



REX : Comment créer une offre IaaS / PaaS complètement Open Source du parefeu au cloud ?

4 décembre 2024



DEMARET Thibaut

Worteks

Société d'expertise, d'édition et d'hébergement Open Source

Contribue activement à de nombreux logiciels libres comme LSC, LemonLDAP::NG, LDAP Tool Box et FusionIAM

Partenaires



Membre fondateur



Worteks

Une offre Open Source globale.

Solution de déploiement d'infrastructure complexe

 **V'Opla**

Portail de travail collaboratif

 **V'Sweet**

Intégration, support et expertise

 **V'ise**

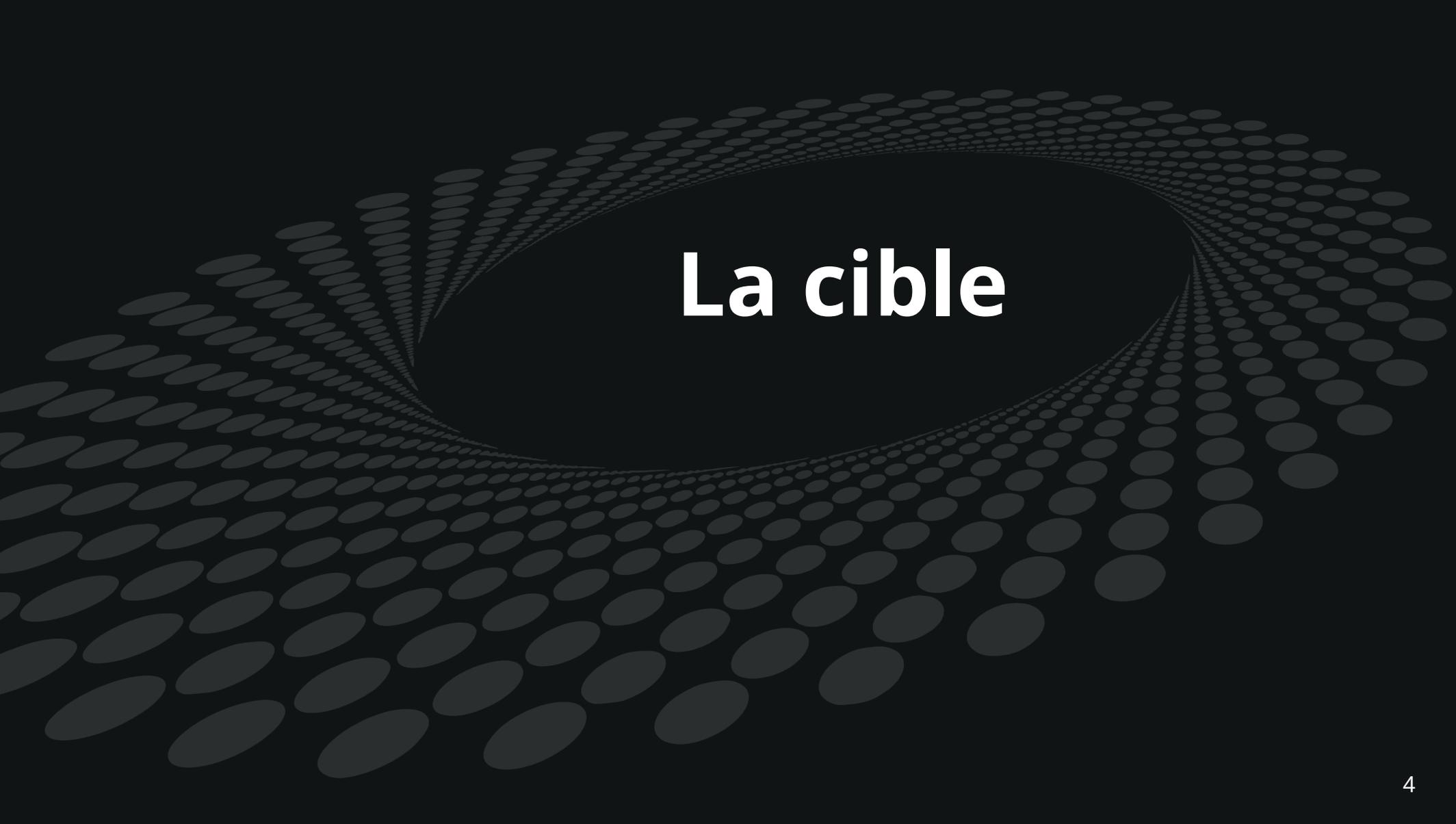
Hébergement souverain

 **V'aaS**

Solution de gestion des identités et des accès

 **V'IDaaS**





La cible

La liste de vœux

- Open Source
- Solutions communautaires
- Répartition sur trois sites
- Résilience
- Hautement disponible : 99,999%
- Facile à administrer
- Automatisable
- Scalable
- Souverain
- Date de livraison : quatre mois



