Systèmes d'exploitation avancés

stephane.louis@l-a.lu

Haute Ecole Libre Mosane

2020 - 2021

>whoami

- **Stéphane LOUIS**
  - Started with ICT when around 6y old
  - Started making money with ICT at around 15y old
  - Now >20y of xp
  - Became security and cybersecurity specialist
  - Mostly active in defense, institutions, finance. – Starting with SME
  - Member of management board of various security companies
  - CISO of a governmental entity
  - https://www.linkedin.com/in/louisstephane/
  - I'm not (yet ???) on FB or other so called « social » media

Contenu du cours

Les modules de cours sont indépendants. Plusieurs modules pourront éventuellement être abordés simultanément

- **Systèmes classiques**
- **La virtualisation**
  - Hyperviseurs
  - Micro-containers
- **Le (public) cloud computing**
  - Terminologie
  - Public cloud (grand) public
- **Travail personnel par groupes**
  - Exécution d'attaques dictionnaire / bruteforce
  - Rapport

Intervenants dans le cours

En fonction de l'évolution de la situation sanitaire, la vitesse de croisière du cours et la disponibilité des intervenants, des variances seront possibles

- Stéphane L ; virtualisation, cloud public, travail personnel
- Renaud D ; Les fonctions lambda, applications « serverless »

Objectifs du cours

- **Au terme de ce cours le futur professionnel sera**
  - **Capable de comprendre et d'expliquer le fonctionnement général des composants des systèmes traditionnels et des systèmes virtualisés qui constituent un cloud**
    - Cours ex cathedra
  - **Sensibilisé aux vulnérabilités**
    - Travail de groupe
  - **Capable de travailler en groupe, s'exprimer avec un langage clair et adéquat**
    - Rapport du travail de groupe

Supports du cours

Tout au long de sa carrière le professionnel doit sans cesse mettre ses connaissances à jour. Il est important d'être curieux et d'acquérir la capacité à trouver et canaliser les informations nécessaires à son apprentissage continu

- **Présentations utilisées pendant les séances de cours**
  - Seront mise à jour régulièrement au fur et à mesure que le cours sera donné
- **Documents éventuels renseignés par le professeur**
- **Notes personnelles**
  - Les transparents proposés sont juste un support de l'exposé oral !
  - Indispensables pour être prêt pour l'examen
  - Chaque étudiant est entièrement responsable de la qualité de ses notes personnelles
- **Toute information utile que l'étudiant aura pu trouver lors de ses recherches personnelles**

Evaluation

L'évaluation mesure l'accomplissement des objectifs du cours qui se résument à l'assimilation de contenu et la capacité à fonctionner au sein d'un groupe de professionnels

- **Travail de groupe (50 points)**
  - **Contenu (40 points)**
  - **Qualité du rapport (10 points)**
    - Présentation
    - Grammaire
    - Orthographe
- **Examen (50 points)**
  - **QCM (+1 / -1)**
    - Contenu abordé dans les slides et les exposés oraux du cours (45 points)
    - Contenu des lectures, et sources documents connexes renseignées ou personnelles (5 points)
- **La note du travail de groupe peut-être reportée d'une session à l'autre pendant la même année académique**
- **Remarque : Le rapport peut-être rédigé au choix en français, en anglais ou en néerlandais**

Bibliographie

- **Elements de bibliographie**
  - HP
  - Dell
  - VMWare
  - AWS
  - Cloudguru
  - Wikipedia
  - Autres cours de S.Louis
  - Et bien d’autre contenu du web.

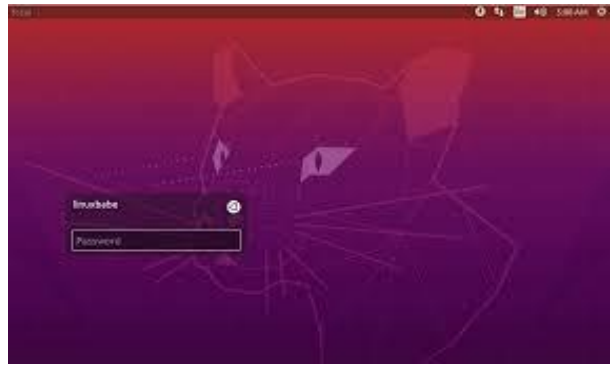
1 Les systèmes classiques

Authentification

- **Définitions**
  - IAM : Identity and Access Management
    - Tout ce qui touche à la gestion des identités, aux authentifications et à la gestion des droits sur les systèmes et les infrastructures (non limité aux infrastructures ICT)
  - Les identités, authentifications et droits s'attribuent à des « objets » (personnes, composants logiciels, …)
  - L'authentification consiste à identifier l'utilisateur en confirmant qu'il est bien celui qu'il prétend être
  - Les droits définissent les actions autorisées d'un « objet » sur un autre « objet »
  - **Le contrôle d'accès désigne les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à un bâtiment ou un site, ou les accès logiques à un système d'information.**

Authentification

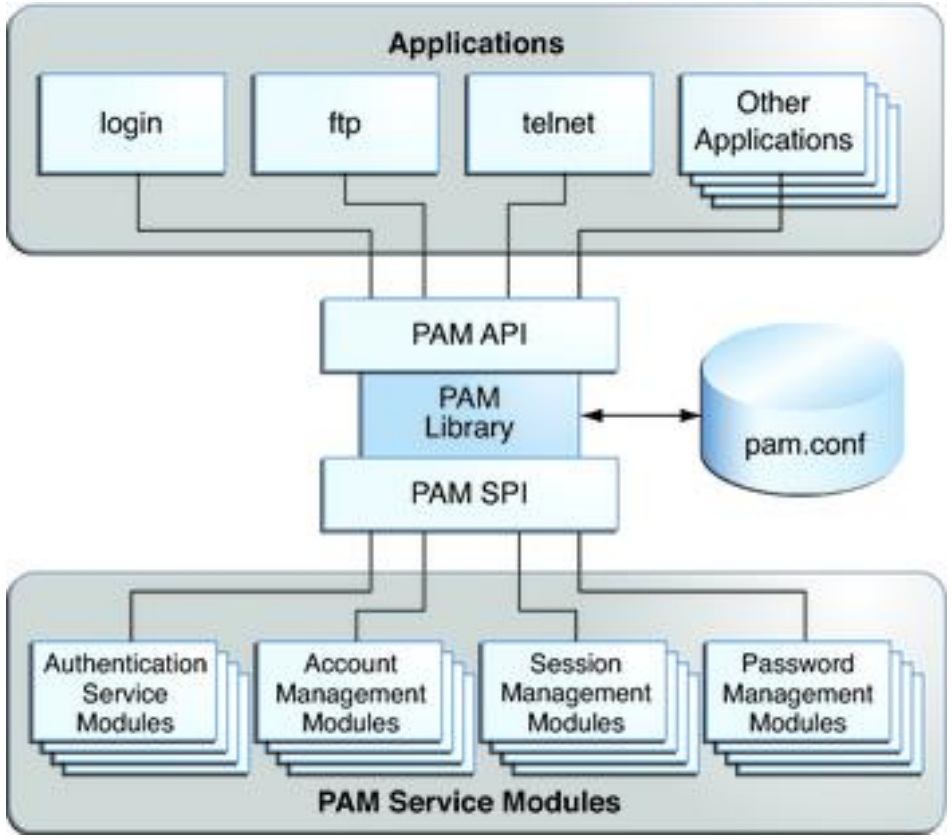
- **Définitions**
  - 2 types d’authentification
    - Authentification locale
      - Base de donnée locale au système
        - Utilisée pour les systèmes individuels (PC personnel, …)
        - Utilisée pour les comptes administrateur locaux pour opérations de bas niveau
    - Authentification centralisée
      - Repose sur une autorité et une base de données centralisées
        - LDAP
        - Radius
        - Les authentifications à 2 facteurs



Authentification locale

La notion PAM de ce cours n'a rien à voir avec la notion PAM (Privilege Access Management) qui sera abordée dans le cours « Principes d'architectures sécurisées »

- **Linux**
  - Suit les standards UNIX
    - Fournie par le module d'authentification pam_unix(8)
      - PAM (Pluggable Authenticaiton Module)



