Retour d'expérience
Mise en place d'un PRA informatique
Délégation Rhône-Auvergne du CNRS

7-8 juin 2022

Journées Proxmox VE & Ceph

Action Audaces & Aramis

PRA PRI ? PCA PCI ? De quoi parlons-nous ?

- Le « i » est important
  - Il s'agit bien ici de Plan de Reprise Informatique ou de Plan de Continuité Informatique
  - Il est un sous-ensemble du Plan de Continuité d'Activité définit par la norme ISO 22301
    - En lecture gracieuse ici : https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:fr
- Définitions et distinction
  - Plan de continuité d'activité (informatique) PCI selon Wikipedia

  « En informatique, un plan de continuité d'activité (PCA), a pour but de garantir la survie de l'entreprise en cas de sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise. »
  - Plan de reprise d'activité (informatique) PRI selon Wikipedia

  « Un plan de reprise d'activité (PRA) est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permettent à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique. »

  D'après Matthieu Bennasar, Plan de Continuité d'Activité et système d'information : vers l'entreprise résiliente, Paris, Dunod, 2006, 266 p. (ISBN 2-10-049603-4), p. 26
- Distinction ténue… nécessite des mises à jour ?

Définitions que nous aimons bien…

PCA PRA PCI PRI et PCC… de quoi s'agit-il ?!! Pierre MRABET sur LinkedIn

- PCA : Haute disponibilité de la production

  « Le Plan de Continuité d'Activité (PCA) définit pour l'entreprise les architectures, les moyens et les procédures nécessaires pour assurer une continuité de son activité. En cas d'incidents, de toute taille et toute nature, l'activité des métiers n'est pas interrompue […] »

- PRA : Reprise en cas de sinistre

  « Organisation palliative en cas d'absence de PCA, ou élément complémentaire du PCA, le Plan de Reprise d'Activité (PRA) est l'ensemble des processus qui permettent de repartir après un sinistre. Bien souvent sont définis des modes dégradés qui permettent à l'entreprise de redémarrer son activité, dans des locaux de transition, avec des solutions de gestion manuelles. […] La priorité est de faire repartir les moyens de production ou de service pour reprendre le service client au plus vite et ne pas entraîner d'impacts commerciaux préjudiciables pour la société. »

- PCI et PRI : Pour les informaticiens

  Les DSI doivent à leur niveau assurer une mise en œuvre de Plan de continuité et de reprise d'activité informatique.

  - *Recovery Time Objective (RTO) qui correspond à la "durée nécessaire à une « remise en production " d'un environnement informatique*
  - *Recovery Point Objective (RPO) qui correspond à la période de données non récupérables, sont parmi les principaux indicateurs.*

- L'amalgame de terminologie est souvent fait entre métiers et DSI. PRA et PCA sont utilisés par tous.

