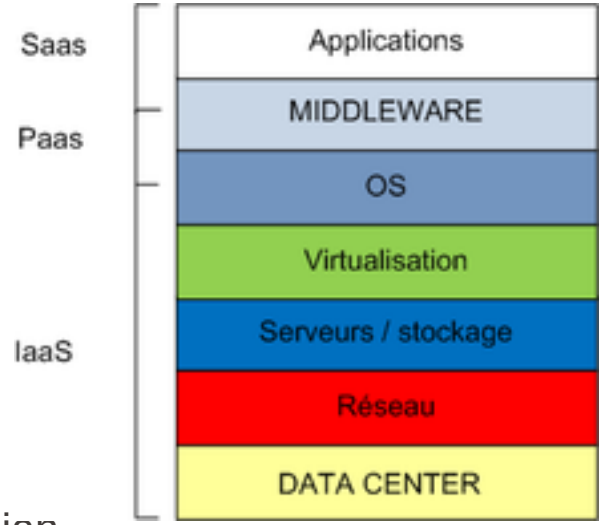
Forum IT IaaS-NSX

École polytechnique fédérale de Lausanne

IaaS@EPFL

Infrastructure as a Service (IaaS): modèle où la VPSI gère l'infrastructure qui permet de déployer des machines virtuelles à la demande, basé sur un catalogue.



Source: Wikipédia

Demandé et validé par la direction VPSI

- Mandant de ce projet: Edouard Bugnion
- Service manager: Christophe Simond
- Chef de projet: Eric Krejci
- Responsable sécurité composant NSX: Alexandre Sutlian
- Responsable organisation NSX: Antoine Osthus
- Support infrastructure et sécurité: VPSI-EXHEB et VPSI-EXAPP

IaaS@EPFL - Périmètres/objectifs

Infrastructure as a Service (IaaS):

- Evolution service "Virtualisation des Serveurs" (MyVM) sur une solution "Self Service Portal" automatisée au maximum
- Plate forme « à la carte»
- Pas de goulot d’étranglement sur la mise en œuvre
- Base pour évoluer dans du XaaS: LBaaS, DBaaS, ObjectStorageaaS, BackupaaS, DevOPS, …

IaaS@EPFL - structure organisationnelle: 2 tenants

EPFL : regroupé par facultés & unités

- Toutes les VMs d'une même unité seront regroupées ensemble
- Tous les membres d'une unité verront leurs VMs sur le portail (demandes nouvelles VMs, modifications existantes, etc…)
- 1 groupe d'approbateurs et 1 groupe de support par faculté

ITServices : regroupé par Services

- Toutes les VMs d'un même service (au sens ServiceNow SVC000XX) seront regroupées ensemble
- Tous les administrateurs d'un service donné verront leurs VMs sur le portail, celles de leur service et les composants liés (demandes nouvelles VMs, modifications existantes, etc…)
- 1 groupe d'approbateurs et 1 groupe de support pour le tenant

NSX@EPFL - Objectifs

Paradigme technique

- Volonté VPSI de tendre vers le Software Defined DataCenter (SDDC)

Services IT

- Exposition des services/applications à des communications non contrôlées
- Flux applicatifs entre services souvent non connus et/ou peu maîtrisés

Objectifs de bonnes pratiques (Direction)

- Séparation des environnements de Production, Test et Développement
- Traitement des risques (sensibilité des applications)
- Auditabilité (cf. segmentation du réseau)
- Responsabilisation des utilisateurs (changement d'habitudes)

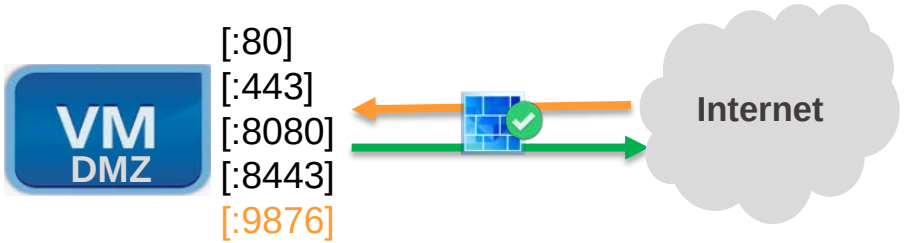
NSX@EPFL - Principes

- L’approche NSX isole les VMs et les services les uns des autres de manière adaptée aux choix stratégiques de la VPSI et permet de fournir un modèle de sécurité moderne pour le data center

- Le principe de mise en œuvre favorise la maitrise des flux et est modulable et dynamique

- Le principe de sécurité repose:
  - sur le cloisonnement des environnements (production, test et développement)
  - sur le contrôle des flux entrants des services au sens Service Now (pour le tenant IT Services)

NSX@EPFL - fonctionnement DMZ

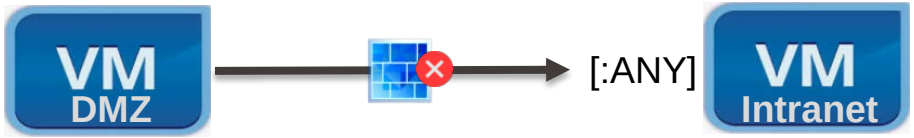


Règles DMZ sortantes

- Les flux sont autorisés sans restriction en sortie

Règles DMZ entrantes

- Ouverture des ports usuels – **processus automatisé**
- Ouverture des ports non usuels soumis à validation et à la réalisation de Secure-IT



Règles DMZ vers Intranet

- Les communications de la DMZ vers Intranet sont bloquées par défaut (sauf les services génériques DMZ)

- **Les exceptions seront traitées via intervention manuelle Secure-IT**

Qu’est ce qu’on ne pourra plus faire?

- Réaliser des transferts directs de données entre environnements (DEV, TEST, PROD)
  - Utiliser GitHub pour le transfert de code
  - Utiliser le NAS pour le transfert de fichiers ou de DB
- Recycler une VM (Pour un autre service par exemple)
- Demander une ouverture complète de la machine
- Administrer les machines DMZ depuis n’importe où, sauf depuis le VPN

Demo


EPFL
Infrastructure as a Service
IT Service Portal
https://portal-xaas.epfl.ch/

Merci!

Forum IT