'un daemon (*containerd*) qui en assure leur gestion

Sondage ☺: `https://www.wooclap.com/GTRUFX`.

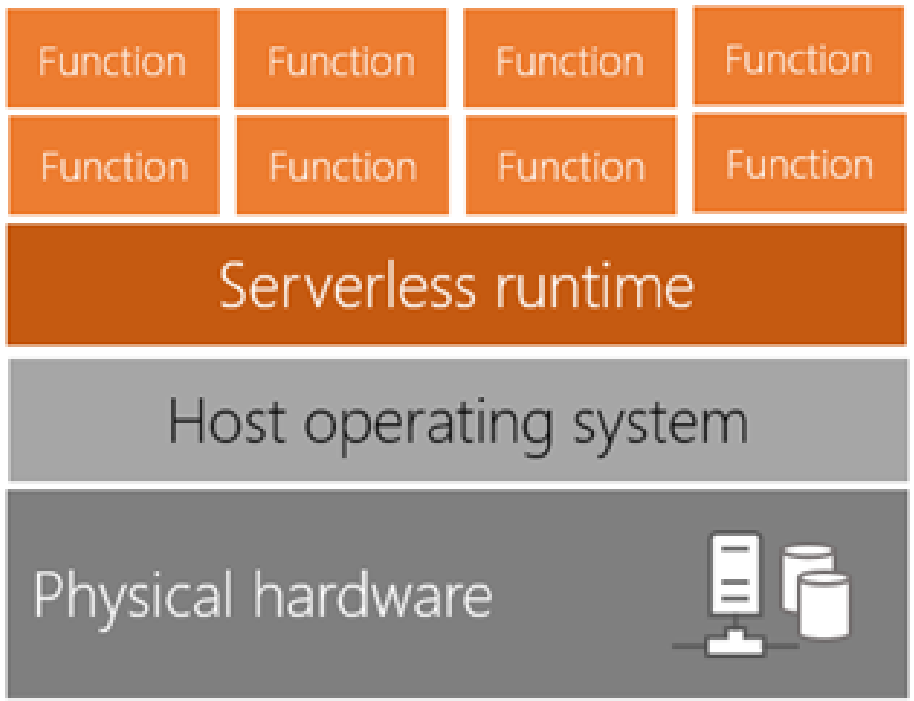
wooclap

Conteneurisation vs Info. sans serveur (serverless)

- Quel est la différence entre la conteneurisation et l'informatique sans serveur ?



credit: Blue Sentry



credit: Piyush Adhikari

Conteneurisation vs Function sans serveur (serverless)