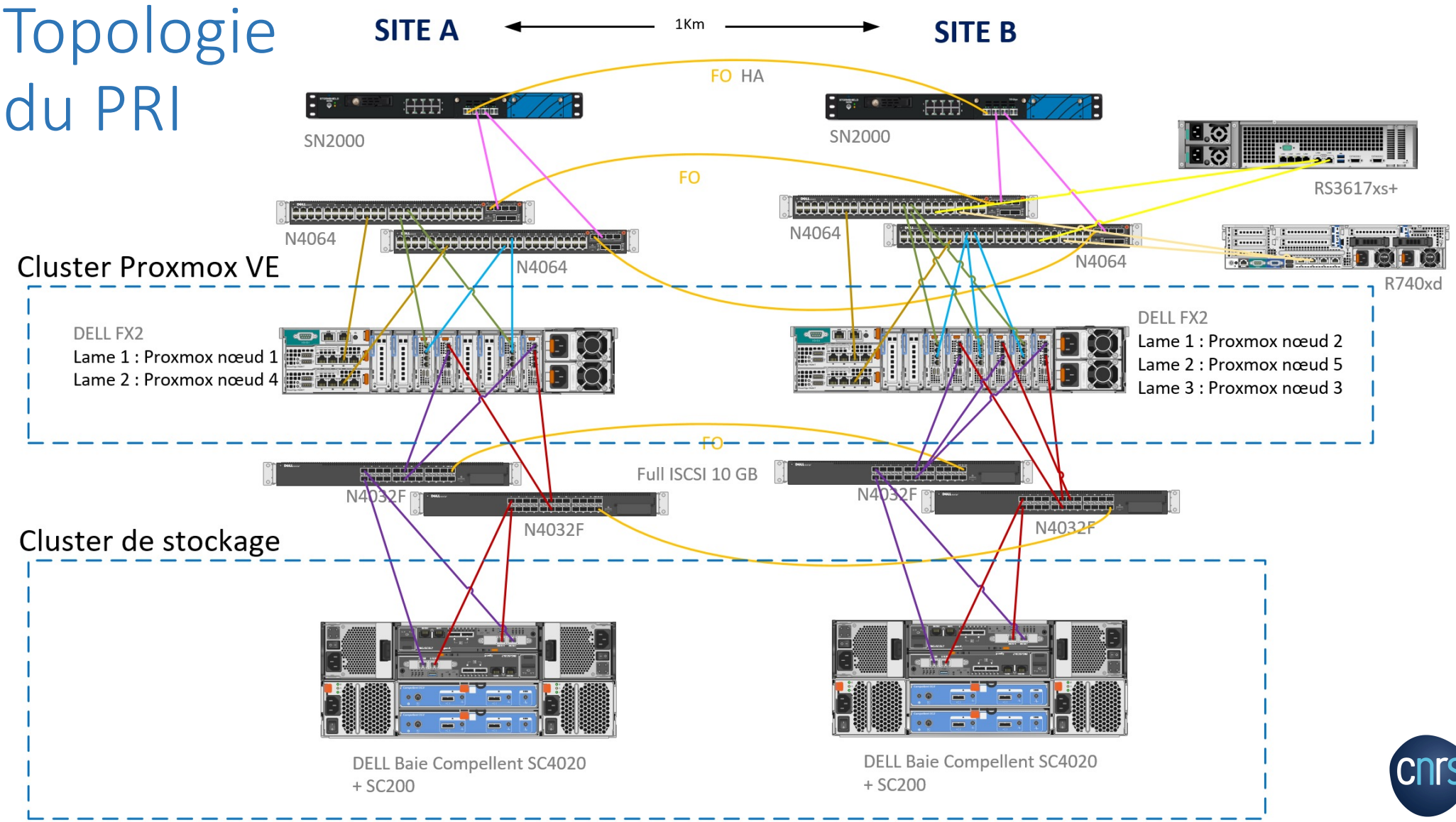
  « Il y a bien une distinction entre les périmètres de responsabilité des métiers et de la DSI. Trop souvent dans entreprises la mise en œuvre d'un PCA et PRA avaient été transmis uniquement à la DSI, DSI qui naturellement et de bonne foi réduisait à son stricte périmètre de responsabilité son étude et mise en œuvre de plans ! »

Contexte et objectifs du ~~PRA~~ PRI de la DR7

« Les 18 délégations en région assurent une gestion directe et locale des laboratoires et entretiennent les liens avec les partenaires locaux et les collectivités territoriales. »
https://www.cnrs.fr/fr/delegations-regionales-du-cnrs

- Contexte
  - La Délégation Rhône Auvergne ne ferme (presque) jamais…
  - Indispensable à l'activité des unités
  - Nécessité de maintenir le SI opérationnel
- Objectifs du PRI
  - Tendre vers une continuité de service (PCI)
  - Pouvoir rétablir les services critiques dans les 4 heures (RTO)
  - Pouvoir revenir aux données de la veille dans le pire des cas (RPO)

Topologie du PRI



Éléments du PRI de l'infrastructure 1/2

- 2 salles sur 2 sites distants d'1km
  - Répartition des serveurs entre les 2 sites
    - 1 cluster d'hyperviseurs Proxmox VE version 6.4, 5 nœuds sur 5 lames
      - 2 nœuds sur 2 lames sur site A
      - 3 nœuds sur 3 lames sur site B
      - 1 lame = 2 Socket (40 CPU Proxmox) / 256 Go de RAM
  - Réplication des données entre les 2 sites
    - 1 cluster de 2 baies de stockage Dell Compellent SC4020
    - Réplication des volumes entre les baies : LiveVolume (réplication synchrone)
- 2 Firewall (actif / passif) répartis sur les 2 sites
- 4 Switchs de distribution répartis sur les 2 sites

