D'une infrastructure à l'ancienne vers des clouds institutionnels

L. Azema, D. Delavennat, P. Depouilly, D. Ferney, R. Theron

Marseille - Mai 2022

mathrice

jres MARSEILLE 2022

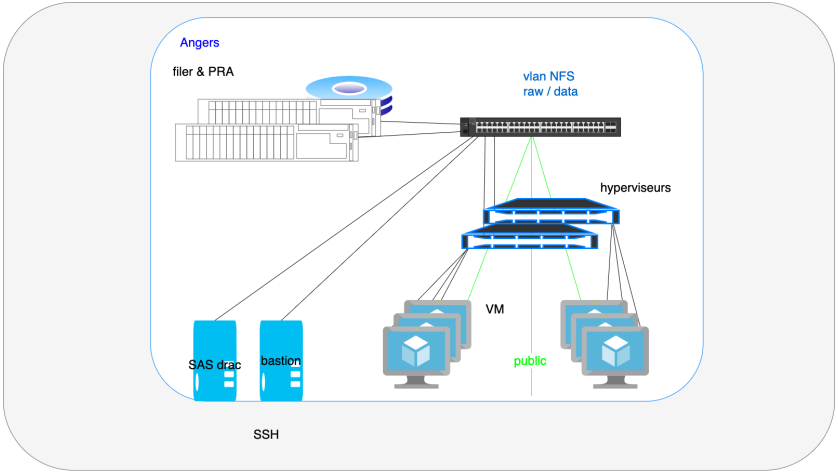
Mathrice

- Mathrice : réseau thématique du CNRS rattaché à l'INSMI[1]
- PLM : Plateforme en Ligne pour les Mathématiques
- PLMteam : 12 mathriciens en charge de l'exploitation de la PLM

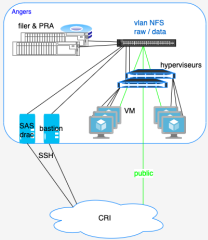
Présentations : Jres2013, Jres2015

[1] Institut National des Sciences Mathématiques et de leurs Interactions du CNRS