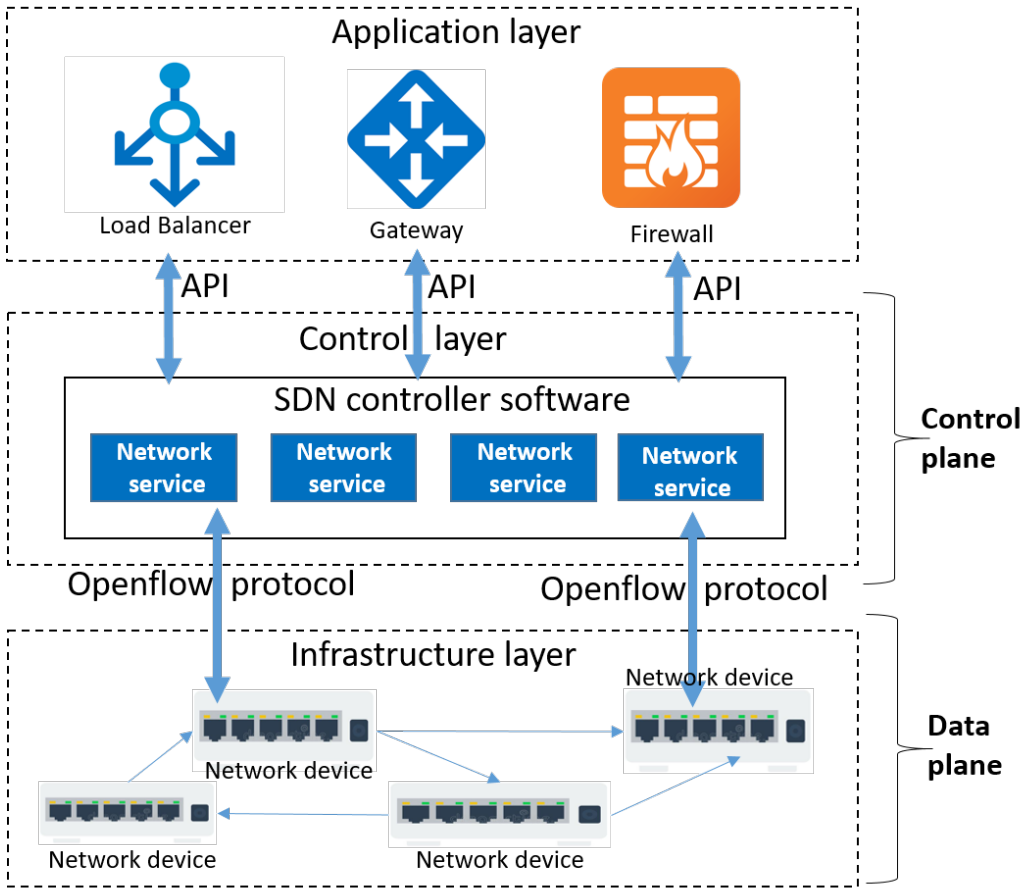
- **Conteneurisation**
  1. creation et exécution de plusieurs *applications isolés possédant leurs propres librairies*
  2. sur un seul OS
  3. à l'aide d'un daemon (*containerd*) qui en assure leur gestion
  4. Exemple: Docker, Kubernetes
- **Function sans serveur**
  1. creation et exécution de bouts de code ou *fonctions* en tant que service
  2. sans se préoccuper des serveurs qui vont les exécuter
  3. la gestion des serveurs et l'exécution des services sont entièrement gérés par le fournisseur
  4. Exemple: AWS Lambda, Azure Functions

Sondage ☺: `https://www.wooclap.com/BPOUMX`.

wooclap

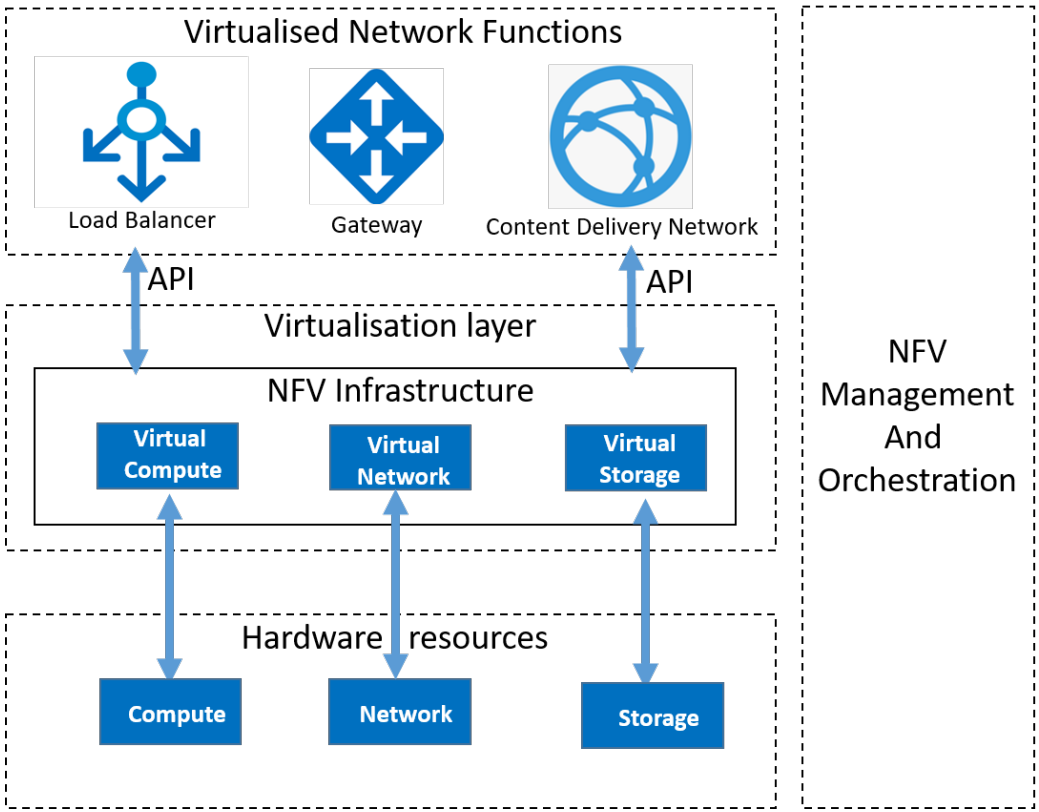
Réseau défini par logiciel (SDN)