Éléments du PRA de l'infrastructure 2/2

- Sauvegarde des postes utilisateurs : Atempo
  - Sur un système indépendant des baies de stockage (Dell PE R740xd CentOS 8)
  - 120 postes de sauvegardés, 30To d'espace disponible, https (sauvegardes PC nomades)

- Sauvegarde des serveurs
  - Sur un système indépendant des baies de stockage (Synology RS3617xs+)
  - 80 serveurs, 30To d'espace disponible (12 disques de 3,6To – Raid 6)
  - 2 types de sauvegardes :
    - Sauvegardes applicatives : Active Backup de Synology (RSync)
    - Sauvegardes des VM : depuis PVE

Chronologie mise en place

Installation de 2 nœuds Proxmox

Ajout d'un 2d châssis FX2, d'un nœud au cluster Proxmox et d'une 2de baie de stockage Dell Compellent

Suite à une défaillance du stockage de l'infra => Sauvegardes sur système indépendant (Synology)

Ajout de 2 nœuds Proxmox au cluster Pour un total de 5 nœuds

2014 2015 2016 2018 2019 2022

Mise en place d'un châssis FX2, remplacement des 2 nœuds installés en 2015 et installation d'une baie de stockage Dell Compellent

Migration d'une partie de l'infrastructure vers un second site
Mise en place d'un PRA multi-site
Test PRA suite rénovation salle site A
Ajout de 2 boîtiers d'extensions aux baies Dell Compellent

Et ensuite ?
Renouvellement des baies de stockage : pourquoi pas

ceph

Bilan du PRI : ½ PCI ?

- Mode PCI : presque haute disponibilité

  transparent pour l'utilisateur

  - Les Firewalls
  - Les switchs de distribution
  - Certains services répartis sur plusieurs sites (DNS…)
- Mode « PCI manuel » : ~~haute~~ human disponibilité

  Très rapide si disponibilité d'un ASR (bascule manuelle des VMs impactées)

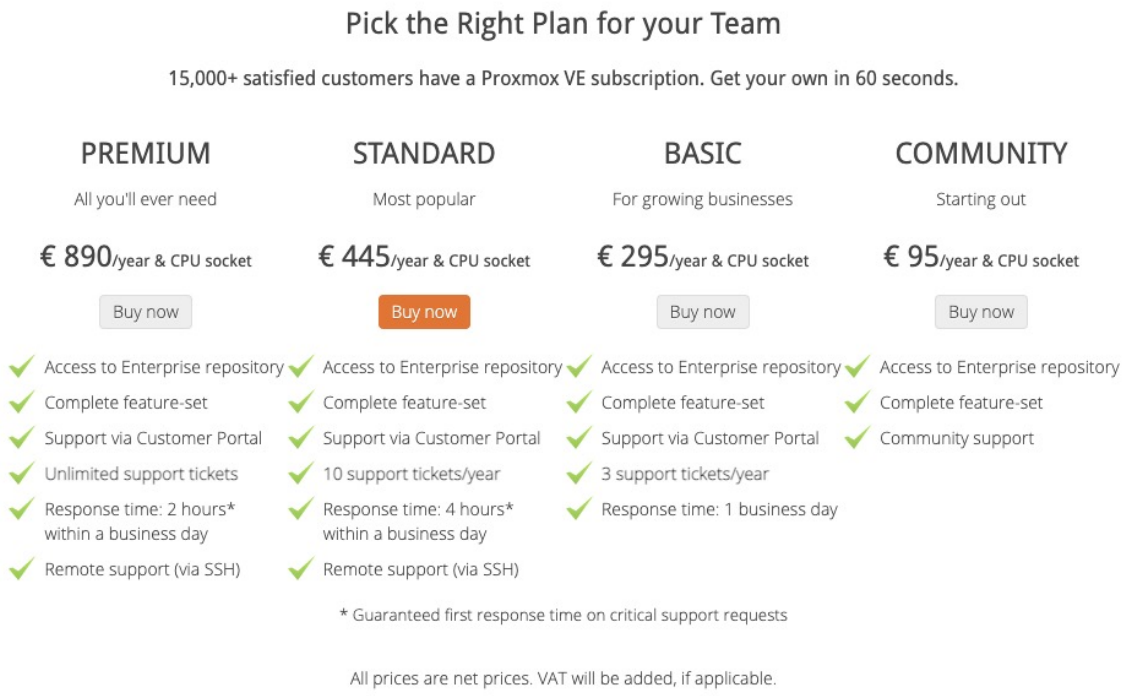
  - Perte d'une ou plusieurs lames
  - Perte d'un FX2
  - Perte d'une baie de stockage (Baies Compellent)
- Mode PRI (cf. objectifs RTO / RPO) : le reste…

