
Fiche technique AgroDataRing

Version du 17 décembre 2020

AgroDataRing

Caractéristiques de la solution de stockage	2
Cas d'usage	2
Brique locale de proximité (dite de niveau 1)	4
Brique distante (dite de niveau 2)	4
Flux des données	6
Durée de conservation des données	6
Coût de la solution	7
Autres serveurs	7
Serveur central d'administration - adrmaster.ingenum.inra.fr	7
Serveur frontal GlusterFS - adrtoulouse.ingenum.inra.fr	7
Serveur GitLab - forgemia.inra.fr	8
Rôles et responsabilités	9
Utilisateur	9
Gestionnaire de données (data manager)	9
Administrateur	9
Compte de service	9
Politique de sécurité, confidentialité et authentification	10
Autres documentations	11

Caractéristiques de la solution de stockage

Cas d'usage

Stockage sur disque orienté moyen/long terme.

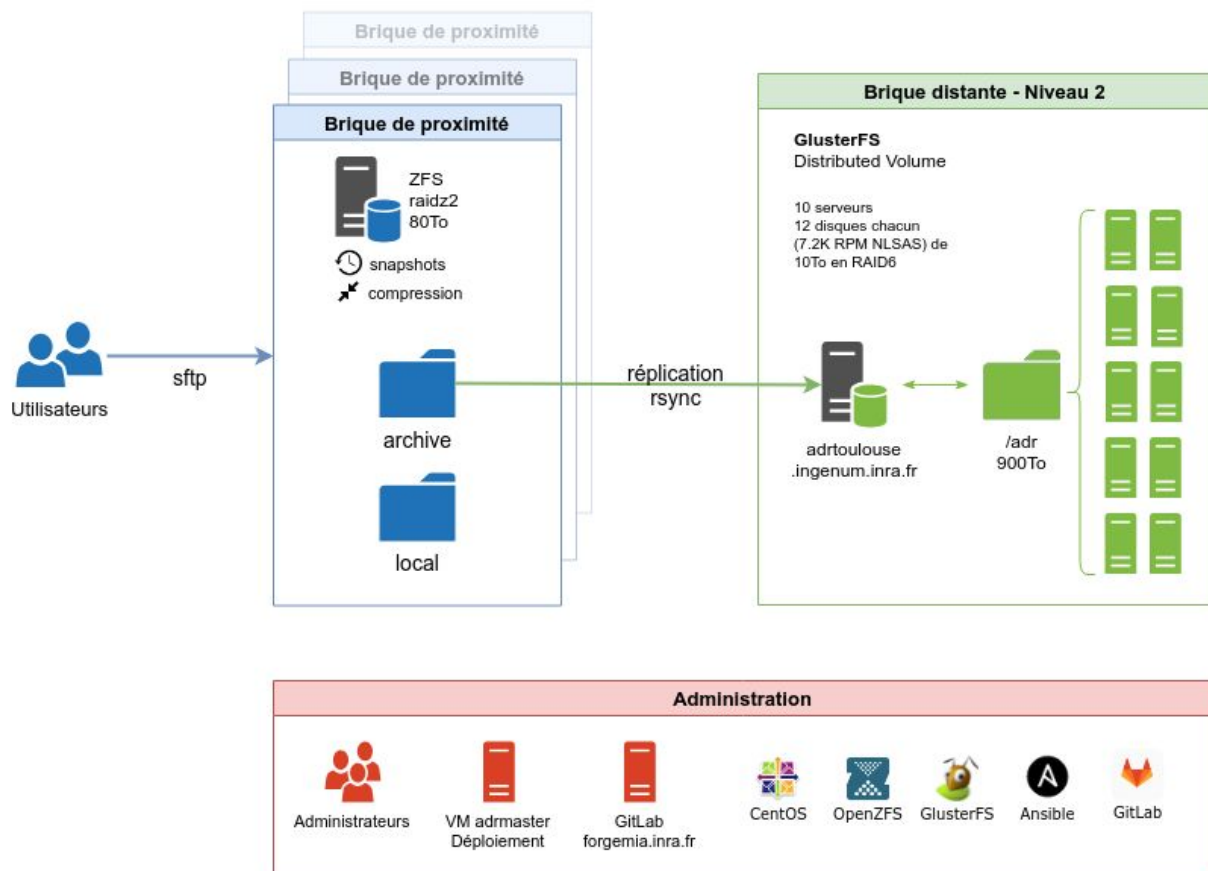
Le coût de revient, sans compter les ressources humaines, tourne autour de 60€/To/an avec réplication.