- configuration et programmation des réseaux
- en temps réel via un logiciel
- SDN permet de séparer la couche de données et de contrôle
  - couche de données: commutateurs, fonctions réseaux virtuelles (e.g., routeurs)
  - couche de contrôle: gère l'accès et la programmation de la couche de données
  - en utilisant le protocol OpenFlow



Virtualisation des fonctions réseau (NFV)

- abstraction des composants réseaux
  - Routeur, Pare-feu
  - Passerelle, équilibreur de charge
- par des fonctions virtuelles
- pouvant être installés, controllées, and manipulées par un logiciel
- déployé sur les noeuds de calcul du nuage



Sondage ☺: `https://www.wooclap.com/KPZFID`.

wooclap

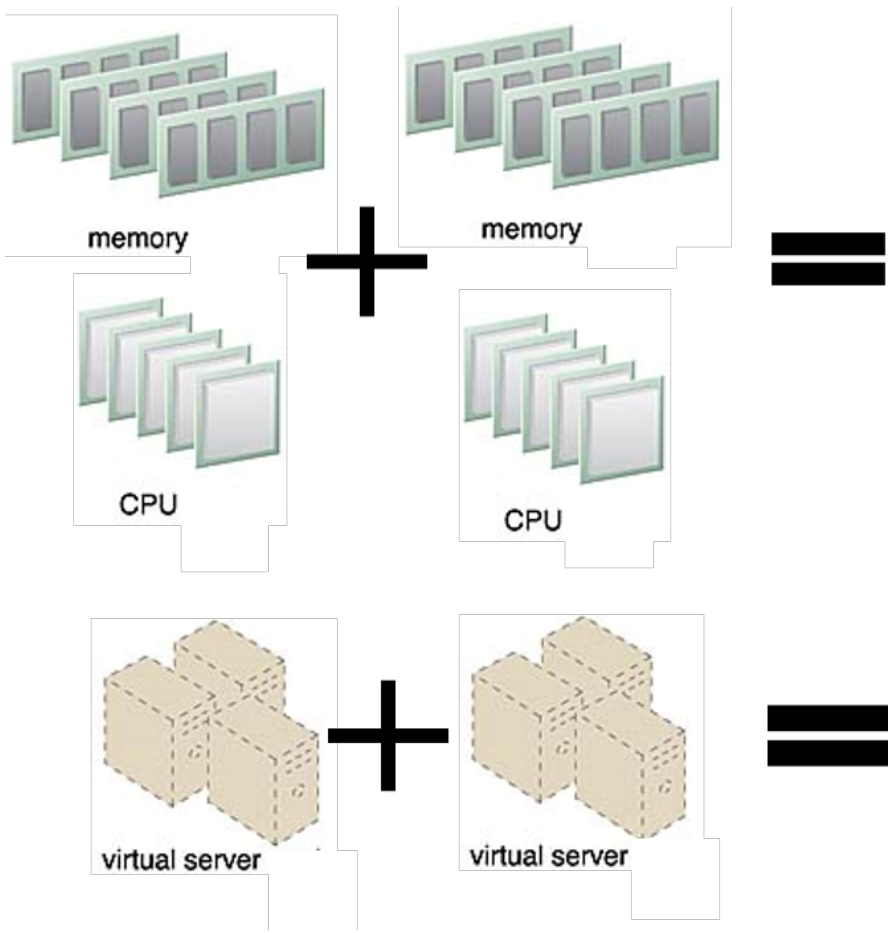
Stockage en bucket VS Réseau de zones de stockage