Authentification locale

- **Linux**
  - Utilisateurs et groupes : 3 fichiers de configuration
    - /etc/passwd
    - /etc/shadow
      - Mots de passes chiffrés (hash)
    - /etc/group
  - Lecture: https://www.shellhacks.com/linux-generate-password-hash/

```
gasmyr@cashme2:~$ tail -f /etc/passwd
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
gasmyr:x:1000:1000:gasmyr,,,:/home/gasmyr:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

Authentification locale

- **MS Windows**

Le système d'exploitation Windows implémente un ensemble de protocoles d'authentification par défaut, notamment Kerberos, NTLM, Transport Layer Security / Secure Sockets Layer (TLS / SSL) et Digest, dans le cadre d'une architecture extensible. En outre, certains protocoles sont combinés dans des packages d'authentification tels que Negotiate et Credential Security Support Provider. Ces protocoles et packages permettent l'authentification des utilisateurs, des ordinateurs et des services; le processus d'authentification, à son tour, permet aux utilisateurs et services autorisés d'accéder aux ressources de manière sécurisée.

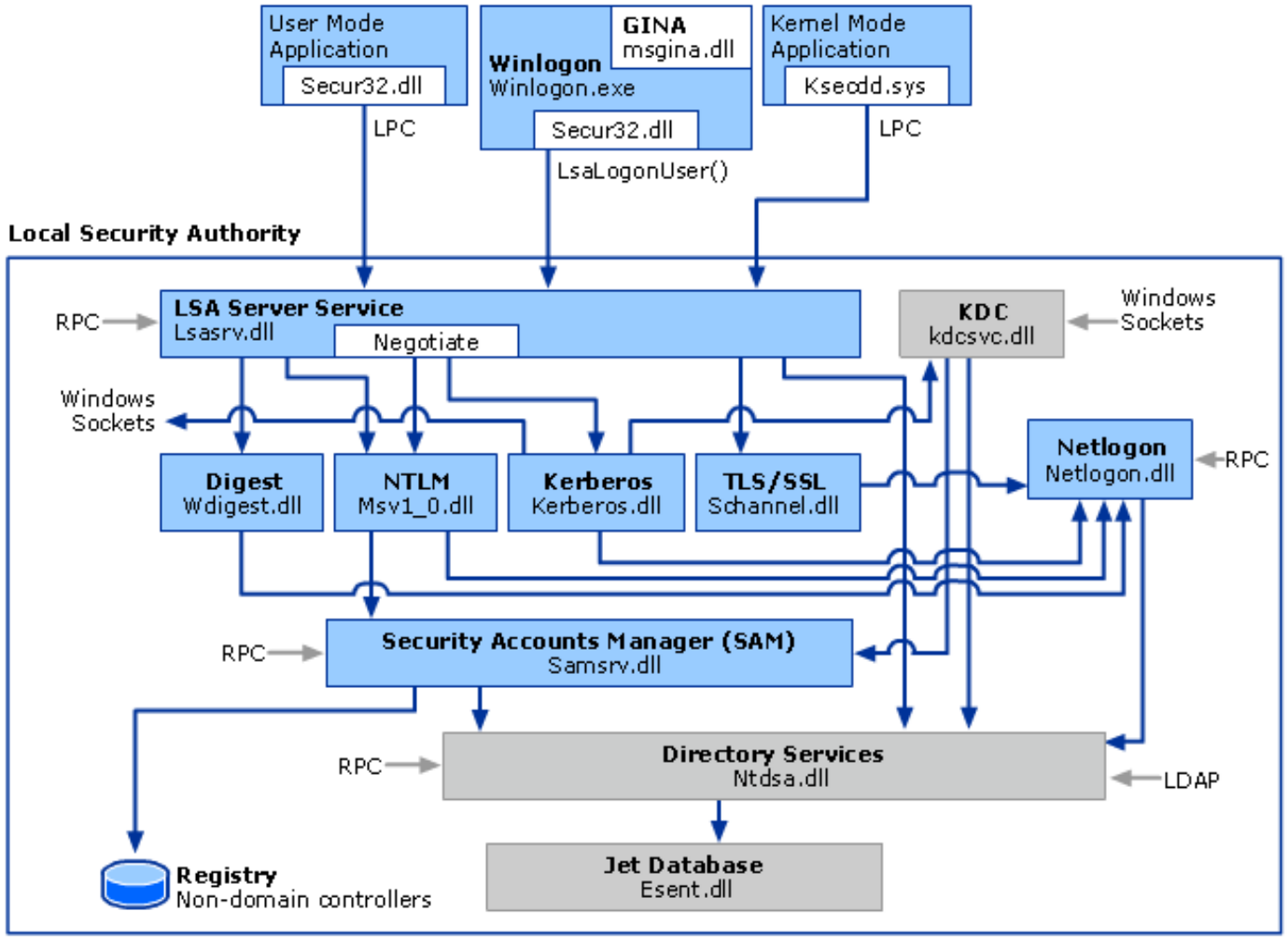
Authentification locale

- MS Windows

Les différentes mécanismes

d'authentification supportés sous windows

- kerberos
- TLS/SSL
- NTLM
- Smart Card
- Passwords



Authentification locale

- **Kerberos:** Les systèmes d'exploitation Windows Server implémentent le protocole d'authentification Kerberos version 5 et les extensions pour l'authentification par clé publique, le transport des données d'autorisation et la délégation.

Les avantages de l'utilisation de Kerberos pour l'authentification basée sur le domaine sont les suivants:

- Authentification déléguée
- Authentification unique(SSO)
- Interopérabilité
- Authentification plus efficace auprès des serveurs.

Authentification locale

- **NTLM:** Les protocoles d'authentification NTLM authentifient les utilisateurs et les ordinateurs en fonction d'un mécanisme de stimulation / réponse qui prouve à un serveur ou à un contrôleur de domaine qu'un utilisateur connaît le mot de passe associé à un compte. Lorsque le protocole NTLM est utilisé, un serveur de ressources doit effectuer l'une des actions suivantes pour vérifier l'identité d'un ordinateur ou d'un utilisateur chaque fois qu'un nouveau jeton d'accès est nécessaire:

- Contactez un service d'authentification de domaine sur le contrôleur de domaine pour le domaine de compte de l'ordinateur ou de l'utilisateur, si le compte est un compte de domaine.

- Recherchez le compte de l'ordinateur ou de l'utilisateur dans la base de données des comptes locaux, si le compte est un compte local.

Authentification locale

- **Passwords:** Les systèmes d'exploitation et les applications d'aujourd'hui sont structurés autour de mots de passe et même si vous utilisez des cartes à puce ou des systèmes biométriques, tous les comptes ont toujours des mots de passe et ils peuvent toujours être utilisés dans certaines circonstances.

Certains comptes, notamment les comptes utilisés pour exécuter des services, ne peuvent même pas utiliser de cartes à puce et de jetons biométriques et doivent donc utiliser un mot de passe pour s'authentifier. Windows protège les mots de passe à l'aide de hachages cryptographiques.

Authentification locale

- **TLS/SSL(channel SSP):** Schannel est un fournisseur de support de sécurité (SSP) qui implémente les protocoles d'authentification standard Internet Secure Sockets Layer (SSL) et Transport Layer Security (TLS). TLS et SSL est utilisé pour authentifier les serveurs et les ordinateurs clients, puis utiliser le protocole pour crypter les messages entre les parties authentifiées.

Utilisations:

- ❖ Transactions sécurisées SSL avec un site e-commerce
- ❖ Accès client authentifié à un site Web sécurisé SSL
- ❖ Accès distance
- ❖ Email
- ❖ Etc

Authentification locale

- **Smart cards:** Les cartes à puce sont des périphériques de stockage portables inviolables qui peuvent améliorer la sécurité des tâches telles que l'authentification des clients, la signature du code, la sécurisation des e-mails et la connexion avec un compte de domaine Windows.

Les cartes à puce fournissent:

- Stockage inviolable pour la protection des clés privées et d'autres formes d'informations personnelles.
- Isolement des calculs critiques pour la sécurité qui impliquent l'authentification, les signatures numériques et l'échange de clés à partir d'autres parties de l'ordinateur. Ces calculs sont effectués sur la carte à puce.
- Portabilité des informations d'identification et autres informations privées entre les ordinateurs au travail, à la maison ou sur la route.

Contrôle d’accès et méthodologie

- Identification: Qui suis-je? (identifiant de l'utilisateur)
- Authentification: prouvez que je suis celui que je dis être
- Autorisation: à quoi suis-je autorisé à accéder
- Audit / responsabilité: journaux d'audit et surveillance pour suivre l'activité des utilisateurs

Contrôle d’accès et méthodologie

- L'identification identifie un utilisateur de manière unique (nom d'utilisateur, UID, adresse e-mail, ...

- Ne partagez pas! Pas de compte du groupe! Doit être unique aux fins de la reddition de comptes et de la responsabilité

Contrôle d’accès et méthodologie

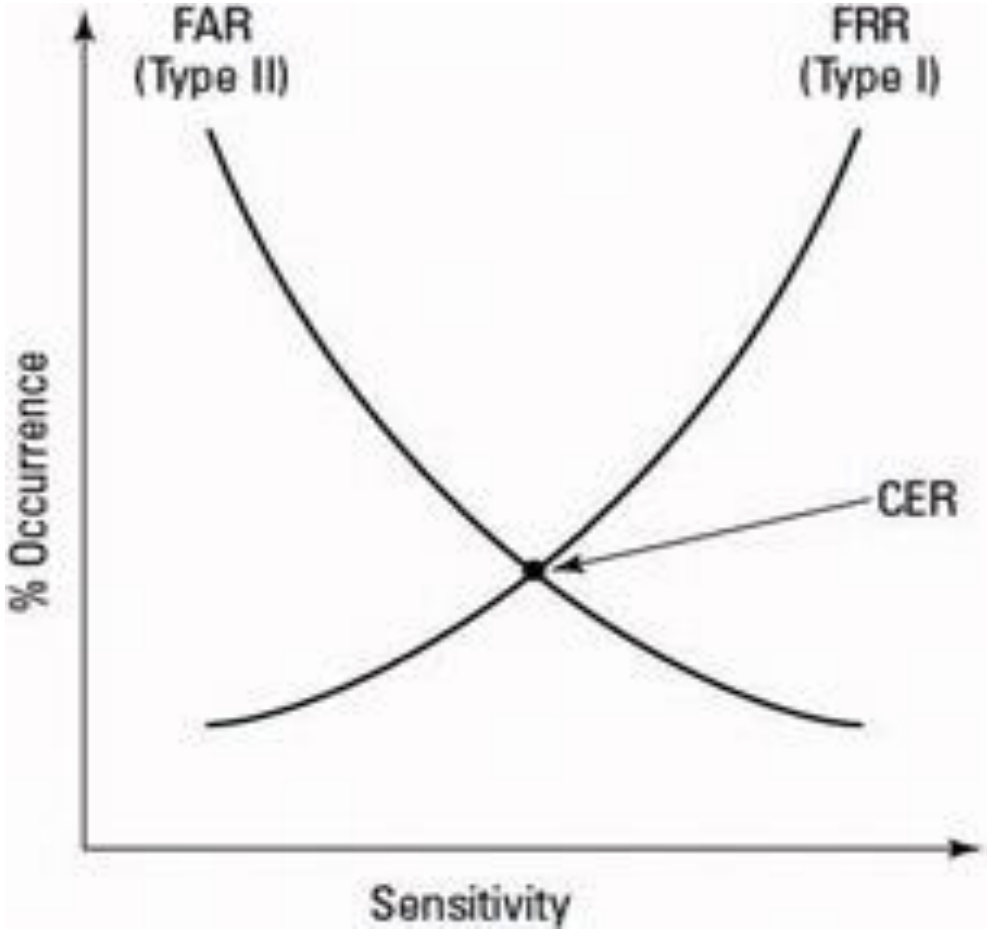
- L'authentification est une phase qui permet à l'utilisateur d'avoir la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question: "Êtes-vous réellement cette personne?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connaît.

- L'authentification basique: utilisation de deux vecteurs à savoir qui je suis(login, email ou nom d’utilisateur) et ce que je sais(mot de passe).
- L’authentification forte: utilisation de plusieurs vecteurs à savoir qui je suis, ce que je sais, ce que je possède, ce que je suis.

Contrôle d'accès et méthodologie

Metrics

- False Reject Rate: le taux de bonnes authorization rejetées
- False Accept Rate: le taux de mauvaises authorization acceptées
- Cross Error Rate: point de jonction entre le FRR et le FAR



Contrôle d’accès et méthodologie

Biométrie

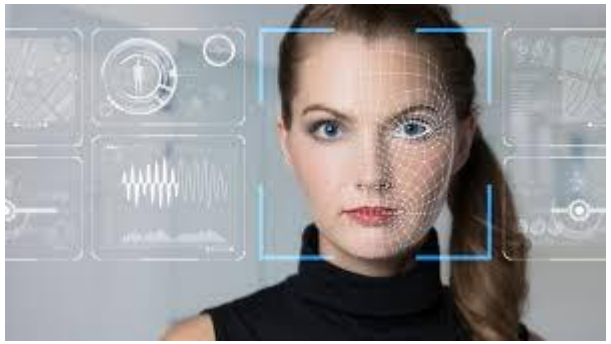
- Attribut personnel unique pour l'authentification (1: 1) ou l'identification (1: N)
- Très cher
- Sophistiqué
- Heure d'inscription
- Peut être basé sur:

- un comportement(signature dynamique)
- un attribut physique(empreinte digitale, scan retinien, iris, etc)

Contrôle d’accès et méthodologie

Les types de biométrie

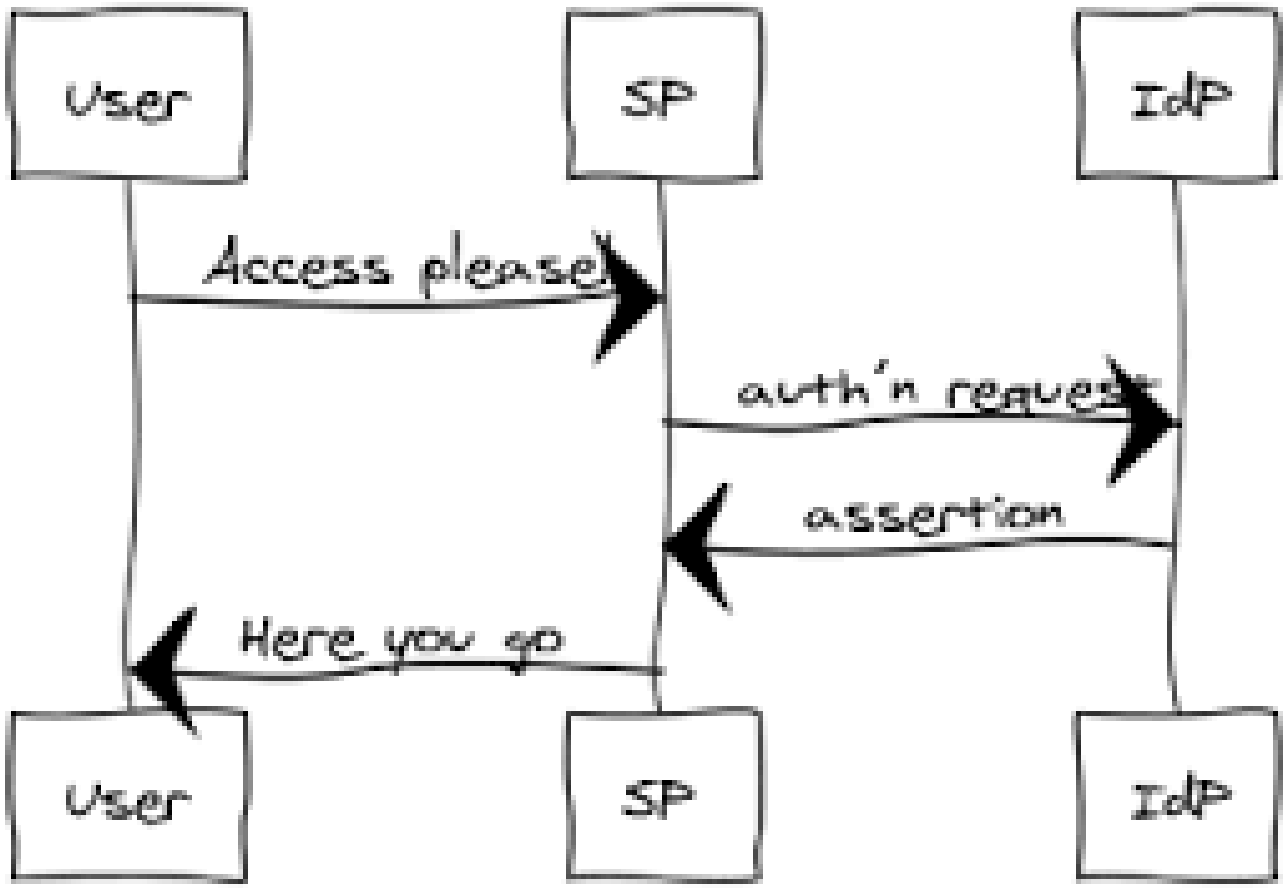
- Empreinte digitale
- Scan de l’Iris
- Scan retinien
- Scan faciale
- Scan de la paume de main
- Empreinte vocale



Contrôle d’accès et méthodologie

Gestion centrale de accès

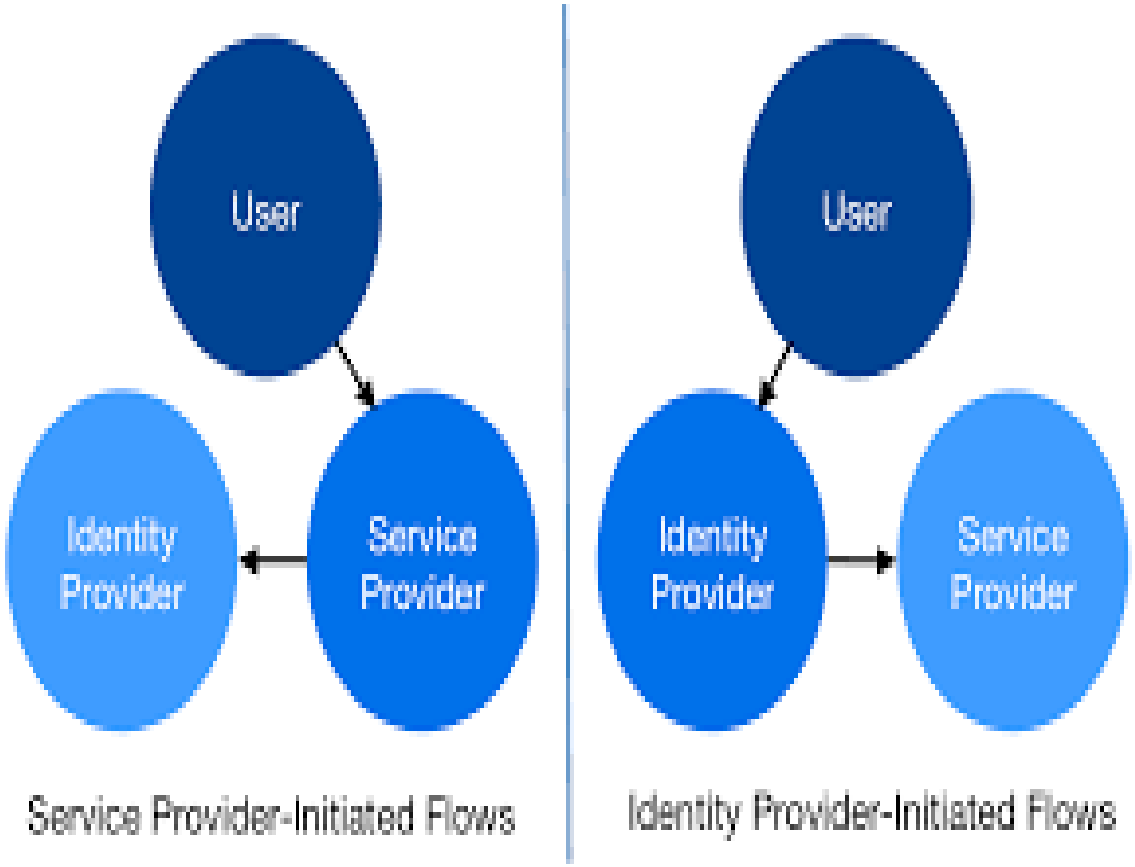
- Service provider: c’est un fournisseur de service(site ecommerce par example)
- Identity provider: c’est un serveur d’authentification and d'autorisation. Il doit authentifier l’utilisateur et pouvoir gérer l’accès aux ressources.



Contrôle d’accès et méthodologie

Gestion centrale de accès

- SP initiated: lorsque c’est le fournisseur de service qui initie le flow
- Identity initiated: lorsque c’est le fournisseur de l’identité qui initie le flow..



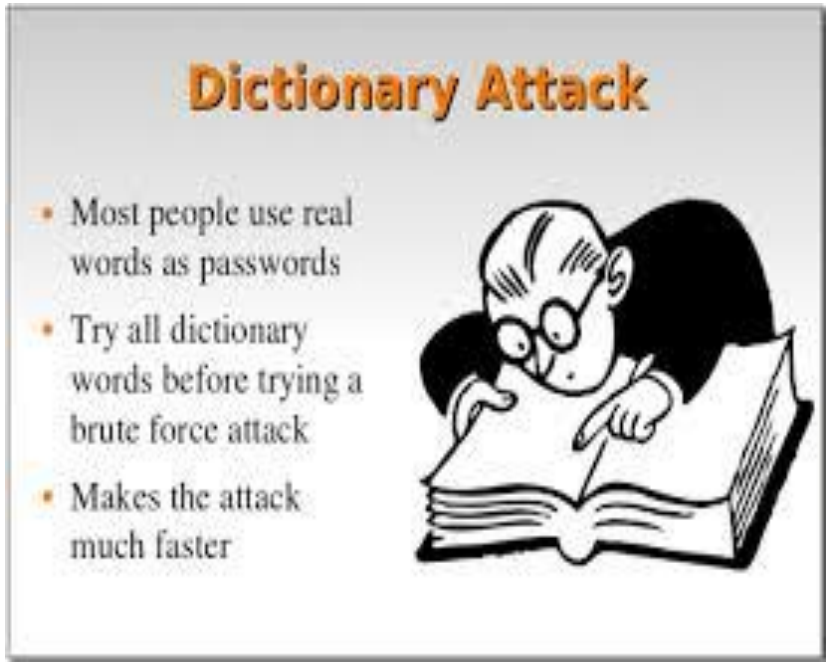
Attaques sur les authentifications locales

- Techniques
- Linux
- MS Windows

Attaques sur les authentifications locales

Techniques:

La plupart des outils de craquage de mot de passe Windows autorisent l'une des trois principales techniques de craquage de mot de passe. Le choix de la technique à utiliser dépend principalement du comportement attendu de la cible.



Attaques sur les authentifications locales

Sous Linux:

Linux bien que plus sécurisé que windows est tout aussi vulnérables à un ensemble d'attaques tels que:

- Brute force sur le SSH
- Scan des ports
- Kernel attack
- Consommation de mémoire

Attaques sur les authentifications locales

Sous windows:

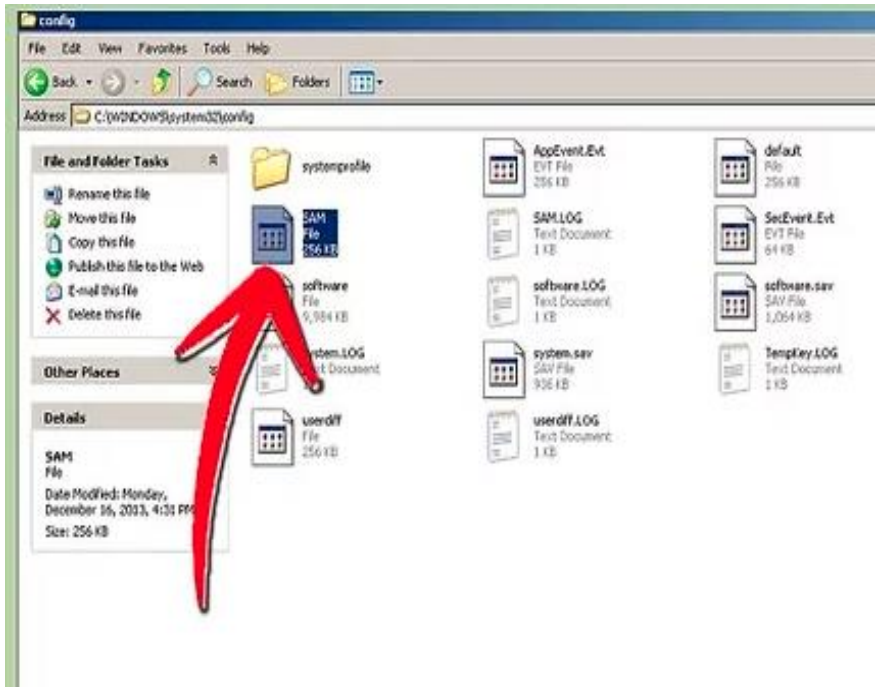
Étant donné que la fonction de hachage de Windows est basée sur l'algorithme MD4 faible, le craquage de ces mots de passe est souvent plus facile que ceux protégés par un chiffrement moderne équivalent. Cracker un hachage de mot de passe Windows est un processus en trois étapes:

- Acquérir le hachage
- Choisir un outil
- Choisir une technique de craquage

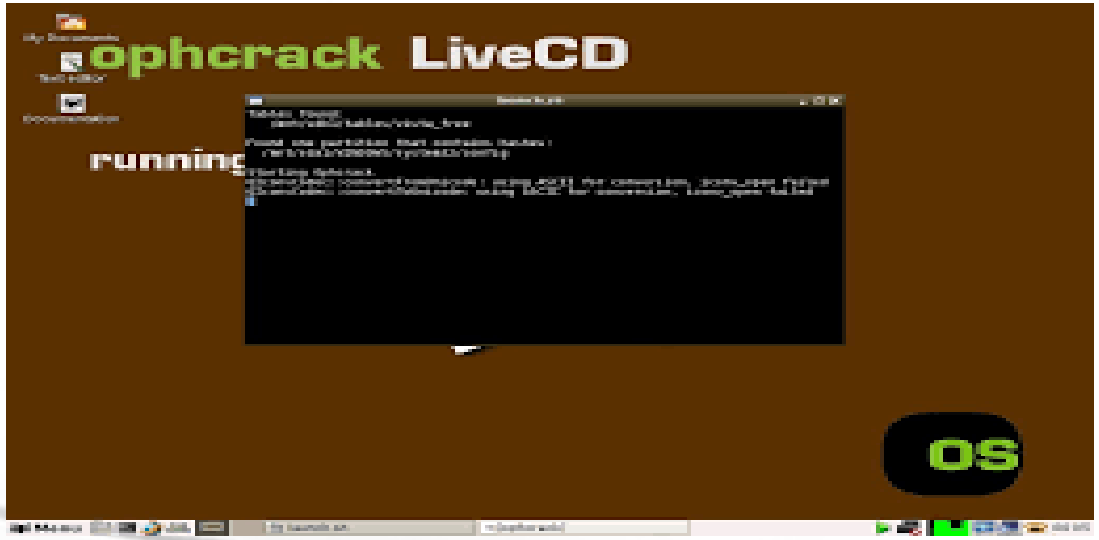
Attaques sur les authentifications locales

- Sous windows:(obtention du hachage)

La technique la plus courante est de les retirer directement de la machine en question. Les hachages de mot de passe Windows sont stockés dans le fichier SAM; cependant, ils sont chiffrés avec la clé de démarrage du système, qui est stockée dans le fichier SYSTEM.



Outils pour cracker les mots de passe



Authentification Centralisée

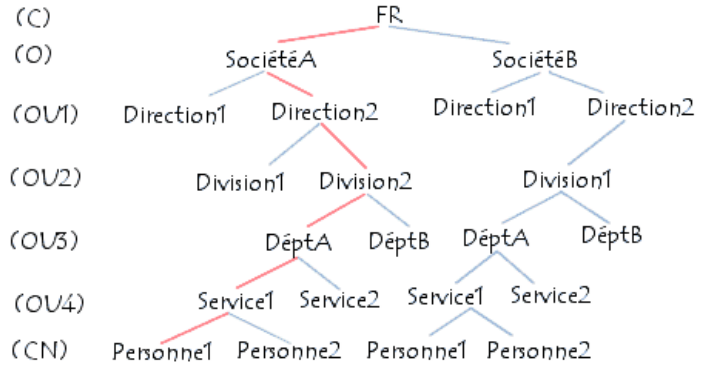
- LDAP (Lightweight Directory Access Protocol)
  - Basé sur l'interrogation d'un annuaire centralisé
  - Implémentations
    - Open LDAP
    - MS AD (Active Directory) (implémentation propriétaire MS)

L'arborescence d'informations (DIT)

LDAP présente les informations sous forme d'une arborescence d'informations hiérarchique appelée **DIT** (*Directory Information Tree*), dans laquelle les informations, appelées **entrées** (ou encore *DSE, Directory Service Entry*), sont représentées sous forme de branches. Une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais *root entry*).

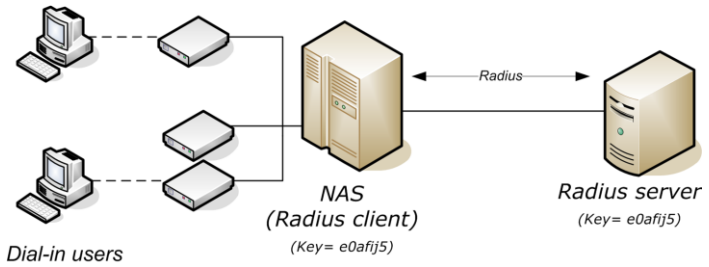
Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...).

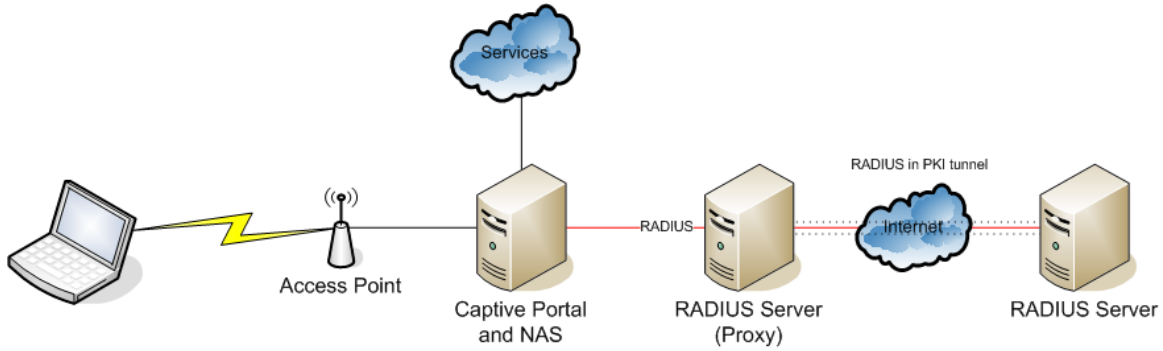
Chaque entrée est constituée d'un ensemble de paires clés/valeurs appelées **attributs**.



Authentification Centralisée

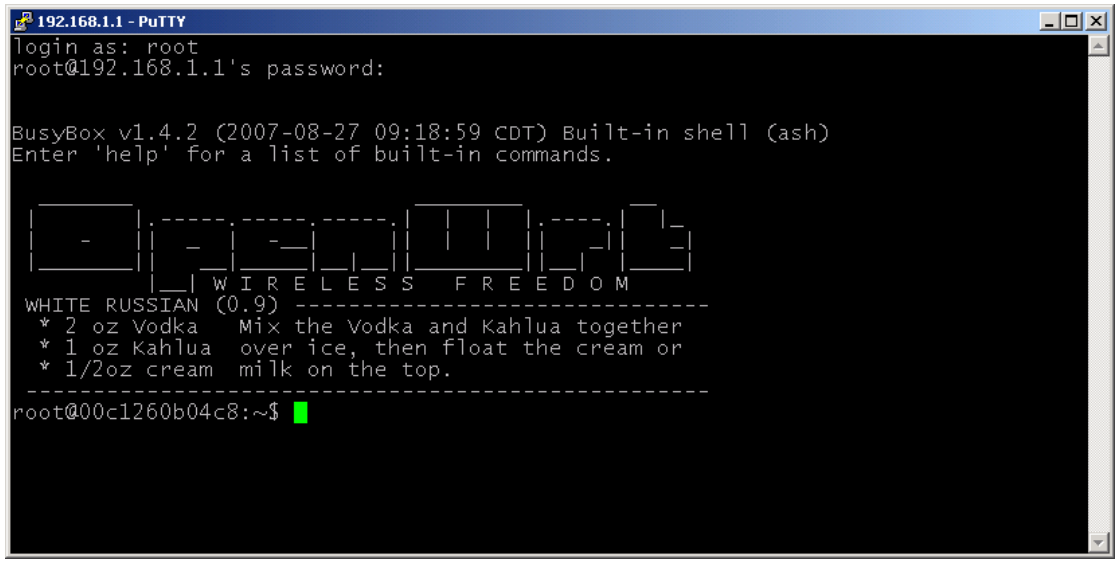
- Remote Authentication Dial-In User Service - RADIUS
  - Basé sur l'interrogation d'un annuaire centralisé
  - Fonctionnement
    - .....





SSH

- **Secure SHell (SSH)**
  - Hybride
    - Peut- fonctionner avec authentification locale
    - Peut être couplé avec un LDAP
  - 2 mécanismes d'authentification
    - Login / Mot de passe
    - Clefs SSH (clef publique / clef privée)
  - Fonctionnement
  - …



SSH

- **Schema explicatif**
  - Cas d'une authentification par clé

Autres types d’authentification

- Authentification à double facteur
- Authentification basée sur les certificats
- Authentification basée sur les tokens
- Authentification biometrique

Authentification à plusieurs facteurs

- Titre
  - Definition
  - Implementations

L'authentification multifacteur (MFA) est une méthode d'authentification qui nécessite deux ou plusieurs méthodes indépendantes pour identifier un utilisateur. Les exemples incluent les codes générés à partir du smartphone de l'utilisateur, les tests Captcha, les empreintes digitales ou la reconnaissance faciale.

Authentification avec plusieurs facteurs

L'authentification à plusieurs facteurs exige que les utilisateurs vérifient leur identité en se basant sur une combinaison de plusieurs éléments : un élément en leur possession, un élément qui les définit et un élément qu'eux seuls peuvent connaître.

Quelques implementations de MFA

Authentification à certificats

- Titre
  - Definition
  - Exemple de CA

Les technologies d'authentification basées sur les certificats identifient les utilisateurs, les machines ou les appareils à l'aide de certificats numériques. Un certificat numérique est un document électronique basé sur l’idée d’un permis de conduire ou d’un passeport.

Authentification à jetons

- Titre
  - Definition
  - Exemple de jeton

Les technologies d'authentification basées sur les jetons permettent aux utilisateurs de saisir leurs informations d'identification une fois et de recevoir en échange une chaîne cryptée unique de caractères aléatoires.

Authentification biométrique

L'authentification biométrique est un processus de sécurité qui repose sur les caractéristiques biologiques uniques d'un individu. Voici les principaux avantages de l'utilisation des technologies d'authentification biométrique:

- Les caractéristiques biologiques peuvent être facilement comparées aux caractéristiques autorisées enregistrées dans une base de données.
- L'authentification biométrique peut contrôler l'accès physique lorsqu'elle est installée sur des portails et des portes.
- Vous pouvez ajouter des données biométriques à votre processus d'authentification multifacteur

Attaques sur l’authentification locale

- BIOS (bypasser le mot de passe), Brute force attack)
- Attaque de démarrage à froid
- Attaque des ongles maléfiques
- Bootcd

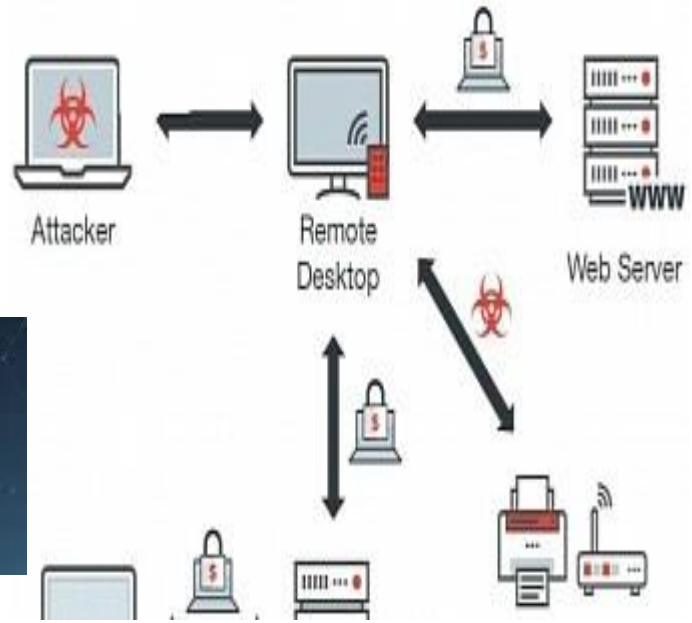
Les attaques "Evil Maid" peuvent être tout ce qui est fait à une machine via un accès physique alors qu'elle est éteinte, même si elle est cryptée.

Les attaques sur les authentifications distantes

- Authentification à double facteur

➔ Ingenierie sociale
➔ Détournement de session de cookie
➔ Générateur de code en double
➔ Brute force
➔ Authentification buggy à deux facteurs

Les différents types d’attaques sur l’authentification centralisé

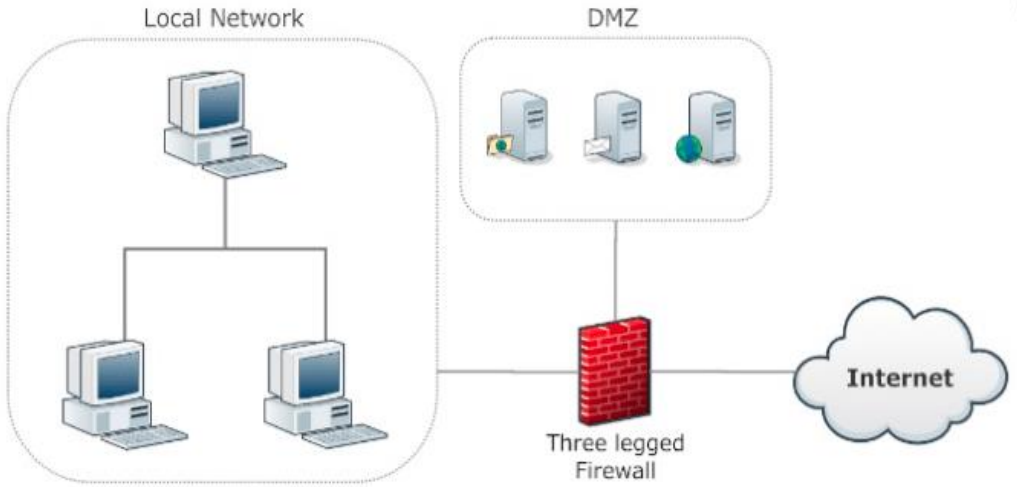


Mesures de protection

- Authentification à double facteur
- Ne jamais écrire un mot de passe sur papier ou dans un document numérique
- Audit regulier
- Ne esposer que les services necessaires
- N’ installer que les services necessaires

Mesures de protection contre les attaques