Et ensuite…

- **La sortie réseau (pas sur le schéma)**
  - Sur un seul site actuellement… Nécessite un déplacement physique sur le 2d site
  - HA planifiée pour fin 2022 début 2023
- **Déport des sauvegardes sur un 3ème site**
  - Plus loin mais toujours dans Lyon… dans une unité qualifiée…
  - A programmer mais prioritaire depuis la rédaction de cette présentation…
  - Avec un point de vigilance : il faut qu'au moins un ASR survive à la destruction des 2 sites… ce qui n'est pas improbable grâce au télétravail…
- **Réflexion sur le renouvellement de nos baies de stockage**
  - Étude sérieuse programmée à l'issue de ces 2 jours ;-)

Licences Proxmox

- Proxmox VE Basic Subscription
  - 2 Socket /lame
  - 590 €HT /an /lame
  - 2950 €HT /an au total (5 lames - 10 Sockets)
  - Accès aux dépôts « entreprise »
  - Accès à 3 tickets /an



Pick the Right Plan for your Team

15,000+ satisfied customers have a Proxmox VE subscription. Get your own in 60 seconds.

PREMIUM	STANDARD	BASIC	COMMUNITY
All you'll ever need	Most popular	For growing businesses	Starting out
€ 890/year & CPU socket	€ 445/year & CPU socket	€ 295/year & CPU socket	€ 95/year & CPU socket
Buy now	Buy now	Buy now	Buy now
✓ Access to Enterprise repository	✓ Access to Enterprise repository	✓ Access to Enterprise repository	✓ Access to Enterprise repository
✓ Complete feature-set	✓ Complete feature-set	✓ Complete feature-set	✓ Complete feature-set
✓ Support via Customer Portal	✓ Support via Customer Portal	✓ Support via Customer Portal	✓ Community support
✓ Unlimited support tickets	✓ 10 support tickets/year	✓ 3 support tickets/year	
✓ Response time: 2 hours* within a business day	✓ Response time: 4 hours* within a business day	✓ Response time: 1 business day	
✓ Remote support (via SSH)	✓ Remote support (via SSH)		

* Guaranteed first response time on critical support requests

All prices are net prices. VAT will be added, if applicable.

Sortons un peu du cadre technique…

Orienté labos

- **Vous vous rappelez de l'article de Pierre MRABET (plus haut)**

  « Il y a bien une distinction entre les périmètres de responsabilité des métiers et de la DSI.

  Trop souvent dans entreprises la mise en œuvre d'un PCA et PRA avaient été transmis uniquement à la DSI, DSI qui naturellement et de bonne foi réduisait à son stricte périmètre de responsabilité son étude et mise en œuvre de plans ! »

- **Un PCI n'est pas un PCA**

- **Le PCI est un sous-ensemble du PCA**

Les normes, les méthodes, les……

- **Nous n'en manquons pas (morceaux choisis)**
  - ISO 22301 2019 (et 22300) en accès libre https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:fr