- Stockage en bucket
  - enregistre les données
    - non-structurées / structurées
    - de grande taille
  - dans des objets
  - sous forme de collection d'objets (bucket)
  - et permet
    - la replication des données
    - pas de duplication de volumes (snapshot)

- Réseau de zones de stockage (SAN)
  - mutualisation/partage
  - des ressources de stockage
    - blocs de disque
    - base de données
    - système de fichiers
  - et permet
    - la replication des données
    - la duplication de volumes (snapshot)

Mise à l'échelle (Scaling)

1. Horizontal scaling vs Vertical scaling



Mise à l'échelle (Scaling)

1. Horizontal scaling
   - Augmentation du nombre de serveurs ou de machines physiques
   - Plus coûteux
   - Adapté pour de larges organisations
2. Vertical scaling
   - Augmentation de la mémoire ou du processeur sur les serveurs existants
   - Moins coûteux
   - Adapté pour de petites organisations (ainsi que des larges organisations afin d'amortir les coûts)

Sondage ☺: `https://www.wooclap.com/LHKABT`.

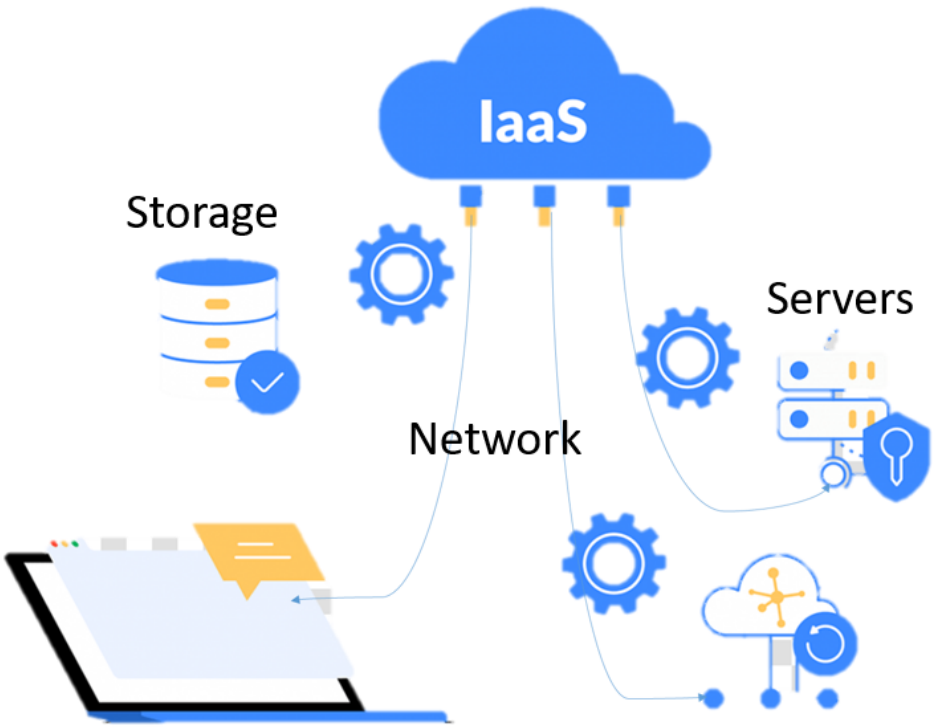
wooclap

Sur site (on-premise)

- L'**organisation** contrôle toute l'infrastructure
- incluant les données
  - en transit, au repos
  - en cours d'utilisation
- l'execution des applications et services
- le système d'exploitation
- le matériel
  - serveurs, dispositifs réseaux
- la virtualization
- le réseau, le stockage

Infrastructure en tant que service (IaaS)

- L'**organisation** contrôle
- les données
  - en transit, au repos
  - en cours d'utilisation
- les applications
- l'exécution des apps et services
- le système d'exploitation
- Le **fournisseur** contrôle
- le matériel
  - serveurs, dispositifs réseaux
- la virtualization
- le réseau, le stockage



Plateforme en tant que service (PaaS)

- L'**organisation** contrôle
- les données
  - en transit, au repos
  - en cours d'utilisation
- les applications
- Le **fournisseur** contrôle
- l'exécution des apps et services
- le système d'exploitation
- le matériel
  - serveurs, dispositifs réseaux
- la virtualization
- le réseau, le stockage