Certifications visées

- SecNumCloud
- ISO 9001
- ISO 27001
- HDS
- PCI-DSS
- Et bien d'autres



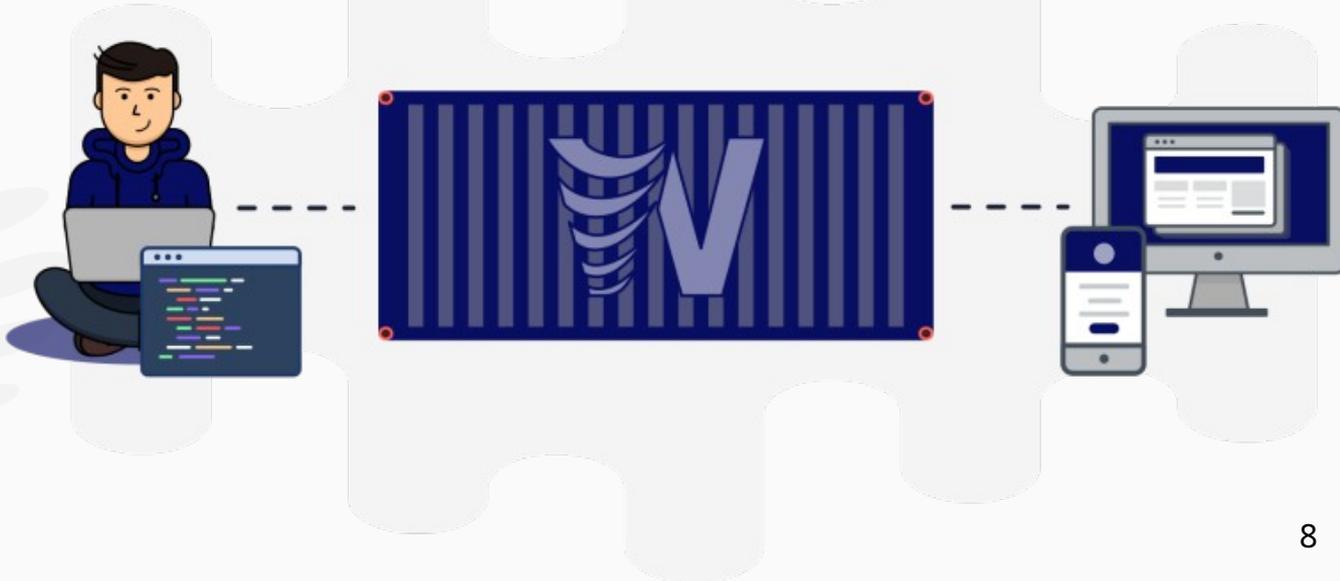


**Dans
un monde idéal**

Dans un monde idéal



Projet W'Opla déjà présenté :
<https://www.worteks.com/edition/wopla/>



Dans un monde idéal



CentOS

okd



ANSIBLE



openstack®

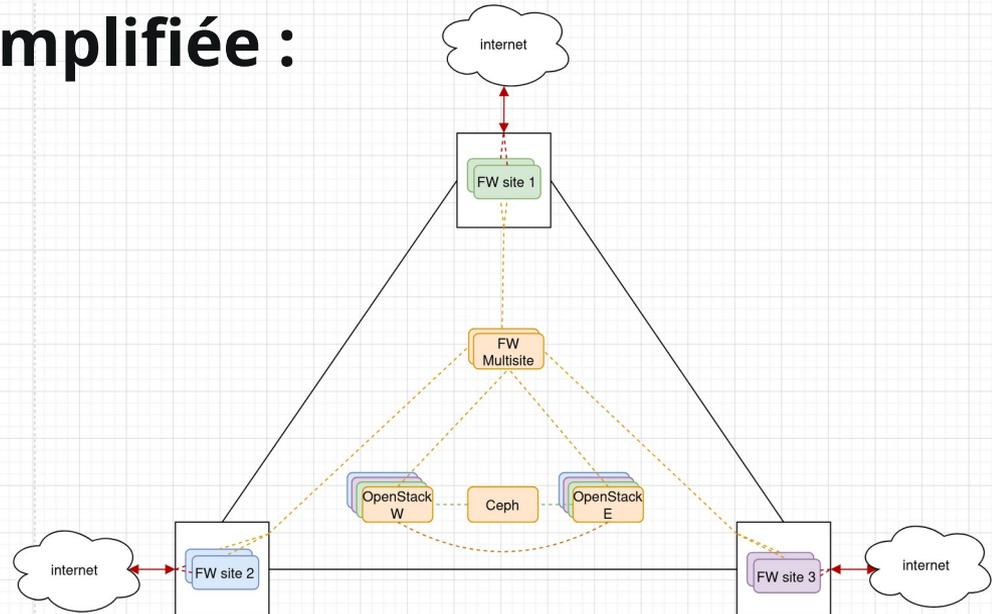
oVirt



Dans un monde idéal



En une vue extrêmement simplifiée :





Versus la réalité

Checklist :

- 3 Centres de données
- 3 lignes Internet
- Un lien MAN entre les sites
- Ensemble d'IP publique (BGP)
- Des parefeux
- Des commutateurs
- Des serveurs
- Une solution de stockage
- Une solution de virtualisation
- Une solution de cloud
- Une solution de conteneurs
- Des liens VPN
- Etc.