Adapté pour le stockage de données peu accédées et peu modifiées (stockage à moyen/long terme, réplication de données, etc.)

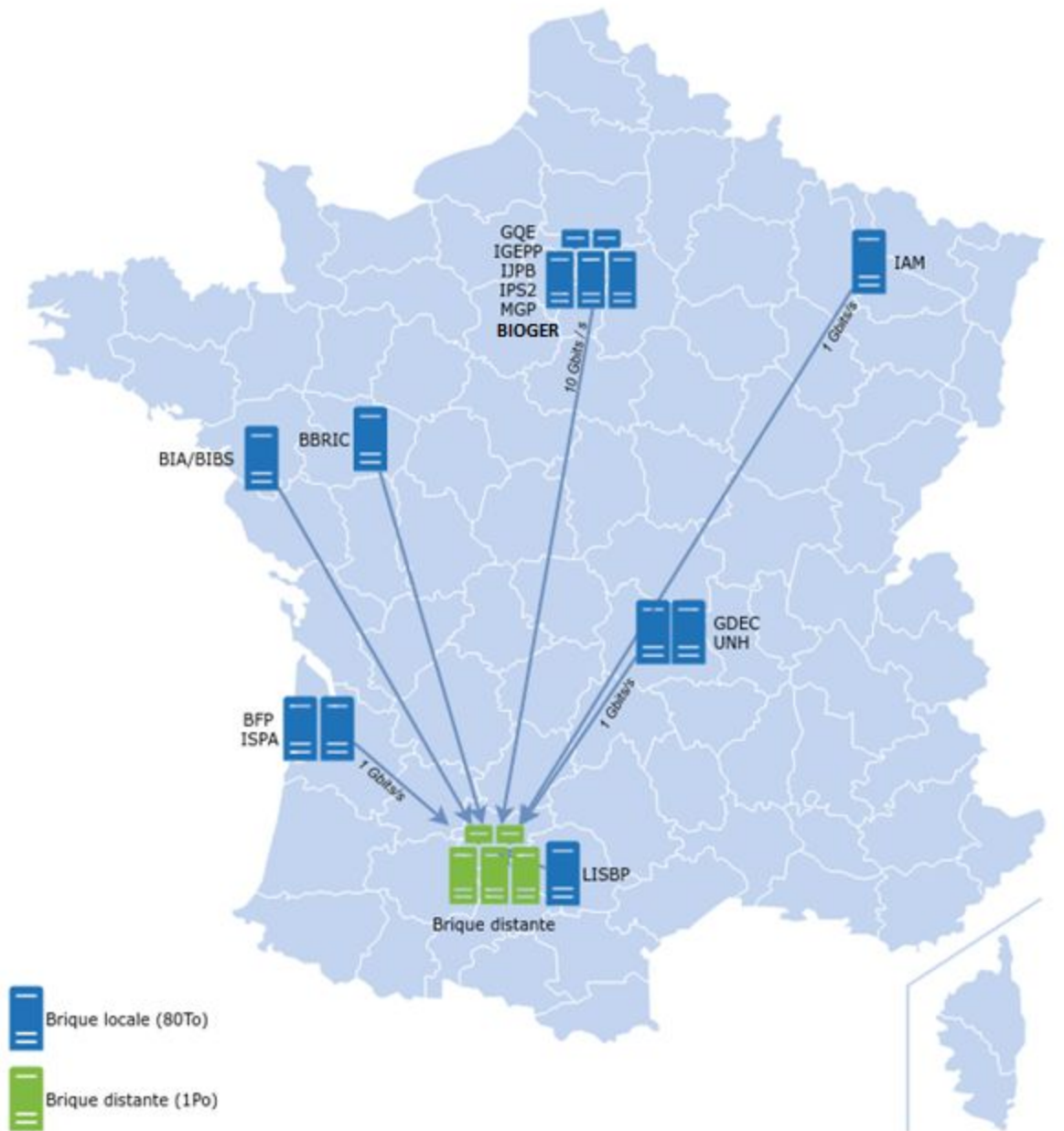
Pas adapté pour être utilisé avec un cluster de calcul (I/O intensifs), pour du stockage temporaire de données (espace tampons, temporaires), pour de la bureautique.

Les métadonnées ne sont pas gérées dans la version actuelle mais font partie des évolutions envisagées.

Pas accrédité à héberger des données à caractère personnel (données de santé par exemple).



Répartition Géographique



06/03/2019

Brique locale de proximité (dite de niveau 1)

Les données stockées sont très hétérogènes.

Elles dépendent des usages et des besoins de chaque membre.