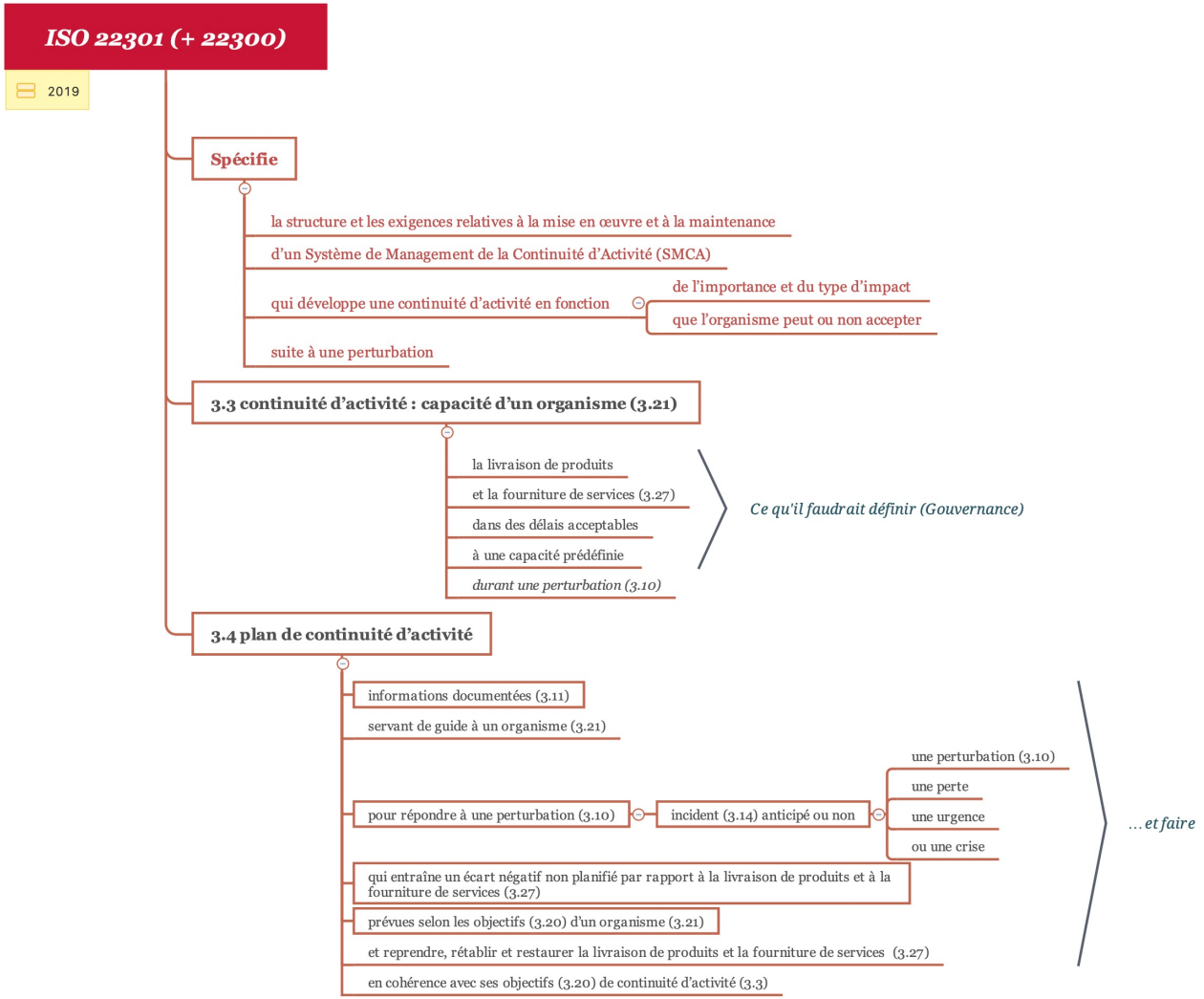
    « Le présent document spécifie la structure et les exigences relatives à la mise en œuvre et à la maintenance d'un Système de Management de la Continuité d'Activité (SMCA) qui développe une continuité d'activité en fonction de l'importance et du type d'impact que l'organisme peut ou non accepter suite à une perturbation. »
  - La PSSI de l'Etat https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/

    Objectif 33 : gestion de la continuité d'activité : se doter de plans de continuité d'activité, et les tester.

    « PCA-LOCAL : définition du plan local de continuité d'activité des systèmes d'information.

