

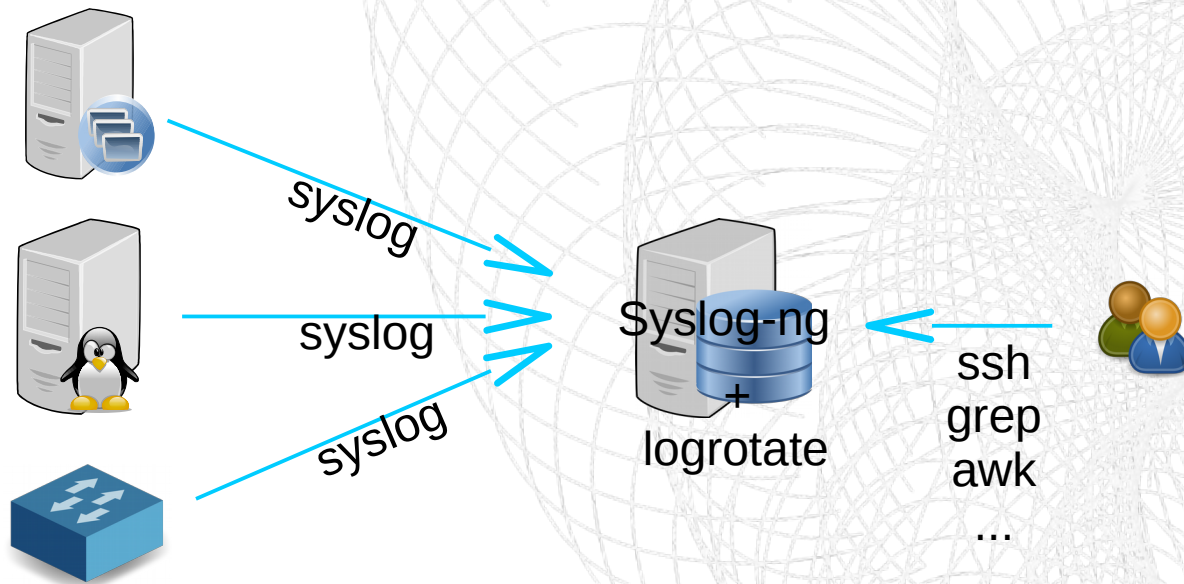
Utilisation des logs à l'INSA de Toulouse

HIER
AUJOURD'HUI
DEMAIN..



Contexte INSA

- ~ 250 serveurs
- ~ 200 équipements réseaux
- Infra (5)
- Support (10)



Objectifs

► Équipe Infrastructure :

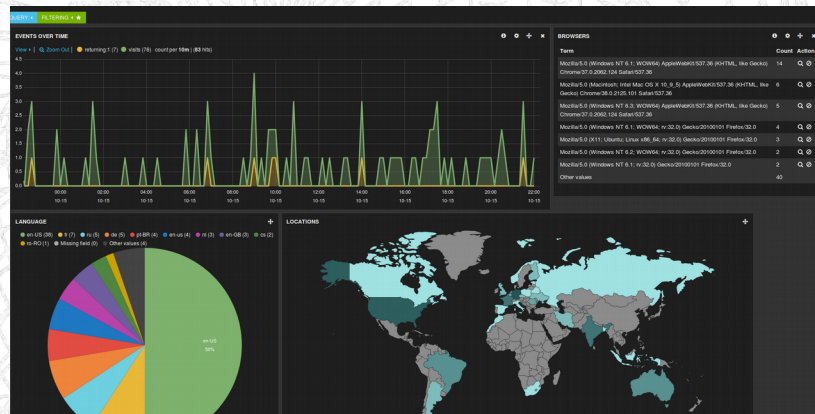
- Exploiter toutes les informations collectées
- Faciliter les opérations d'exploitation
 - Recherches sur incident
 - Évaluation/Analyse des tendances
- Capitaliser la connaissance « métier/applicative » des équipes
- Pas d'usine à gaz....