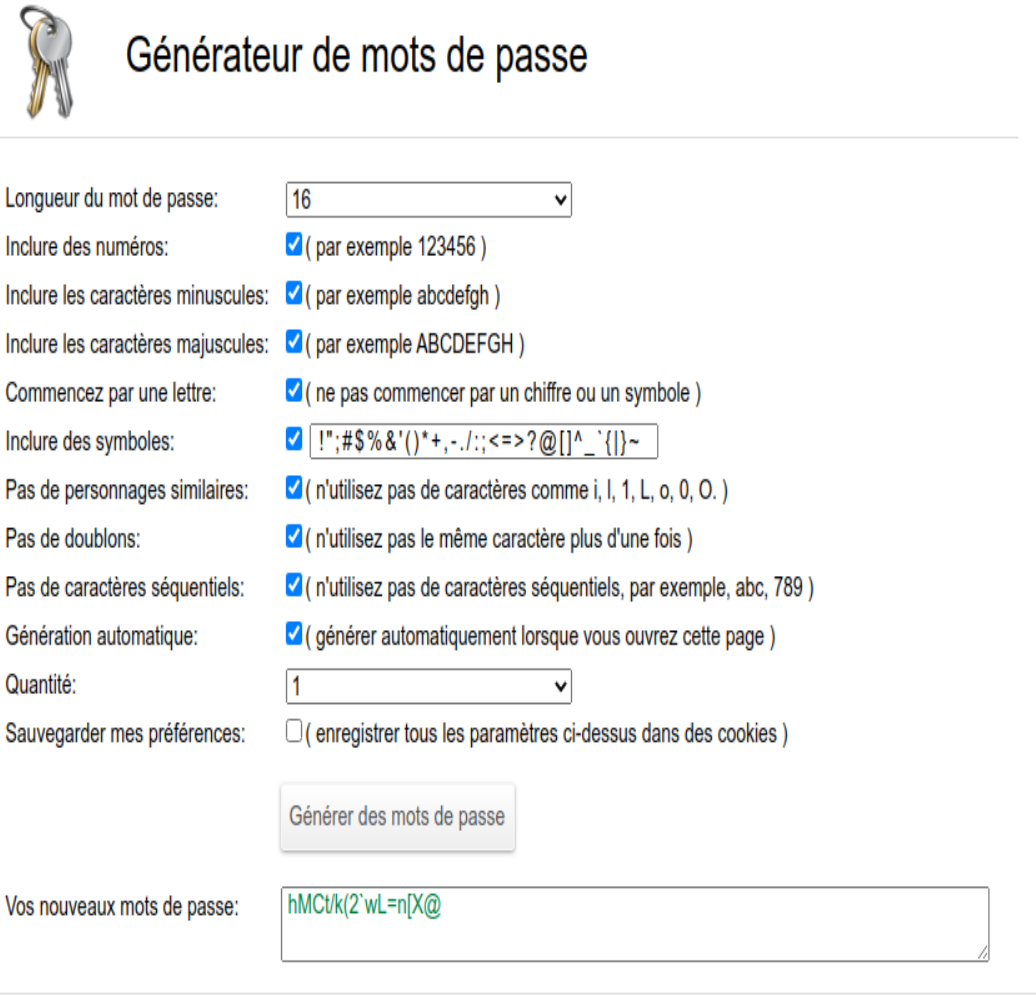
- SÉCURITÉ PHYSIQUE DU SERVER
- ANNULER LE SUPPORT DES CLÉ USB ET DU LECTEUR CD/DVD SUR LE SERVEUR
- MISE EN PLACE THE PAREFEU ET D'UN DMZ
- MISE EN PLACE DU SYSTÈME DE DÉTECTION D INTRUSION
- ETC



Bonne pratique pour le choix du mot de passe

Lors de la création d'un mot de passe il vous faudra choisir un bon mot de passe qui respecte les critères suivants:

- Au moins 8 caractères
- Au moins une majuscule
- Au moins une minuscule
- Au moins un chiffre
- Au moins un caractère spécial
- Etc



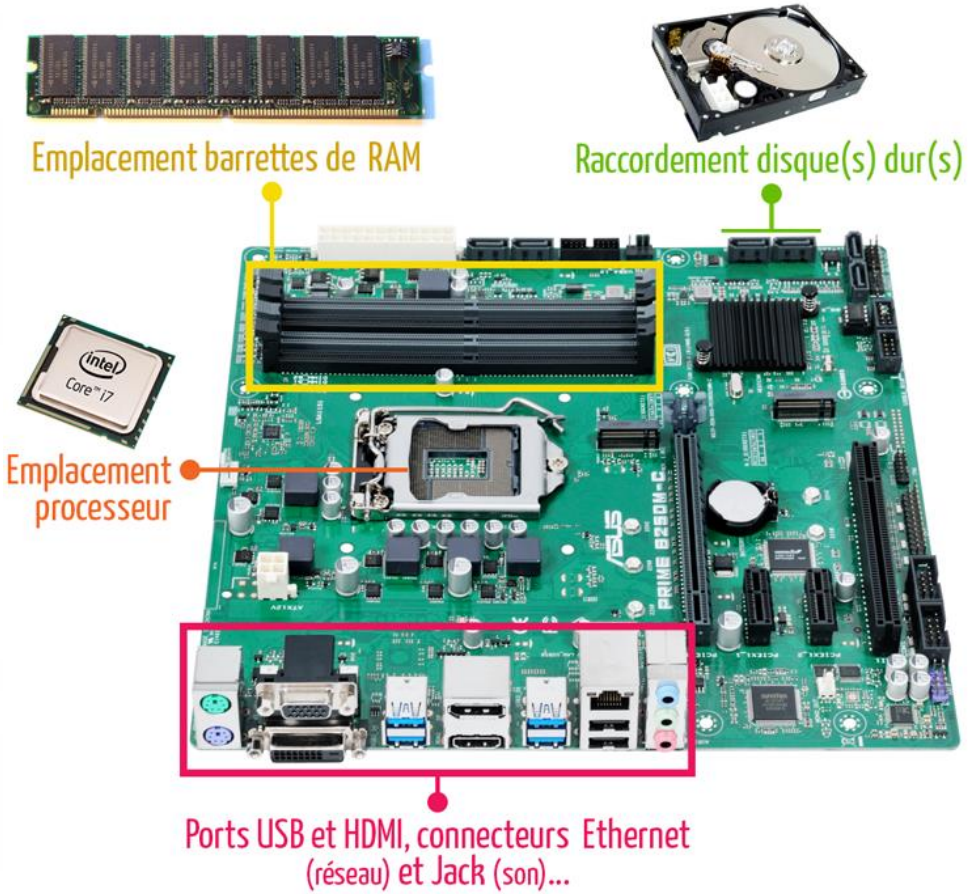
https://passwordsgenerator.net/fr/

La virtualisation et les systèmes virtualisés

Rappels

Ces rappels ne sont pas exhaustifs. Pour pouvoir suivre ce cours il faut maitriser les composants d'infrastructure ainsi que l'architecture des ordinateurs

- **Eléments principaux d'un ordinateur**
  - Bios
  - Mémoire vive (ram)
  - Processeur
  - Stockage longue durée (disque dur)
  - Réseau
  - Autres périphériques



Rappels

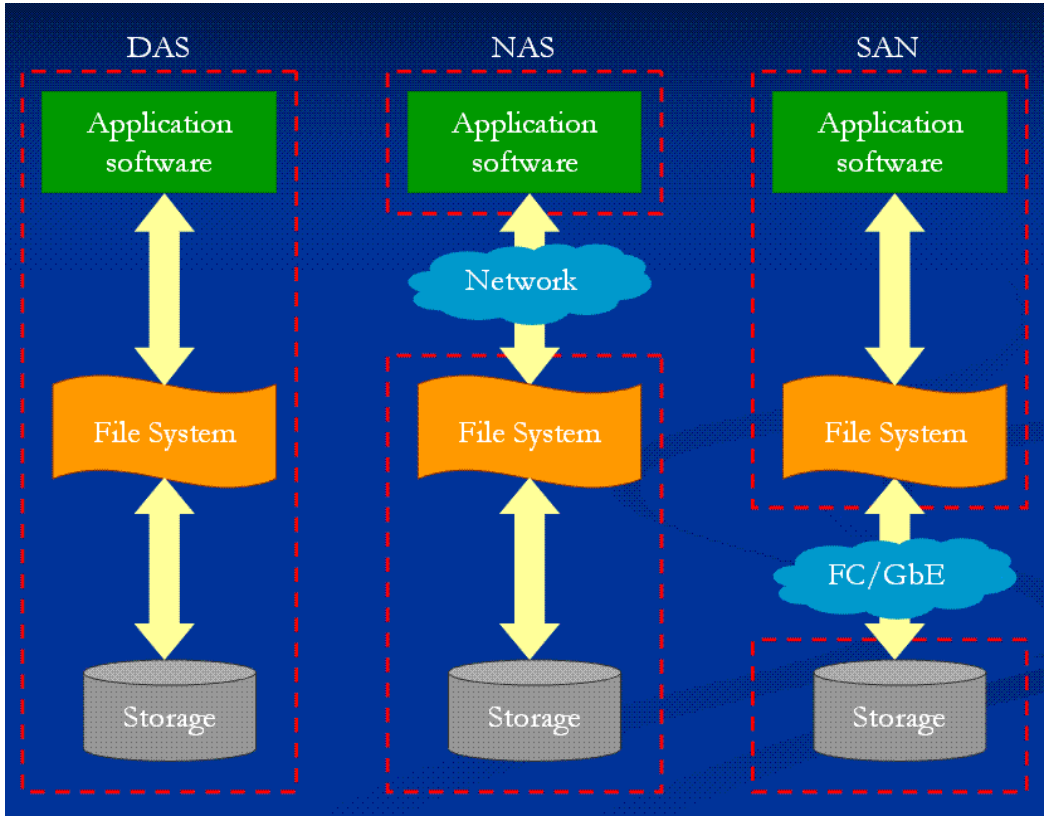
Ces rappels ne sont pas exhaustifs. Pour pouvoir suivre ce cours il faut maitriser les composants d'infrastructure ainsi que l'architecture des ordinateurs

- **Eléments d'infrastructure**
  - Serveurs
  - Stockage
    - Raid
  - Composants réseau

Stockage

Dans le cadre de ce cours nous nous intéresserons plus aux SAN

- **Terminologie**
  - DAS (Direct Attached Storage
    - Disque dur directement connecté à l'ordinateur
  - NAS (Network Attached Storage)
    - Serveur de fichiers autonome relié en réseau
  - SAN (Storage Area Network)
    - Les disques sont présentés à plus bas niveau (pas de serveur de fichier embarqué)

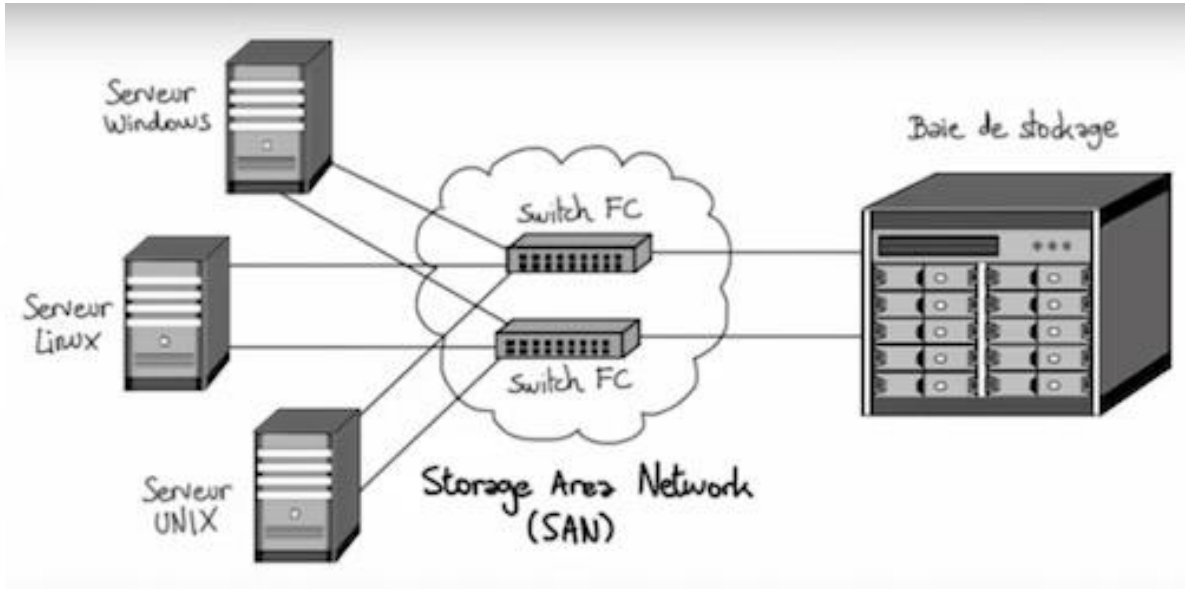


Les SAN

- SAN
  - Composés
    - de baies de diques (disk arrays)
      - Organisés en groupe de RAID
    - De modules d'alimentation
    - de contrôleurs

Les SAN

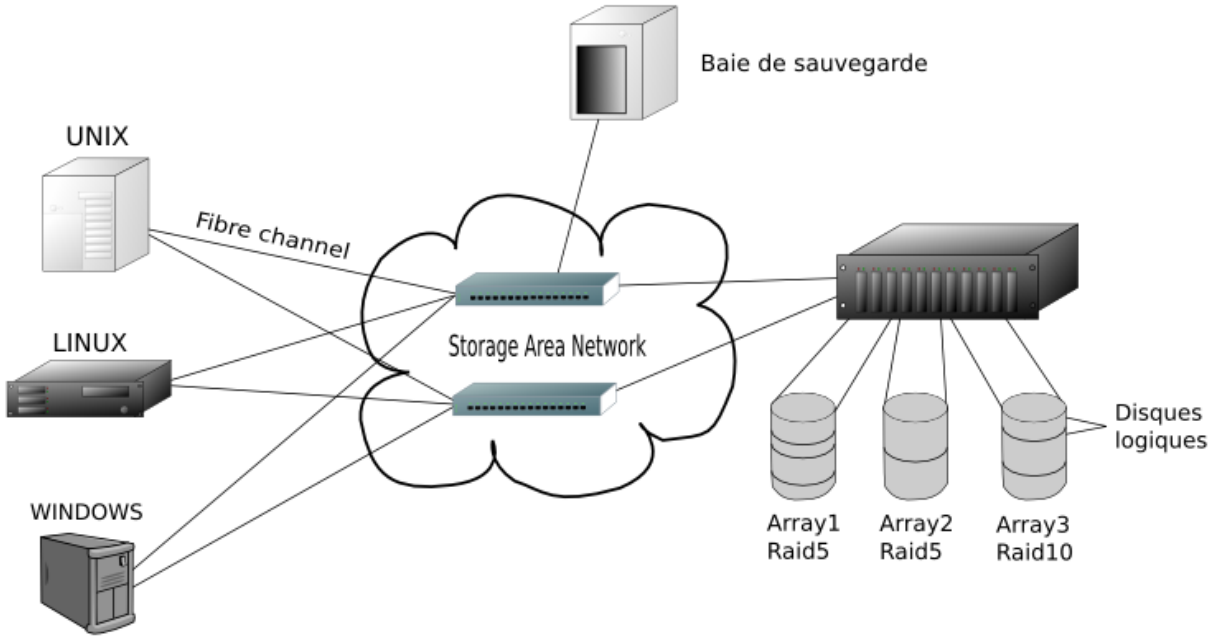
- SAN
  - Les contrôleurs
    - Gèrent les disques
    - Gèrent les raids
      - Les disques physiques sont regroupés en RAID
    - Gèrent les LUN's (= disques logiques présentés sur le réseau SAN)
      - Un LUN est un disque logique qui est présenté au serveur physique à travers l'infrastructure Storage Area Network



Plus tard nous verrons que parfois des LUN peuvent être présentés à plusieurs machines. Il s'agit d'un cas d'usage particulier.

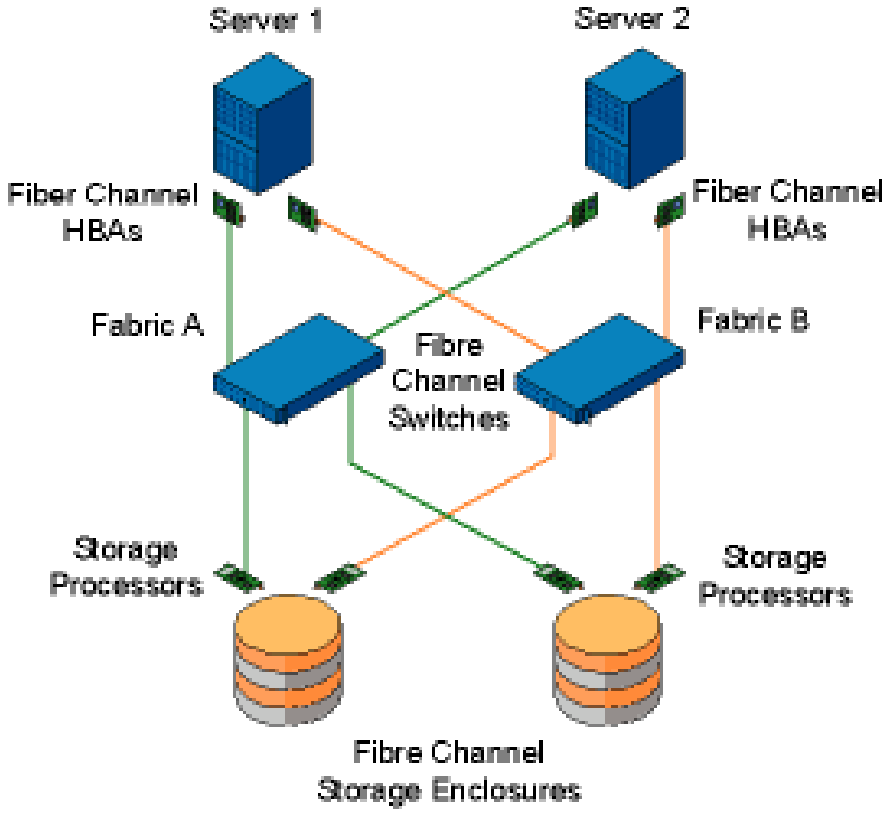
Les SAN

- SAN
  - Les contrôleurs
    - Remarque: LUN signifie Logical Unit Number
      - C'est le numéro d'identification d'une unité de stockage SAN
      - Par extension de langage on utilise cet acronyme pour désigner les disques virtuels (hardware, à ne pas confondre avec les disques virtuels (disques logiques) créés par les systèmes de virtualisation (hyperviseurs))
    - Pour améliorer la disponibilité et donc la résilience les contrôleurs sont souvent redondés



Les SAN

- **SAN - Infrastructure**
  - Les SAN switchs permettent la connection des serveurs aux stockage externalisés
    - Ils sont appelés Fiber Channels Switchs
    - Le protocole utilisé est le protocole « Fibre Channel »
      - Permet des vitesses de débit allant juqu'à 32 Gibabit/s
  - Les interfaces serveurs permettent de connecter les serveurs aux SAN switchs (ou directement aux storages) et sont appelées HBA (Host Bus Adapter)
  - Les interfaces connectant les Storage enclosures sont gérées par les contrôleurs et sont appelées SP (Storage Processor)

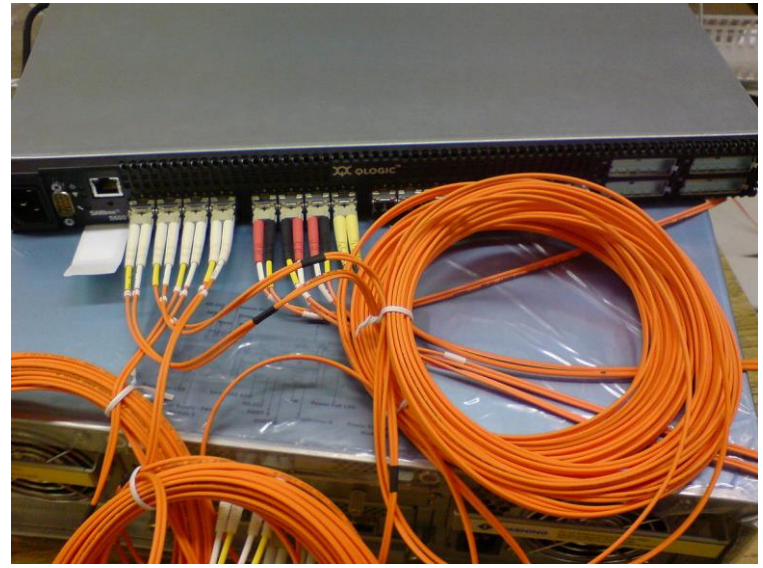


iSCSI

- **iSCSI (Internet Small Computer System Interface)**
  - Définition wikipedia

    iSCSI est une abréviation de Internet Small Computer System Interface. C'est un protocole de stockage en réseau basé sur le protocole IP destiné à relier les installations de stockage de données.

  - La généralisation des réseaux Ethernet avec un débit >= 1Gb/s permet de remplacer les infrastructures SAN switchs dédiées (HBA, fabric, SP) par des éléments réseaux classiques
    - Economies
    - Simplification de gestion



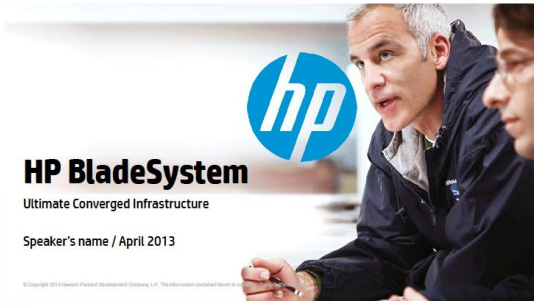
Ceci est un switch « fibre channel »

Rappels – Les serveurs à lame

- **Les serveurs à lame (blades servers)**
  - Optimisent la place occupée dans les racks
  - Aident à la standardisation de l'infrastructure
  - Permettent des remplacements plus faciles des serveurs (lames)

Rappels – Les serveurs à lame

- **Les serveurs à lame sont composés**
  - D'un chassis
  - De lames qui se branchent sur le « backpane »
    - Comme une grosse carte électronique avec tous les connecteurs
    - Chez certains constructeurs le « backpane » est redondant (2 « backpanes »)
  - L'arrière du châssis présente les modules d'alimentation ainsi que la connectique
  - → Document à lire « Hp Blade System »



Les infrastructures grande échelle 2020

- **Aujourd'hui (2020) nous parlons**
  - D'infrastructures convergées (début des années 2010)
    - Les blades embarquent du matériel comme des switches (et câbles)
  - D'infrastructures-hyper convergées (à partir de 2012 mais dans les faits, en Europe, après 2015)
  - Lectures
    - https://fr.wikipedia.org/wiki/Infrastructure_converg%C3%A9e
    - https://fr.wikipedia.org/wiki/Hyper-convergence

La virtualisation

- **Définition wikipedia**

La **virtualisation** consiste, en informatique, à exécuter sur une machine hôte, dans un environnement isolé, des systèmes d'exploitation[1] — on parle alors de **virtualisation système** — ou des applications[2] — on parle alors de **virtualisation applicative**. Ces ordinateurs virtuels sont appelés serveur privé virtuel (*Virtual Private Server* ou VPS) ou encore environnement virtuel (*Virtual Environment* ou VE).

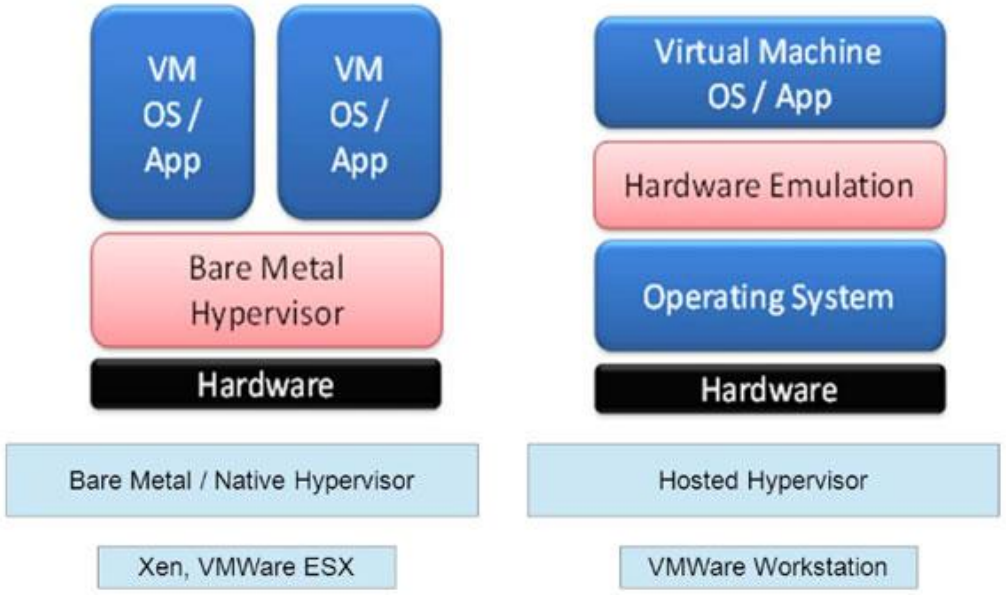
- **Machines virtuelles (aka virual machines – VM)**
  - Bios virtuel
  - CPU virtuel
  - RAM virtuelle
  - Disques durs virtuels
  - Cartes réseaux virtuelles
  - Autres périphériques virtuels

Les hyperviseurs

- **Définition wikipedia**

En informatique, un **hyperviseur** est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.

- **2 types d'hyperivseurs**
  - **Type 1: Natif – « Bare Metal »**
    - Le logiciel hyperviseur s'exécute directement sur une plate-forme matérielle
    - Exemples : Vmware ESXi, XEN, KVM, PolyXene, LPAR (IBM)
  - **Type 2 : « Hosted »**
    - Le logiciel hyperviseur s'exécute à l'intérieur d'un autre système d'exploitation
    - Exemples : VMWare Workstation, VMWare Fusion, Virtual Box, Virtual PC, Parallels Desktop (mac)



La virtualisation : Pourquoi ?

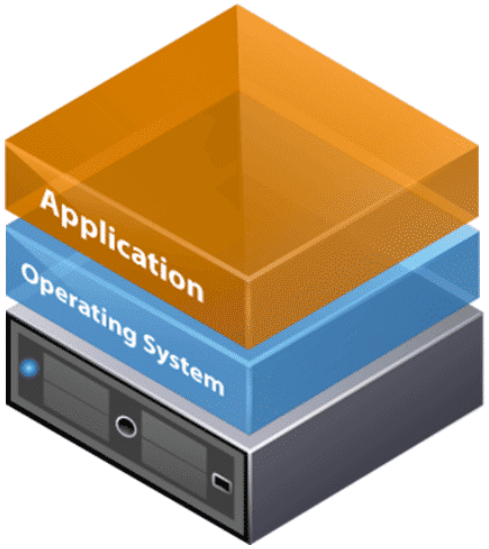
- **La virtualisation des systèmes offre un tas d'avantages (liste non exhaustive !)**
  - Optimisation des ressources
    - Allocation dynamique des ressources physique
      - Allocation dynamique de la puissance de calcul
      - Electricité
  - Facilité du provisionnement des ressources
  - Isolation (logique) des environnements
  - Résilience

La virtualisation : VMWare

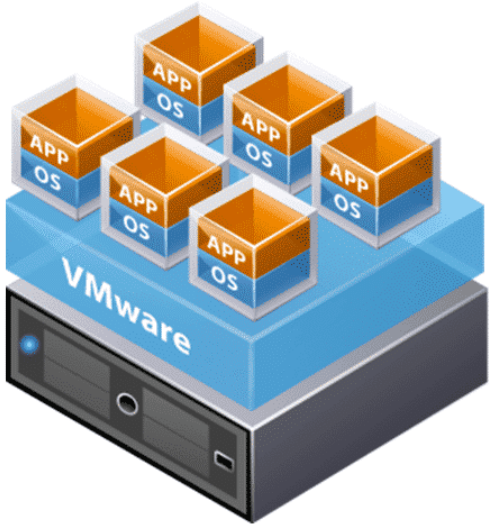
- **Historique VMWAre**
  - Création : 1998
  - Racheté par EMC en 2004
  - Dell a acheté EMC en 2016

La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi**
  - Bare Metal
  - Permet de faire tourner plusieurs machines virtuelles sur une seule machine physique



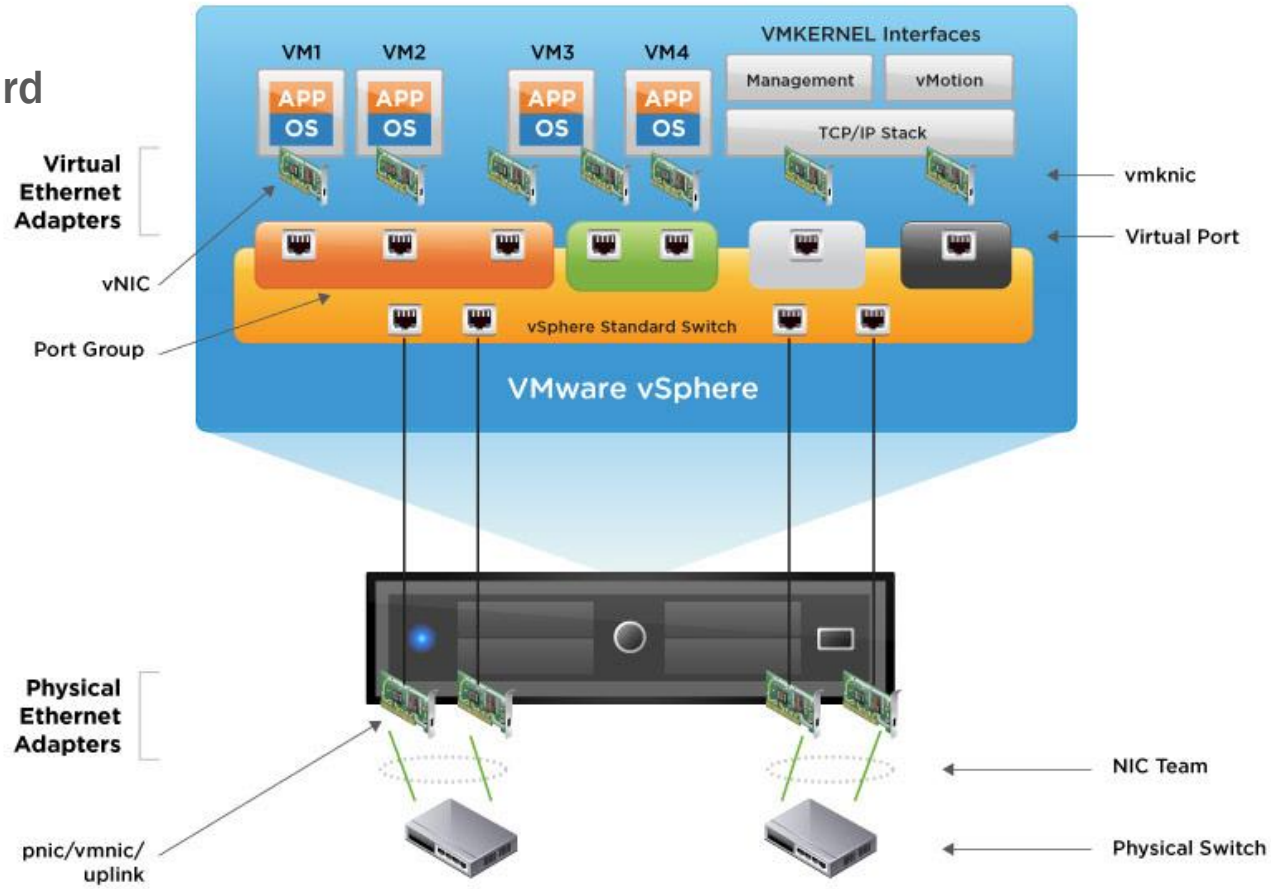
Traditional Architecture



Virtual Architecture

La virtualisation : Hyperviseur VMWare ESXi

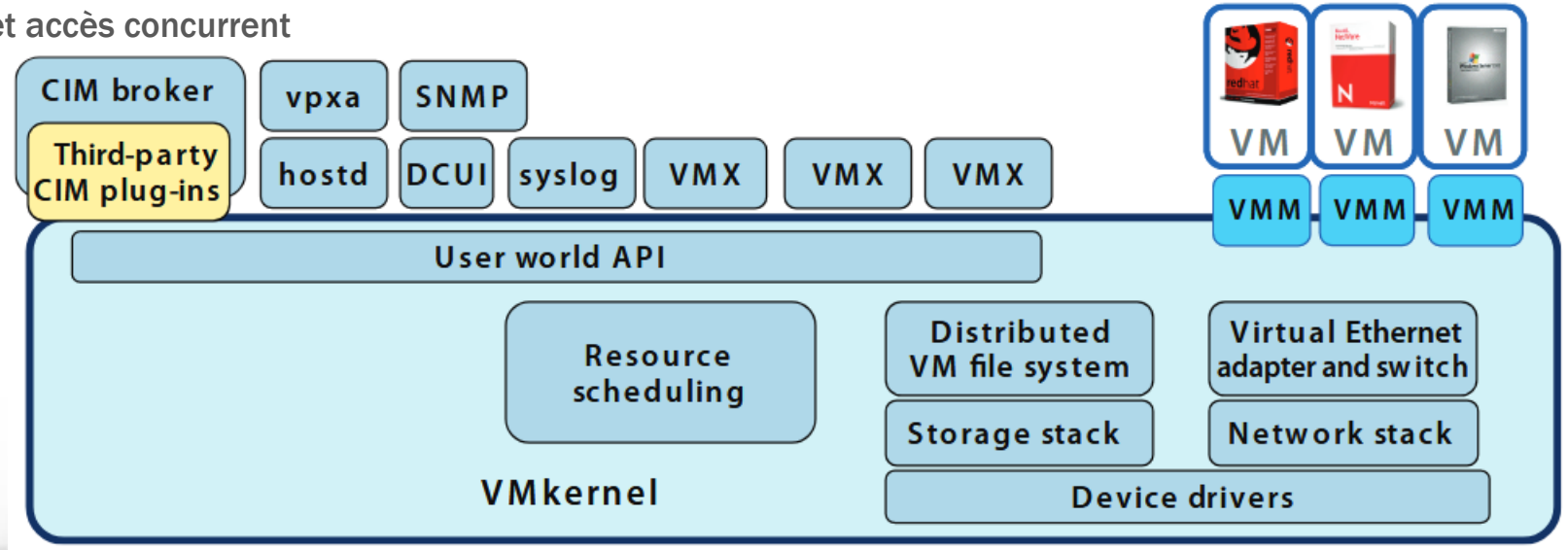
- **Virtualisation réseau**
  - Au sein d'un host ESXi la virtualisation du réseau se fait à l'aide d'un « vSphere Standard Switch »



Plus tard nous aborderons le concept de « vSphere Distributed Switch » qui est en fait un switch virtuel qui s'étend sur plusieurs serveurs physiques

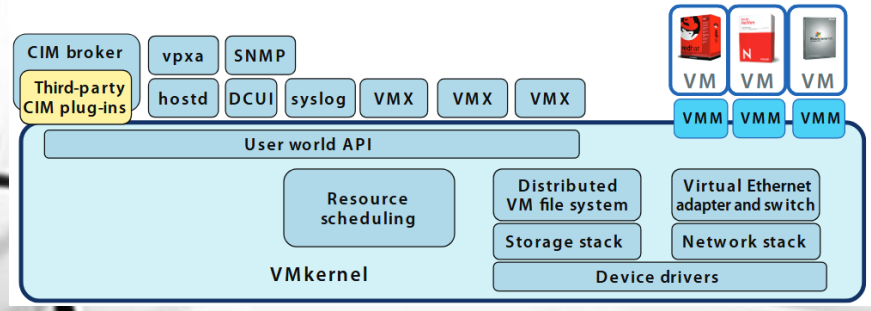
La virtualisation : Hyperviseur VMWare ESXi

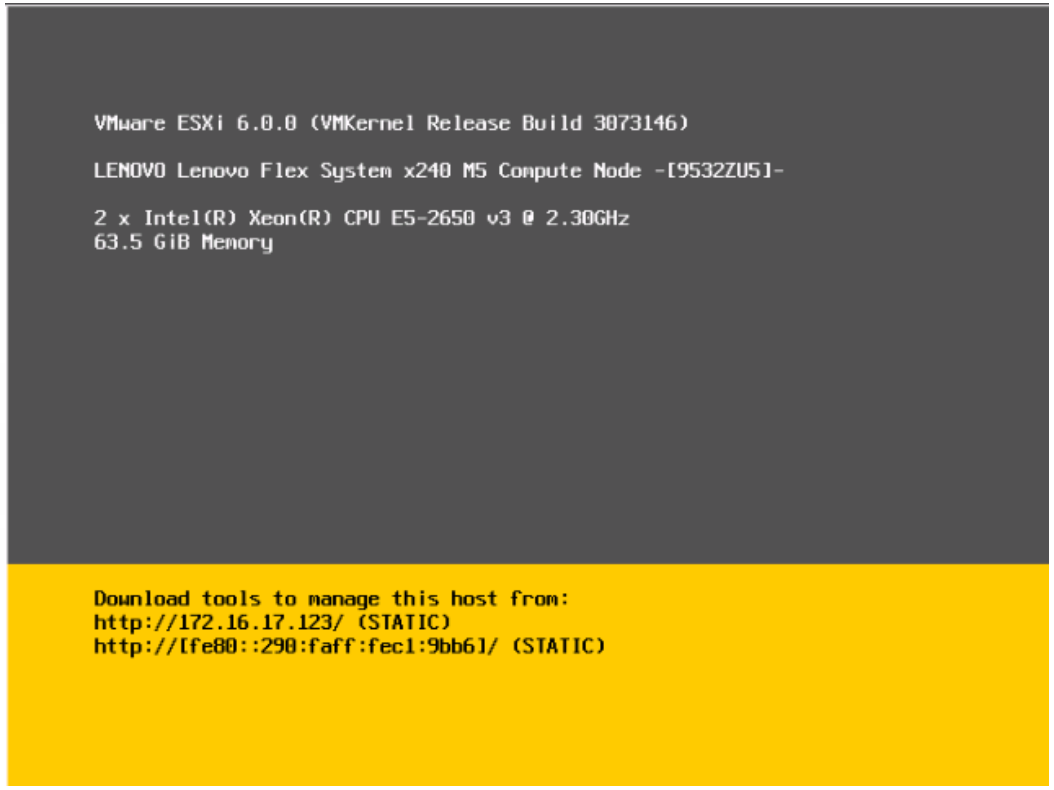
- **L'hyperviseur ESXi – footprint < 32MB ram**
  - ***VMkernel = underlying operationg system***
    - Drivers génériques (remarque : ESXi capricieux)
    - Ordonnanceurs
      - CPU
      - Mémoire
      - Accès disques
    - VMware File System (VMFS)
      - FS optimisé pour gros fichiers et accès concurrent



La virtualisation : Hyperviseur VMWare ESXi

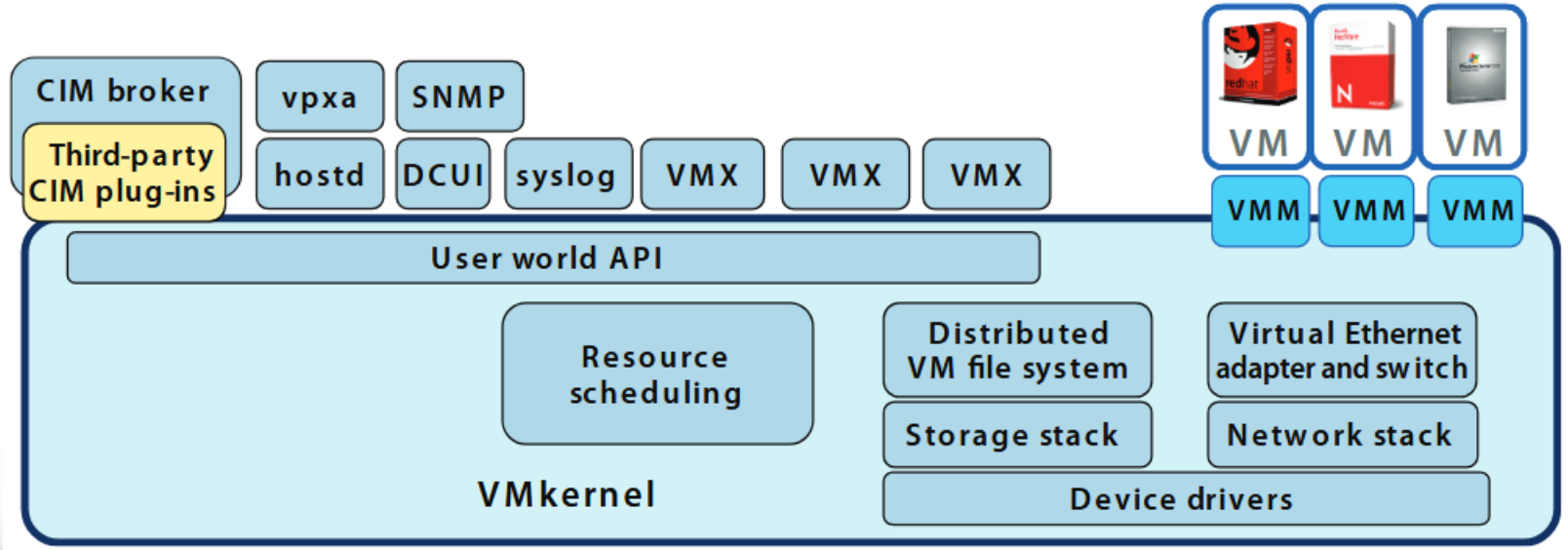
- **L'hyperviseur ESXi – Processus principaux tournant au dessus de VMkernel**
  - ***Direct Console User Interface (DCUI)***
    - Console serveur
    - Principalement utilisée pour les configurations basiques après installation
      - Mot de passe « admin » du « host » (machine physique)
      - Configuration réseau
    - Aussi pour « troubleshooting
      - Tests réseau
      - Logs
      - Redémarrer des agents
      - Restaurer les paramètres par défaut





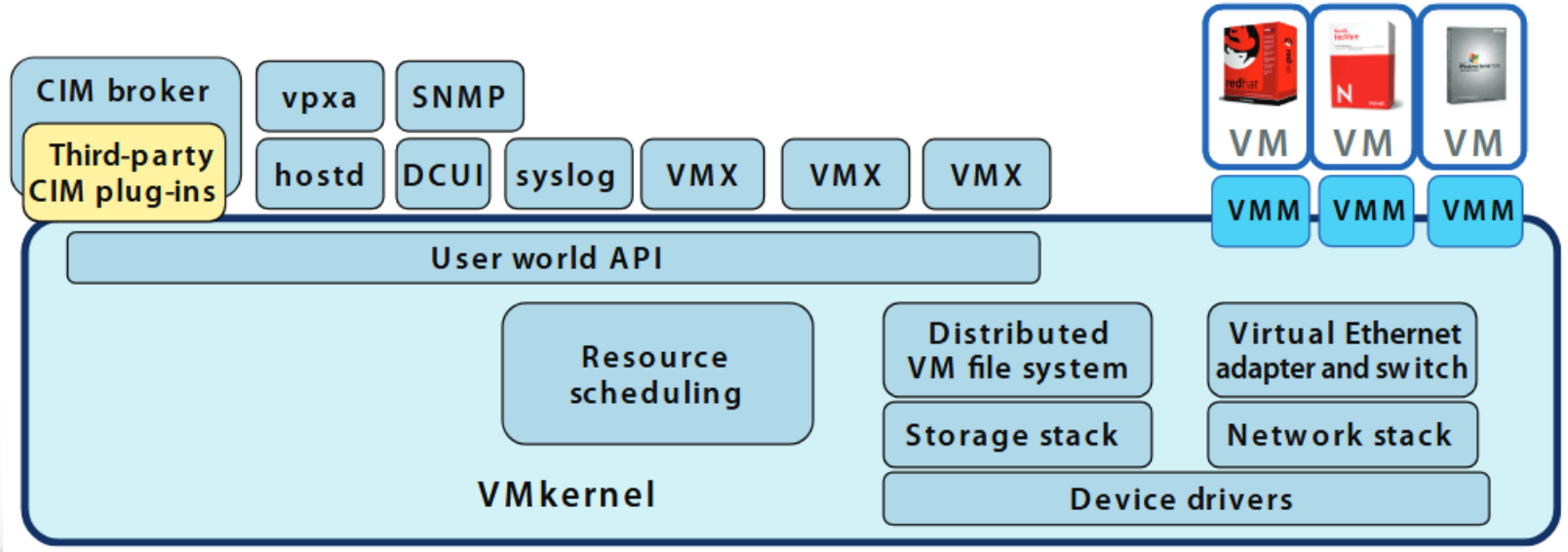
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Processus principaux tournant au dessus de VMkernel**
  - ***Virtual Machine Monitor (VMM)***
    - Fournit environnement d'exécution pour une VM
    - En combinaison avec processus « helper » VMX
    - Chaque VM a son propre processus
      - VMM
      - VMX



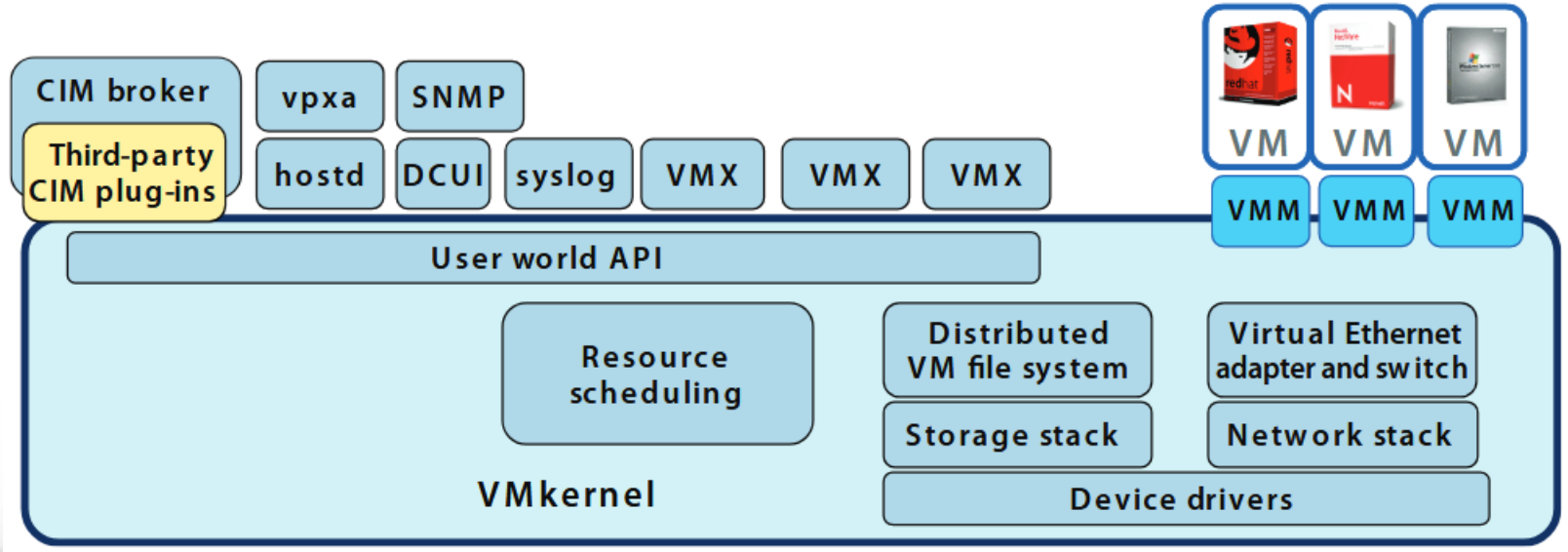
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Processus principaux tournant au dessus de VMkernel**
  - ***Common Information model (CIM)***
    - Utilisé principalement pour le monitoring du matériel



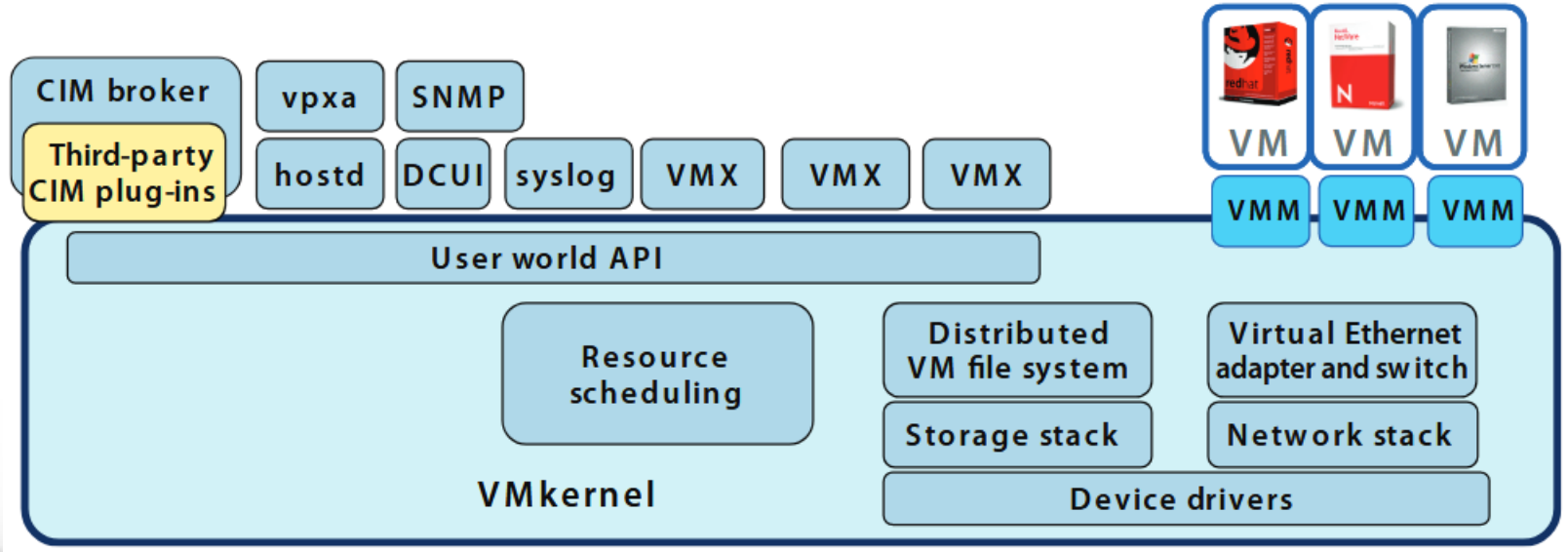
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Processus principaux tournant au dessus de VMkernel**
  - **Autres processus : hostd**
    - Connexions directes du VI client
    - Connexions via l'API VI
    - Authentifie les utilisateurs locaux
    - Gère la DB des utilisateurs locaux



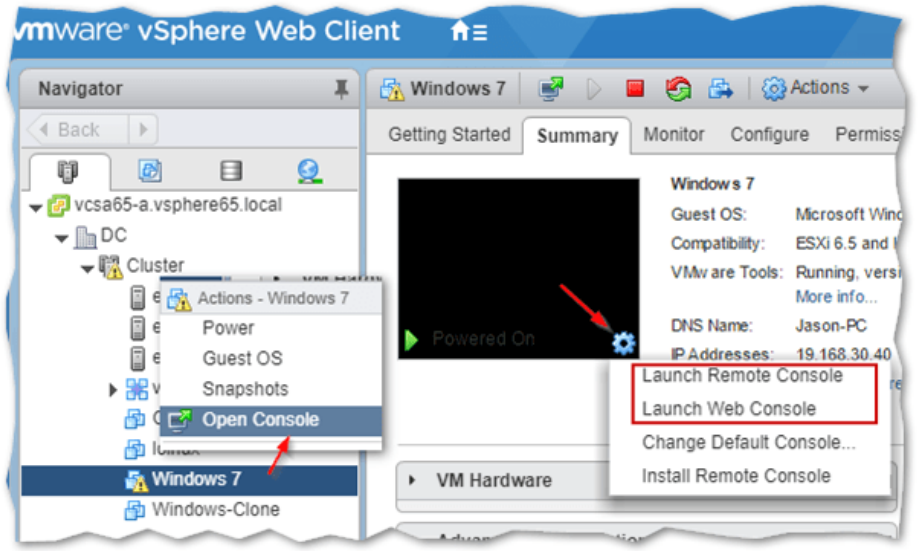
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Processus principaux tournant au dessus de VMkernel**
  - **Autres processus : vpxa**
    - Agent utilisé pour se connecter au « Virtual Center »
    - Tourne en tant qu'utilisateur « vpxuser »
    - Est intermédiaire entre l'agent « hostd » et le « Virtual Center »



La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Ports réseau utilisés**
  - **Obligatoires**
    - 22 - SSH (TCP)
    - 53 - DNS (TCP and UDP)
    - 80 - HTTP (TCP/UDP)
    - 902 - vCenter Server / VMware Infrastructure Client - UDP for ESX/ESXi Heartbeat (UDP and TCP)
    - 903 - Remote Access to VM Console (TCP)
    - 443 - Web Access (TCP)
    - 27000, 27010 - License Server (Valid for ESX/ESXi 3.x hosts only)



La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Ports réseau utilisés**
  - **Optionnels**
    - 123 - NTP (UDP)
    - 161, 162 - SNMP (UDP)
    - 88 - Kerberos (UDP and TCP)
    - 464 - Active Directory (TCP and UDP)
    - 3260 - Software iSCSI (TCP)

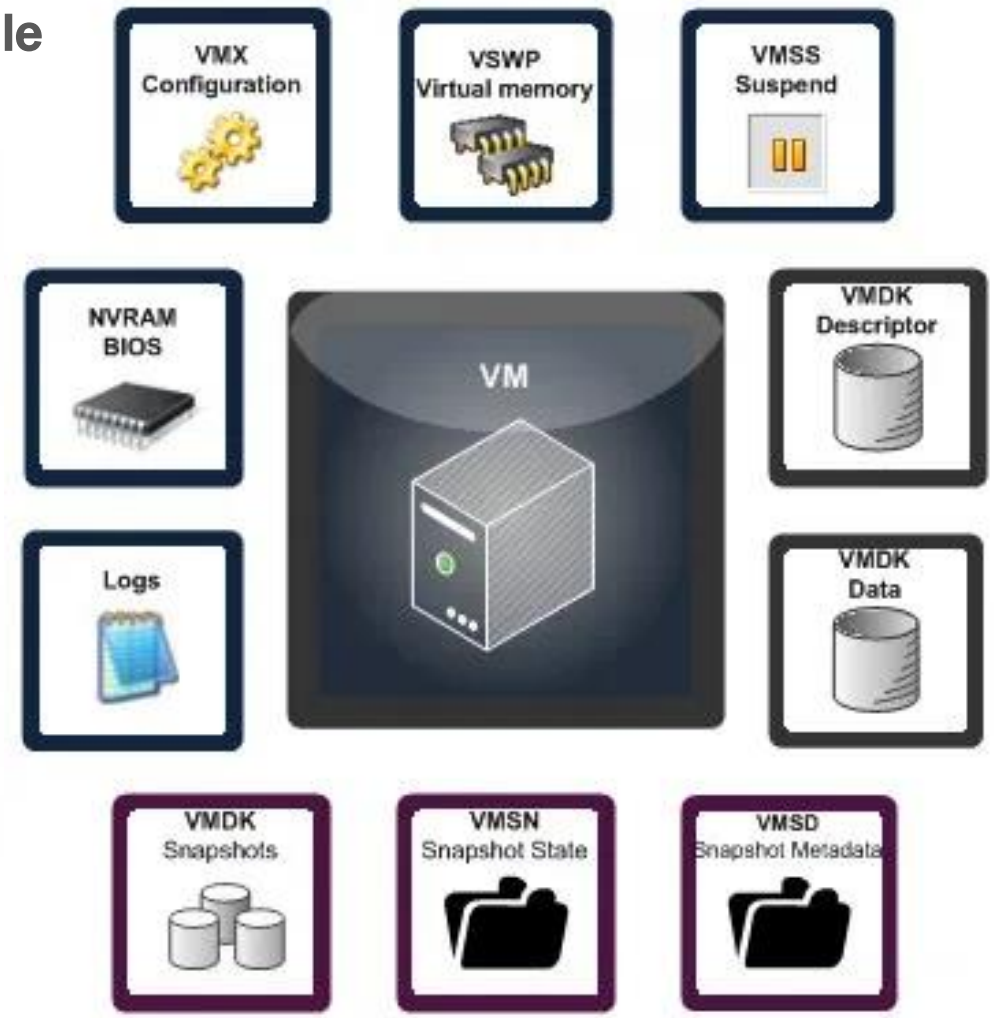
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Structure d'une machine virtuelle**
  - **Machine virtuelle = Ensemble de fichiers**

Icefyre

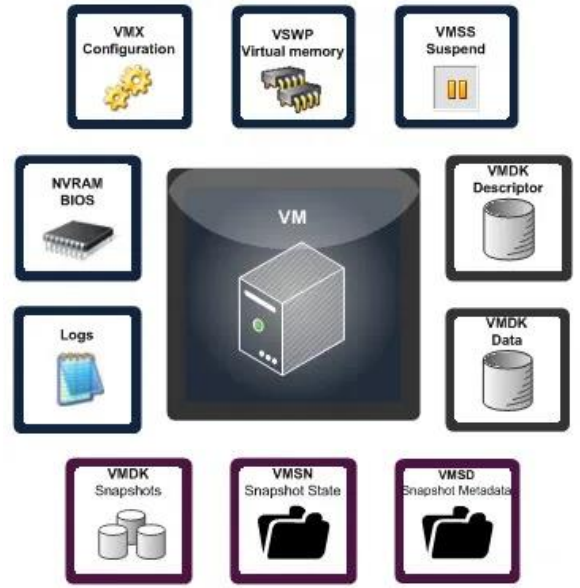
/vmfs/volumes/442d541b-cb5a815d-6083-0017a4a9c074/Icefyre

Name	Ext	Size	Changed	Rights	Owner
..			11/11/2008 4:57:20 PM	rwxrwxrwt	root
Icefyre.nvram		8,684	11/11/2008 4:54:33 PM	rw-------	root
Icefyre.vmdk		336	11/11/2008 4:06:25 PM	rw-------	root
Icefyre.vmsd		1,075	7/10/2008 3:00:46 PM	rw-------	root
Icefyre.vmx		3,336	11/11/2008 4:56:34 PM	rwxr-xr-x	root
Icefyre.vmxf		274	11/11/2008 4:56:34 PM	rw-------	root
Icefyre-flat.vmdk		21,474,836,480	11/11/2008 4:53:57 PM	rw-------	root
vmware.log		32,579	11/11/2008 4:54:35 PM	rw-r--r--	root
vmware-19.log		31,281	11/11/2008 2:30:39 PM	rw-r--r--	root
vmware-20.log		31,178	11/11/2008 3:31:55 PM	rw-r--r--	root
vmware-21.log		31,112	11/11/2008 3:34:49 PM	rw-r--r--	root
vmware-22.log		30,575	11/11/2008 3:37:34 PM	rw-r--r--	root
vmware-23.log		30,575	11/11/2008 3:40:04 PM	rw-r--r--	root
vmware-24.log		38,607	11/11/2008 3:42:01 PM	rw-r--r--	root



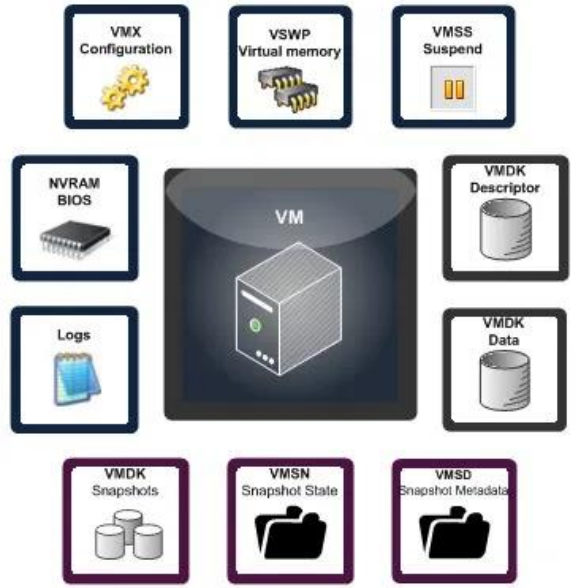
La virtualisation : Hyperviseur VMWare ESXi

- L'hyperviseur ESXi – Structure d'une machine virtuelle
  - Machine virtuelle = Ensemble de fichiers
    - .vmx
      - Fichier de configuration de la VM
        - Format texte
        - Contient les informations de configuration de la VM
          - RAM
          - Infos carte réseau
          - Infos disques durs virtuels
          - Infos ports parallèles, série
          - Paramètres avancés d'alimentation et de ressources
          - Options des « vmware tools »
        - Possible de le modifier manuellement
          - Backup vivement conseillé avant



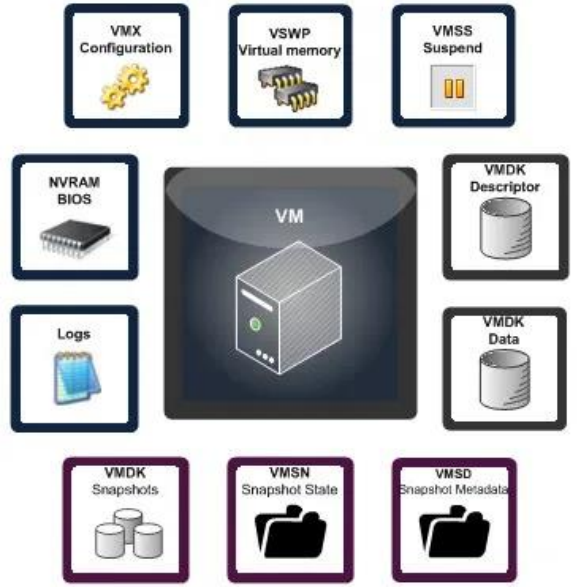
La virtualisation : Hyperviseur VMWare ESXi

- L'hyperviseur ESXi – Structure d'une machine virtuelle
  - Machine virtuelle = Ensemble de fichiers
    - .nvram
      - BIOS de la VM
        - Format binaire
        - Press F2 to enter bios
        - Modifications de configurations sont enregistrées
        - Automatiquement recréé si supprimé

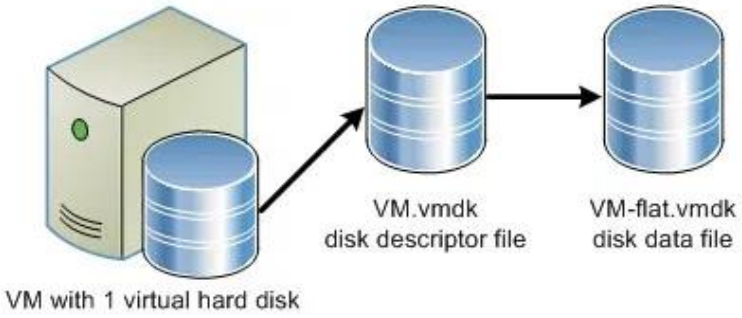


La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Structure d'une machine virtuelle**
  - **Machine virtuelle = Ensemble de fichiers**
    - **.vmdk :** Tout ce qui concerne les HD virtuels
    - Chaque HD virtuel a au moins 2 vmdk
      - Un ou des gros fichiers qui contiennent les données
      - Petit fichier texte qui contient le descriptif
        - Taille, géométrie, …

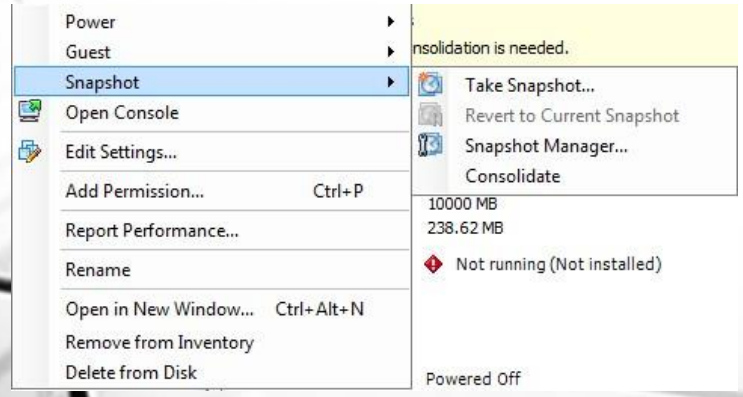


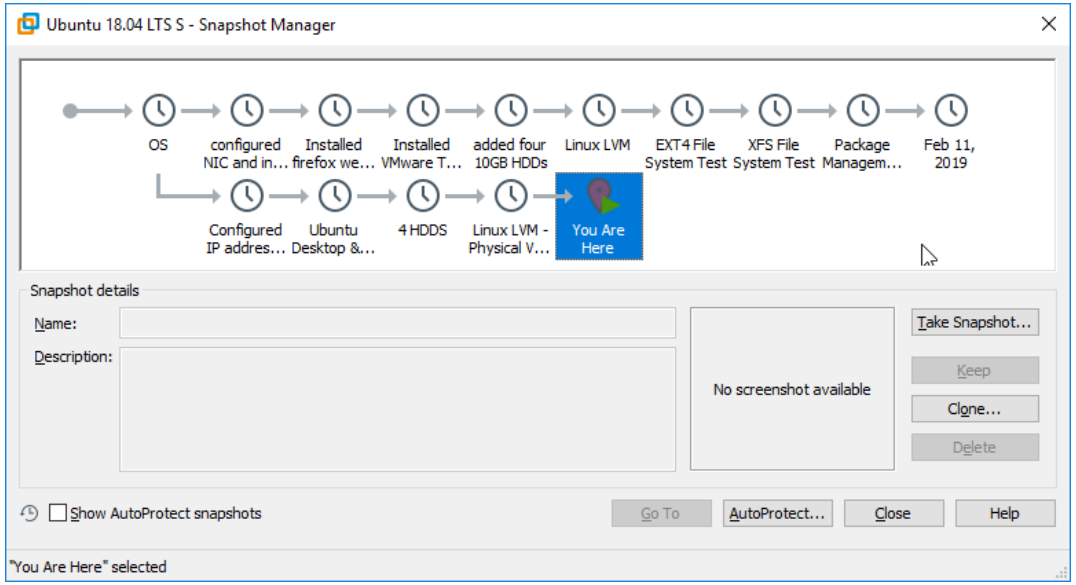