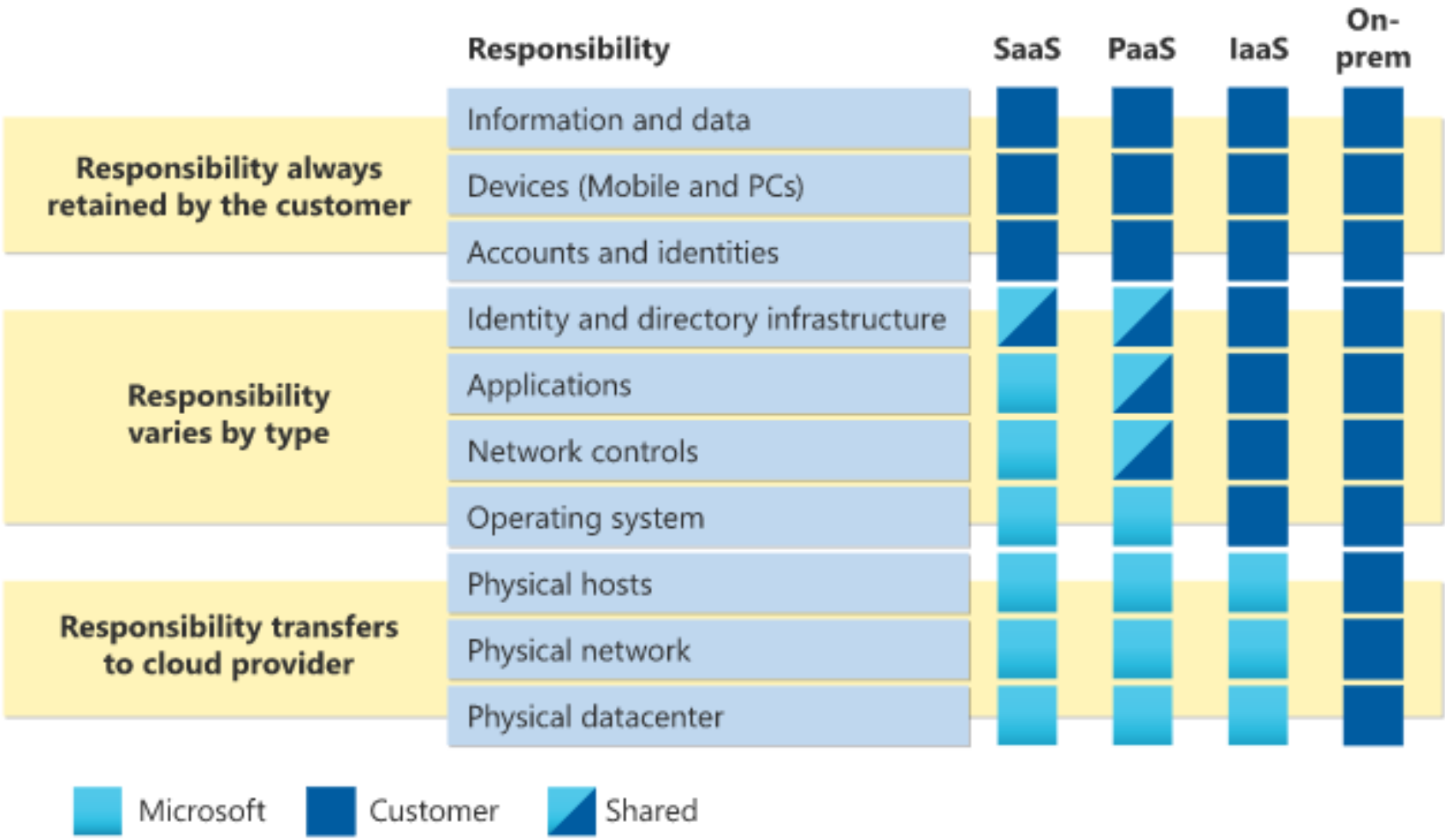
Software en tant que service (SaaS)

- Le **fournisseur** contrôle
- les données
  - en transit, au repos
  - en cours d'utilisation
- les applications
- l'execution des apps et services
- le système d'exploitation
- le matériel
  - serveurs, dispositifs réseaux
- la virtualization
- le réseau, le stockage