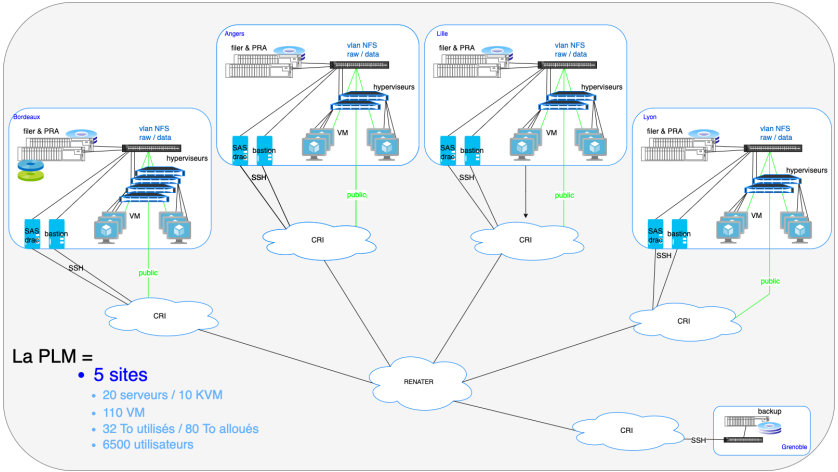
Infrastructure Historique de la PLM



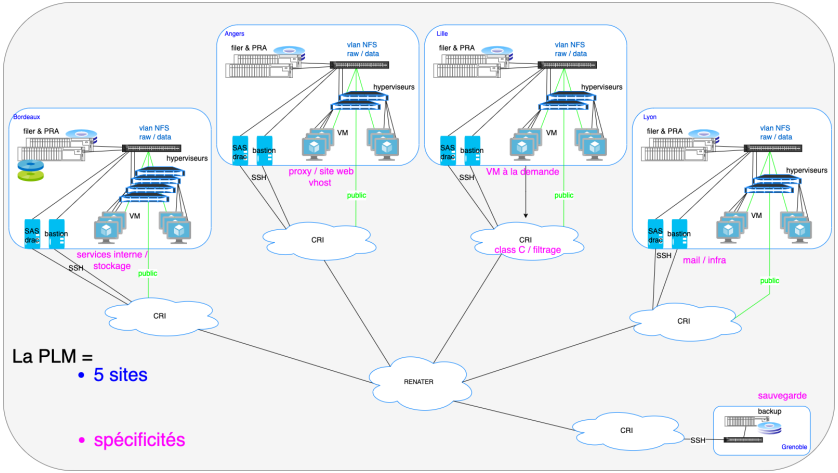
Infrastructure Historique de la PLM



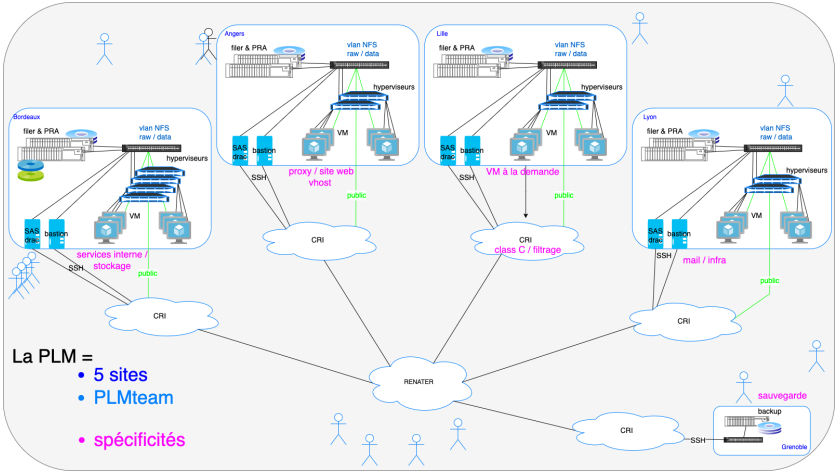
Infrastructure Historique de la PLM



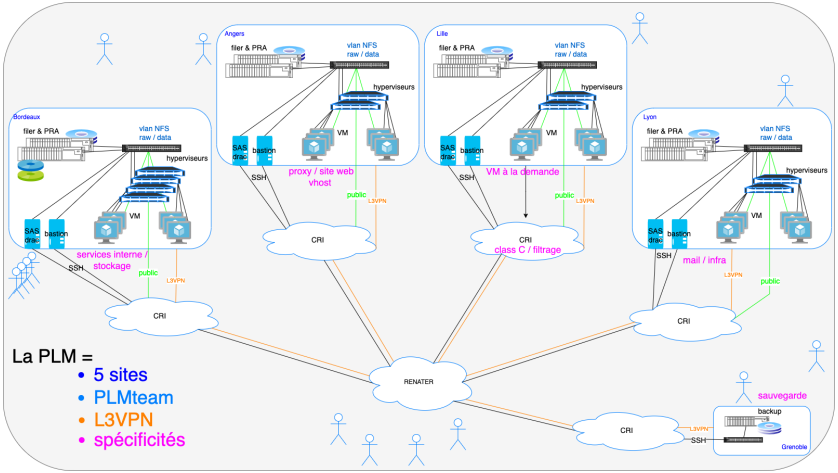
Infrastructure Historique de la PLM



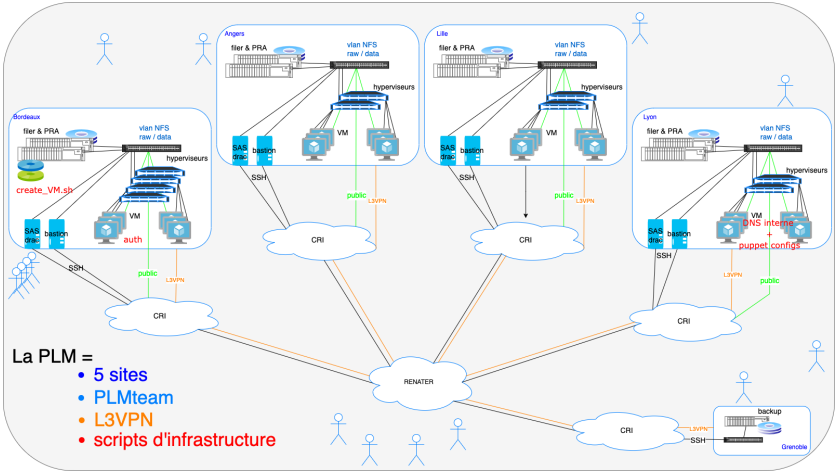
Infrastructure Historique de la PLM



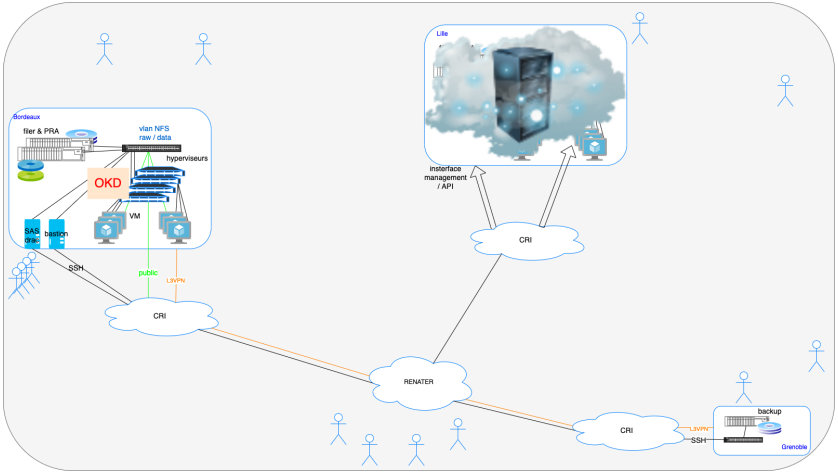
Infrastructure Historique de la PLM



Infrastructure Historique de la PLM



Infrastructure Historique de la PLM



simplifier et sécuriser la PLM :
Plateforme-**a**s-**a**-**S**ervice / **I**nfrastructure-**a**s-**a**-**S**ervice :

Le contexte

La PLM dans les Nuages

Évolution de la PLM

Pourquoi

- utiliser un hébergement efficient
- se décharger de l'administration de l'infrastructure physique
- s'approprier une démarche DevOps à travers l'*Infrastructure-as-Code*.
- dissocier le déploiement applicatif de celui de l'infrastructure
- intégrer de nouvelles recrues, susciter des vocations

Pourquoi

- utiliser un hébergement efficient
- se décharger de l'administration de l'infrastructure physique
- s'approprier une démarche DevOps à travers l'*Infrastructure-as-Code*.
- dissocier le déploiement applicatif de celui de l'infrastructure
- intégrer de nouvelles recrues, susciter des vocations

Pourquoi

- utiliser un hébergement efficient
- se décharger de l'administration de l'infrastructure physique
- s'approprier une démarche DevOps à travers l'*Infrastructure-as-Code*.
- dissocier le déploiement applicatif de celui de l'infrastructure
- intégrer de nouvelles recrues, susciter des vocations

Pourquoi

- utiliser un hébergement efficient
- se décharger de l'administration de l'infrastructure physique