```
# Disk DescriptorFile
version=1
CID=fb2357fd
parentCID=ffffffff
createType="vmfs"

# Extent description
RW 41943040 VMFS "Icefyre-flat.vmdk"

# The Disk Data Base
#DDB

ddb.toolsVersion = "0"
ddb.virtualHWVersion = "4"
ddb.geometry.cylinders = "2610"
ddb.geometry.heads = "255"
ddb.geometry.sectors = "63"
ddb.adapterType = "lsilogic"
```



La virtualisation : Hyperviseur VMWare ESXi

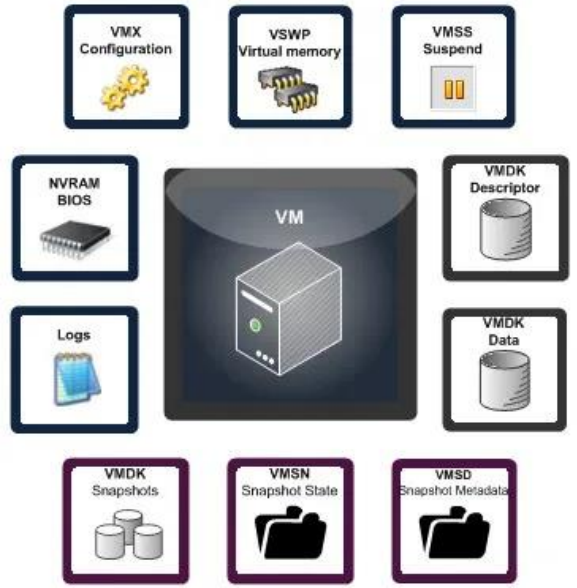
- **L'hyperviseur ESXi – Les snapshots**
  - **Permettent de figer l'état d'une VM à un instant donné et d'y revenir à tout moment**
    - **Snapshot à froid**
      - Snapshot effectué lorsque machine virtuelle est éteinte
        - Intégrité des données garantie
    - **Snapshot à chaud**
      - Snapshot effectué lorsque la machine virtuelle est allumée
        - Inclus snapshot de la ram
          - Copie de la RAM dans le fichier associé .vmsn
        - Pas de garantie de préservation de l'intégrité des données

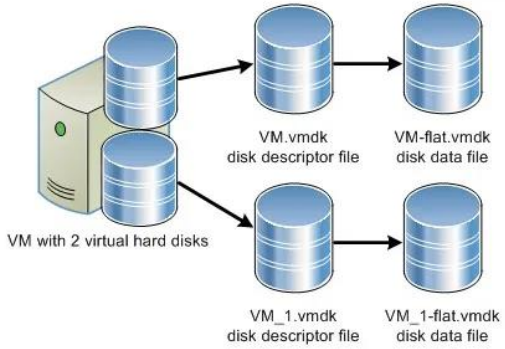




La virtualisation : Hyperviseur VMWare ESXi

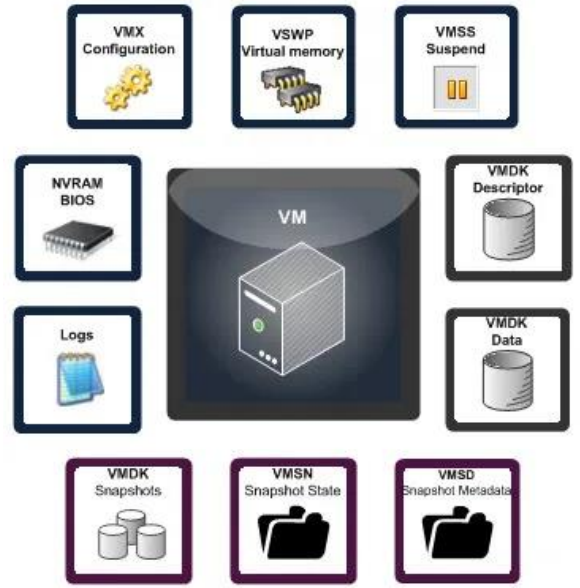
- L'hyperviseur ESXi – Structure d'une machine virtuelle
  - Machine virtuelle = Ensemble de fichiers
    - -delta.vmdk
    - Créés en cas de « snapshot »
      - -flat.vmdk est figé
      - Les modifications apportées au disque virtuel sont écrites dans les fichiers –delta.vmdk
        - Taille des fichiers –delta.vmdk incrémente par 16MB
        - Taille max = taille virtual HD
        - 1 ficher -delta.vmdk par snapshot
          - Plusieurs snapshots possibles pour une VM
    - Les fichiers –delta.vmdk disparaissent (avec ou sans fusion dans fichier –flat.vmdk d'origine)





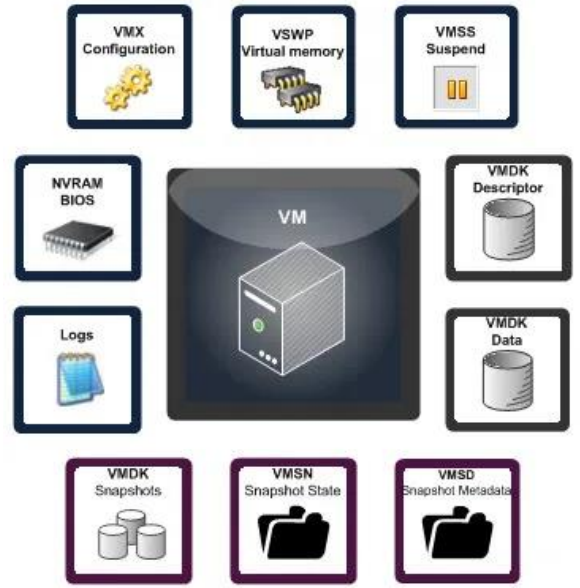
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Structure d'une machine virtuelle**
  - **Machine virtuelle = Ensemble de fichiers**
  - **Les snapshots**
    - Un seul fichier **.vmsd** qui contient les metadata
      - Format texte
      - Taille initiale : 0 octet
    - Un fichier **.vmsn** par snapshot
      - Format binaire
      - contient une copie de la RAM en cas de snapshot à chaud
        - < 32Kb sinon
      - Supprimé lorsque le snapshot est supprimé



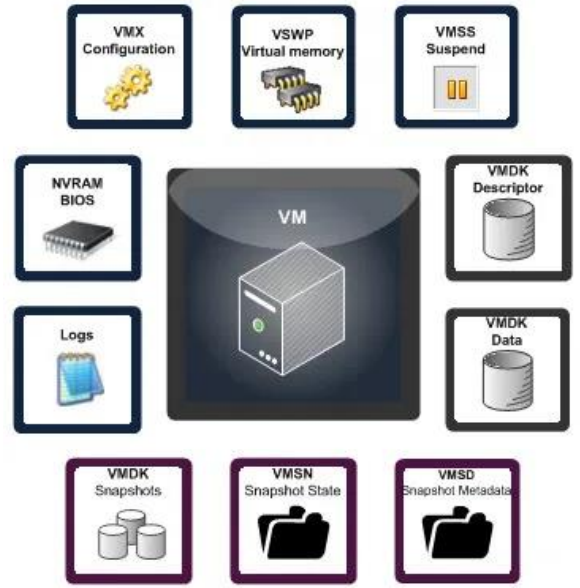
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Structure d'une machine virtuelle**
  - **Machine virtuelle = Ensemble de fichiers**
    - **.vswp – swap file**
    - Format binaire
    - Créés lors de l'allumage d'une VM
    - Taille = taille RAM VM – taille réservation éventuelle
    - Attention
      - Perfs
      - Remplit le système de stockage vmware (vmfs)
        - VM ne s'allumera pas s'il ne reste pas assez d'espace pour stocker .vswp
    - Supprimé
      - Lorsque VM est éteinte
      - Lorsque VM est suspendue



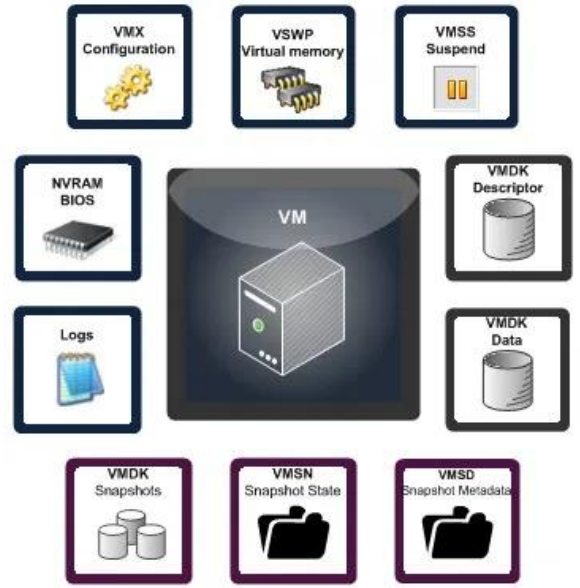
La virtualisation : Hyperviseur VMWare ESXi

- L'hyperviseur ESXi – Structure d'une machine virtuelle
  - Machine virtuelle = Ensemble de fichiers
    - .vmss – lorsque VM est suspendue
    - Format binaire
    - Créés lorsqu'on suspend une VM
      - Copie de la RAM de la VM
        - Y inclus les contenus vides
    - Effacé lorsque VM est éteinte
      - Pas effacé si VM est redémarrée
    - Réécrit si VM suspendue à nouveau
    - Lorsqu'une VM sort de l'état de suspension le contenu du fichier est copié dans la RAM physique du serveur hôte



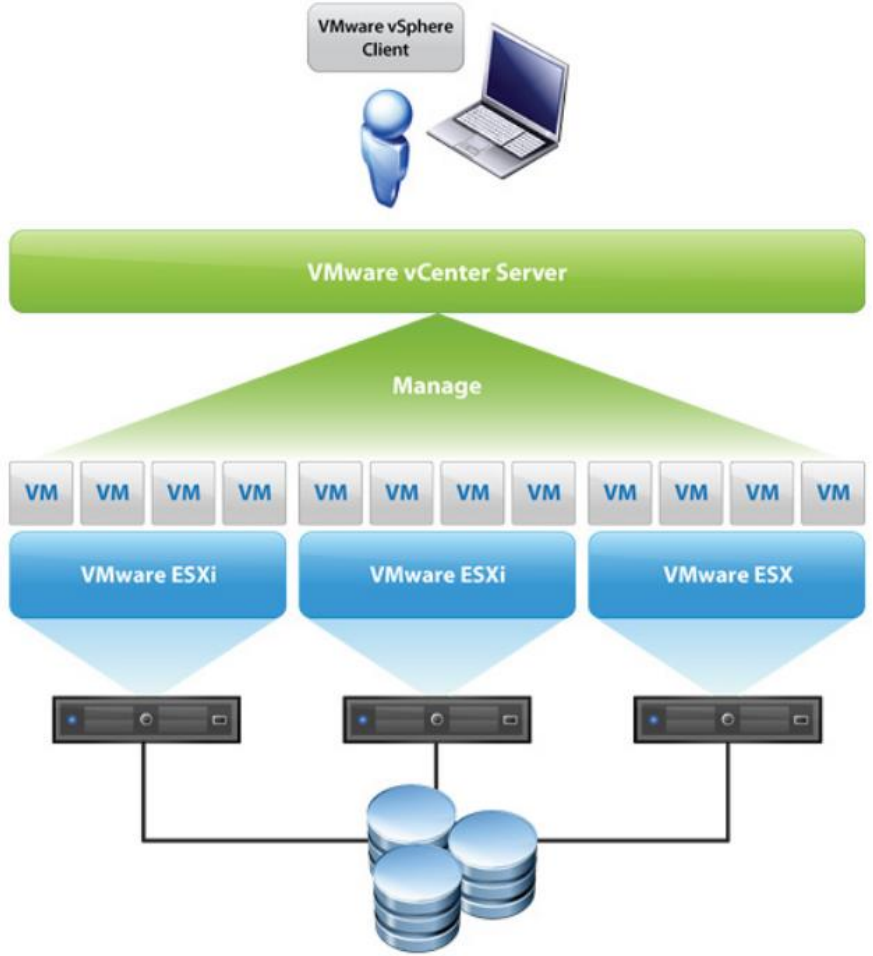
La virtualisation : Hyperviseur VMWare ESXi

- **L'hyperviseur ESXi – Structure d'une machine virtuelle**
  - **Machine virtuelle = Ensemble de fichiers**
    - **.log – fichies « log »**
    - Format texte
    - Utilisés pour dépannage
    - Nouveau fichier créé
      - lorsque VM est éteinte
      - Lorsque taille max est atteinte (log.rotateSize, en kilobytes)
    - 6 fichiers sont conservés par défaut (log.keepOld)



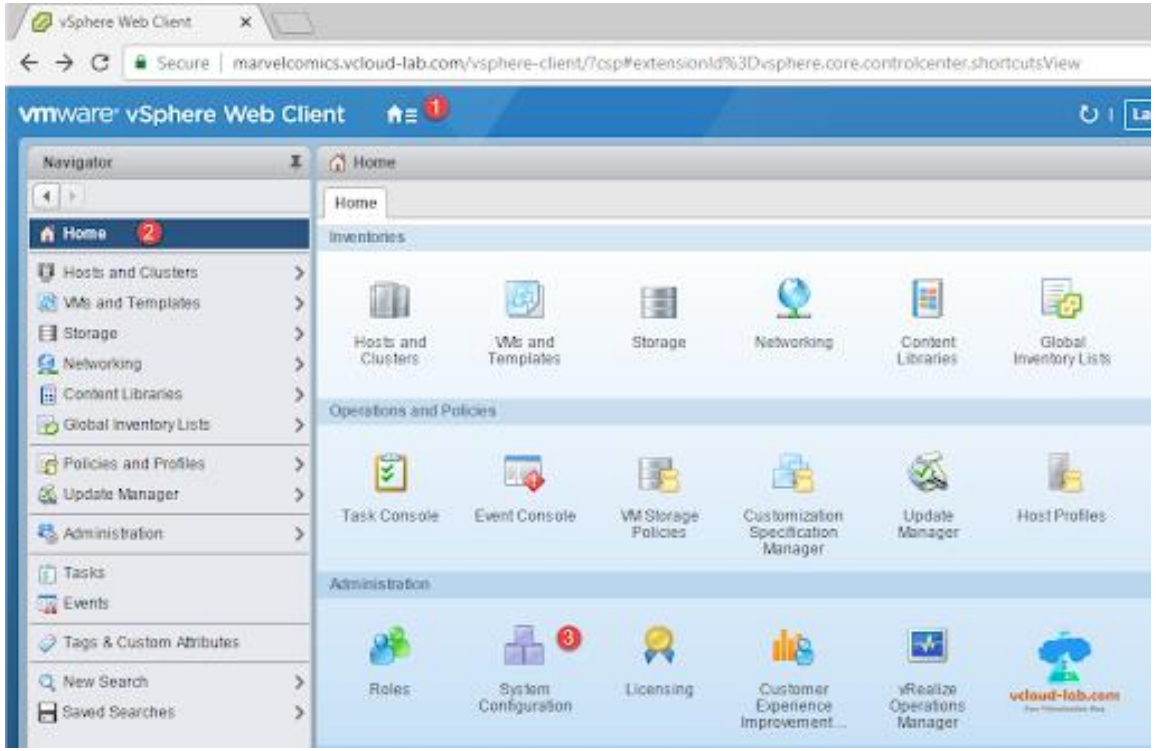
La virtualisation : Ecosystème vSphere

- Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud
  - Composants minimum requis
    - 2 serveurs physique
    - Un stockage partagé
      - Peut-être virutalisé avec les dernières versions de vmware (vSan)
    - Swichs réseau et interconnexion des serveurs



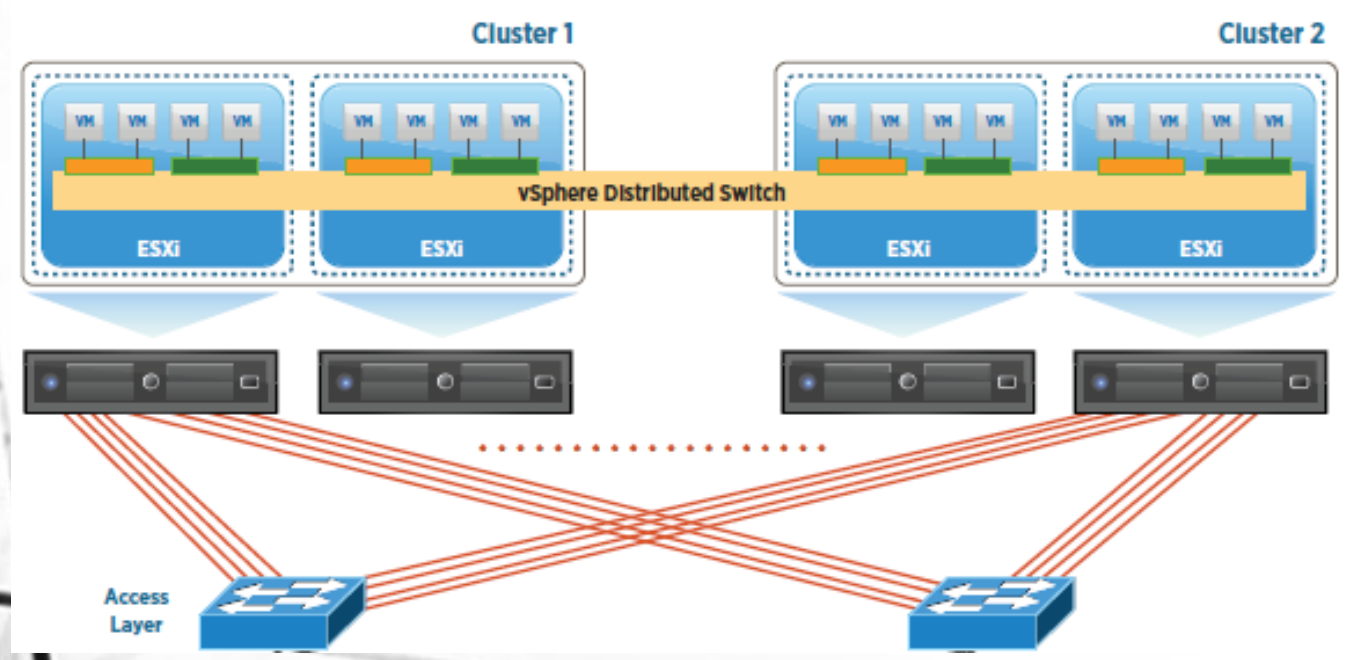
La virtualisation : Ecosystème vSphere

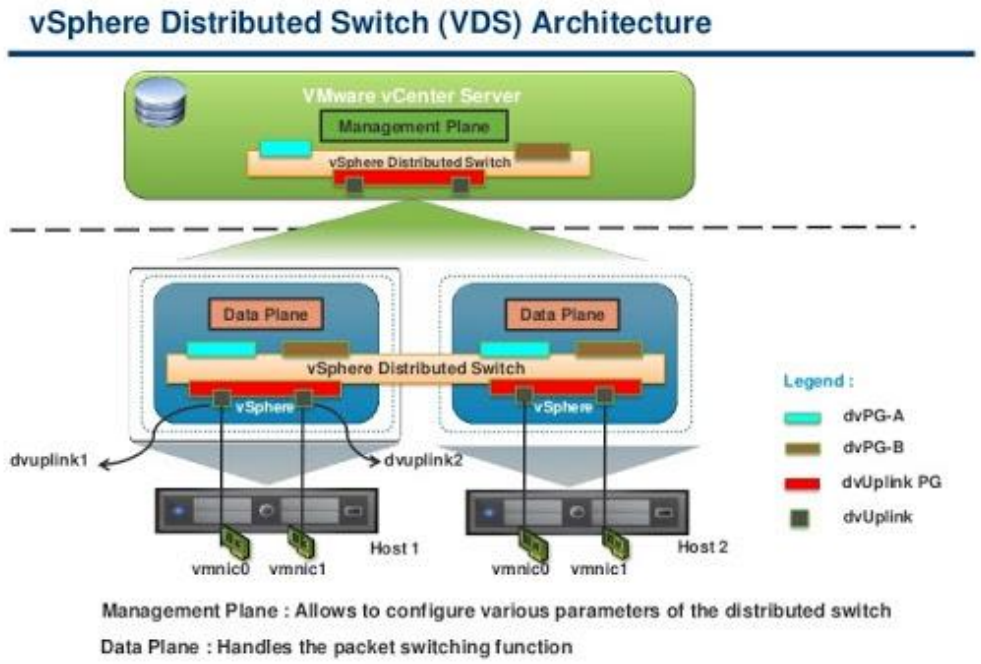
- Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud
  - Permet (entre autres)
    - Gestion centralisée (vCenter)
      - Gestion complète de l'écosystème
        - Serveurs physiques
        - Systèmes de fichiers vmfs
        - Réseau virtuel
        - Backups
        - Alertes
        - Machines virtuelles
        - ...



La virtualisation : Ecosystème vSphere

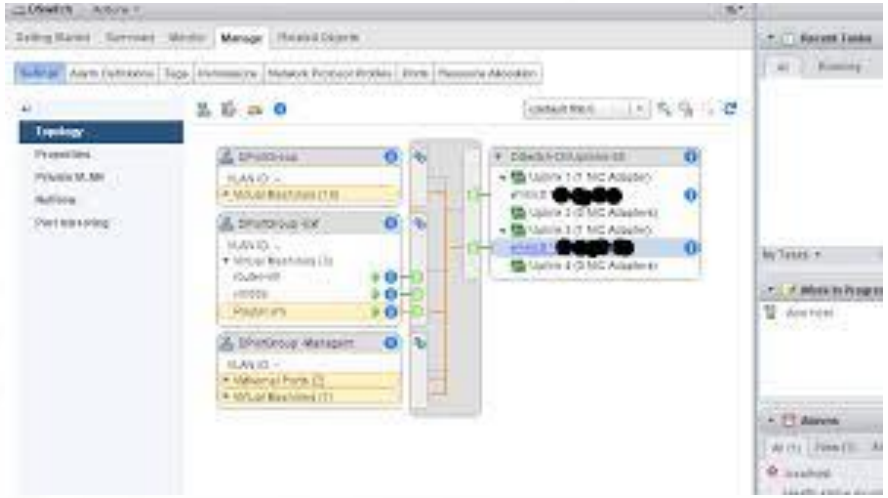
- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **Switchs distribués (vSphere Distributed Switchs)**
    - La configuration se propage sur un ensemble de serveurs physiques

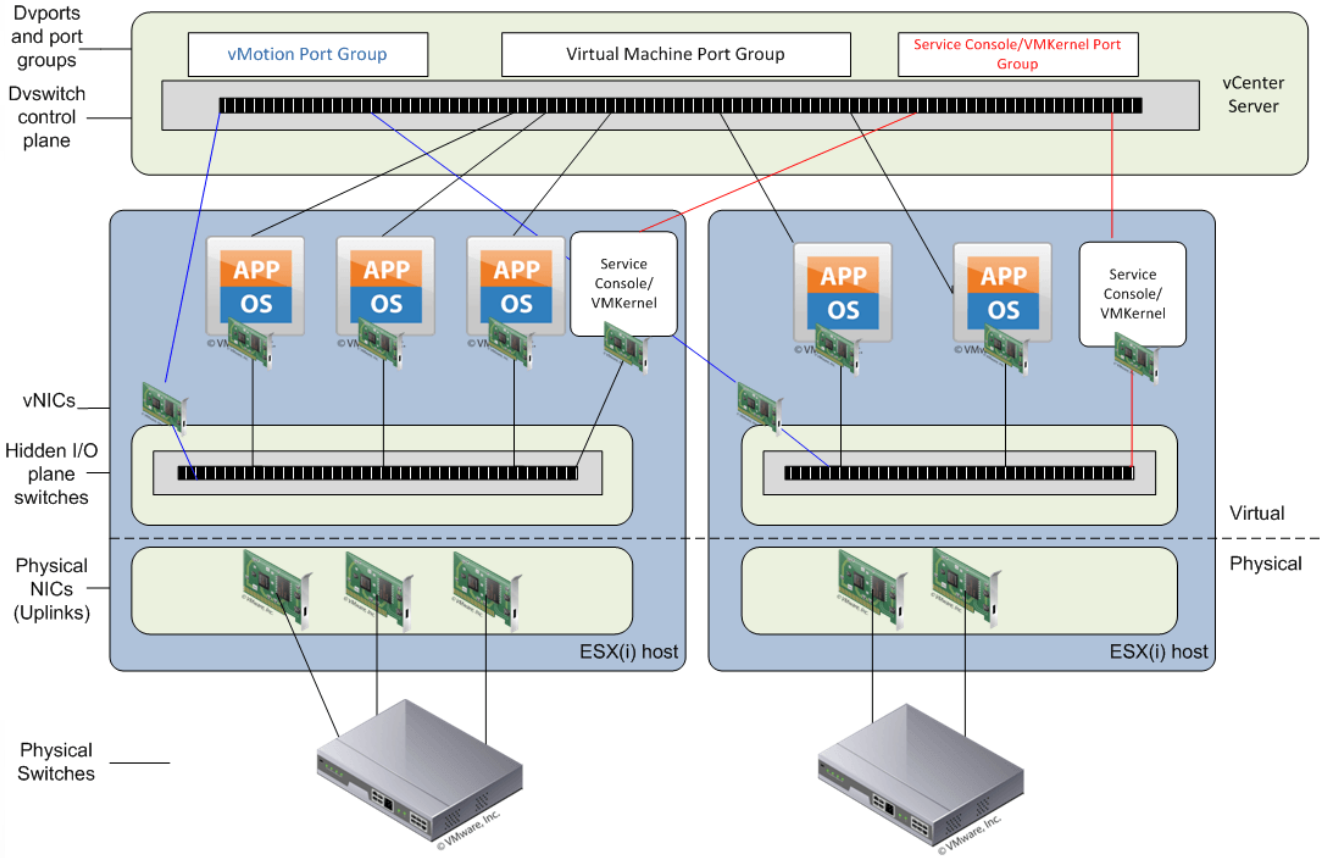




La virtualisation : Ecosystème vSphere

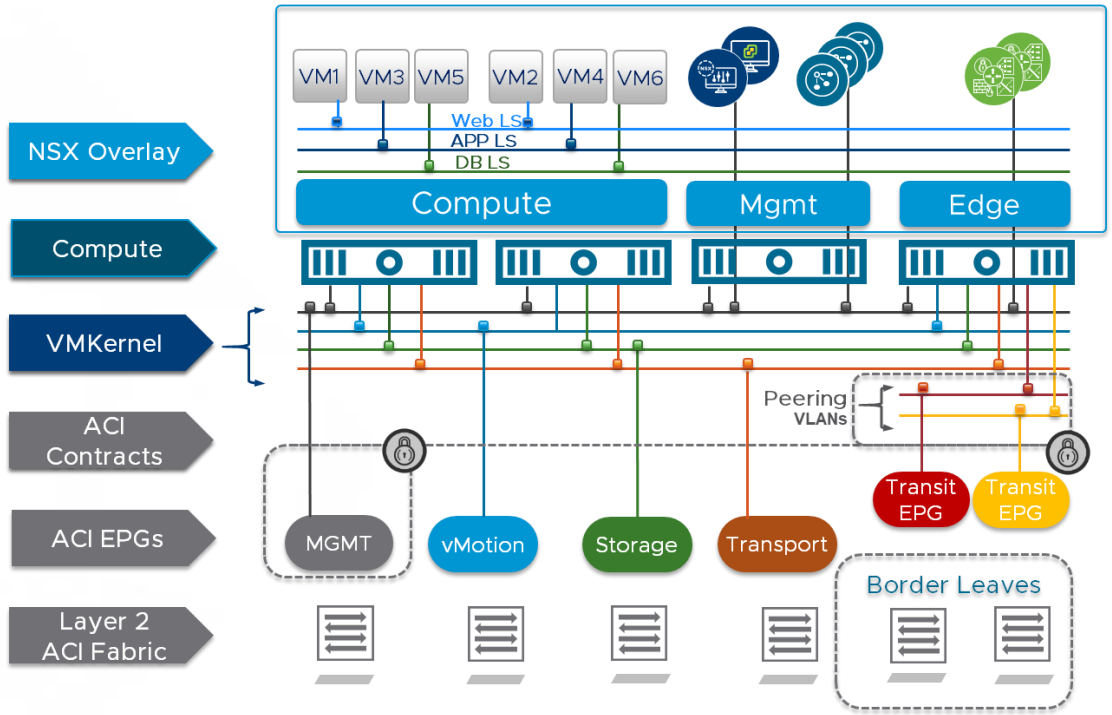
- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **Switchs distribués (vSphere Distributed Switchs)**
    - Port Groups
    - vNics
    - Physical nics
    - pNics / vmnics / uplinks





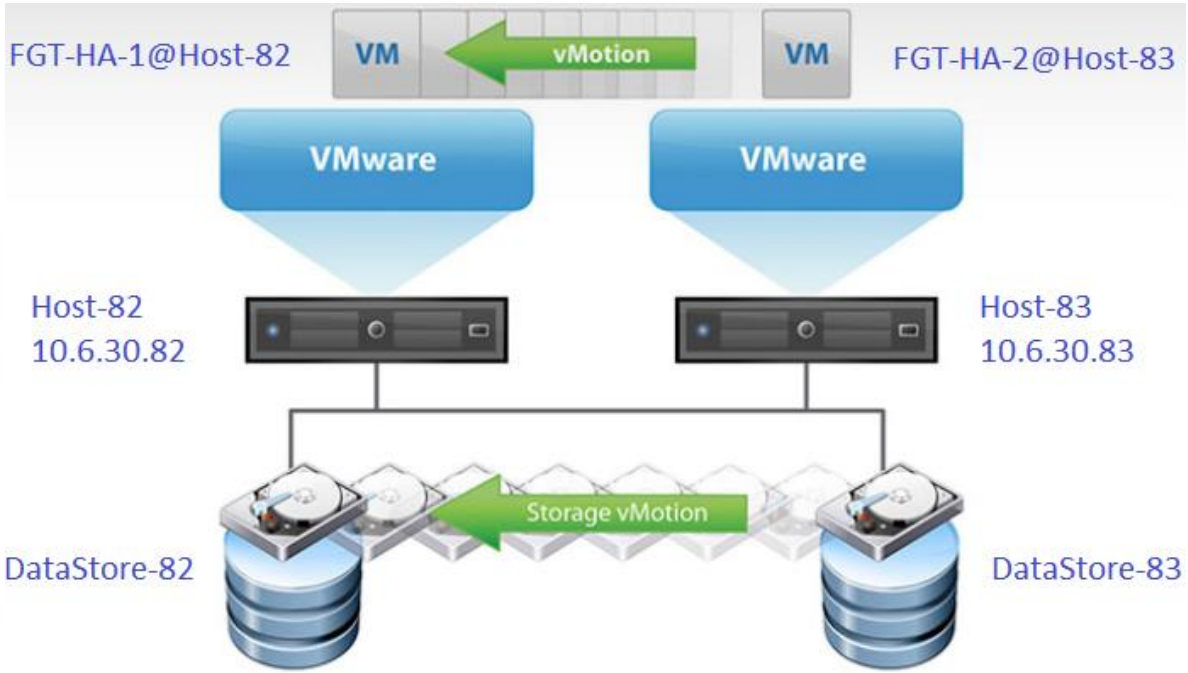
La virtualisation : Ecosystème vSphere

- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **Switchs distribués (vSphere Distributed Switchs)**
    - Différents « Port Groups » pour couvrir les besoins
      - Management de l'infrastrucutre
      - vMotion
      - Storage (via IP)
      - Production. Traffic des machines virtuelles
      - …



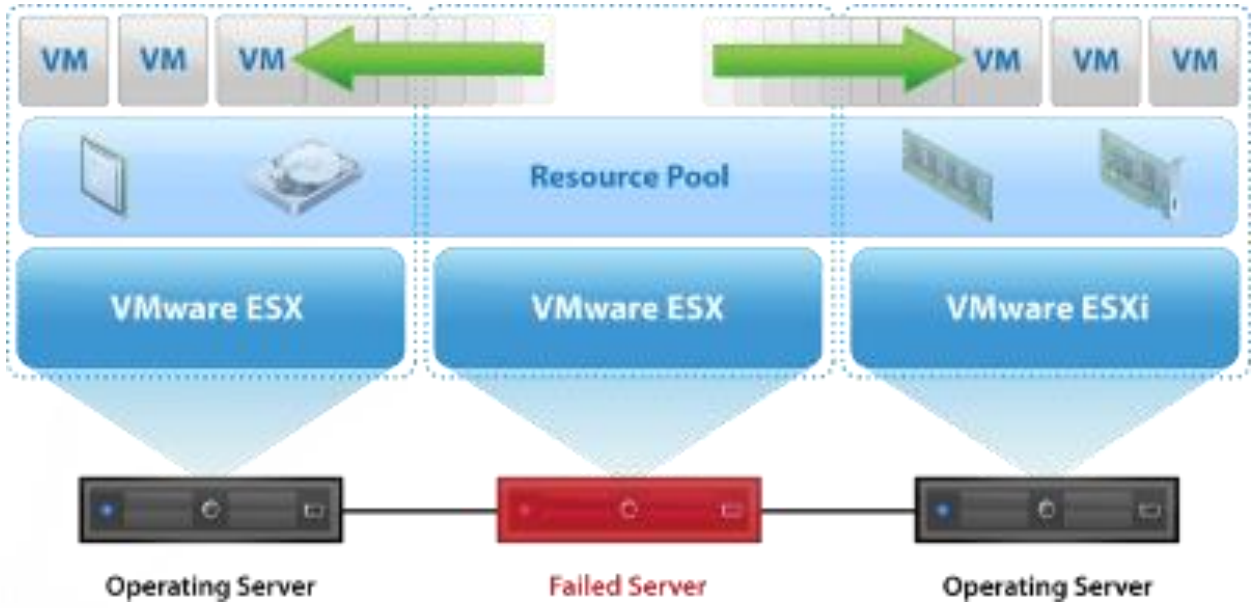
La virtualisation : Ecosystème vSphere

- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **Le déplacement des VM (vMotion)**
    - Une machine virtuelle peut être déplacée d'un serveur physique à un autre sans arrêt de la VM
    - Les fichiers constituant une machine virtuelle peuvent être déplacés d'un espace de stockage à un autre sans arrêt de la VM
  - Possible grâce
    - Au stockage partagé
      - VMFS permet de présenter un LUN à plusieurs serveurs physiques
    - Grâce à la virtualisation du réseau
      - Avec des « vSphere Standard Switch »
      - Ou avec des « vSphere Distributed Switch »



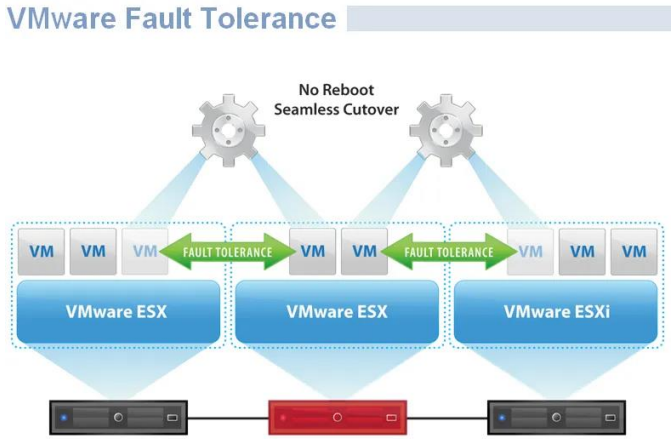
La virtualisation : Ecosystème vSphere

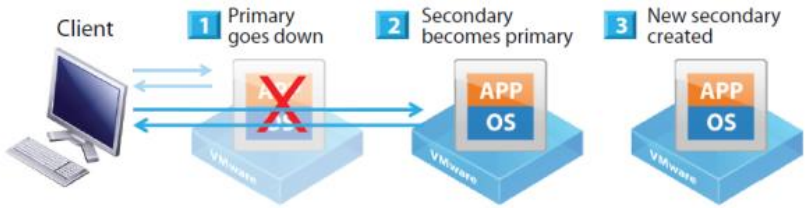
- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **La haute disponibilité (HA)**
    - En cas de panne HW les VM impactées redémarrent automatiquement sur des autres serveurs
  - **Possible grâce**
    - Au stockage partagé

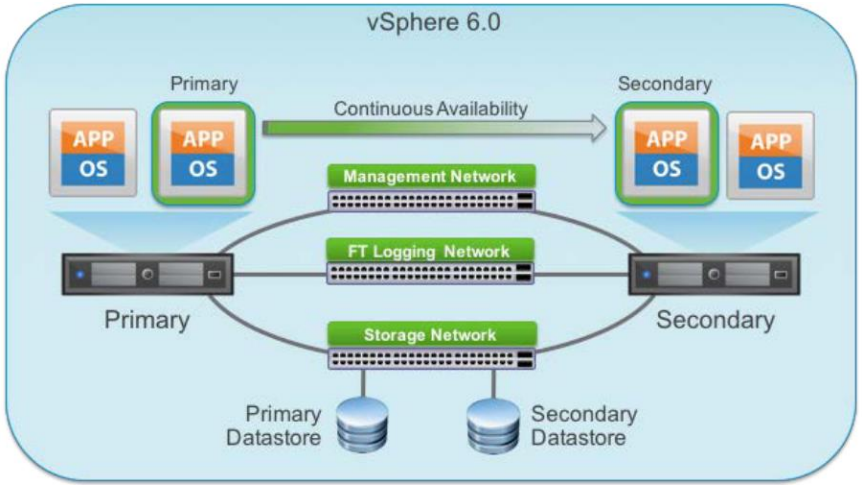


La virtualisation : Ecosystème vSphere

- **Ecosystème Vmware vSphere – la route de la haute disponibilité et du cloud**
  - **La tolérance de panne (FT – Fault Tolerance)**
    - Limitations au niveau compatibilité des OS
    - Attention à bande passante nécessaire
  - **Chaque instance a**
    - Ses propres vmx synchronisés
    - Ses propres vmdk synchronisés
  - **Possible grâce à**
    - Stockage partagé
    - Synchronisation
      - CPU
      - RAM
      - Réseau

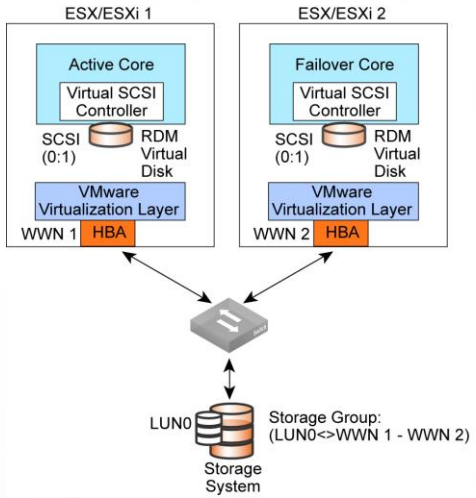


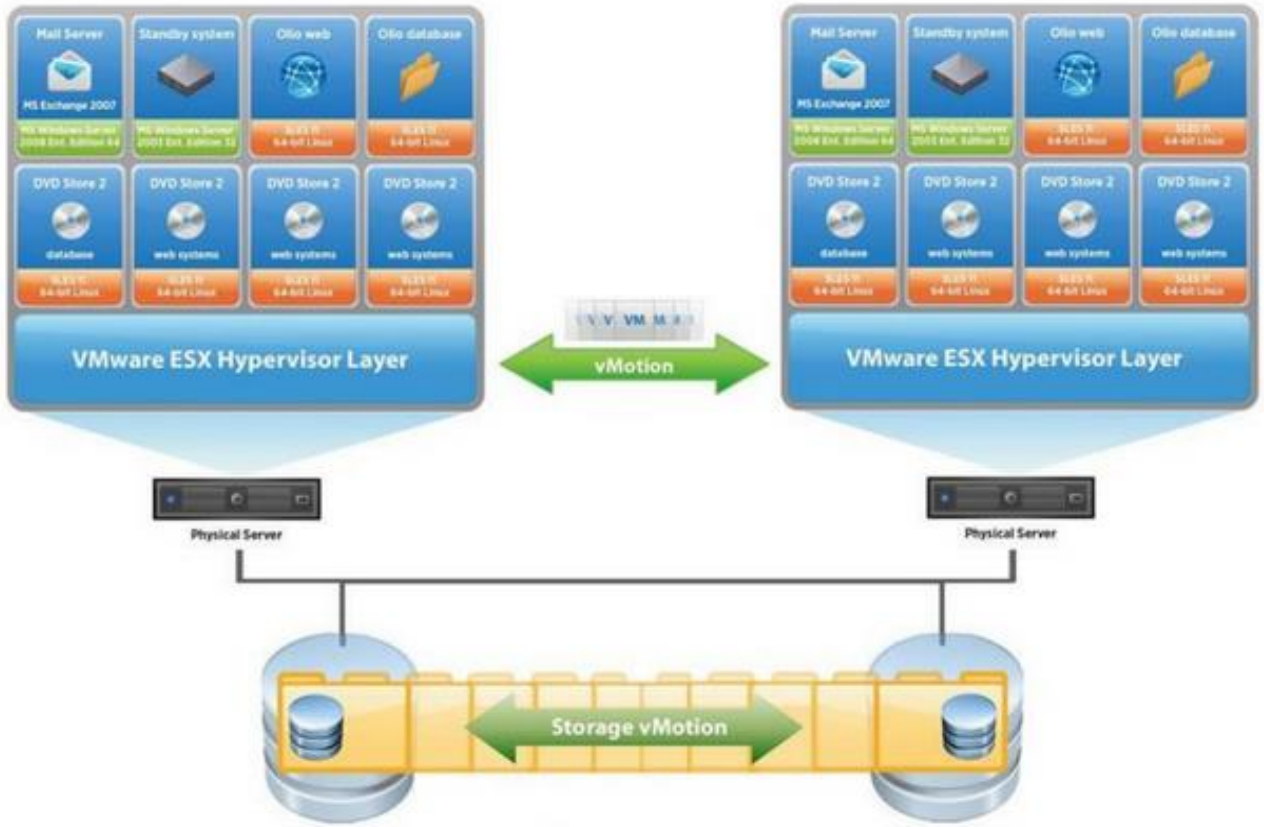




La virtualisation : Ecosystème vSphere

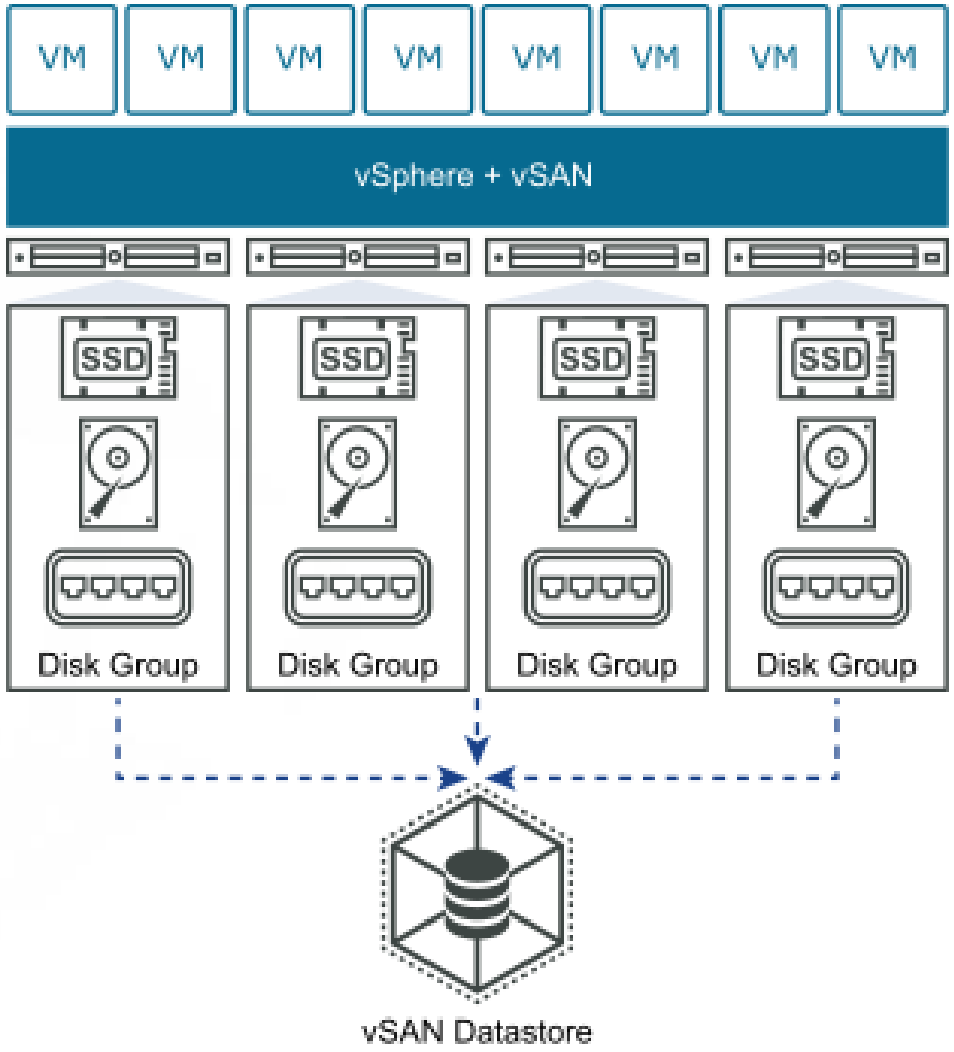
- **Le stockage partagé**
  - **VMFS**
    - Permet l'écriture simultanée sur le FS par différentes machines
    - Pas les fichiers
      - Fichiers « lock »





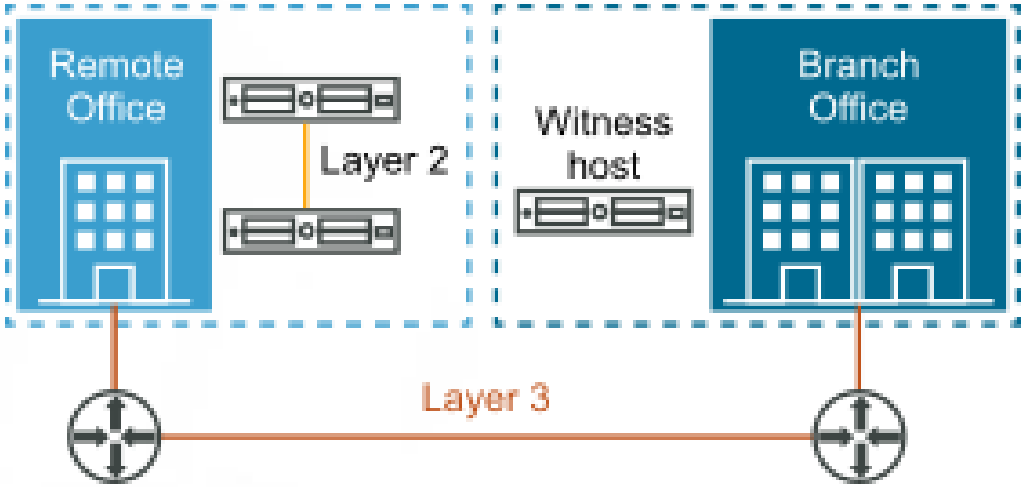
La virtualisation : Ecosystème vSphere