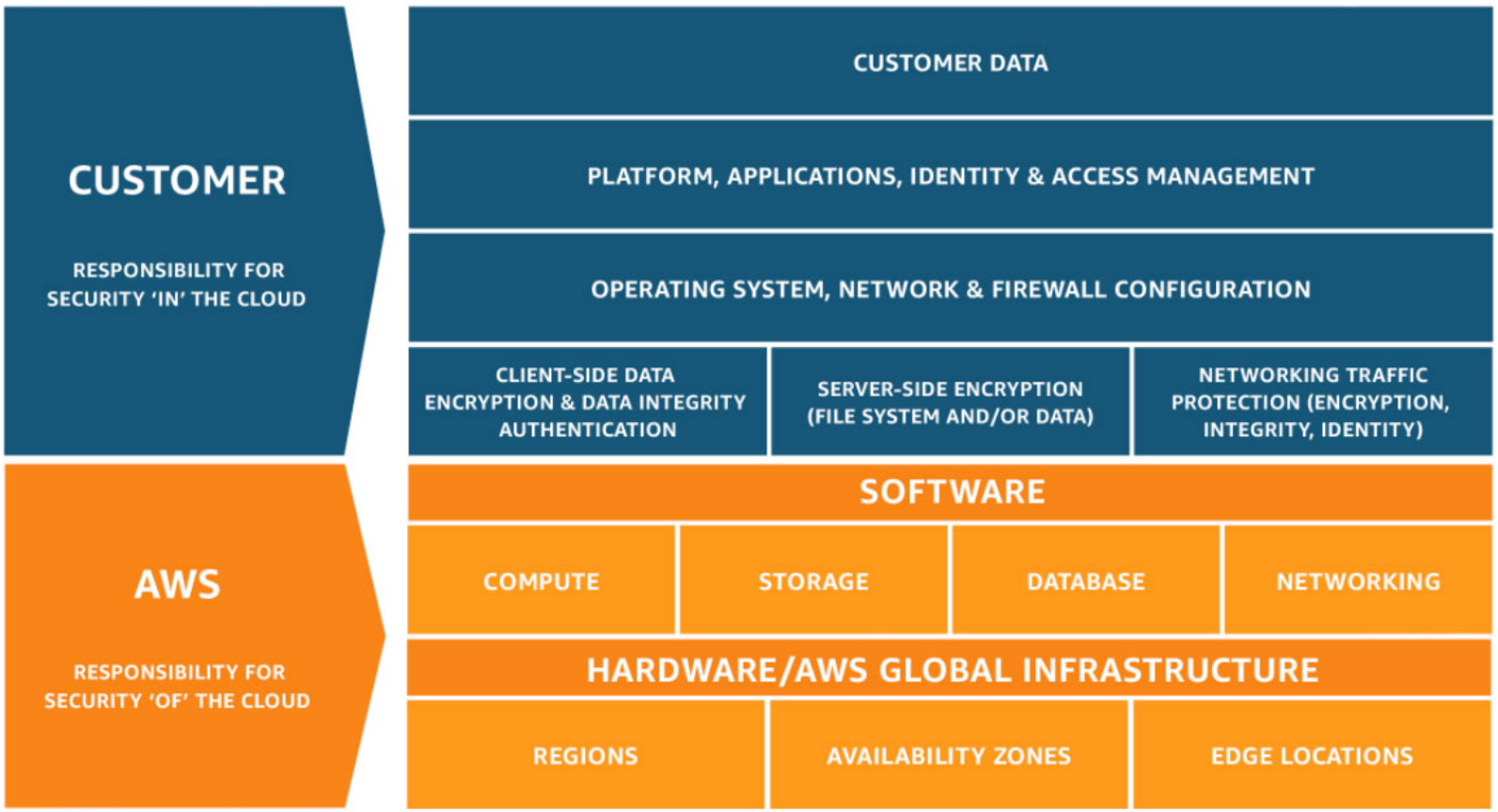
Sondage ☺: `https://www.wooclap.com/SXOUKP`.

wooclap

Modèle de responsabilités de Microsoft



Modèle de responsabilités d'Amazon



Free Quiz (10 min):
https://www.extrahop.com/lp/shared-responsibility/.