    Le directeur des systèmes d'information ou le RSSI d'une entité définit la structure et les attendus du plan de continuité d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité. »
  - Guide pour réaliser un plan de continuité d'activité http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

    Secrétariat général de la défense et de la sécurité nationale
  - Les guides de l'ANSSI
    - Guide Hygiène Informatique
    - ANSSI Guide Cartographie des SI 2018 v1
  - Un doigt d'EBIOS ?


ISO 22301 (+ 22300)
2019
Spécifie
la structure et les exigences relatives à la mise en œuvre et à la maintenance
d'un Système de Management de la Continuité d'Activité (SMCA)
qui développe une continuité d'activité en fonction
de l'importance et du type d'impact
que l'organisme peut ou non accepter
suite à une perturbation
3.3 continuité d'activité : capacité d'un organisme (3.21)
la livraison de produits
et la fourniture de services (3.27)
dans des délais acceptables
à une capacité prédéfinie
durant une perturbation (3.10)
Ce qu'il faudrait définir (Gouvernance)
3.4 plan de continuité d'activité
informations documentées (3.11)
servant de guide à un organisme (3.21)
pour répondre à une perturbation (3.10)
incident (3.14) anticipé ou non
une perturbation (3.10)
une perte
une urgence
ou une crise
qui entraîne un écart négatif non planifié par rapport à la livraison de produits et à la fourniture de services (3.27)
prévues selon les objectifs (3.20) d'un organisme (3.21)
et reprendre, rétablir et restaurer la livraison de produits et la fourniture de services (3.27)
en cohérence avec ses objectifs (3.20) de continuité d'activité (3.3)
...et faire

Au secours…

- **Par où commencer ?**
  - Plusieurs centaines de pages…
  - Quelle approche…
- **RETEX terrain**
  - Hum… compliqué
  - Toujours quelques trous dans la raquette ? (En fait on a pas les cordes…)
  - J'ai un truc qui tombe… Je le relance… J'ai des backups… (hum…)

~~Evènements redoutés, menaces, risques…~~

Nos ennemis

Le TEMPS & les RH euh… c'est pas lié ? Pas toujours ;-)

Quelques réflexions…

Orienté labos (et DRs…)