- **Le stockage virtualisé**
  - **vSAN Cluster**
    - Minimum 3 hosts
    - Same location
    - 10Gb network



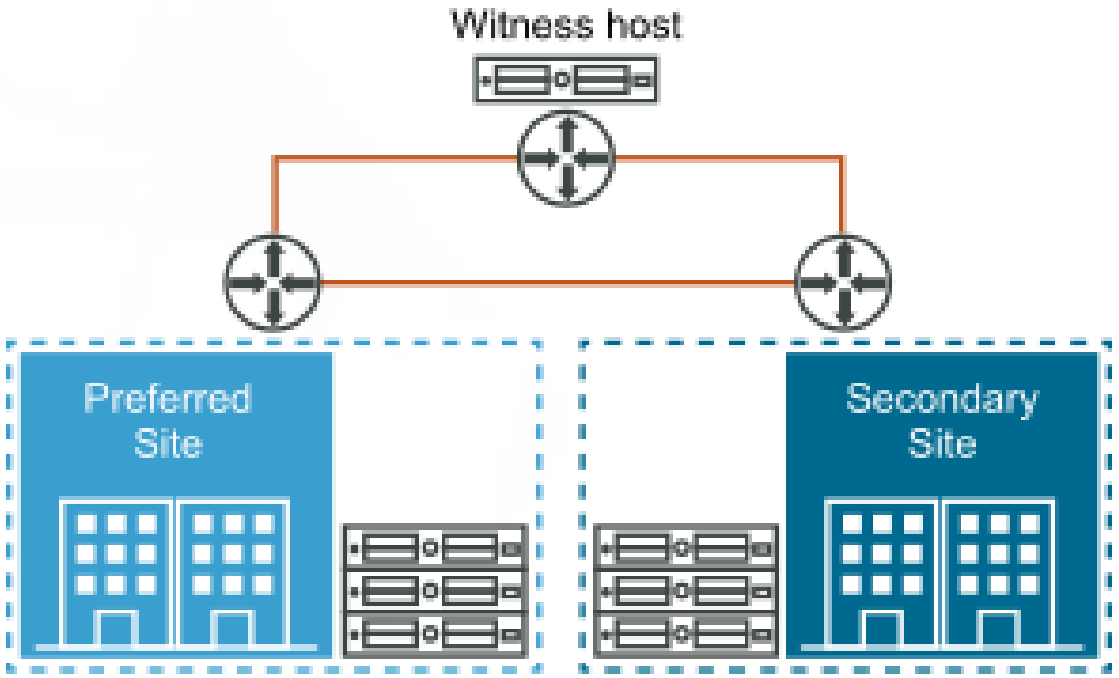
La virtualisation : Ecosystème vSphere

- **Le stockage virtualisé**
  - **Two host vSAN Cluster**
    - Same location



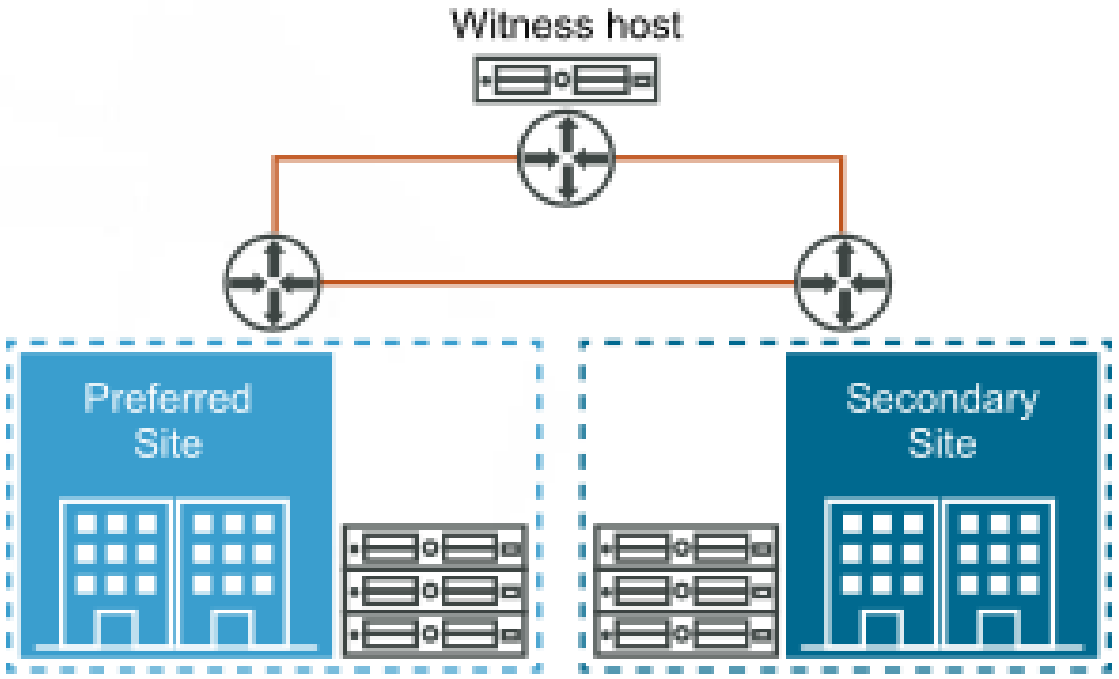
La virtualisation : Ecosystème vSphere

- **Le stockage virtualisé**
  - **vSAN Stretched Cluster**
    - Résilience à la perte d'un site entier
    - 2 sites différents
      - Latence réseau <= 5ms



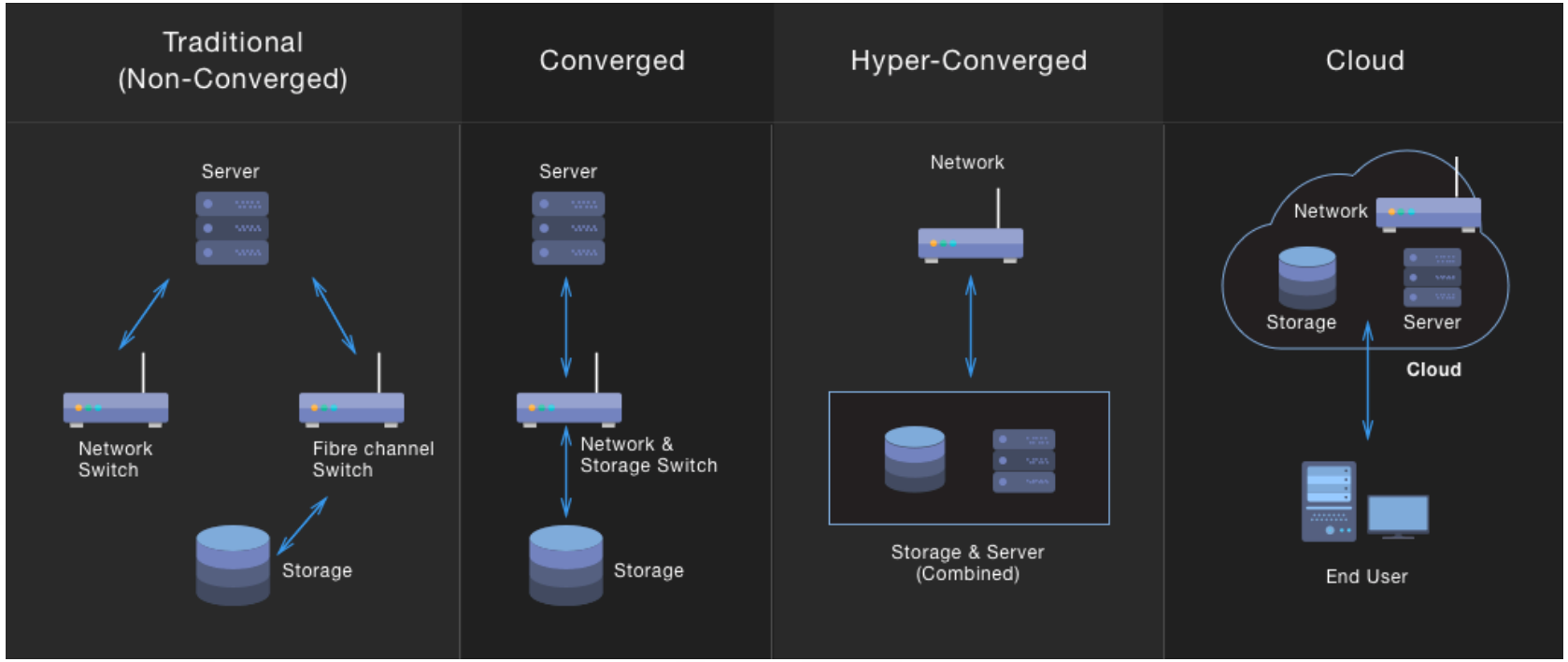
La virtualisation : Ecosystème vSphere

- **Le stockage virtualisé**
  - **Witness host**
    - Sur 3e site
    - Seulement des métadata
    - can use low bandwidth/high latency links
    - cannot run VMs
    - A single witness host can support only one vSAN stretched cluster
    - must have one VMkernel adapter with vSAN traffic enabled



La virtualisation : Infrastructures

- **L'évolution des schémas d'infrastructure**



3 Le (public) cloud computing

Différents types de cloud et modèles

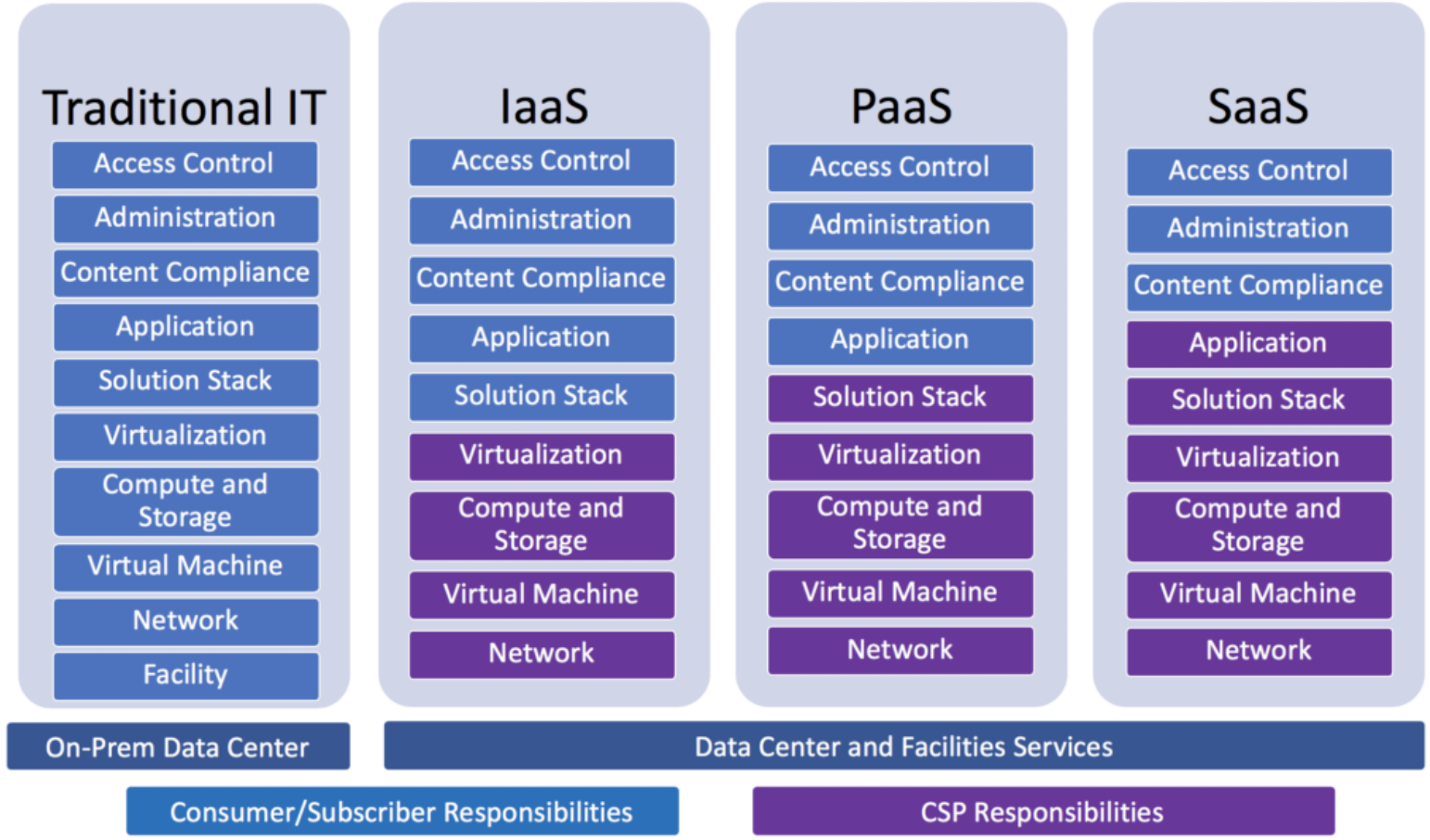
- Cloud types
  - Public
  - Private
    - Community
  - Hybryd
- Cloud delivery model
  - IaaS
  - PaaS
  - SaaS

CAUTION: Cloud type is considered from “cloud consumer and cloud owner perspective ! AWS is a public cloud because I’m not owning it. For AWS organization AWS is a private cloud

Definitions from Arcitura – Cloud Agnostic Vendor

Reminder : Cloud responsibility model

- Reality of cloud
  - You have to trust your provider for the part you do not manage
    - For everything !
    - Including security !

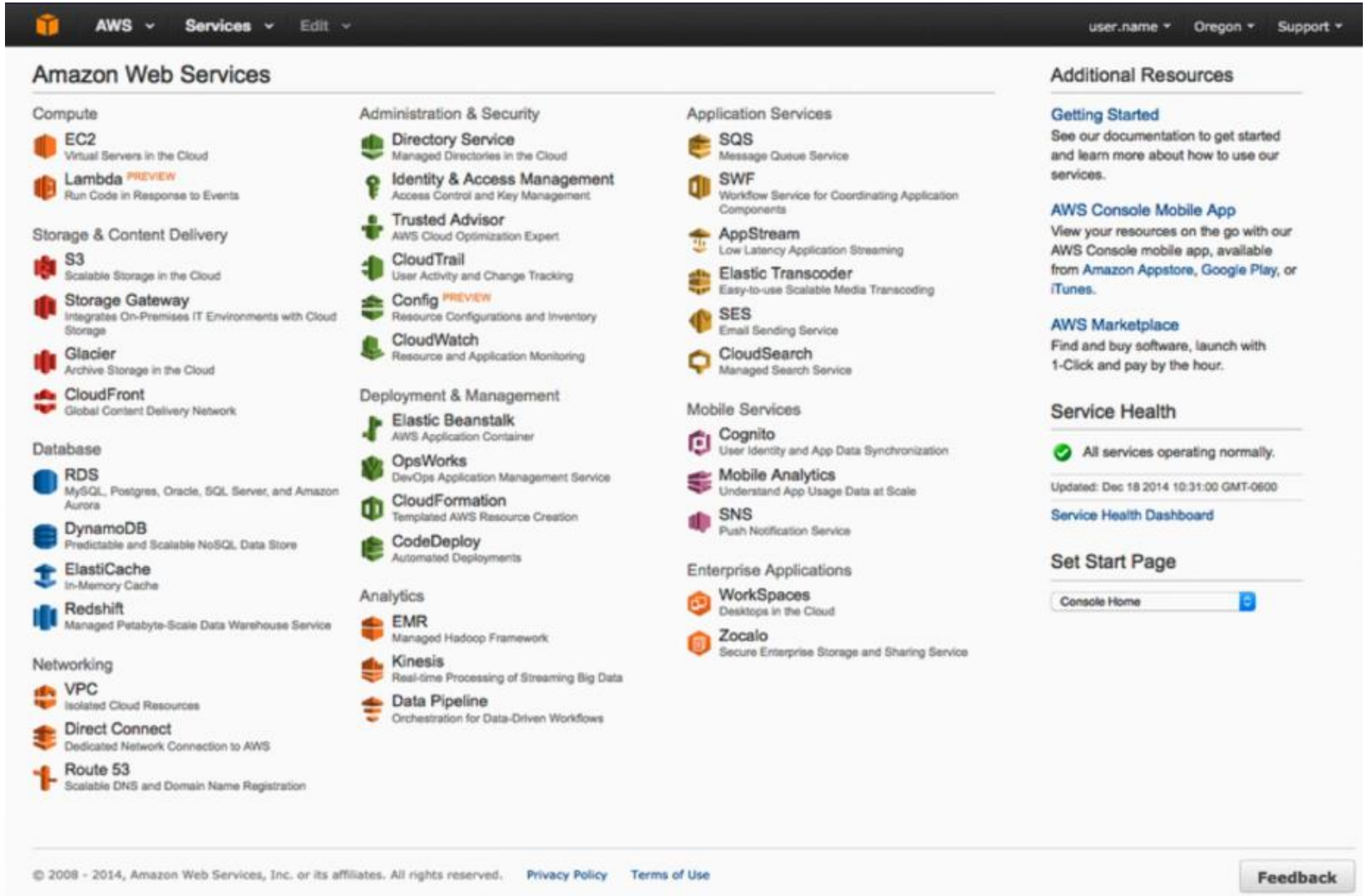


Le cloud (grand) public

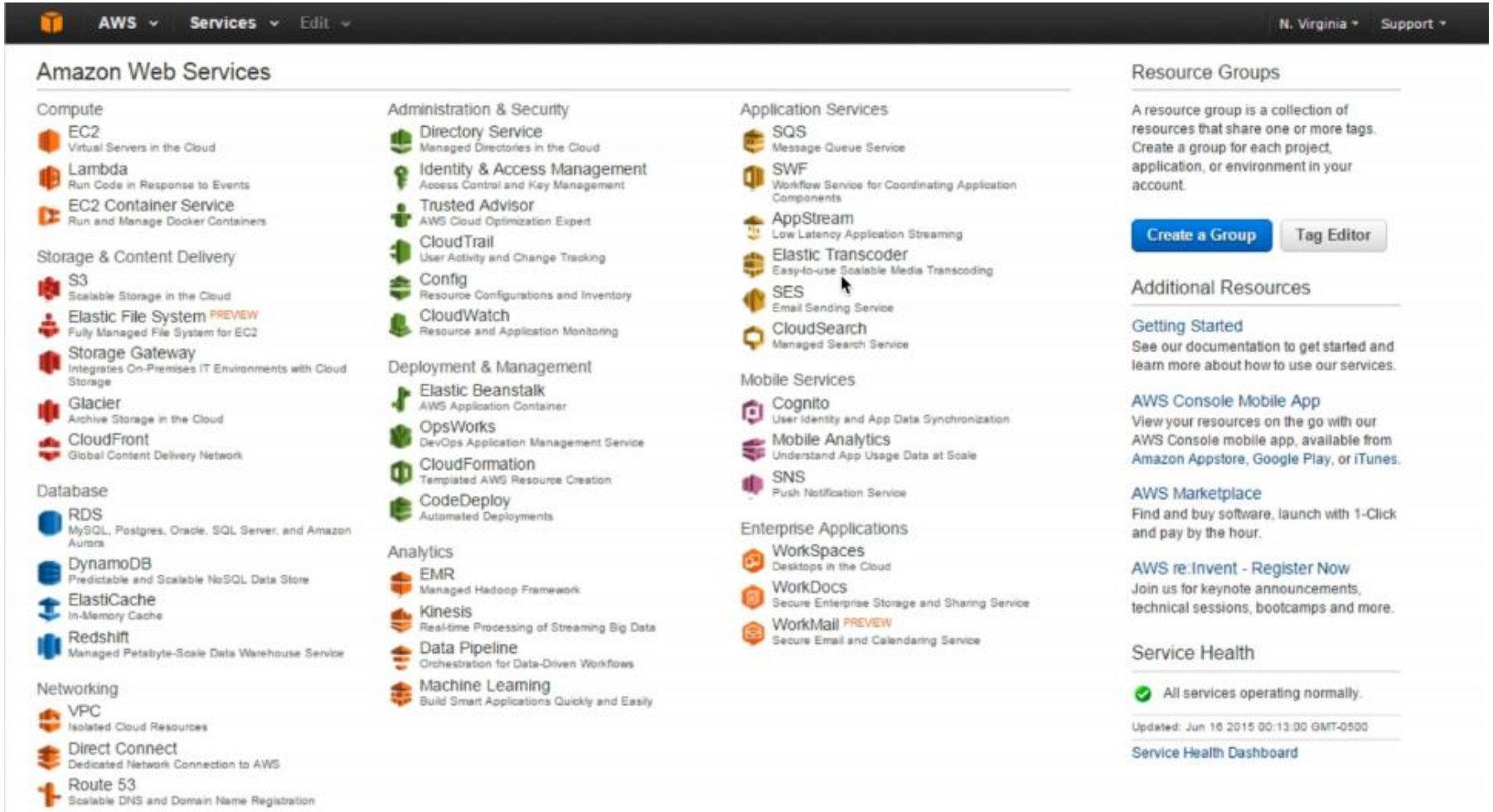
- Conditions minimales pour Cloud public
  - Virtualisation
  - Orchestration
    - Provisionning des ressources
      - Compute
      - Storage
      - Network
    - Billing

Google Cloud

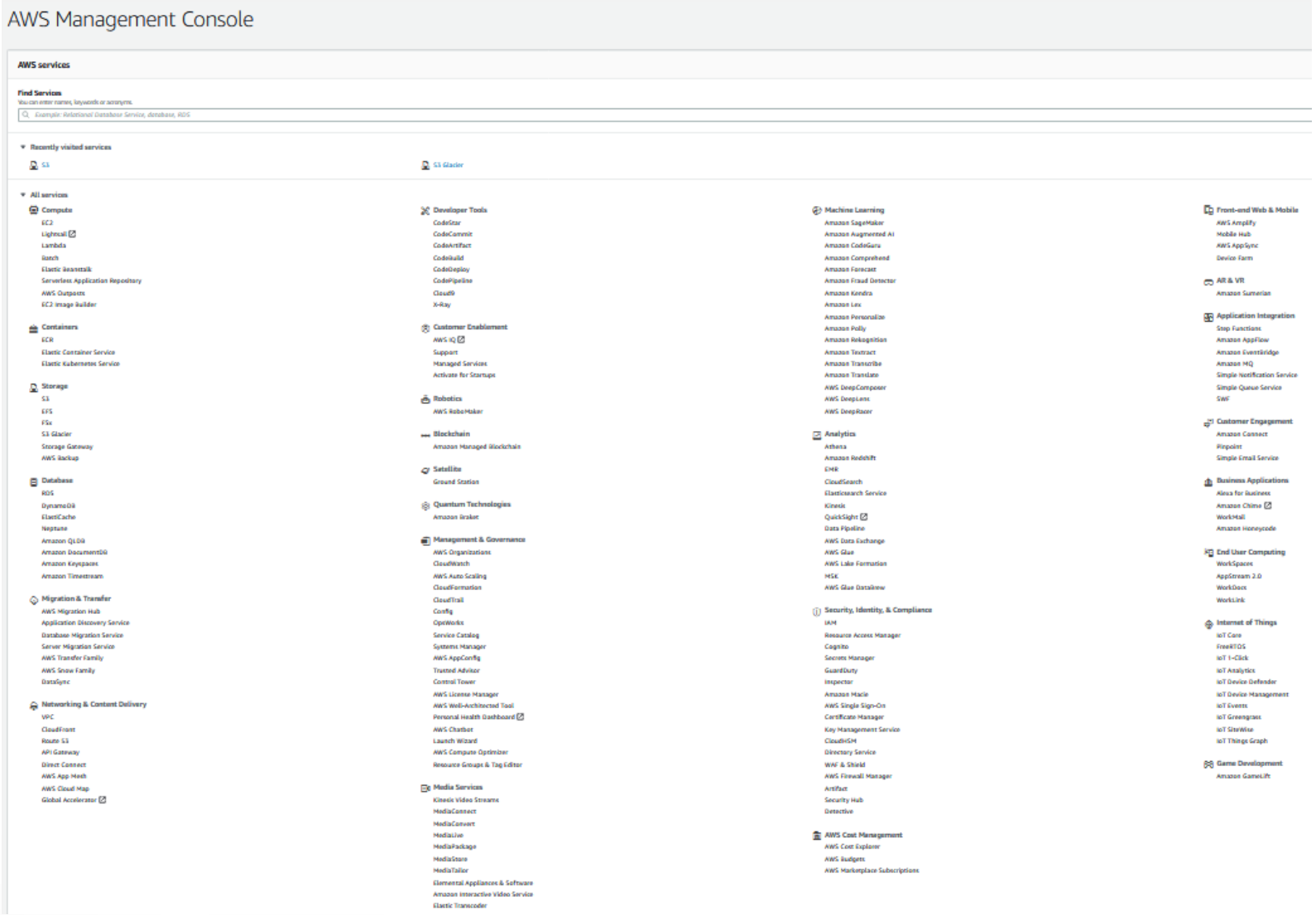
AWS 2015


AWS
Services
Edit
user.name
Oregon
Support
Amazon Web Services
Compute
EC2
Virtual Servers in the Cloud
Lambda PREVIEW
Run Code in Response to Events
Storage & Content Delivery
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage
Glacier
Archive Storage in the Cloud
CloudFront
Global Content Delivery Network
Database
RDS
MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
Redshift
Managed Petabyte-Scale Data Warehouse Service
Networking
VPC
Isolated Cloud Resources
Direct Connect
Dedicated Network Connection to AWS
Route 53
Scalable DNS and Domain Name Registration
Administration & Security
Directory Service
Managed Directories in the Cloud
Identity & Access Management
Access Control and Key Management
Trusted Advisor
AWS Cloud Optimization Expert
CloudTrail
User Activity and Change Tracking
Config PREVIEW
Resource Configurations and Inventory
CloudWatch
Resource and Application Monitoring
Deployment & Management
Elastic Beanstalk
AWS Application Container
OpsWorks
DevOps Application Management Service
CloudFormation
Templated AWS Resource Creation
CodeDeploy
Automated Deployments
Analytics
EMR
Managed Hadoop Framework
Kinesis
Real-time Processing of Streaming Big Data
Data Pipeline
Orchestration for Data-Driven Workflows
Application Services
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components
AppStream
Low Latency Application Streaming
Elastic Transcoder
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
CloudSearch
Managed Search Service
Mobile Services
Cognito
User Identity and App Data Synchronization
Mobile Analytics
Understand App Usage Data at Scale
SNS
Push Notification Service
Enterprise Applications
WorkSpaces
Desktops in the Cloud
Zocalo
Secure Enterprise Storage and Sharing Service
Additional Resources
Getting Started
See our documentation to get started and learn more about how to use our services.
AWS Console Mobile App
View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.
AWS Marketplace
Find and buy software, launch with 1-Click and pay by the hour.
Service Health
All services operating normally.
Updated: Dec 18 2014 10:31:00 GMT-0600
Service Health Dashboard
Set Start Page
Console Home
© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

AWS 2016


AWS
Services
Edit
N. Virginia
Support
Amazon Web Services
Compute
EC2
Virtual Servers in the Cloud
Lambda
Run Code in Response to Events
EC2 Container Service
Run and Manage Docker Containers
Storage & Content Delivery
S3
Scalable Storage in the Cloud
Elastic File System PREVIEW
Fully Managed File System for EC2
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage
Glacier
Archive Storage in the Cloud
CloudFront
Global Content Delivery Network
Database
RDS
MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
Redshift
Managed Petabyte-Scale Data Warehouse Service
Networking
VPC
Isolated Cloud Resources
Direct Connect
Dedicated Network Connection to AWS
Route 53
Scalable DNS and Domain Name Registration
Administration & Security
Directory Service
Managed Directories in the Cloud
Identity & Access Management
Access Control and Key Management
Trusted Advisor
AWS Cloud Optimization Expert
CloudTrail
User Activity and Change Tracking
Config
Resource Configurations and Inventory
CloudWatch
Resource and Application Monitoring
Deployment & Management
Elastic Beanstalk
AWS Application Container
OpsWorks
DevOps Application Management Service
CloudFormation
Templated AWS Resource Creation
CodeDeploy
Automated Deployments
Analytics
EMR
Managed Hadoop Framework
Kinesis
Real-time Processing of Streaming Big Data
Data Pipeline
Orchestration for Data-Driven Workflows
Machine Learning
Build Smart Applications Quickly and Easily
Application Services
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components
AppStream
Low Latency Application Streaming
Elastic Transcoder
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
CloudSearch
Managed Search Service
Mobile Services
Cognito
User Identity and App Data Synchronization
Mobile Analytics
Understand App Usage Data at Scale
SNS
Push Notification Service
Enterprise Applications
WorkSpaces
Desktops in the Cloud
WorkDocs
Secure Enterprise Storage and Sharing Service
WorkMail PREVIEW
Secure Email and Calendaring Service
Resource Groups
A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.
Create a Group
Tag Editor
Additional Resources
Getting Started
See our documentation to get started and learn more about how to use our services.
AWS Console Mobile App
View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.
AWS Marketplace
Find and buy software, launch with 1-Click and pay by the hour.
AWS re:Invent - Register Now
Join us for keynote announcements, technical sessions, bootcamps and more.
Service Health
All services operating normally.
Updated: Jun 16 2015 00:13:00 GMT-0500
Service Health Dashboard

AWS 2020


AWS Management Console
AWS services
Find Services
Recently visited services
S3
S3 Glacier
All services
Compute
EC2
Lightsail
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository
AWS Outposts
EC2 Image Builder
Containers
ECR
Elastic Container Service
Elastic Kubernetes Service
Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup
Database
RDS
DynamoDB
ElastiCache
Neptune
Amazon QLDB
Amazon DocumentDB
Amazon Keyspaces
Amazon Timestream
Migration & Transfer
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer Family
AWS Snow Family
DataSync
Networking & Content Delivery
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator
Developer Tools
CodeStar
CodeCommit
CodeArtifact
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray
Customer Enablement
AWS IQ
Support
Managed Services
Activate for Startups
Robotics
AWS RoboMaker
Blockchain
Amazon Managed Blockchain
Satellite
Ground Station
Quantum Technologies
Amazon Braket
Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
AWS AppConfig
Trusted Advisor
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard
AWS Chatbot
Launch Wizard
AWS Compute Optimizer
Resource Groups & Tag Editor
Media Services
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor
Elemental Appliances & Software
Amazon Interactive Video Service
Elastic Transcoder
Machine Learning
Amazon SageMaker
Amazon Augmented AI
Amazon CodeGuru
Amazon Comprehend
Amazon Forecast
Amazon Fraud Detector
Amazon Kendra
Amazon Lex
Amazon Personalize
Amazon Polly
Amazon Rekognition
Amazon Textract
Amazon Transcribe
Amazon Translate
AWS DeepComposer
AWS DeepLens
AWS DeepRacer
Analytics
Athena
Amazon Redshift
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Data Exchange
AWS Glue
AWS Lake Formation
MSK
AWS Glue DataBrew
Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
AWS Firewall Manager
Artifact
Security Hub
Detective
AWS Cost Management
AWS Cost Explorer
AWS Budgets
AWS Marketplace Subscriptions
Front-end Web & Mobile
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm
AR & VR
Amazon Sumerian
Application Integration
Step Functions
Amazon AppFlow
Amazon EventBridge
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF
Customer Engagement
Amazon Connect
Pinpoint
Simple Email Service
Business Applications
Alexa for Business
Amazon Chime
WorkMail
Amazon Honeycode
End User Computing
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink
Internet of Things
IoT Core
FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph
Game Development
Amazon GameLift

AWS Global infrastructure

- 24 régions (2020)
  - 5 nouvelles annoncées
- 77 Availability Zones (2020)
- 245 pays et territoires

AWS Global infrastructure

- Availability Zone (AZ) = Datacenter

AWS Global infrastructure

- Availability Zone (AZ) = Datacenter

AWS Global infrastructure

- **Région**
  - Constituée de 2 (ou plus) AZ relativement proches
  - AWS backbone network assure la communication entre les régions

AWS Global infrastructure

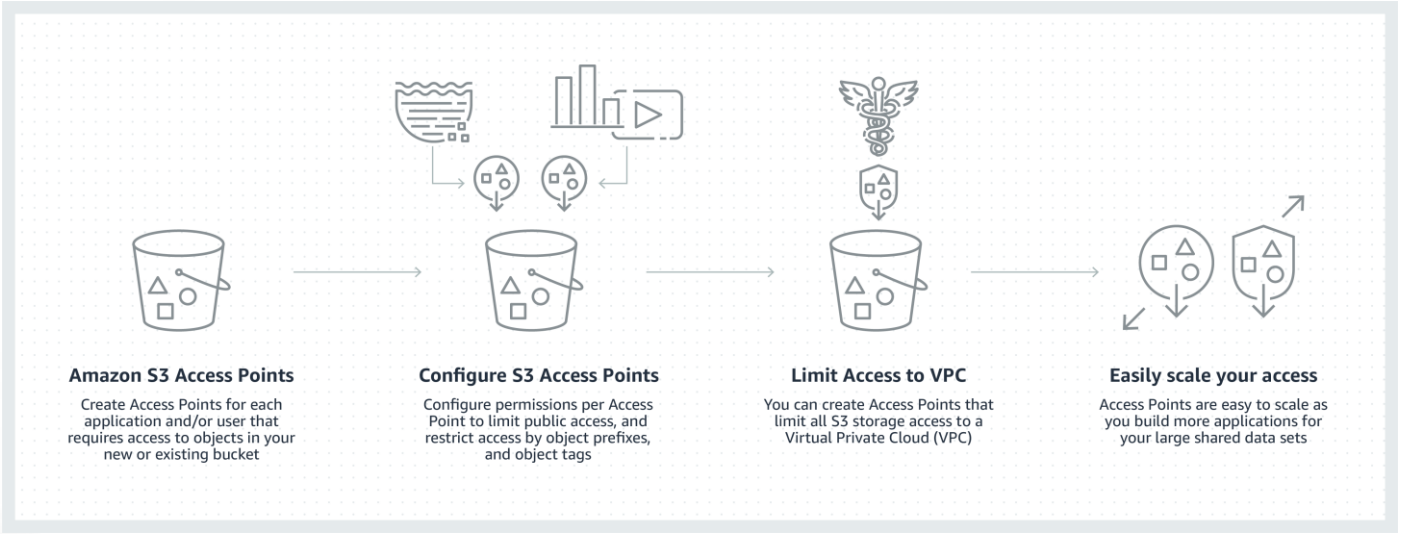
- **Edge Location**
  - EndPoints utilisés pour faire du caching (cloudfront – AWS CDN)
  - Sert à réduire la latence

AWS Composants

- **S3 : Simple Cloud Storage**
  - Espace de stockage – object base (fichiers)
  - On charge les fichiers
  - Entre 0 Byte jusque 5TB
  - Taille illimité
  - Les fichiers sont stockés dans des « buckets »
    - Comme répertoire/folder
  - Le nom d'un bucket doit être unique (mondial)
    - Les buckets sont accessibles via le net et l'url contient leur nom
  - Peut-être privé
  - Peut-être public (bientôt plus supporté)

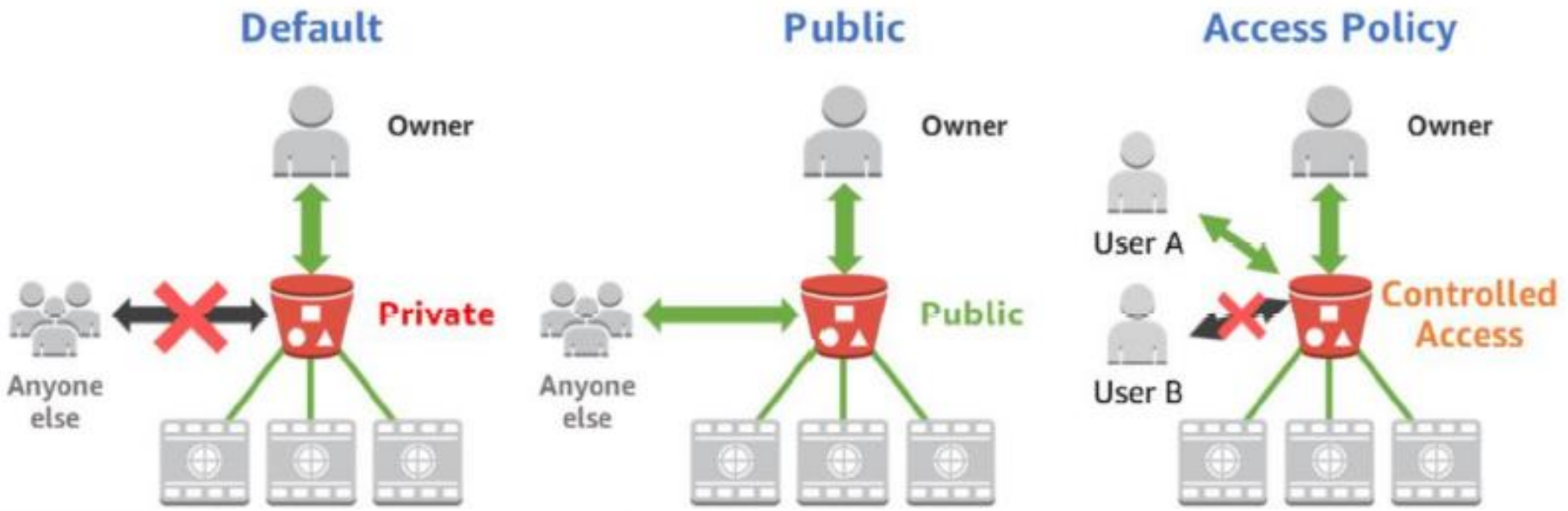
AWS Composants

- **S3 : Simple Cloud Storage**
  - Dans un bucket chaque objet a
    - Clef (nom de l'object)
    - Valeur (= contenu du fichier)
    - Version ID
    - Metadata (données concernant la nature de l'objet)



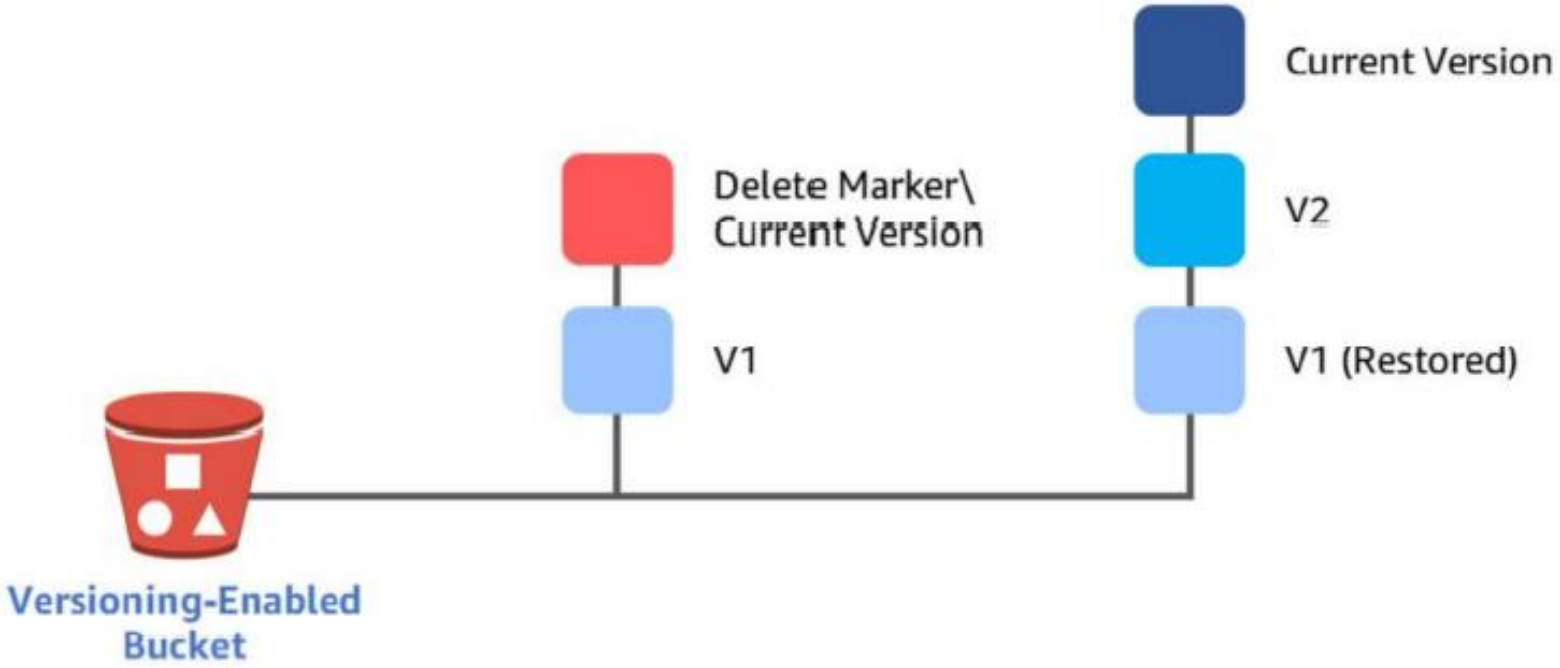
AWS Composants

- **S3 : Simple Cloud Storage**



AWS Composants

- **S3 : Simple Cloud Storage**



AWS Composants

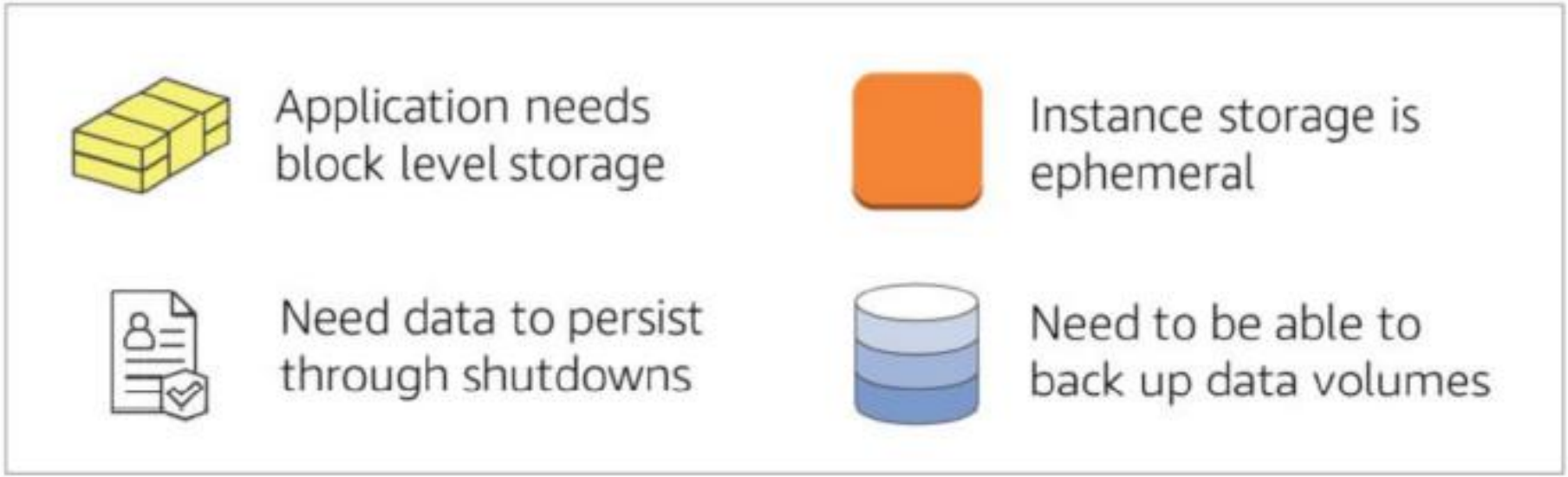
- **EC2 = Elastic Compute Cloud**
  - Web Service pour provisionner des ressources de compute (machine virtuelles appelées « instances »)
  - 4 types de pricing
    - On demand
      - Paye à l'heure ou à la seconde sans engagement
    - Reserved
      - On réserve une capacité pour un prix réduit
      - Engagement de 1 à 3 ans
    - Spot
      - On définit un prix qu'on veut payer et l'instance tourne lorsque possible
      - Idéal pour applications avec temps d'utisation flexible
    - Dedicated host
      - Serveur physique dédié
      - Parfois utile lorsque les licences sont liées au serveur

AWS Composants

- **EBS = Elastic Bloc Store**
  - = virtual hard disk (DAS)
  - Persistent block storage
  - Chaque EBS est automatiquement répliqué dans son AZ afin d'offrir redondance (comme pour du raid1)
  - Différents types
    - General purpose SSD
    - Provisioned IOPS (SSD)
    - Throughput Optimized Hard disk drive (magnetic)
    - Cold hard disk drive (magnetic)
    - Magnedit

AWS Composants

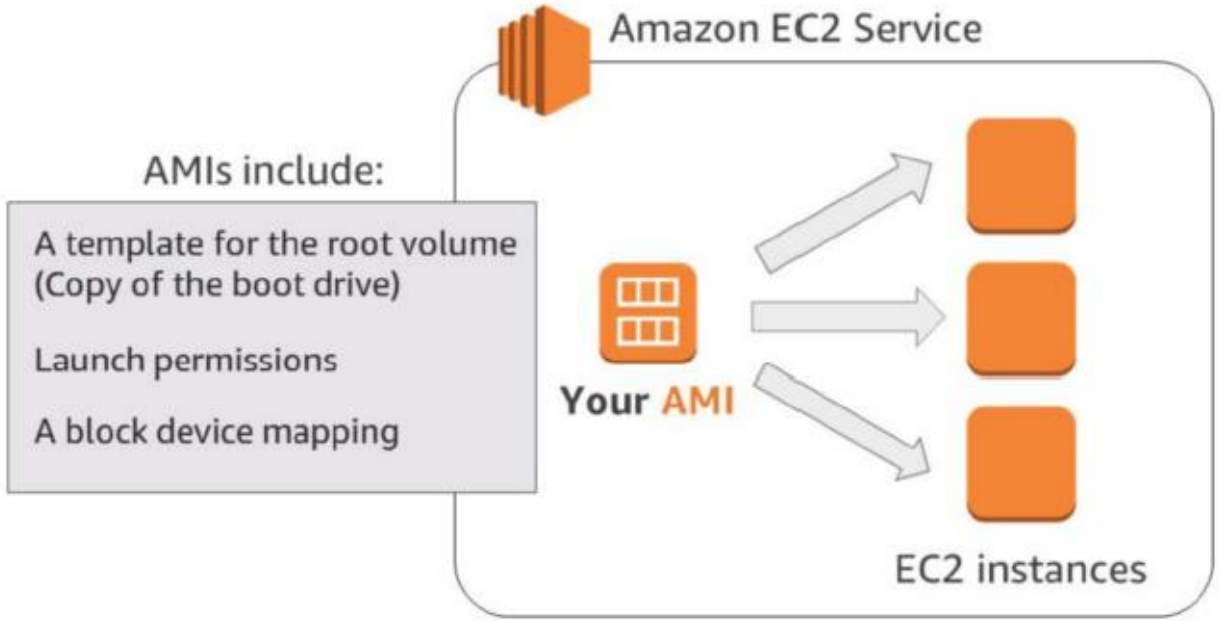
- **EBS = Elastic Bloc Store**



Keep in mind: Amazon EBS can only be linked to one instance at a time. It must be in the same Availability Zone as the volume.

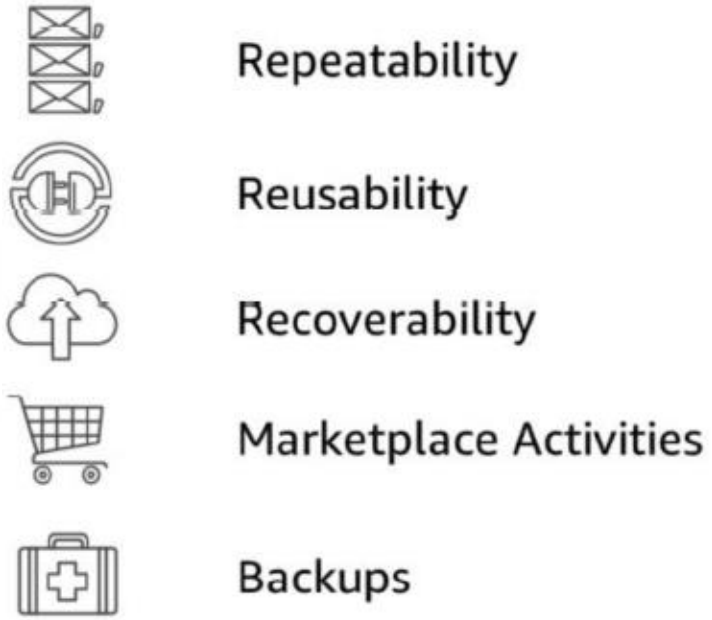
AWS Composants

- **AMI = Amazon Machine Image**
  - = image OS quipermet de lancer une instance



AWS Composants

- **AMI = Amazon Machine Image**



AWS Composants

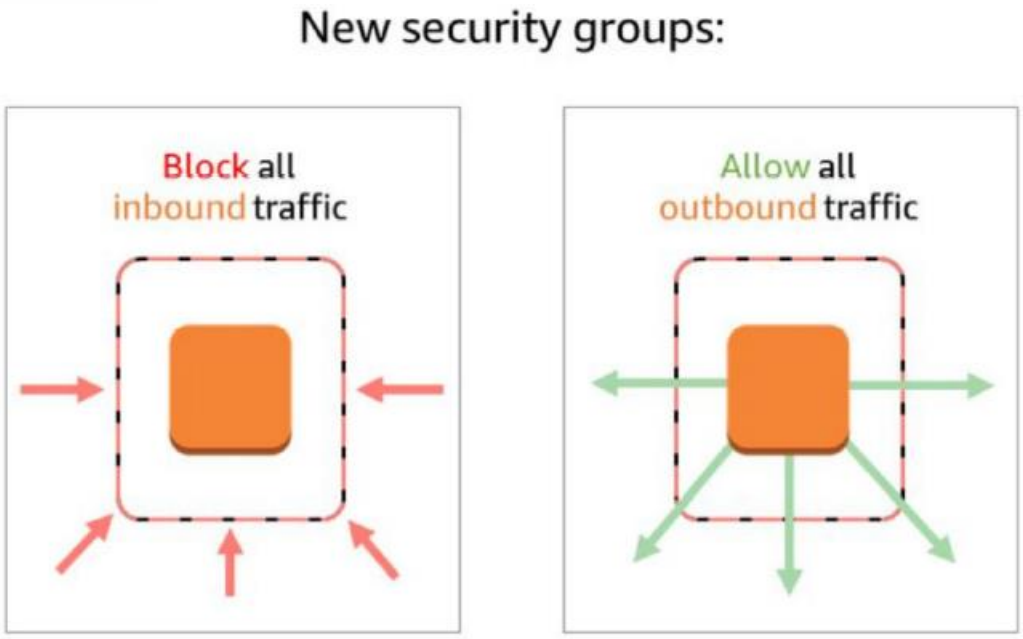
- **Elastic Network Interface**
  - = carte réseau
  - Particularités
    - Peut-être attachée à n'importe quelle instance EC2
    - Peut-être réassignée à une autre instance
      - Conserve
        - IP privée
        - IP pubique
        - MAC Address

AWS Composants

Solid-State Drives (SSD)			Hard disk Drives (HDD)		
Volume Type	**General Purpose SSD**	**Provisioned IOPS SSD**	**Throughput Optimized HDD**	**Cold HDD**	**EBS Magnetic**
Description	General purpose SSD volume that balances price and performance for a wide variety of transactional workloads	Highest-performance SSD volume designed for mission-critical applications	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads	Previous generation HDD
Use Cases	**Most Work Loads**	**Databases**	**Big Data & Data Warehouses**	**File Servers**	**Workloads where data is infrequently accessed**
API Name	gp2	io1	st1	sc1	Standard
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB	1 GiB-1 TiB
Max. IOPS**/ Volume	16,000	64,000	500	250	40-200

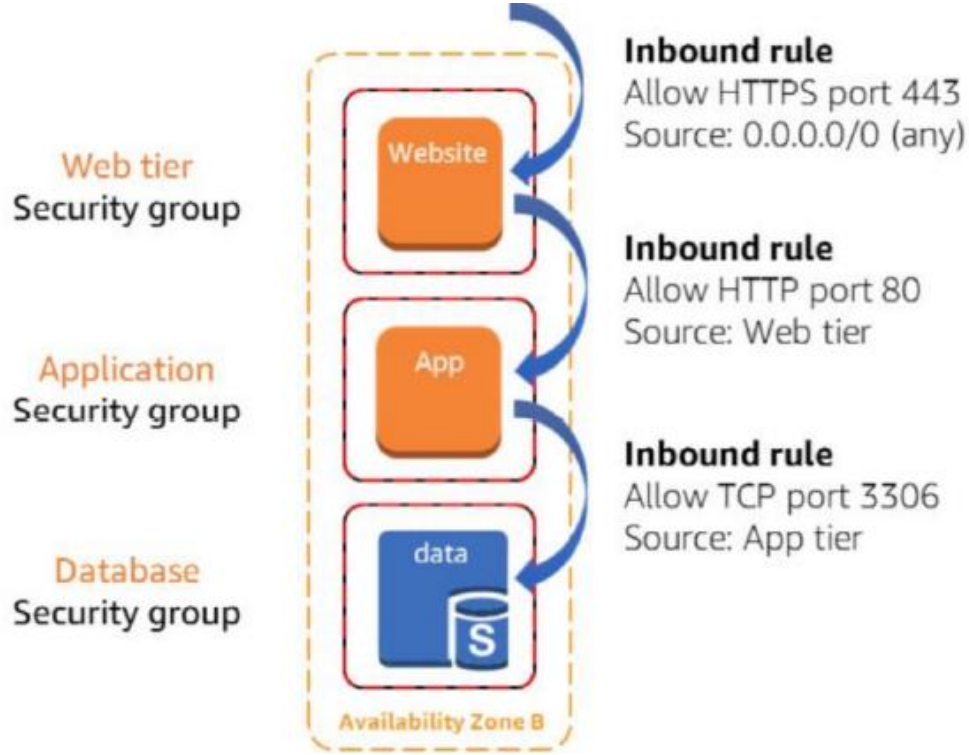
AWS Composants

- **Security groups**
  - = Firewall virtuel
  - Trafic entrant (inbound) bloqué par défaut
  - Trafic sortant (outbound) autorisé par défaut
  - Les changement prennent effet immédiatement
  - Pas de limite de nombre d'instances EC2 dans un security group
  - Plusieurs security groups peuvent être attachés à une seule instance EC2



AWS Composants

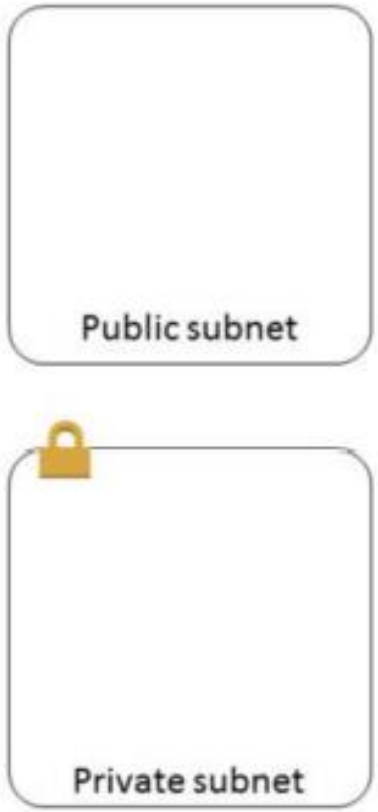
- **Security groups**
  - Stateful
    - Si on crée une règle inbound pour autoriser du trafic le trafic retour est automatiquement autorisé
  - Pas possible de bloquer des adresses IP spécifiques (pour ça on utilise Network Access Control List)
  - On peut définir des règles « allow » mais pas de règles « deny »
    - « deny all » par défaut
    - Possibilité de restreindre le trafic
      - Par protocole
      - Service port
      - Source IP (IP ou CIDR)
      - Security group
      - ➔ white list ; pas black list



AWS Composants

- **VPC (Virtual Private Cloud)**
  - = Datacenter virtuel
  - Permet de provisionner un réseau isolé logiqement
  - Permet un contrôle du réseau virtuel défini
    - Subnets
    - IPv4
    - IPv6
    - Permet de définir des CIDR
    - Règles strictes pour trafic inbound et oudbound
    - Contient des ressources de n'importe quelle AZ dans la même région

AWS Composants



Use subnets to define internet accessibility.

Public subnets

- Include a routing table entry to an internet gateway to support inbound/outbound access to the public internet

Private subnets

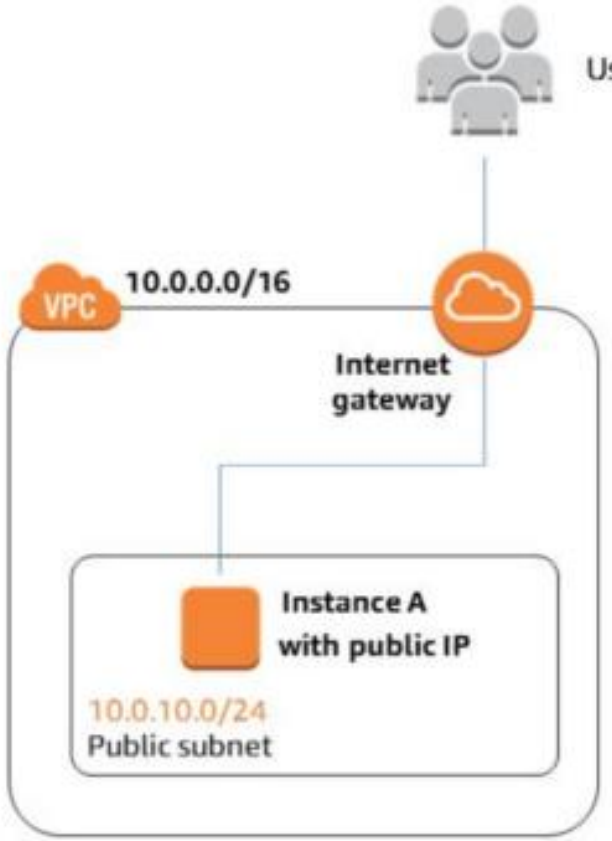
- Do not have a routing table entry to an internet gateway
- Are not directly accessible from the public internet