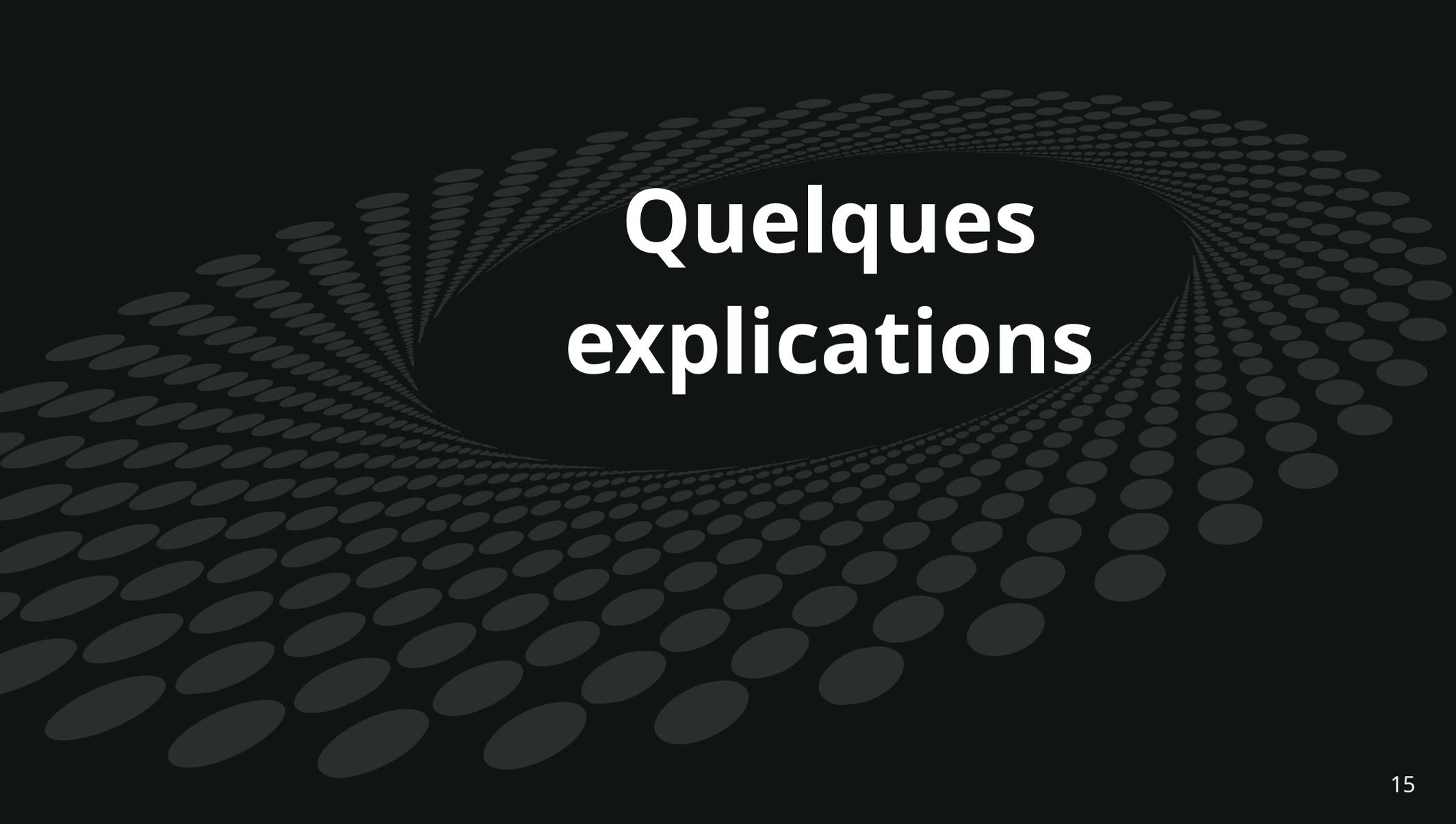
Checklist dans W'opla

- 3 Centres de données
- 3 lignes Internet
- Un lien MAN entre les sites
- Ensemble d'IP publique (BGP)
- Des parefeux ✓
- Des commutateurs
- Des serveurs ✓
- Une solution de stockage ✓
- Une solution de supervision ✓
- Une solution de virtualisation ✓
- Une solution de cloud ✓
- Une solution de conteneurs ✓
- Des liens VPN ✓



