

# Modèle de déploiement

M346 – Concevoir et réaliser des solutions cloud

Jérôme Frossard

EPAI

29 juillet 2024

Selon le NIST, un cloud doit avoir les cinq caractéristiques suivantes :

- Libre-service à la demande (*on-demand self-service*)
- Accès ubiquitaire (*broad network access*)
- Mutualisation des ressources (*resource pooling*)
- Élasticité rapide (*rapid elasticity*)
- Mesure de l'utilisation des services (*measured service*)

Mais cela ne dit pas où l'infrastructure doit être déployée, qui possède cette infrastructure, et qui peut y avoir accès.

C'est précisément ce que permet de déterminer le modèle de déploiement.

- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé
- 4 Cloud communautaire
- 5 Cloud hybride

- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé
- 4 Cloud communautaire
- 5 Cloud hybride

# Qu'est-ce qu'un modèle de déploiement ?

Un modèle de déploiement détermine :

- Où l'infrastructure du cloud est déployée et exploitée,
- Qui possède et gère cette infrastructure, et
- La manière dont les ressources et les services sont mis à la disposition des consommateurs.

Le modèle de référence du NIST, définit quatre modèles de déploiement :

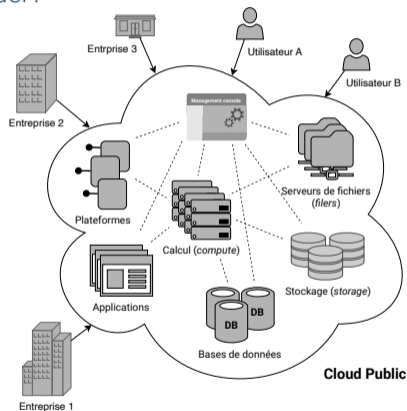
- Nuage public (*public cloud*)
- Nuage privé (*private cloud*)
- Nuage communautaire (*community cloud*)
- Nuage hybride (*hybrid cloud*)

- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé
- 4 Cloud communautaire
- 5 Cloud hybride

# Cloud public – Définition

Un cloud public est un modèle de déploiement dans lequel :

- L'infrastructure réside dans les centres de données du fournisseur, généralement répartie dans plusieurs régions et plusieurs zones de disponibilité.
- Le fournisseur possède et gère l'infrastructure.
- Les ressources et les services cloud sont accessibles à travers l'Internet public.
- Les ressources partagées par les différents consommateurs (multilocataire ou *mutli-tenant*).



# Cloud public – Gestion des ressources et des services cloud

Les consommateurs approvisionnent et gèrent eux-mêmes les ressources et les services cloud qu'ils consomment à l'aide de :

- Consoles Web
- API (*application programming interface*)

L'utilisation d'API permet de :

- Gérer les ressources et les services avec des outils en ligne de commande (CLI)
- Réaliser des scripts pour automatiser des procédures.

Dans un cloud public, les consoles et les API sont accessibles depuis l'Internet.



L'un des inconvénients majeurs du cloud public est la sécurité.

Certains fournisseurs attribuent encore, par défaut, une adresse IP publique (statique ou dynamique selon les cas) aux machines virtuelles. Cette adresse permet notamment :

- D'avoir accès à l'Internet pour installer du logiciel ou mettre à jour le système.
- De gérer la machine avec SSH ou RDP.
- De faire fonctionner un serveur HTTP.

Dans une infrastructure informatique, la plupart des serveurs ne devraient pas avoir d'adresse publique. Même s'il ne suffit pas d'avoir l'adresse d'une machine pour y avoir accès, cela augmente néanmoins la surface d'attaque.

Dans un cloud public moderne :

- L'adresse IP publique est pratique, mais elle n'est pas nécessaire comme c'était le cas jusque dans les premières années des années 2010.
- Les machines virtuelles ont par défaut une adresse IP privée dans un réseau virtuel, par exemple 10.0.0.0/24.
- Le trafic sortant peut être géré à l'aide d'une passerelle NAT avec une adresse publique.
- Le trafic entrant peut être géré à l'aide d'un répartiteur de charge (*load balancer*) avec une adresse publique.

Pour gérer les machines, il existe plusieurs possibilités :

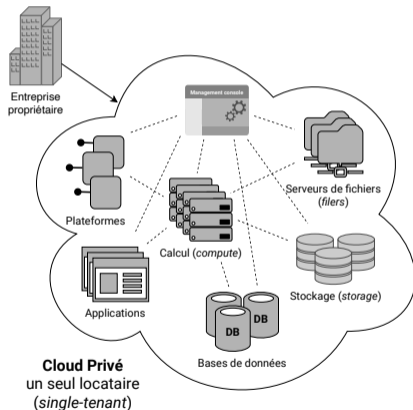
- Un *jump host* avec une adresse publique.
- Une console sérielle qui peut être connectée à une console dans le portail web.
- Une connexion VPN au réseau virtuel.

Avec un VPN, on obtient essentiellement un **cloud privé virtuel**.

- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé**
- 4 Cloud communautaire
- 5 Cloud hybride

Un cloud privé est un modèle de déploiement dans lequel :

- L'infrastructure réside dans un centre de données privé ou en colocation.
- L'entreprise possède ou loue l'infrastructure.
- Les ressources et les services cloud sont accessibles depuis un réseau privé ou un réseau privé virtuel (VPN).
- Les ressources sont à l'usage exclusif de l'entreprise, mais peuvent être partagées entre des utilisateurs de différent département (locataire unique ou *single-tenant*).



On peut distinguer plusieurs types de clouds privés :

- **Cloud privé sur site (*on premisses*)**. L'entreprise possède et gère l'infrastructure.
- **Cloud privé géré**. L'infrastructure est hébergée et gérée par un fournisseur, mais l'entreprise en est propriétaire et en a l'usage exclusif.
- **Cloud privé virtuel**. L'infrastructure est celle d'un cloud public, mais qui permet un niveau d'isolation semblable à un cloud privé géré ou sur site, notamment avec des réseaux virtuels et des serveurs physiques dédiés.

Parmi les cas d'utilisation d'un cloud privé, on peut mentionner :

- **Charges de Travail critiques.** Des charges de travail critiques nécessitant un contrôle accru sur la performance, la sécurité, ou la conformité.
- **Protection des Données.** Des exigences strictes en matière de protection des données dans un secteur réglementé (santé, finance, etc.).
- **Personnalisation.** Des applications nécessitant un degré de personnalisation et d'intégration que ne permet pas un cloud public.

Parmi les éléments à prendre en considération dans le cloud privé, en particulier d'un cloud privé sur site, on peut mentionner :

- **Coûts d'investissement élevés.** : Les frais de démarrage (CAPEX initial) pour la construction, l'exploitation et la gestion de l'infrastructure d'un cloud privé élevés, notamment en raison du niveau d'expertise nécessaire.
- **Maintenance complexe et continue.** La maintenance d'un cloud privé sur site implique des tâches telles que la surveillance des performances, l'application de correctifs logiciels et la planification des mises à jour matérielles et logicielles.
- **Évolutivité moindre.** En raison de ressources en quantité limitée, un cloud privé sur site souvent moins évolutif qu'un cloud public. La montée en puissance nécessite des achats de matériel et de logiciel de plus en plus conséquents.
- **Accès mobile limité.** Des politiques de sécurité plus strictes peuvent restreindre les accès mobiles et rendre le cloud privé moins flexible pour les utilisateurs finaux.

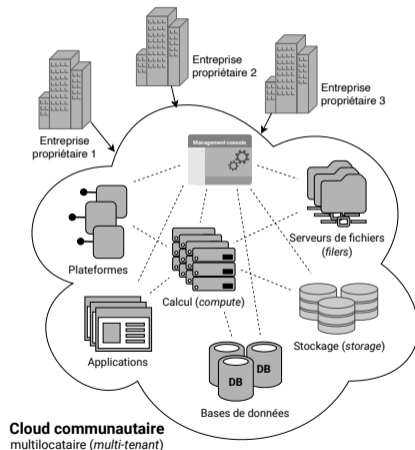
Les inconvénients du cloud public peuvent généralement être mitigés d'une manière ou d'une autre :

- **Coûts d'investissement élevés.** : Les frais de démarrage peuvent être réduits et transformés en OPEX avec un cloud privé virtuel. Un cloud communautaire multilocataire pour un regroupement d'organisations peut également permettre de réduire ces frais en les mutualisant.
- **Maintenance complexe et continue.** Avec un cloud privé géré, les tâches de maintenance sont prises en charge à un fournisseur de service.
- **Évolutivité moindre.** Si les ressources d'un cloud privé sont insuffisantes, la montée en charge peut être réalisée avec l'interconnexion du cloud privé et d'un cloud privé virtuel avec une liaison à faible latence.

- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé
- 4 Cloud communautaire**
- 5 Cloud hybride

Un cloud communautaire est un cloud privé multilocataire :

- L'infrastructure réside dans un centre de données privé ou en colocation.
- L'infrastructure appartient à un groupement d'organisations avec des exigences réglementaires et opérationnelles communes.
- Les utilisateurs ont accès aux ressources et aux services cloud depuis un réseau privé ou un réseau privé virtuel (VPN).
- Les ressources sont à l'usage exclusif du groupement d'organisation, mais sont partagées entre ses membres.



- 1 Modèles de déploiement
- 2 Cloud public
- 3 Cloud privé
- 4 Cloud communautaire
- 5 Cloud hybride

un cloud hybride est un cloud privé étendu par des ressources dans un cloud privé virtuel :

- Le cloud privé est interconnecté avec un cloud privé virtuel.
- Les utilisateurs ont accès aux ressources et aux services cloud depuis un réseau privé ou un réseau privé virtuel (VPN).
- Les ressources du cloud privé sont à l'usage exclusif de l'entreprise.
- Les ressources du cloud privé virtuel peuvent être partagées ou dédiées, selon les besoins.