- Typically use a NAT gateway to support restricted, outbound public internet access

AWS Composants

- **AWS Internet Gateway**
  - Permet la communication entre les instances du VPC et internet
  - Scalable horizontalement, redondant et haute disponibilité
  - Fournit une target à la table de routage pour le trafic routable sur internet

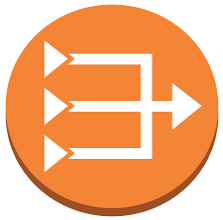
Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>



AWS Composants

- **AWS NAT Gateways**
  - Permet aux instances du VPC d'initier du trafic sortant ver internet ou d'autres services AWS
  - Permet aux instances de ne pas être directement exposées au trafic venant d'internet

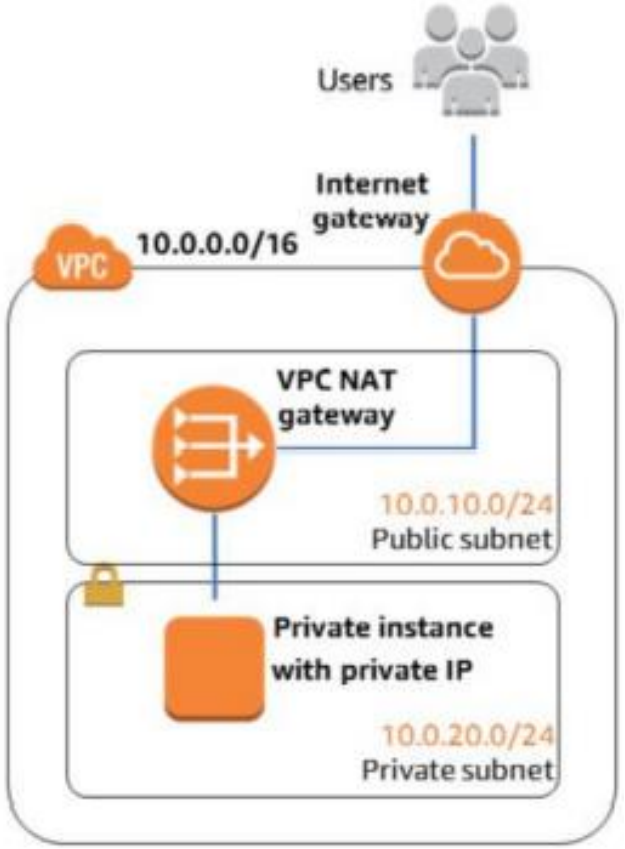


Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

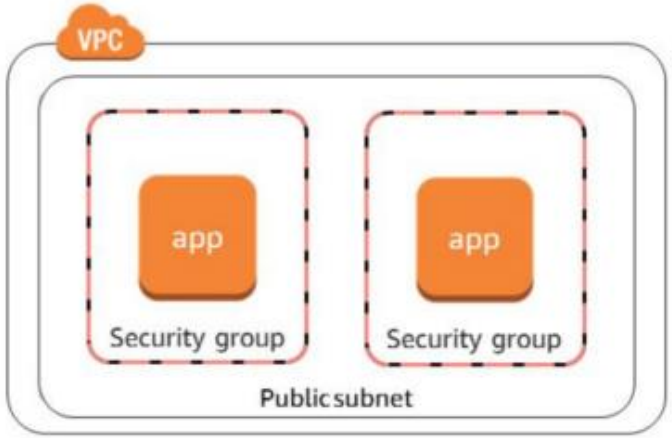
Private route table

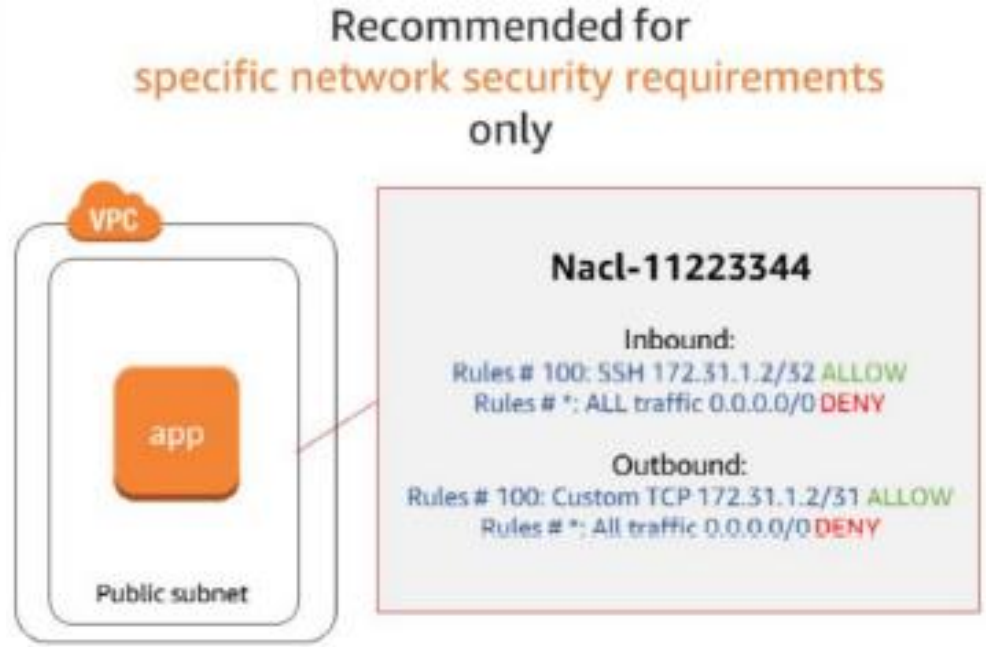
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



AWS Composants

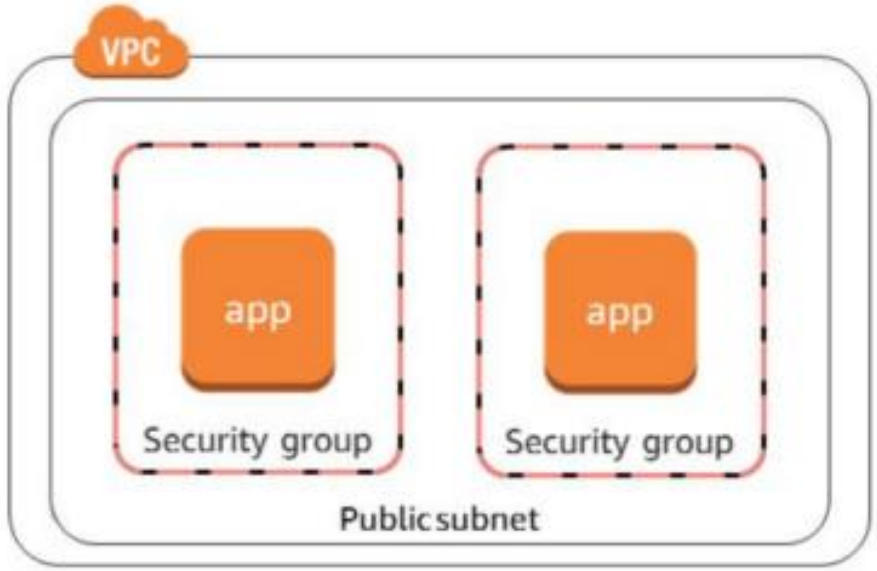
- **Network Acces Control Lists (ACLs)**
  - = Firewall à la frontière des subnets
  - Par défaut laisse passer le trafic entrant et sortant
  - Stateless
    - Nécessite règles explicites tant pour le trafic entrant que le trafic sortant





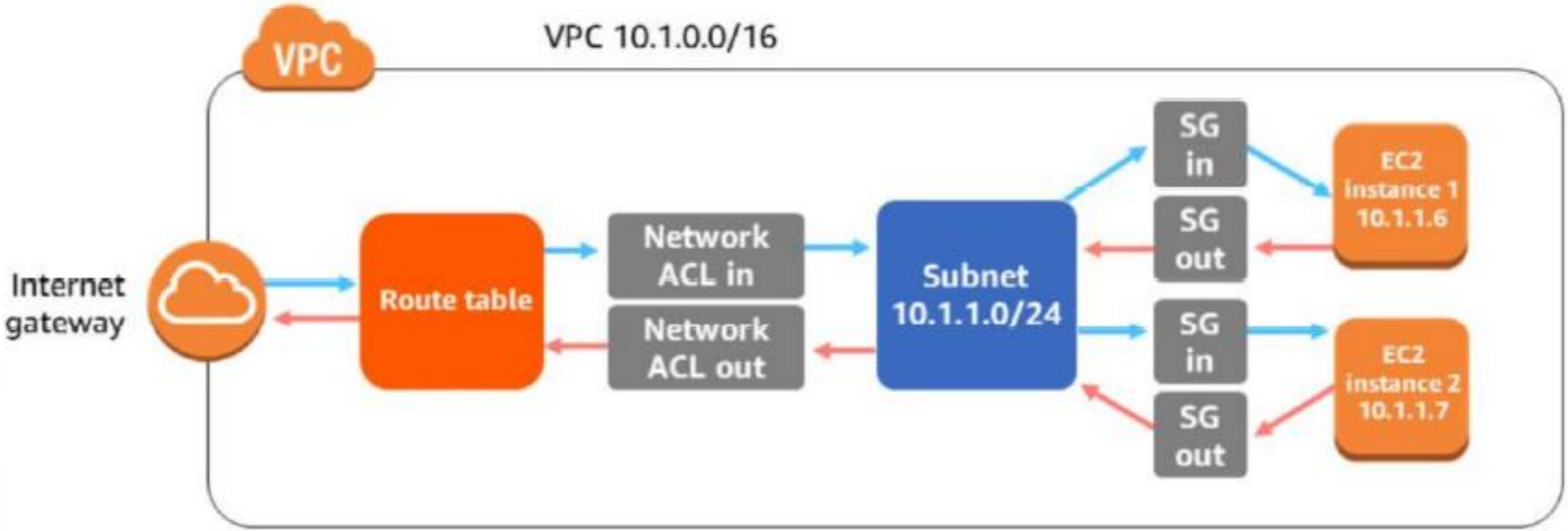
AWS Composants

- **Network Acces Control Lists (ACLs)**
  - = Firewall à la frontière des subnets
  - Par défaut laisse passer le trafic entrant et sortant
  - Stateless
    - Nécessite règles explicites tant pour le trafic entrant que le trafic sortant



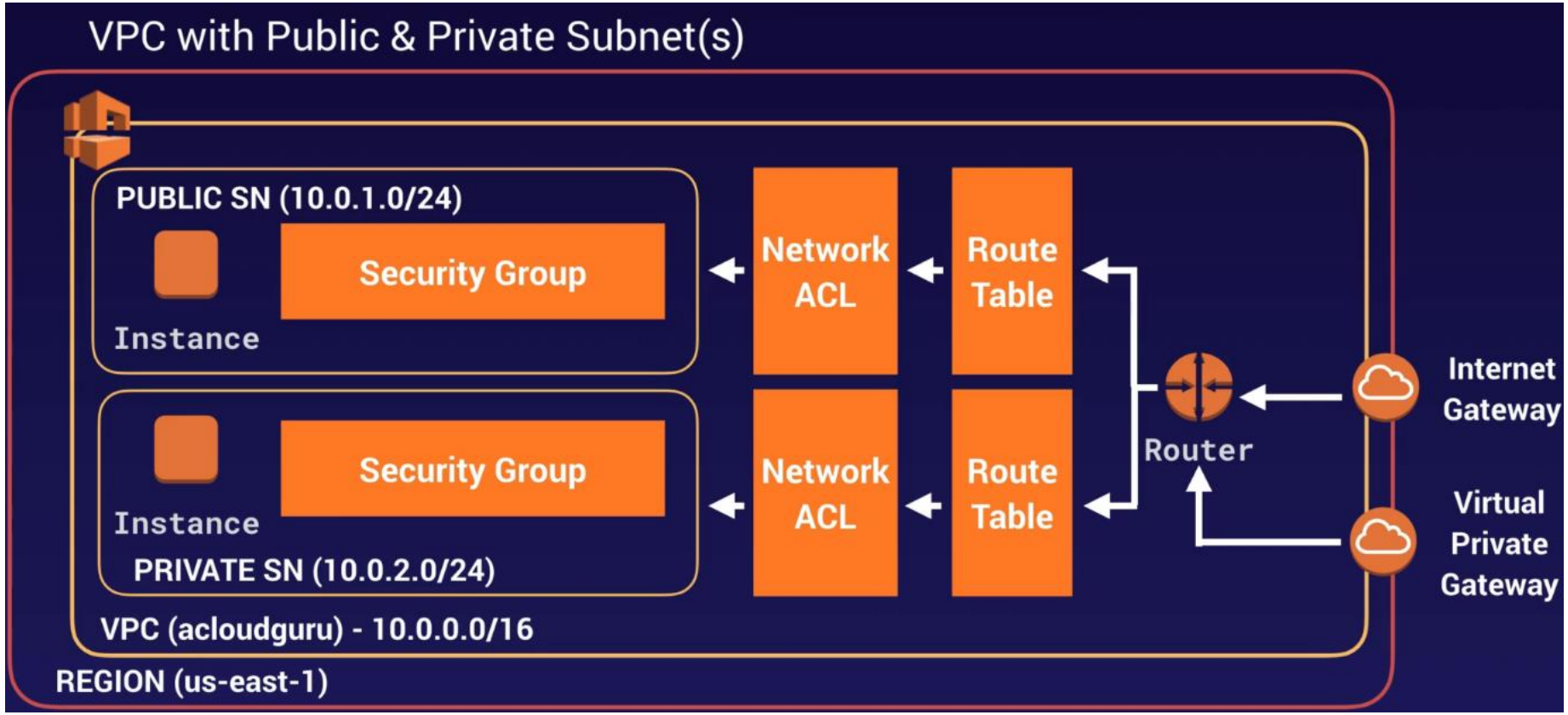
AWS Composants

- **VPC (Virtual Private Cloud) : Récapitulatif**



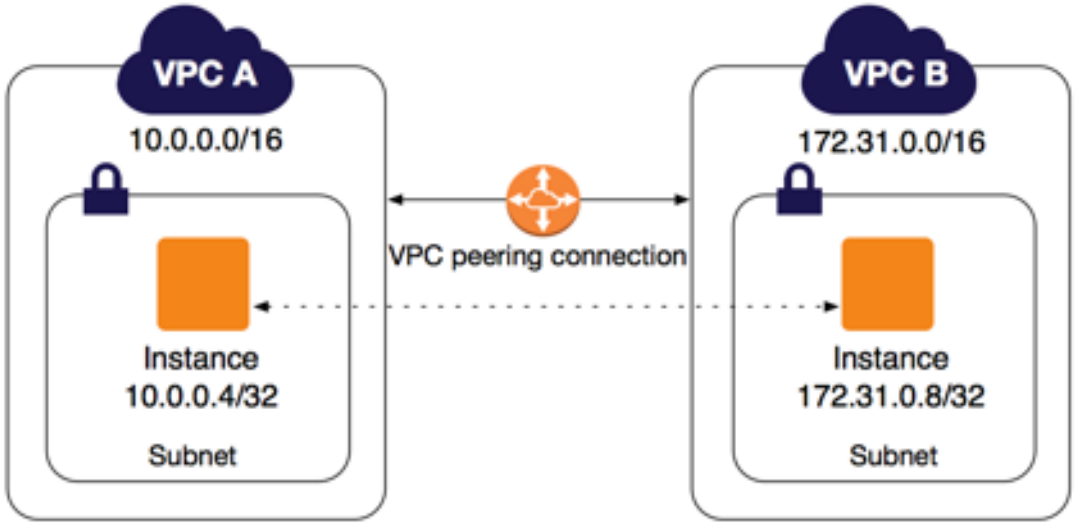
AWS Composants

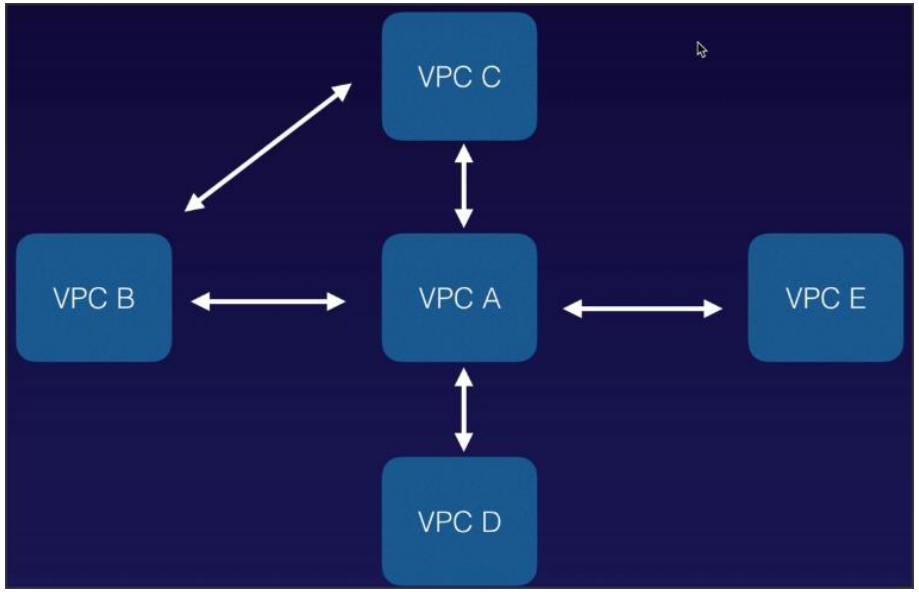
- VPC (Virtual Private Cloud)



AWS Composants

- **VPC Peering**
  - Non transitive





AWS Composants

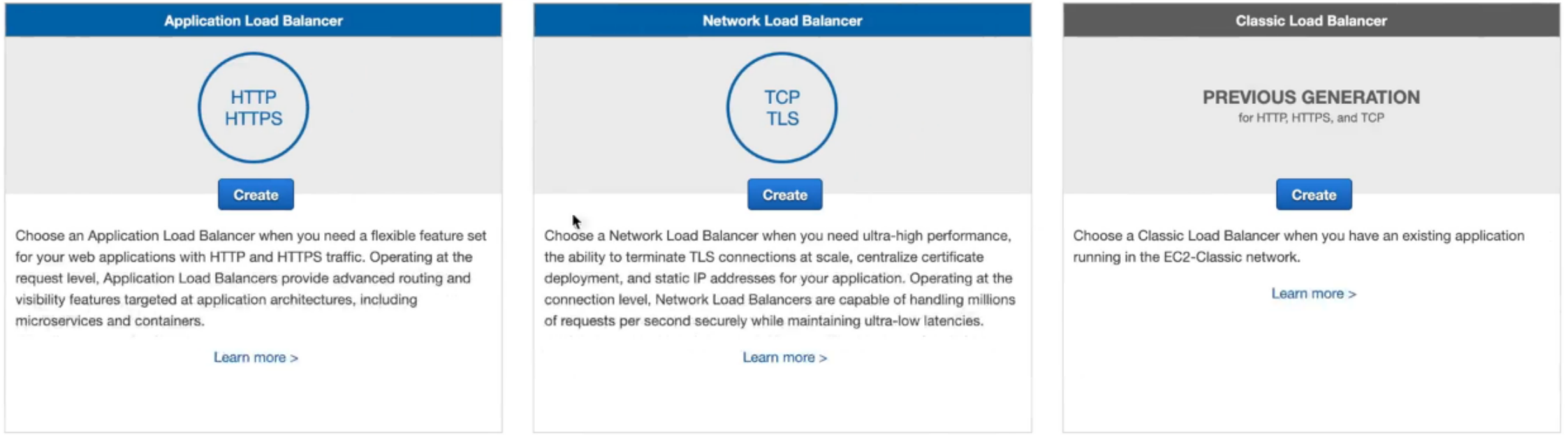
- **VPC (Virtual Private Cloud) : résumé**
  - = Datacenter logique dans AWS
  - Composé de IGWs (ou Virtual Private Gateways), Tables de routage (route tables), réseau, Network Access Control Lists, Subnets et Security groups
  - 1 Subnet = 1 availability Zone
    - Subnets do not span AZ, VPC's do
  - Security groups sont stateful
  - Network Access Control lists sont stateless
  - No transitive peering

Continuity and resiliency

- Continuity → still working (even degraded) when input errors / subsystems failure
- Resiliency → deal with unanticipated failures / errors without crashing or causing unacceptable data loss / process interruption (ms word versionning / auto save)
- Load Balancers → provides continuity and some resiliency

Continuity and resiliency

- ELB – Elastic Load Balancer
  - Needs at least 2 subnet to create a LB



Continuity and resiliency

A managed load balancing service that distributes incoming application traffic across multiple Amazon EC2 instances, containers, and IP addresses.

Continuity and resiliency

- Uses HTTP, HTTPS, TCP and SSL (secure TCP) protocols.
- Can be external or internal facing
- Each load balancer is given a DNS name
- Recognizes and responds to unhealthy instances

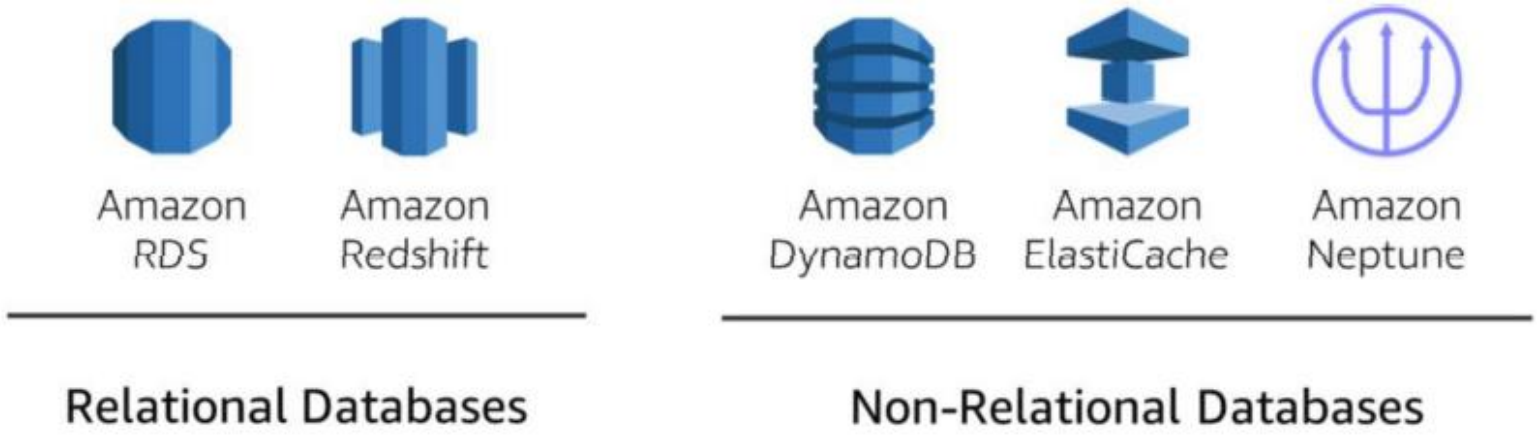
AWS Databases

- **Relationelles**
  - Lignes
  - Colonnes
- **Non relationelles**
  - Clef/valeur
  - Non structuré
    - Schéma dynamique

	Relational/SQL	NoSQL
Data Storage	Rows and columns	Key value, documents, and graphs
Schemas	Fixed	Dynamic
Querying	SQL-based querying	Focused on collection of documents
Scalability	Vertical	Horizontal

AWS Databases

- **Relationelles**
  - **AWS RDS**
    - SQL Server
    - Oracle
    - MySQL Server
    - PostgreSQL
    - Aurora (Amazon propriétaire)
    - MariaDB
  - **Amazon RedShift**
- **Non relationnelles**
  - **Amazon DynamoDB**
  - **Amazon Elastic Cache**
  - **Amazon Neptune**

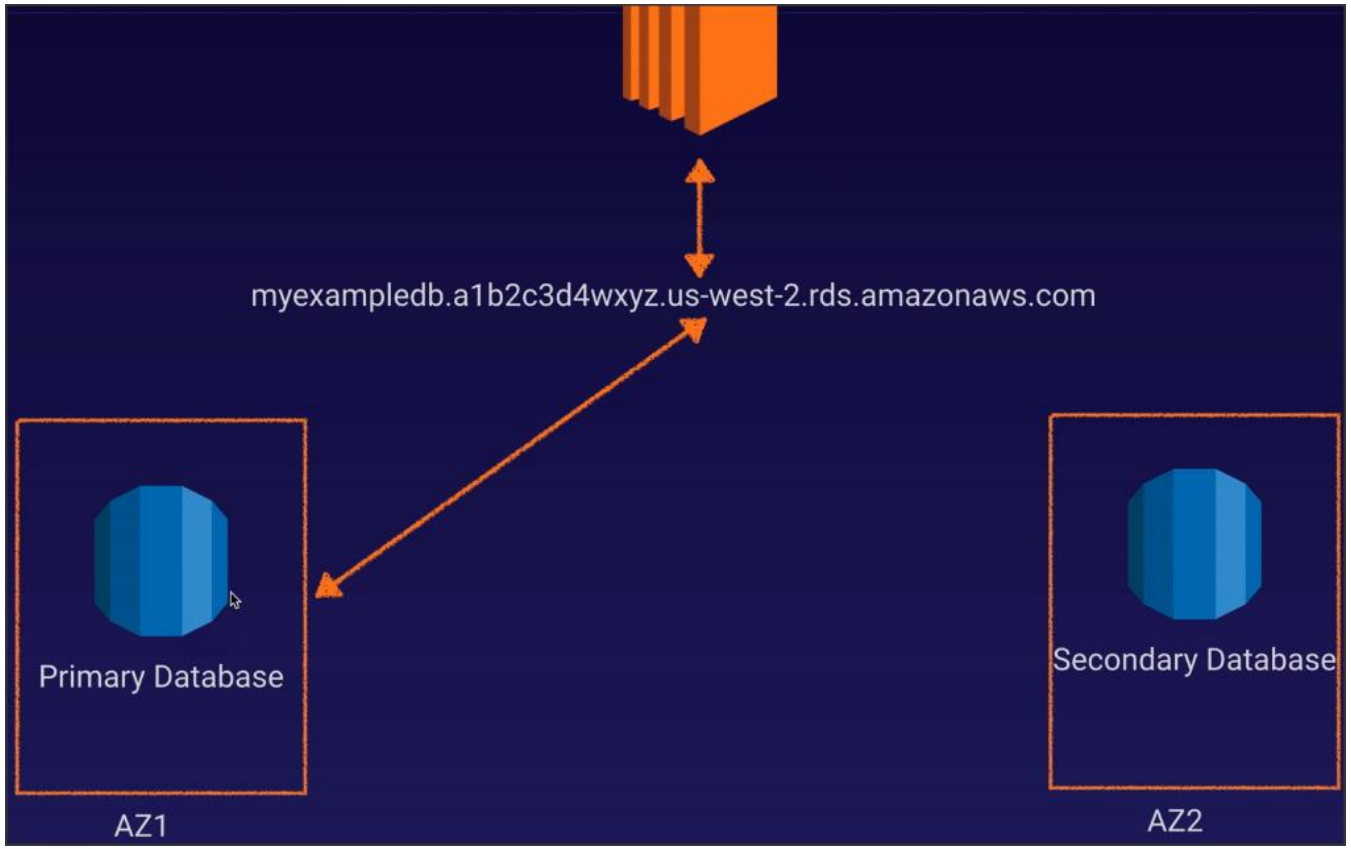


AWS Databases

- Relationelles
  - AWS RDS – OLTP
    - OnLine Transaction Processing
      - Optimisé pour retrouver des « lignes »
  - Amazon RedShift – OLAP
    - OnLine Analytics Processing
    - Architecture différente
    - Datawarewhouse

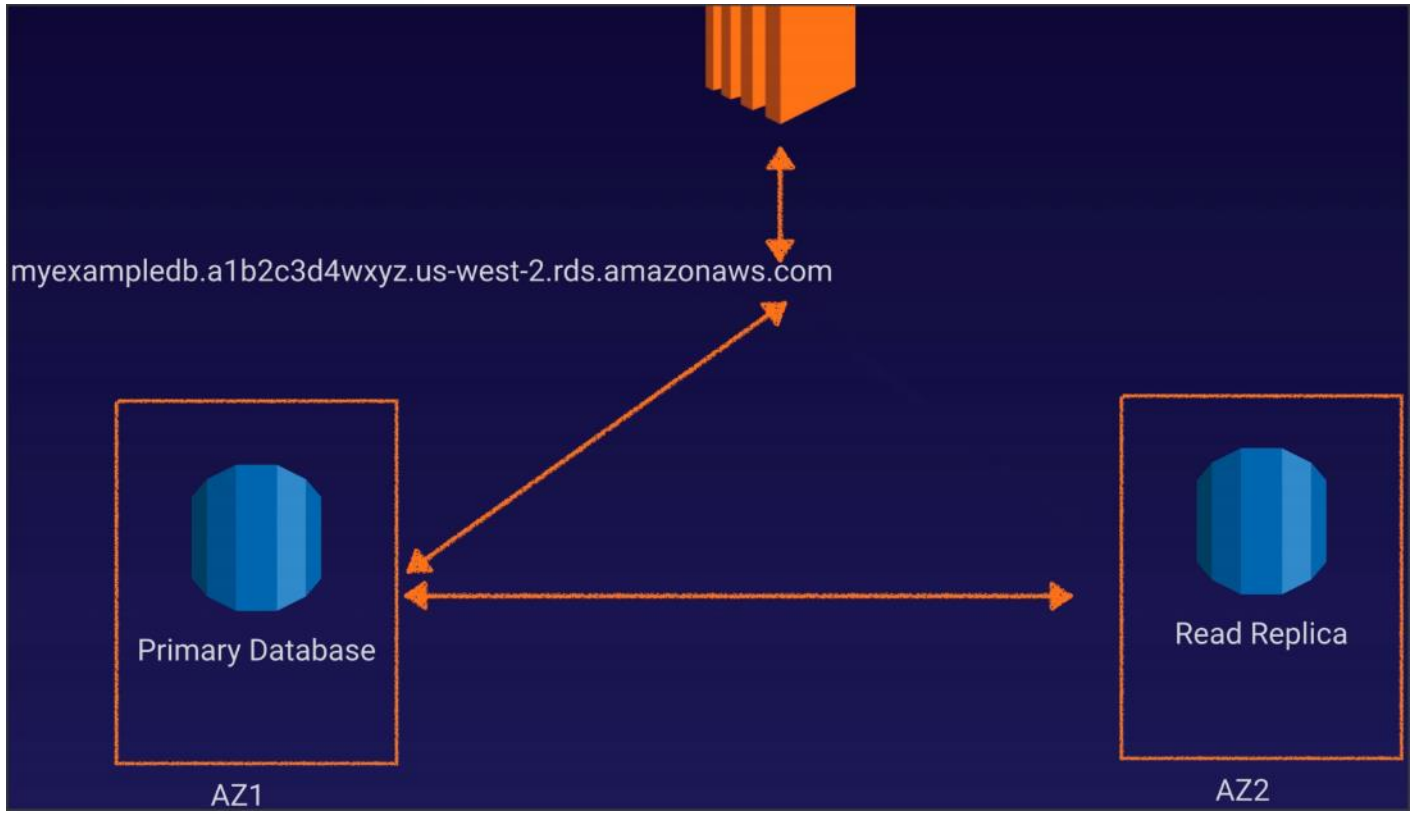
AWS Databases

- **AWS RDS**
  - Multi-AZ
    - disaster recovery
  - Read Replicas
    - PerformanceSQL Server
    - (no automatic failover)

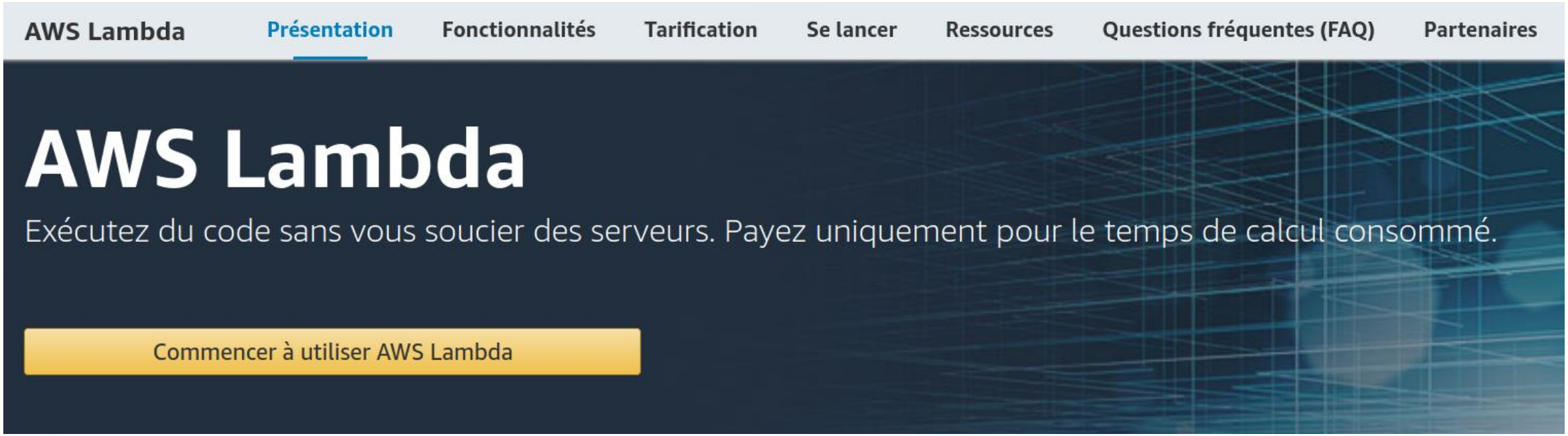


AWS Databases

- **AWS RDS**
  - Multi-AZ
    - disaster recovery
  - Read Replicas
    - PerformanceSQL Server
    - (no automatic failover)
    - Up to 5 copies



AWS Lambda



Since 11/2014

Why AWS Lambda ?

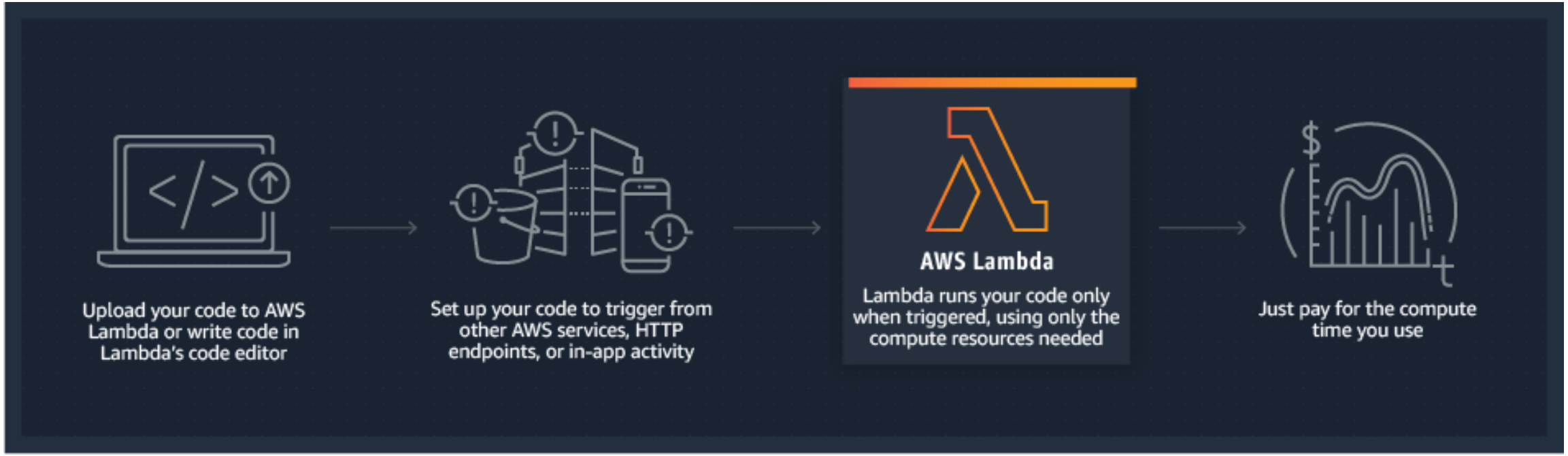
Virtual server in the cloud

Limited RAM and VCPU

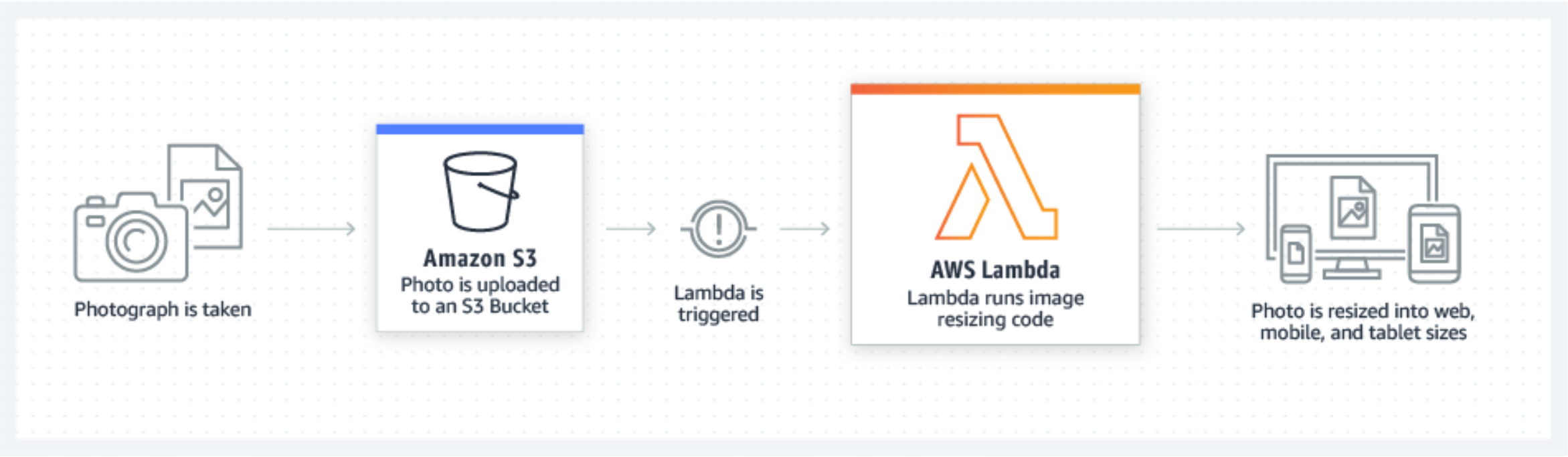
Usually running (day & night)

Scaling by adding/removing servers

AWS Lambda


Upload your code to AWS Lambda or write code in Lambda's code editor
Set up your code to trigger from other AWS services, HTTP endpoints, or in-app activity
AWS Lambda
Lambda runs your code only when triggered, using only the compute resources needed
Just pay for the compute time you use

AWS Lambda


Photograph is taken
Amazon S3
Photo is uploaded to an S3 Bucket
Lambda is triggered
AWS Lambda
Lambda runs image resizing code
Photo is resized into web, mobile, and tablet sizes

AWS Lambda

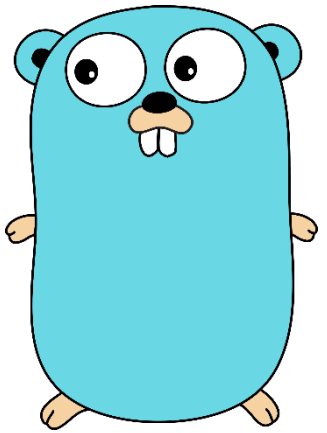
Scale: simple scaling without costly and time consuming data migrations

Simplicity: concentrate on the application, not on the servers, OS or even middleware's

Availability: based on the SLA of the cloud provider

Cost: pay as you run based on the served requested and the computing time required to run your code

AWS Lambda – computer languages



AWS Lambda configuration

Computer resource

Maximum execution time (timeout)

IAM role (permission during execution)

Handler name

Logging with AWS CloudWatch log

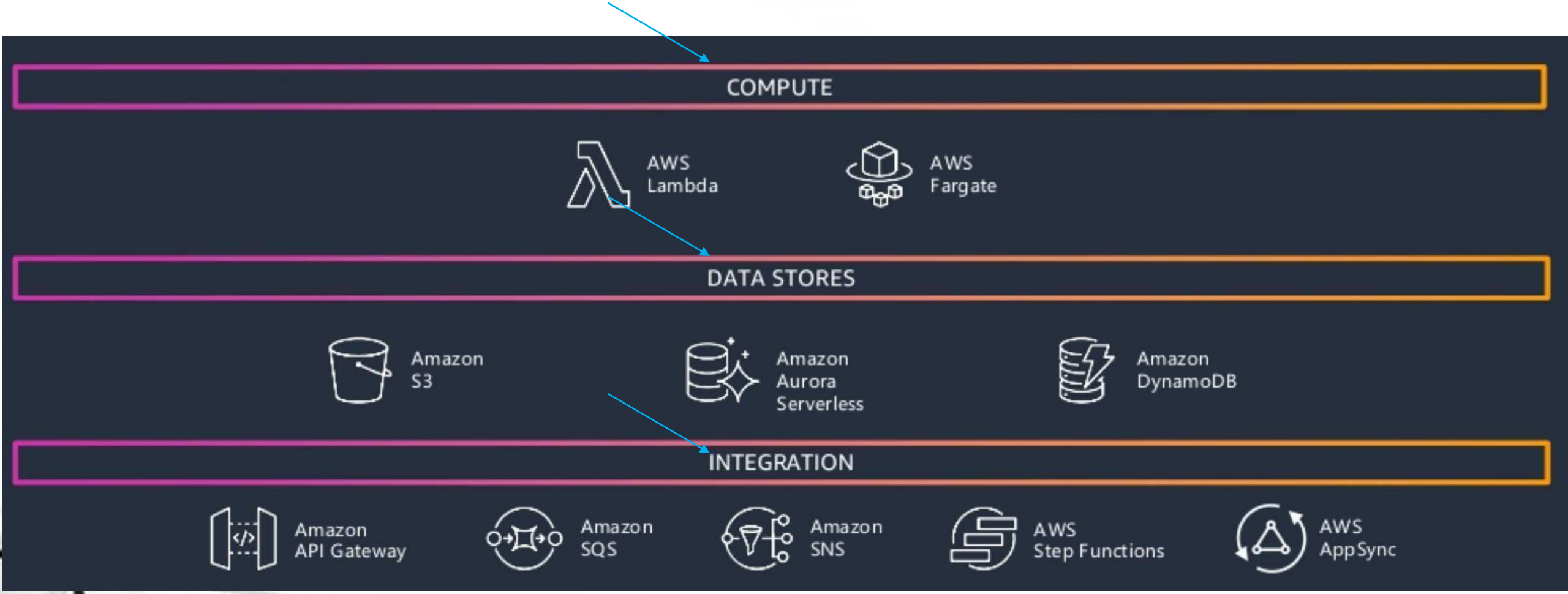
AWS Lambda pro's en con's

- Scaling
- Operation management
- Costs
- High availability

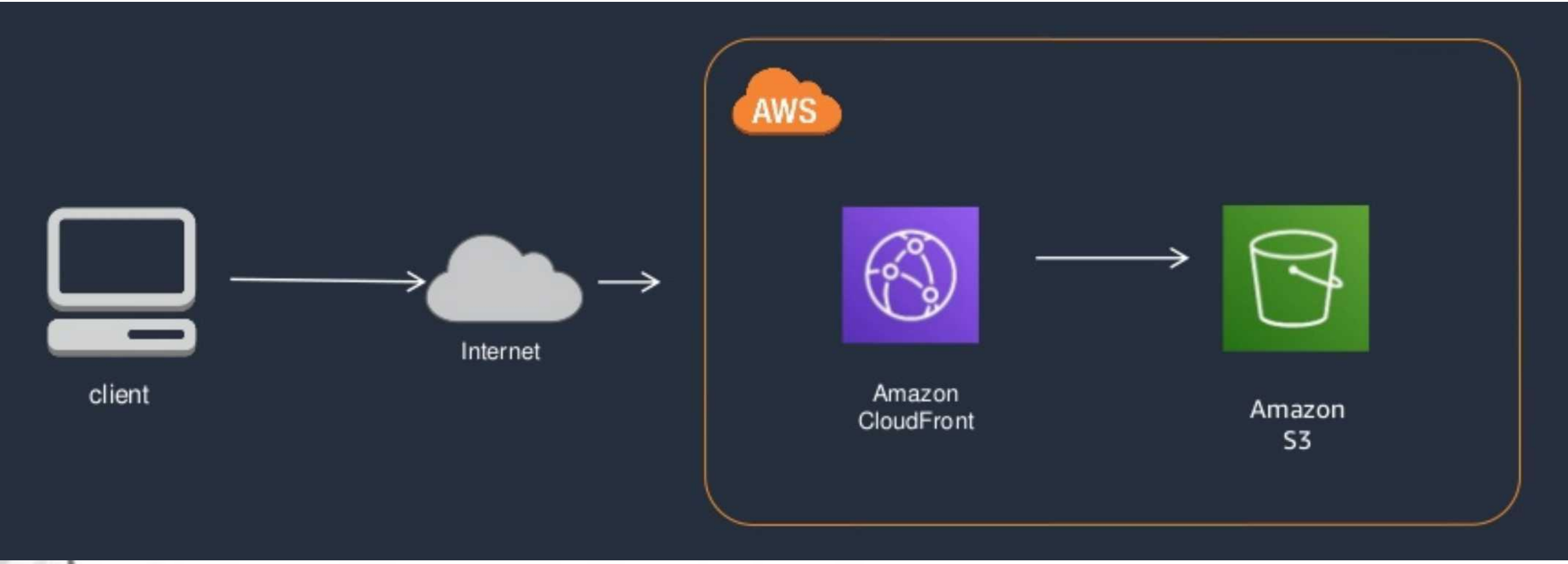
- Stateless
- Monitoring & debugging
- Tracking

Serverless

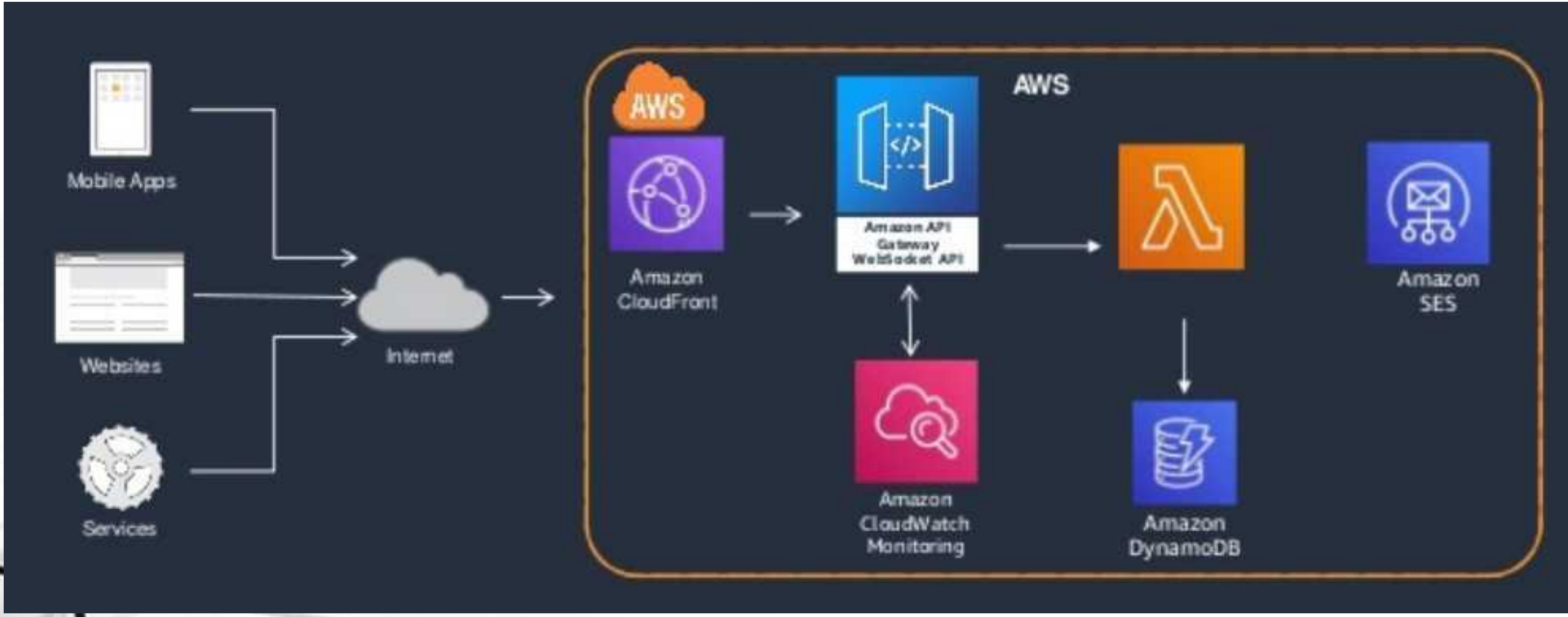
Serverless computing or how to build and run application without thinking about servers



Frontend application architecture

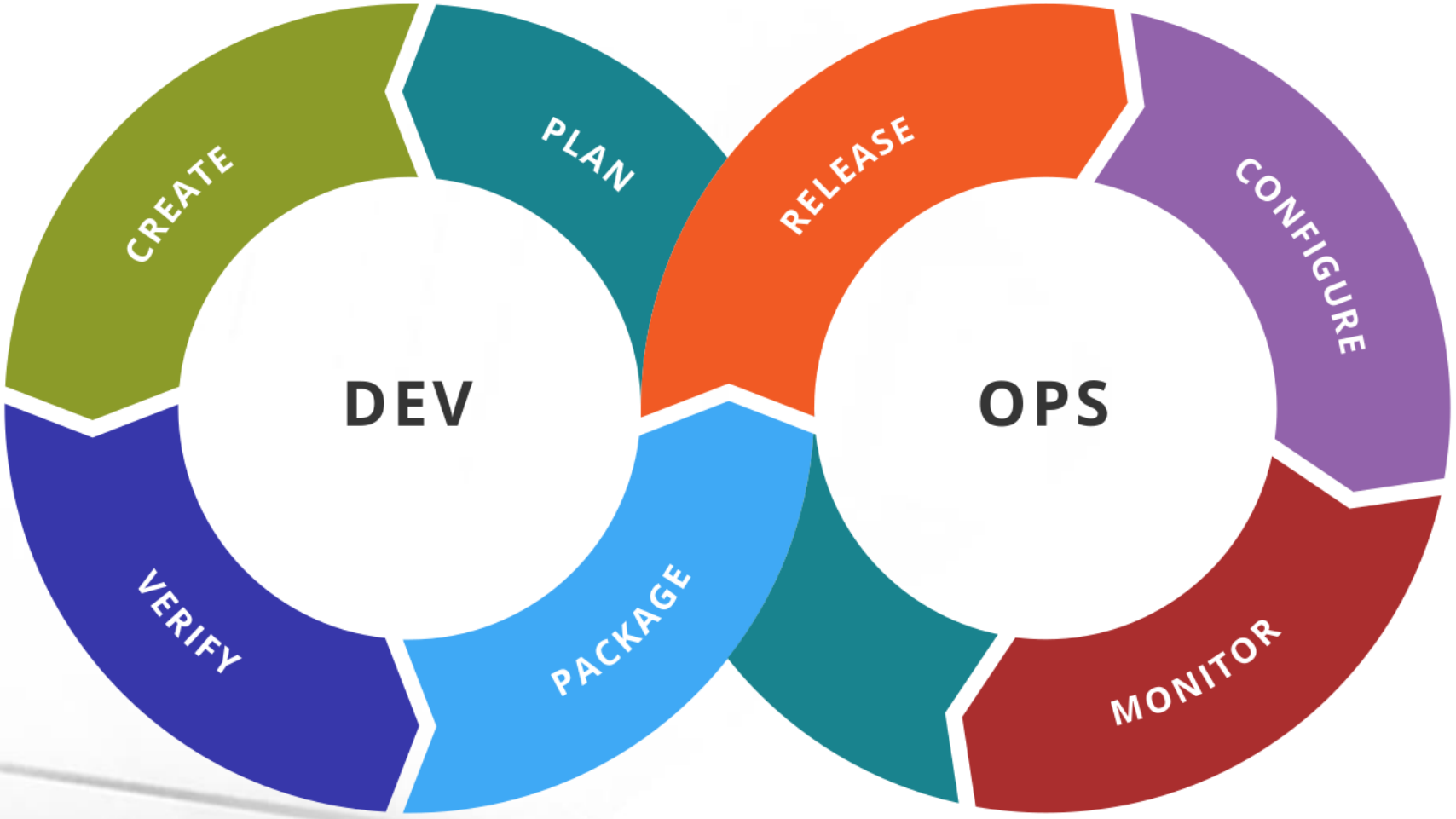


Backend application architecture



Serverless Deployment components

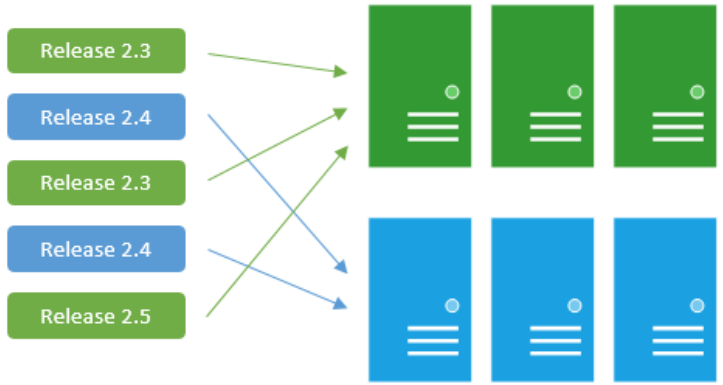
Current version (v 1.0) → new version (v 1.1)



Serverless Deployment patterns

All at once
Updating existing content and all traffic goes to the new version

Blue/green
Swapping alternating production and staging servers



Canaries/Linear
New version of the application first available for a smaller group of users (beta release).
The traffic is then shifted incrementally to the new version.

Source https://dotnet.developpez.com/actu/113645/DevOps-Feature-Flags-Canary-Release-Blue-Green-Deployment-etc-quelle-technique-adopter-en-deploiement-continu-un-tutoriel-de-Hinault-Romaric/

Serverless Deployment

Static website in AWS S3

Wat is a static website ?
Static vs Dynamic

Permissions

Index page
Error page

Source https://dotnet.developpez.com/actu/113645/DevOps-Feature-Flags-Canary-Release-Blue-Green-Deployment-etc-quelle-technique-adopter-en-deploiement-continu-un-tutoriel-de-Hinault-Romaric/

Serverless Deployment

Why using it ?

- Geat performance
- Secure
- Low cost – pay as you use
- Scale

Source https://dotnet.developpez.com/actu/113645/DevOps-Feature-Flags-Canary-Release-Blue-Green-Deployment-etc-quelle-technique-adopter-en-deploiement-continu-un-tutoriel-de-Hinault-Romaric/

Serverless Deployment