- s'approprier une démarche DevOps à travers l'*Infrastructure-as-Code*.
- dissocier le déploiement applicatif de celui de l'infrastructure
- intégrer de nouvelles recrues, susciter des vocations

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2] BBB une réponse à l'explosion des besoins en visioconférence? — Jeudi 11:00 — IRE522

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2] BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2]BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2] BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2]BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2]BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Quand - 2020(!)

- renouvellement quinquénal, recherche d'hébergeurs potentiels
- Covid =
  - utilisation des services distants en forte hausse
  - déploiement de nouveaux services codimd, rocketchat, BigBlueButton[2]
  - instanciation personnalisée de services pour des groupes (ModCov19)
  - redondance entre plusieurs sites pour sécuriser le fonctionnement
  - reliquats exceptionnels
- projet PIA3 autour de la science ouverte
  avec Mathrice, groupe Calcul, Virtualdata et Gricad

[2]BBB une réponse à l'explosion des besoins en visioconférence? - Jeudi 11:00 - JRES22

Où

critères : sites institutionnels, cloud recherche, redondance, résilience

- GRICAD
  - Gricad-Nova (*OpenStack*)
  - WINTER (*VMware vSphere*)
  - SUMMER (*NetApp*)
- IJClab
  - Virtualdata (*OpenStack*)
- RENATER (*VMware VMRA*)

Combien

- faire l'inventaire des ressources utilisées.
- déterminer les besoins à venir :

Site	Coeurs	Mémoire	Stockage	FIP Max
Gricad-Nova	576	2,3To	53To	512
Gricad-Winter /Summer	20	28Go	10To	/
Virtualdata	512	1To	64To	256

Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

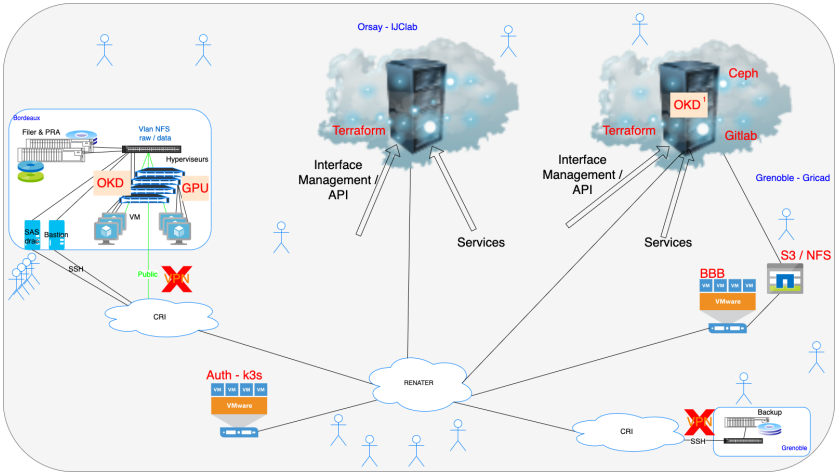
Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

Comment

- trouver la bonne adéquation :
  - mode de financement (investissement / fonctionnement)
  - contrat d'hébergement
  - relationnel (contacts privilégiés, authentifications locales, cohabitation difficile de plusieurs systèmes de tickets , ...)
- adapter la PLM aux choix d'architecture et d'implémentation :
  - différents modes de configuration du réseau :
    - *Linux Bridge* / *Open vSwitch* (problème *arp responder*)
    - adressage direct / *Floating IP*
  - étendre l'interconnexion des sites :
    - *Cisco ACI* : difficile de transporter le L3VPN
    - *Wireguard* : filtrage de l'UDP, *antispoofing* d'*OpenStack*
    - réseau interne partagé entre projets *OpenStack* contourne le modèle de sécurité par défaut.
  - se restreindre aux gabarits de VM proposés

Nouvelle architecture



[3] Tuto PaaS - jeudi 08:40 - JRES22

Nouveau paradigme de configuration : Infrastructure-as-Code

- nouveaux outils : CLI *OpenStack*, *terraform*, *packer*, *consul-template*, *task*, *direnv*, *asdf*...
- *gitlab* devient LE référentiel de la configuration
  - découpage en objets : VM avec ses services, projet avec ses ressources, image système, déploiement de plateforme
  - équipés de constructeur et provisionneur (paramétrés par variables d'environnement)
  - paramétrage aux niveaux sites, projets et VM ou services
- richesse de l'outil *gitlab* :
  - ensembles versionnés de fichiers de configuration
  - gestion des contributions et des droits
  - registres d'images de conteneur, d'états d'infrastructure, de paquets
  - publication de la documentation utilisateurs
  - ouverture des codes avec des dépôts publics archivés par *software heritage*
- gestion des secrets, partage de paramètres et annonce de services : *vault* et *consul*

Nouveau paradigme de configuration : Infrastructure-as-Code

- nouveaux outils : CLI *OpenStack*, *terraform*, *packer*, *consul-template*, *task*, *direnv*, *asdf*...
- *gitlab* devient LE référentiel de la configuration
  - découpage en objets : VM avec ses services, projet avec ses ressources, image système, déploiement de plateforme
  - équipés de constructeur et provisionneur (paramétrés par variables d'environnement)
  - paramétrage aux niveaux sites, projets et VM ou services
- richesse de l'outil *gitlab* :
  - ensembles versionnés de fichiers de configuration
  - gestion des contributions et des droits
  - registres d'images de conteneur, d'états d'infrastructure, de paquets
  - publication de la documentation utilisateurs
  - ouverture des codes avec des dépôts publics archivés par *software heritage*
- gestion des secrets, partage de paramètres et annonce de services : *vault* et *consul*

Nouveau paradigme de configuration : Infrastructure-as-Code

- nouveaux outils : CLI *OpenStack*, *terraform*, *packer*, *consul-template*, *task*, *direnv*, *asdf*...
- *gitlab* devient LE référentiel de la configuration
  - découpage en objets : VM avec ses services, projet avec ses ressources, image système, déploiement de plateforme
  - équipés de constructeur et provisionneur (paramétrés par variables d'environnement)
  - paramétrage aux niveaux sites, projets et VM ou services
- richesse de l'outil *gitlab* :
  - ensembles versionnés de fichiers de configuration
  - gestion des contributions et des droits
  - registres d'images de conteneur, d'états d'infrastructure, de paquets
  - publication de la documentation utilisateurs
  - ouverture des codes avec des dépôts publics archivés par *software heritage*
- gestion des secrets, partage de paramètres et annonce de services : *vault* et *consul*