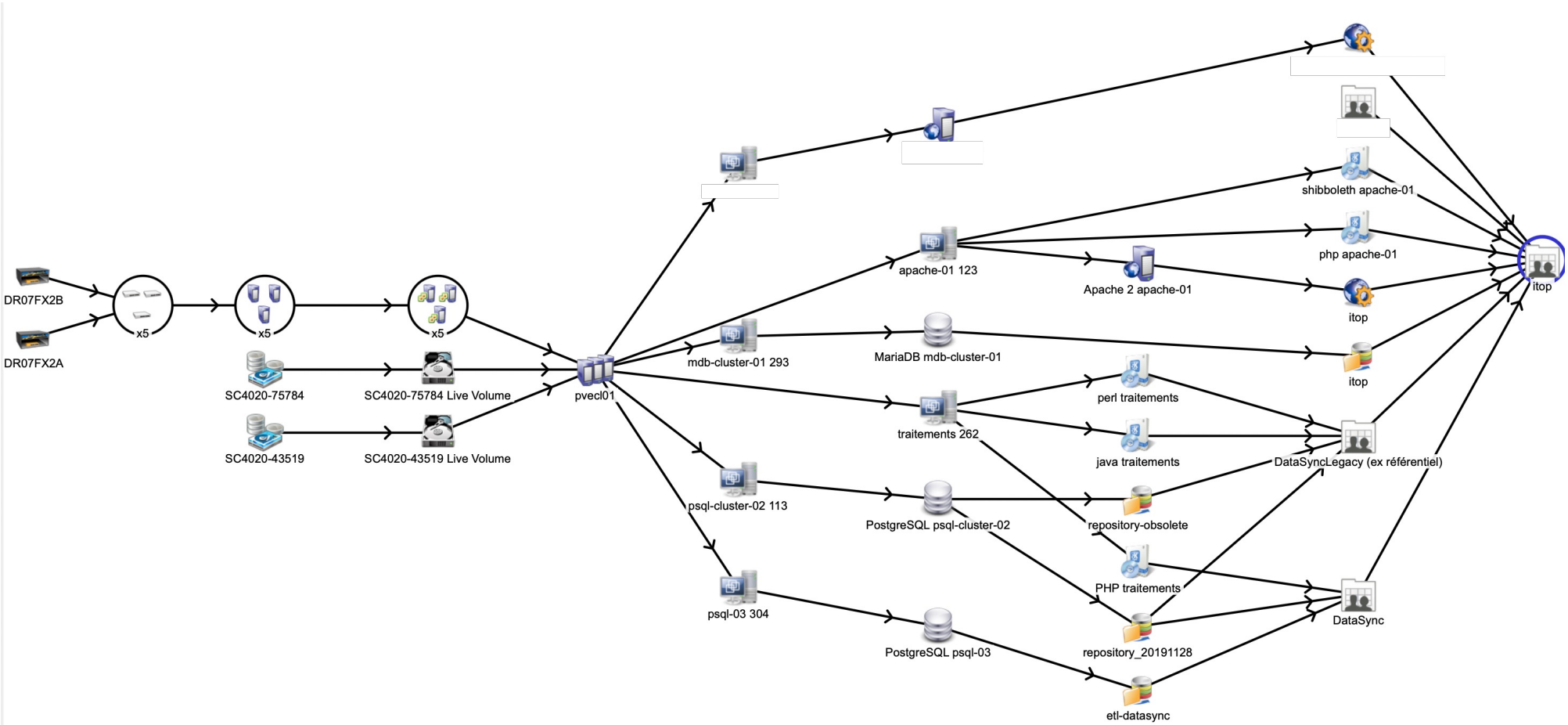
- **Le PCA est de la responsabilité de la Gouvernance**
  - … Mais vous pouvez poser la question ?
  - Patron(ne), que souhaiteriez-vous conserver en cas de destruction du labo ?
  - Nous pouvons donc nous concentrer ensuite sur le PCI
- **Le PCI relève de la nôtre**
  - Quelles briques du SI devez-vous conserver en cas de destruction du labo ?
    - Considérez qu'il va renaitre de ses cendres ailleurs…
    - Et que le SI est probablement une brique ~~importante~~ critique…
- **Une bonne blague ?**

Mendel 2019…

Le kit de survie (KISS)

Orienté labos (et DRs…)

- **Connais~~-toi~~ ton SI toi-même : documenter le SI**
  - Prendre le temps pour ça…
  - Vous ne devez pas ignorer l'inventaire…
  - Utilisez ITIL (les bonnes pratiques qui vous intéressent…)
  - Connaissez-vous iTop ? (https://www.combodo.com/itop)
- **A la DR7**
  - La CMDB
  - Les changements
  - Le service support…
  - L'adressage IP…
  - Et plus…


DR07FX2B
DR07FX2A
x5
x5
x5
SC4020-75784
SC4020-75784 Live Volume
SC4020-43519
SC4020-43519 Live Volume
pvecl01
mdb-cluster-01 293
psql-cluster-02 113
psql-03 304
apache-01 123
MariaDB mdb-cluster-01
traitements 262
PostgreSQL psql-cluster-02
PostgreSQL psql-03
shibboleth apache-01
php apache-01
Apache 2 apache-01
itop
itop
perl traitements
java traitements
repository-obsolete
PHP traitements
repository_20191128
etl-datasync
DataSyncLegacy (ex référentiel)
DataSync
itop

Le kit de survie : approche bottom-up

Orienté labos (et DRs…)

- **Votre SI est documenté**
  - Les sauvegardes ?
  - Et les utilisateurs / manips ?
  - Un autre site ?
  - Possible de relancer les services ?
- **Je respire, j'ai les bases… sûr ?**
  - Avez-vous redondé les RH ?
  - Le sinistre majeur est plus rare que :
    - La mutation (les NOEMIES)…
    - La promotion…
    - Les CDD…
- **J'oubliais… nous avons les bases ?**

Nous sommes prêts pour les normes et méthodes

SOS Tutelles… en guise de conclusion

Le CNRS dispose

- **D'un PCA**
- **De plusieurs cellules de crise… dont une par DR**