```
{
   "Version": "2008-10-17",
   "Id": "PolicyForPublicWebsiteContent",
   "Statement": [
      {
         "Sid": "PublicReadGetObject",
         "Effect": "Allow",
         "Principal": {
            "AWS": "*"
         },
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::mybucket0000000000000002/*"
      }
   ]
}
```

Source https://dotnet.developpez.com/actu/113645/DevOps-Feature-Flags-Canary-Release-Blue-Green-Deployment-etc-quelle-technique-adopter-en-deploiement-continu-un-tutoriel-de-Hinault-Romaric/

API deployment

aws s3 website s3://www.website.com/ –index-document index.html –error-document error.html

aws s3api put-bucket-policy –bucket www.website.com –policy file://policy.json

Source https://dotnet.developpez.com/actu/113645/DevOps-Feature-Flags-Canary-Release-Blue-Green-Deployment-etc-quelle-technique-adopter-en-deploiement-continu-un-tutoriel-de-Hinault-Romaric/

Travail de groupe

Exigences et modalités

- Exigences
  - Voir slides début du cours
    - Attention présentation
    - Les numéros de matricules des étudiants doivent figurer sur le rapport
- Modalités
  - Groupes de 5 étudiants
  - Chaque énoncé peut être « consommé » deux fois maximum
  - L'inscription se fera via une feuille excel publiée dans le groupe team lors de la séance du 19/3
  - L'inscription aux travaux est clôturée à l'issue de la séance de cours du 26/03

Proposition 1 : Authentification Linux

- **Ce travail permet de manipuler l'authentification Linux et les concepts PAM vus en première partie du cours**
  - Provisioning d'une machine virtuelle Linux
  - Configuration d'un compte local admin avec mot de passe faible
  - Exécution d'une attaque « dictionnaire » (hydra) sur ssh
  - Exécution d'une attaque « bruteforce » (hydra) sur ssh
  - Prise des évidences et rapport de conclusion
  - Changement du mot de passe local admin pour un mot de passe complexe
  - Exécution d'une attaque « dictionnaire » sur ssh
  - Exécution d'une attaque « bruteforce » sur ssh
  - Prise des évidences et rapport de conclusion
  - Rédaction d'une conclusion générale. Quelles améliorations possibles sur l'authentification ?

Proposition 2 : Authentification Windows

- **Ce travail permet de manipuler l'authentification windows abordée dans la première partie du cours**
  - Provisioning d'une machine virtuelle Windows 10 (et activez rdp)
  - Configuration d'un compte local admin avec mot de passe faible
  - Exécution d'une attaque « dictionnaire » (hydra) sur rdp
  - Exécution d'une attaque « bruteforce » (hydra) sur rdp
  - Prise des évidences et rapport de conclusion
  - Changement du mot de passe local admin pour un mot de passe complexe
  - Exécution d'une attaque « dictionnaire » (hydra) sur rdp
  - Exécution d'une attaque « bruteforce » (hydra) sur rdp
  - Prise des évidences et rapport de conclusion
  - Rédaction d'une conclusion générale. Quelles améliorations possibles sur l'authentification ?

Proposition 3 : Bitlocker

- **Ce travail permet de manipuler le chiffrage des disques windows**
  - Afin de mettre en avant les risques liés à l'utilisation de disques non chiffrés en cas de vol ou perte d'un ordinateur sous Windows, un test est effectué en bootant l'ordinateur via un Live CD et vérifiant la facilité d'accès aux dossiers personnels. Ensuite le chiffrage des disques (via Bitlocker) est activé et l'exercice est répété.
  - Le travail consiste à mettre en place une vm Windows, y écrire un fichier dans un dossier personnel (My documents), booter avec un live CD/ISO Linux et aller voir le contenu de la partition Windows. Ensuite, activer la fonctionnalité Bitlocker sur Windows (Chiffrement de la partition) et retenter l'opération.

Proposition 3 : Bitlocker

- **Ce travail permet de manipuler le chiffrage des disques windows**
  - Provisioning d'une machine virtuelle Windows (ou éventuellement réutilisation d'un vm existante) avec une partition NTFS
  - Création d'un fichier nommé helmo.txt dans « My documents ».
  - Démarrage d'un live CD/ISO Linux (par exemple Ubuntu) et lecture de la partition Windows (*sudo mount -t ntfs-3g -o ro <partition> /mnt/windisk*)
  - Lecture du fichier helmo.txt

Proposition 3 : Bitlocker

- **Ce travail permet de manipuler le chiffrage des disques windows**
  - Redémarrer le Windows et activer bitlocker (protection par mot de passe)
  - Répéter l'étape du démarrage du live CD/ISO Linux et tentative de lecture de la partition Windows
  - Mount de la partition Linux (*sudo dislocker <partition> -u<password> – /media/windisk*)
  - Prise des évidences et rapport de conclusion
  - Rédaction d'une conclusion générale

Proposition 4 : DM-Crypt

- **Ce travail permet de manipuler le chiffrage des disques Linux**
  - Afin de mettre en avant les risques liés à l'utilisation d'une partition non chiffrée sur un serveur linux,en cas de vol ou perte des disques, un test est effectué en bootant l'ordinateur via un Live CD et vérifiant la facilité d'accès aux dossiers personnels. Ensuite le chiffrage des disques (via dm-crypt) est activé et l'exercice est répété.
  - Le travail consiste à mettre en place une vm Linux, y écrire un fichier dans un dossier personnel (/home), booter avec un live CD/ISO Linux et aller voir le contenu de la partitio. Ensuite, activer la fonctionnalité dm-crypt sur Linux (chiffrage de la partition) et retenter l'opération.

Proposition 4 : DM-Crypt

- **Ce travail permet de manipuler le chiffrage des disques Linux**
  - Provisioning d'une machine virtuelle Linux (ou éventuellement réutilisation d'un vm existante)
  - Création d'un fichier nommé helmo.txt dans /home
  - Démarrage d'un live CD/ISO Linux (par exemple Ubuntu) et lecture de la partition (*sudo mount -t ntfs-3g -o ro <partition> /mnt/windisk*)
  - Lecture du fichier helmo.txt

Proposition 4 : DM-Crypt

- **Ce travail permet de manipuler le chiffrage des disques Linux**
  - Redémarrer Linux et activer dmcrypt (ou réinstaller une autre vm avec les options d'encryption) (protection par mot de passe/passphrase)
  - Répéter l'étape du démarrage du live CD/ISO Linux et tentative de lecture de la partition
  - Mount de la partition encryptée
  - Prise des évidences et rapport de conclusion
  - Rédaction d'une conclusion générale

Proposition 5 : Guide hardening Windows

- **Il s'agit de renforcer un serveur windows 2019**
- **Sur un serveur windows 2019**
  - **Implémentez les éléments suivants**
    - **Politiques de mot de passe** (secpol.msc (local security policy), …)
      - 15 caractères minimum, 20 maximum, des majuscules, des minuscules, des chiffres et au moins 2 caractères spéciaux
      - Account lockout policy : (account lockout duration 15 minutes, Acount lockout thresehold « 5 invalid attempts », « reset account lockout » 10 minutes)
    - **Messages de connexion qui annonce que le système est réservé aux personnes habilitées**
    - **Créez 2 utilisateurs**
      - Un avec des droits administrateur
      - Un avec des droits standards
      - Renommez les comptes administrateur et guest
        - Vérifiez que le compte « gest » est désactivé
      - Testez l'efficacité des politiques de mot de passe
      - Testez les connexions distantes (rdp)

Proposition 5 : Guide hardening Windows

- **Il s'agit de renforcer un serveur windows 2019**
- **Sur un serveur windows 2019**
  - Interdisez la connection au serveur aux compte non administrateurs (« allow log on locally is set to « administrators »)
    - Vérifiez que cette règle fonctionne grâce aux 2 comptes utilisateur précédemment créés)
  - Idem pour rdp (seulement les utilisateurs administrateurs peuvent se connecter)
  - Forcez un « lock screen » après 2 minutes d'inactivité via une politique de sécurité (gpo locale)
  - Choisissez 5 mesures supplémentaires du CIS (https://paper.bobylive.com/Security/CIS/CIS_Microsoft_Windows_Server_2019_RTM_Release_1809_Benchmark_v1_0_0.pdf)
    - Ces 5 mesures ne peuvent pas avoir été choisies par un autre groupe (mettez-vous d'accord)
    - Proposez les 5 mesures que vous avez choisie pour validation

Proposition 6 : Guide hardening Linux

- **Il s'agit de renforcer une station Linux**
- **Sur une distribution de Linux basée debian de votre choix**
  - Implémentez un mot de passe à GRUB
  - Sécurisez le compte root
    - Pas de connexion directe en root
    - Système d'élévation de privilèges sudo
  - Créez 2 utilisateurs
    - Un utilisateur a le droit à l'élévation de privilèges (sudo) et pas l'autre
  - Implémentez une politique de mot de passe (10 caractères minimum, 15 maximum, des majuscules, des minuscules, des chiffres et au moins 2 caractères spéciaux)
  - Implémentez les clefs publiques et privées ssh pour les 2 utilisateurs
    - Testez et validez avec une connexion ssh depuis une autre machine Linux
    - Testez et validez avec une connexion ssh depuis un poste windows qui utilise putty

Proposition 6 : Guide hardening Linux

- **Il s'agit de renforcer une station Linux**
  - Choisissez 5 mesures supplémentaires du CIS (https://paper.bobylive.com/Security/CIS/CIS_Ubuntu_Linux_18_04_LTS_Benchmark_v1_0_0.pdf)
    - Ces 5 mesures ne peuvent pas avoir été choisies par un autre groupe (mettez-vous d'accord)
    - Proposez les 5 mesures que vous avez choisie pour validation
  - **Faites un rapport soigné**
    - avec les explications et captures d'écran pertinentes qui démontrent la véracité et la qualité de votre travail
    - Expliquer vos conclusions. Ce que vous avez appris, ce qu'on pourrait faire pour sécuriser d'avantage le serveur Windows (pas besoin de me recopier le CIS, soyez « high level »)

Proposition 6 : Guide hardening Linux

- **Sur une distribution de Linux basée debian de votre choix**
  - Faites un rapport soigné
    - avec les explications et captures d'écran pertinentes qui démontrent la véracité et la qualité de votre travail
    - Expliquer vos conclusions. Ce que vous avez appris, ce qu'on pourrait faire pour sécuriser d'avantage la station Linux

Proposition 7 : auditd

- **Préparation au forensic**
  - De nombreuses règlementations et standards imposent de tracer les actions réalisées par les utilisateurs d'un système. Le framework « auditd » est disponible nativement sur la majeure partie des distributions GNU/Linux et permet de répondre à ces exigences. Il permet de générer des journaux d'événements afin d'enregistrer des informations sur les différentes activités qui rythment la vie d'un système, des accès aux fichiers en passant par les processus exécutés par des administrateurs.
  - Ces informations sont précieuses pour le suivi des évènements, surtout en cas d'incident ou d'analyse « forensic ».
  - Le travail consiste à mettre en place une vm Linux, y activer auditd, le configurer et écrire les logs sur une autre machine virtuelle distante (via syslog).

Proposition 7 : auditd

- **Préparation au forensic**
  - Provisioning d'une machine virtuelle Linux (ou éventuellement réutilisation d'un vm existante)
  - Installation auditd et création de règles « /etc/auditd/audit.rules »
  - Configuration suivant les recommandations de l'ANSSI (R50, page 41 - https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf)
  - Ensuite, mise en place d'une machine virtuelle supplémentaire (serveur rsyslog dans le même réseau) et configuration syslog afin d'envoyer les logs auditd vers le syslog
  - Prise des évidences étape par étape
  - Rédaction d'une conclusion générale

Systèmes d'exploitation avancés

Tuyaux examen juin 2021 – Document officieux non engageant

stephane.louis@l-a.lu

Haute Ecole Libre Mosane

2020 - 2021

Clarification importante

- Ce document reprends les explications d'évaluation données lors du cours. Il propose aussi des conseils et des tuyaux pour la préparation de l'examen
- Ces tuyaux sont fournis de manière spontanée. Le professeur n'a aucune obligation de fournir ce genre d'information
- Les informations présentes dans ce document visent à aider les étudiants dans la préparation de leur examen.
- Les informations données dans ce document sont données à titre indicatif.
  - Il n'y a aucun engagement du professeur concernant leur complétude, leur exactitude ni leur pertinence.
  - Chaque étudiant est seul responsable de l'utilisation qu'il fera de ces informations.
  - En aucun cas le contenu de ce document ne pourra être utilisé pour formuler une quelconque réclamation concernant le processus d'examen et encore moins sont résultat.

Contenu du cours

Les modules de cours sont indépendants. Plusieurs modules pourront éventuellement être abordés simultanément

- **Systèmes classiques**
- **La virtualisation**
  - Hyperviseurs
  - Micro-containers
- **Le (public) cloud computing**
  - Terminologie
  - Public cloud (grand) public
- **Travail personnel par groupes**
  - Exécution d'attaques dictionnaire / bruteforce
  - Rapport

Objectifs du cours

- **Au terme de ce cours le futur professionnel sera**
  - **Capable de comprendre et d'expliquer le fonctionnement général des composants des systèmes traditionnels et des systèmes virtualisés qui constituent un cloud**
    - Cours ex cathedra
  - **Sensibilisé aux vulnérabilités**
    - Travail de groupe
  - **Capable de travailler en groupe, s'exprimer avec un langage clair et adéquat**
    - Rapport du travail de groupe

Supports du cours

Tout au long de sa carrière le professionnel doit sans cesse mettre ses connaissances à jour. Il est important d'être curieux et d'acquérir la capacité à trouver et canaliser les informations nécessaires à son apprentissage continu

- **Présentations utilisées pendant les séances de cours**
  - Seront mise à jour régulièrement au fur et à mesure que le cours sera donné
- **Documents éventuels renseignés par le professeur**
- **Notes personnelles**
  - Les transparents proposés sont juste un support de l'exposé oral !
  - Indispensables pour être prêt pour l'examen
  - Chaque étudiant est entièrement responsable de la qualité de ses notes personnelles
- **Toute information utile que l'étudiant aura pu trouver lors de ses recherches personnelles**

Evaluation

L'évaluation mesure l'accomplissement des objectifs du cours qui se résument à l'assimilation de contenu et la capacité à fonctionner au sein d'un groupe de professionnels

- **Travail de groupe (50 points)**
  - **Contenu (40 points)**
  - **Qualité du rapport (10 points)**
    - Présentation
    - Grammaire
    - Orthographe
- **Examen (50 points)**
  - **QCM (+1 / -1)**
    - Contenu abordé dans les slides et les exposés oraux du cours (45 points)
    - Contenu des lectures, et sources documents connexes renseignées ou personnelles (5 points)
- **La note du travail de groupe peut-être reportée d'une session à l'autre pendant la même année académique**
- **Remarque : Le rapport peut-être rédigé au choix en français, en anglais ou en néerlandais**

Bibliographie

- **Elements de bibliographie**
  - HP
  - Dell
  - VMWare
  - AWS
  - Cloudguru
  - Wikipedia
  - Autres cours de S.Louis
  - Et bien d’autre contenu du web.

1 Les tuyaux

A propos de l'examen

- QCM 20 questions, 50 minutes
- Si les propositions « tout est vrai » ou « rien n'est vrai » vous sont proposés c'est que ces réponses sont de l'ordre du possible nonobstant la formulation de l'énoncé et de l'usage du nombre et des genres
- +1 pour chaque bonne réponse, -1 pour chaque mauvaise réponse, 0 pour les abstentions
  - Dans votre vie professionnelle vous gagnerez votre vie en travaillant, ne la gagnerez pas en ne faisant rien et payerez des pénalités pour réparer vos erreurs
  - En cas de choix d'une seule réponse alors que toutes les réponses étaient correctes pénalité moins forte (sauf si vous aviez choisi « rien n'est vrai » bien entendu)
- Toute tricherie ou comportement suspect qui donnerait lieux à penser qu'il y a peut-être tricherie verra son auteur sanctionné par un zéro avec interdiction de repasser l'examen à la session suivante

A propos de l'examen

- L'examen sert à évaluer votre capacité à vous intégrer dans un environnement professionnel
  - Maitrise des concepts vus au cours
  - Assimilation du vocabulaire professionnel
- Ce n'est pas un test de grammaire
  - La différence entre propositions de réponse ne réside pas dans la subtilité de la tournure des phrases ou l'emplacement d'une négation ou d'une virgule
- 1 à 2 questions sur les 20 viseront à évaluer si vous avez fait des recherches au-delà du cours
- Une note peut-être reportée d'une session à l'autre pendant la même année scolaire, quelle que soit sa valeur
- Un étudiant est libre de repasser l'examen en 2e session même s'il a réussi en 1e session. Dans ce cas la note de la 2e session sera retenue (soyez sûr de votre coup ☺)

Première section : authentification

- Attendez-vous à avoir des questions sur
  - les concepts des protocoles d'authentification locale et centralisée vocabulaire et cas pratiques (quand faire quoi et comment)
  - Concepts liées à l'authentification biométrique, vocabulaire (CER, FER, BQR) et cas pratiques (quand et comment utiliser la biométrie, avantages, …)
  - Protocoles d'authentification chiffrées et leurs fonctionnement (mécanismes clef privée, publique)
  - Authentification forte

Première section : autentification

- Exemple de question :
  - Parmi les propositions suivantes, laquelle décrit une authentification forte
    - Pin + token
    - Pin + jeton physique
    - Pin + jeton software
    - Toutes les propositions sont vraies
    - Toutes les propositions sont fausses
  - Réponse : Toutes les propositions sont vraies

Deuxième section : Virtualisation

- Attendez-vous à avoir des questions sur
  - les concepts concernant les types de hardware (serveurs, stockage de données (type de stockage (DAS,NAS, SAN – ce qui les différentie), contrôleurs, raids, LUN,protocoles)). Ces concepts ont été largement expliqués dans le cours vous aurez des questions là-dessus
  - Concepts liés à la virtualisation (qu'est-ce que c'est, avantages, inconvénients) et les hyperviseurs (type d'hyperviseurs,…)
  - Hyperviseurs vus au cours (vmware esxi, workstation, etc), les fichiers qui les composent, leur utilité, les fonctionnalités comme snapshot, vmotion, HA, VSAN…
  - Concepts pratiques (c'est ici qu'on va juger si vous êtes prêts à aller travailler): avec quel type de stockage esxi peut il travailler ?

Deuxième section : Virtualisation

- Exemples (réels) de questions (sans les propisitions ni les réponses)
  - Concernant les systèmes de stockage quelle proposition est (sont) vraie(s) ?
    - Concepts SAN, NAS, DAS
    - Qu'est ce qui fonctionne avec esxi, vmware workstation
  - A propos des serveurs « blades » → propositions sur leurs avantages / inconvénients
  - A propos des fichier .vmdk → proposition sur leur fonction et leur structure
  - A propose de HA et FT → proposition suer leur utilité, ce qu'ils apportent dans la vraie vie
  - Qu'est-ce un « vSphere Distributed Vswitch » ?
  - Limites de l'hyperviseur
  - Snapshots
  - vSan

Troisième section : Cloud public

- Attendez-vous à avoir des questions sur
  - les concepts concernant les types de cloud (privé, …) et leur «delivery model» ainsi que la frontière des responsabilités
  - Les concepts de datacenter, AZ, région, edge location, ..
  - Les stockages comme S3 et leurs capacités / fonctionnalités
  - Les instances AWS et leurs composants (ENI, EBS, …)
  - Concepts comme AMI, VPC, security groups, concepts statefull/stateless, internet gateways, nat gateways, ELB, IAM, security hub, fonctions lamda
  - Les différents types de base de données (relationnelles, …)
    - Les différentes base de données proposées par aws (RDS (c'est quoi, qu'est-ce que ça inclus)), Oracle, redshift, Mariadb, neptune, aurora, neptune (quels types de sgbd ils sont)
    - Principe bases de données structurées, non structurée (clef/valeur)

Troisième section : Cloud public

- Attendez-vous à avoir des questions sur
  - Bien différentier l'informatique locale, cloud privé, et le responsibility model.
    - Responsabilités de l'équipe informatique dans laquelle vous faites partie et responsabilité du cloud provider qui vous fournit des services → quelques questions avec des cas concrets
    - Exemple : Pour des raisons de compliance, il faut stocker tous les journaux d'accès aux données (logs) pendant 10 ans. Dans quels cas l'équipe informatique doit-elle analyser l'impact de cette mesure ?
      - Hébergement SaaS uniquement
      - Hébergement On-prem et IaaS
      - Hébergement On-prem et IaaS et PaaS
      - Hébergement On-prem, IaaS, PaaS et SaaS
      - Hébergement On-prem

Troisième section : Cloud public

- Attendez-vous à avoir des questions sur
  - Bien différentier l'informatique locale, cloud privé, et le responsibility model.
    - Exemple : Dans le cadre du « Shared Responsibility model», quelle la part de responsabilité de l'utilisateur du cloud ?
  - Concepts CVE. Qu'est-ce qu'une vulnérabilité, que fait on et sur quel environnement lorsqu'une cve est publiée ?
  - Matrice de contrôle dans un cloud
    - Security of the cloud
    - Security from the cloud
    - Security to the cloud
    - Security with the cloud
    - Security in the cloud

Troisième section : Cloud public

- Autres exemples indicatifs (sans les propositions)
  - AWS : Lequel de ces SGBD (n')est (pas) relationnel ?
  - Quelle affirmation est correcte concernant les fonctions AWS Lambda ?
  - Comment protéger l'accès à la console web AWS ?
  - Quelles sont certaines caractéristiques d'un environnement cloud ?
  - Comment l'authentification SSH par défaut vers une AWS EC2 Linux est réalisée ?