► Équipe Support :

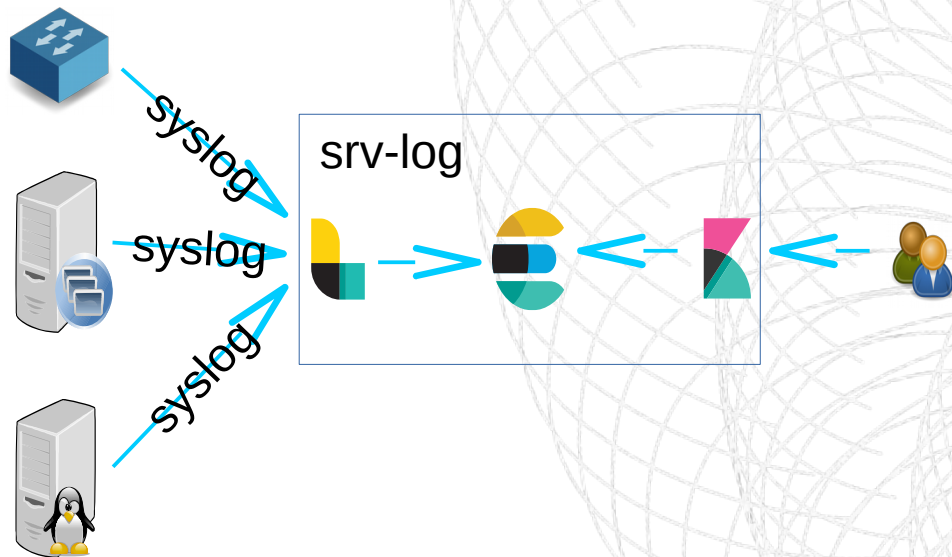
- Simplifier l'accès à l'information
- Disposer d'un outil supplémentaire d'aide au diagnostic
- Améliorer la qualité du diagnostic



La solution à tous nos besoins (En théorie...)



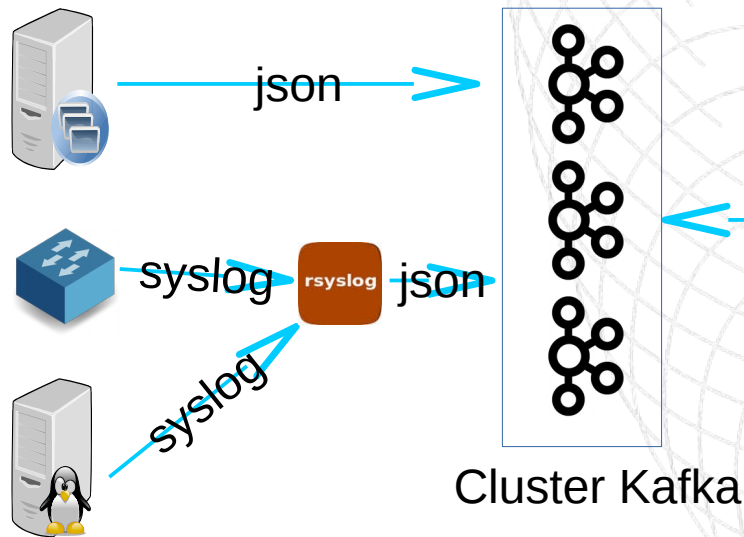
La solution (Implémentation...V1)



L'heure des « mauvais » choix :

- ▶ Logstash
 - Collecteur syslog
 - Stockage en mode fichier
- ▶ Elasticsearch
 - Performances
 - Exploitation
- ▶ Kibana :
 - Sauvegardes !!!

La solution (Implémentation....Vxxxxxxxxxxxxxx)



L'heure des « bons » choix ?

- ▶ rsyslog
 - Stockage en mode fichier
 - Forwarder kafka [omkafka]
- ▶ Kafka
 - Broker de message
 - Apache Zookeeper
 - Producers / Topics / ConsumerGroup
- ▶ Logstash
 - Grok / mutate / geoip
- ▶ Elasticsearch
 - Templates logstash
 - Curator
- ▶ Kibana :
 - Valeur pivots