Ce qui n'a pas fonctionné out of box :

- 3 Centres de données ✓
- 3 lignes Internet ✓
- Un lien MAN entre les sites ✓
- Ensemble d'IP publique (BGP) ✓
- Des parefeux ✓
- Des commutateurs ✓
- Des serveurs ✓
- Une solution de stockage ✓
- Une solution de supervision
- Une solution de virtualisation ✓
- Une solution de cloud ✓
- Une solution de conteneurs ✓
- Des liens VPN



Quelques explications

Petits contretemps :

- 3 centres de données
 - Livraison rapide
 - Accès plus compliqué
- 3 lignes Internet
 - Ligne opérationnelle
 - Débit 1G au lieu de 10G à la livraison
 - Correction en deux semaines
- Un lien MAN entre les sites
 - Arrivé au centre de données
 - Pas dans la baie



Connectivité :

- Ensemble d'IPs publiques (BGP)
- Comprendre le monde du telco
- BGP que sur un seul site ????
- Faire fonctionner avec un parefeu pour le BGP
- Serveur d'annonce différent
- Ouverture de flux non documentée

Temps passé : 3 semaines pleines



Le monde magique des parefeux :

- Des parefeux physiques :
 - Le BGP on ne va pas en reparler
 - Interface 10G pas reconnue sous BSD
- Des parefeux virtualisés :
 - Interface Virtio bridée
 - Lien 10G/s plafonne à 2G/s



Le matériel :

- Des commutateurs
 - Livraison sur le mauvais site
 - Mauvaise connectivité
 - Inversion de câblage entre deux centres de données
- Des serveurs
 - BIOS configuré à l'heure française mais sur le fuseau horaire UTC
 - Des cartes de contrôle à distance qui se bloquent (obligé d'aller en DC)
- Une solution de stockage
 - Jbod pour les disques impossible,
 - RAID 0 pour chaque disque



Logiciel :

- Une solution de stockage
 - Changement de version de ceph durant le projet
 - Incompatibilité avec les autres composants
- Une solution de virtualisation
 - Bugs dans l'installateur d'Ovirt
 - Fin de CentOS 8 Stream
- Une solution de cloud
 - Disparition du projet Tripleo
 - Passage à Kayobe rapide
- Une solution de conteneurs
 - Okd ne supporte plus Ovirt
 - Passage à Kubernetes pour le core





Au final

Tout est bien qui finit bien !

 VaaS



Tout est bien qui finit bien

Automatisation du déploiement, de rien à une architecture sur trois sites :

- Configuration des switches
- Configuration des serveurs physiques via la carte de management
- Configuration des firewalls
- Configuration de Ceph
- Installation d'Ovirt et configuration
- Déploiement des premières Vms
- Déploiement des Openstacks (et oui, il n'y en a pas qu'un)
- Retrait des configurations temporaires du déploiement
- Supervision et autres plaisirs...



Quelques tests pour valider

	Test
Perte Connexion Internet	Ok
Bascule BGP	Ok
Perte Firewall Site 1	Ok
Perte Firewall Site 2	Ok
Perte Firewall Site 3	Ok
Perte un nœud Ovirt	Ok
Perte un nœud Ceph	Ok
Perte d'un lien MAN	Ok
Perte de Switch	Ok
Shutdown port au hasard (hors MAN)	Ok
Shutdown d'un port MAN	Ok
Bascule CARP	Ok
Bascule des Firewalls Virtuels	Ok
Arrêt forcé des FW Virtuels	Ok
Arrêt Contrôleur Openstack 1	Ok
Arrêt Contrôleur Openstack 2	Ok
Arrêt Compute Openstack 1	Ok
Arrêt Compute Openstack 2	Ok



Quelques cas critiques ?!

	Test	Commentaire
Attaque de Godzilla sur un site	Ok	On a des sauvegardes sur un autre site
Notre fournisseur perd internet	Ok	On a des liens de secours et des automates de bascule DNS
Une pelleteuse coupe un lien MAN	Ok	On a déjà eu l'occasion de le tester

Retrouvez-nous au stand B13

- Rencontrez nos experts, nos clients et nos partenaires
- Assistez à plusieurs mini-conférences
- Et bien d'autres surprises à découvrir sur place !



Membre fondateur du groupement



Retrouvez les au stand B15 !



www.worteks.com

✉ info@worteks.com

☎ +33 1 84 20 86 47

🌐 [worteks_com](https://www.worteks.com)

📱 [worteks](#)

Merci