Nouveau paradigme de configuration : Infrastructure-as-Code

- nouveaux outils : CLI *OpenStack*, *terraform*, *packer*, *consul-template*, *task*, *direnv*, *asdf*...
- *gitlab* devient LE référentiel de la configuration
  - découpage en objets : VM avec ses services, projet avec ses ressources, image système, déploiement de plateforme
  - équipés de constructeur et provisionneur (paramétrés par variables d'environnement)
  - paramétrage aux niveaux sites, projets et VM ou services
- richesse de l'outil *gitlab* :
  - ensembles versionnés de fichiers de configuration
  - gestion des contributions et des droits
  - registres d'images de conteneur, d'états d'infrastructure, de paquets
  - publication de la documentation utilisateurs
  - ouverture des codes avec des dépôts publics archivés par *software heritage*
- gestion des secrets, partage de paramètres et annonce de services : *vault* et *consul*

Bilan

- distance avec la couche physique
- abstraction de la configuration de la PLM
  - généricité / portabilité / isolation des projets / admin autonome / code ouvert
- élasticité de la configuration de la PLM
  - reproductibilité / maquettage / adaptation à la charge / agilité
- efficience énergétique de l'hébergement
  - quelle mesure de l'efficacité globale de la PLM ?
- arrivée de nouveaux collègues dans la PLMteam
- ANF : "Infrastructure, plate-forme ou application en tant que service, quels choix technologiques pour les ASR de laboratoire ?" 20-25 Nov 2022, CIRM - Marseille

Bilan

- distance avec la couche physique
- abstraction de la configuration de la PLM
  - généricité / portabilité / isolation des projets / admin autonome / code ouvert
- élasticité de la configuration de la PLM
  - reproductibilité / maquettage / adaptation à la charge / agilité
- efficience énergétique de l'hébergement
  - quelle mesure de l'efficacité globale de la PLM ?
- arrivée de nouveaux collègues dans la PLMteam
- ANF : "Infrastructure, plate-forme ou application en tant que service, quels choix technologiques pour les ASR de laboratoire ?" 20-25 Nov 2022, CIRM - Marseille

Bilan

- distance avec la couche physique
- abstraction de la configuration de la PLM
  - généricité / portabilité / isolation des projets / admin autonome / code ouvert
- élasticité de la configuration de la PLM
  - reproductibilité / maquettage / adaptation à la charge / agilité
- efficience énergétique de l'hébergement
  - quelle mesure de l'efficacité globale de la PLM ?
- arrivée de nouveaux collègues dans la PLMteam
- ANF : "Infrastructure, plate-forme ou application en tant que service, quels choix technologiques pour les ASR de laboratoire ?" 20-25 Nov 2022, CIRM - Marseille

Bilan

- distance avec la couche physique
- abstraction de la configuration de la PLM
  - généricité / portabilité / isolation des projets / admin autonome / code ouvert
- élasticité de la configuration de la PLM
  - reproductibilité / maquettage / adaptation à la charge / agilité
- efficience énergétique de l'hébergement
  - quelle mesure de l'efficacité globale de la PLM ?
- arrivée de nouveaux collègues dans la PLMteam
- ANF : "Infrastructure, plate-forme ou application en tant que service, quels choix technologiques pour les ASR de laboratoire ?" 20-25 Nov 2022, CIRM - Marseille

Bilan

- distance avec la couche physique
- abstraction de la configuration de la PLM
  - généricité / portabilité / isolation des projets / admin autonome / code ouvert
- élasticité de la configuration de la PLM
  - reproductibilité / maquettage / adaptation à la charge / agilité
- efficience énergétique de l'hébergement
  - quelle mesure de l'efficacité globale de la PLM ?
- arrivée de nouveaux collègues dans la PLMteam
- ANF : "Infrastructure, plate-forme ou application en tant que service, quels choix technologiques pour les ASR de laboratoire ?" 20-25 Nov 2022, CIRM - Marseille

Questions ?

Merci de votre attention!