Bilan

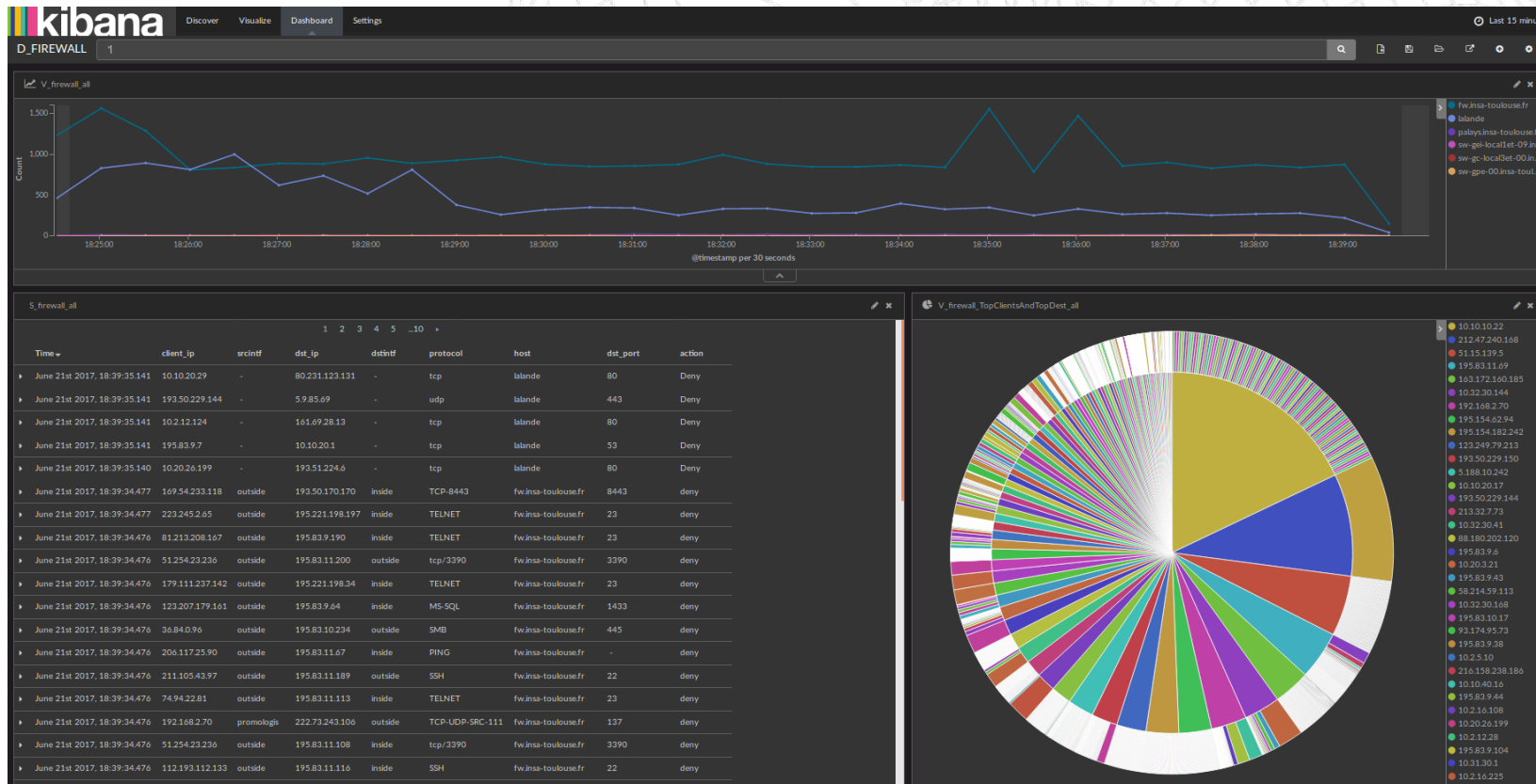
▶ Aujourd'hui

- Outil devenu incontournable au quotidien
- Permet le partage de l'information/connaissance
- Outil demandant un gros investissement notamment pour générer des graphes/tableaux de bords pertinents/utiles.

▶ Demain :

- Augmentation du volume de données traité
- Utilisation des outils Beats [Producer Kafka]:
 - PacketBeat / etc..
- Module X-Pack
 - Sécurité
 - Machine learning





Rappelez vous
surtout pas d'usine à gaz !!!