- Hébergement : dépendant du site local. A proximité du producteur de données. Tous les établissements sont des Établissements publics à caractère scientifique et technologique (EPST).
- Volumétrie d'environ 80 To
Quota ZFS positionné à 65 To (permet de garder une réserve, de l'espace pour les snapshots et prévient une saturation de l'espace ZFS)
- Compression activée (transparent pour l'utilisateur)
- Serveur équipé de 12 disques (7.2K RPM NLSAS) de 10To
- ZFS (raidz2, équivalent RAID-6, tolérance de panne de 2 disques)
Scrub hebdomadaire (vérification)
- Instantanés (snapshots) :
Tous les 4h, rétention : 1 semaine
Tous les jours, rétention : 1 mois
Tous les dimanches, rétention : 1 an
- Accès au stockage : SFTP
- Réplication
Tout ou partie des données stockées sur cette brique peuvent être dupliquées sur la brique distante, suivant le dossier utilisé :
 - dossier "local", non répliqué,
 - dossier "archive", répliqué sur la brique distante suivant la politique locale du site (type, fréquence, durée de rétention, synchronisation ou copie, etc.).
- Restauration sur demande : la demande doit être faite à l'administrateur local de la brique ou adr.admin@inra.fr (en cas d'absence). La demande sera prise en charge sous 2 jours ouvrés. Le délai de restauration dépendra de la situation.

Brique distante (dite de niveau 2)

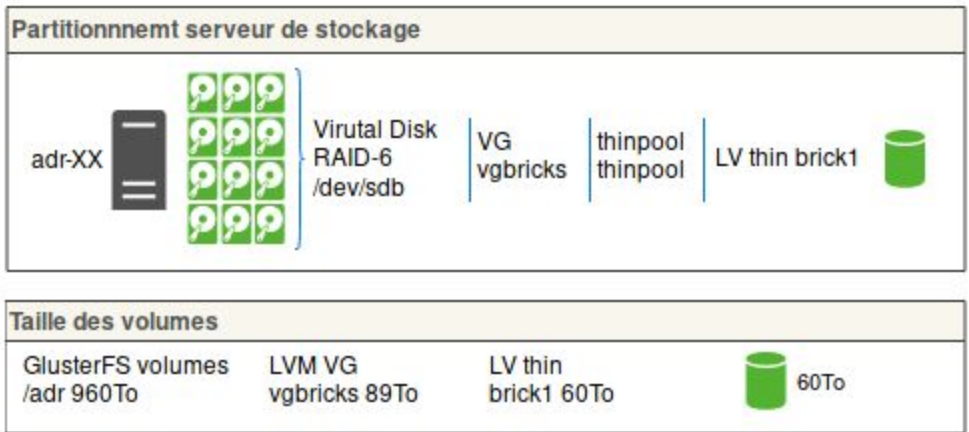
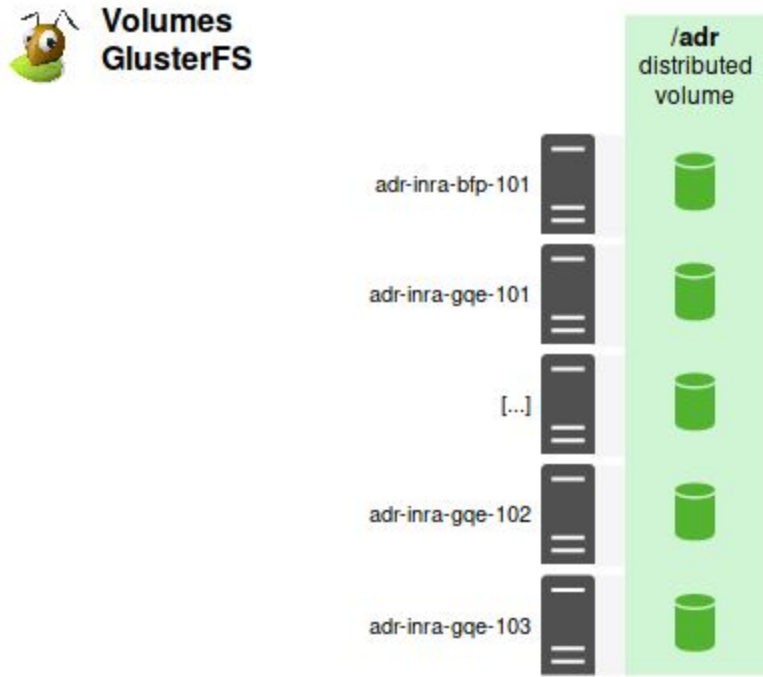
Héberge les données répliquées.

Cette brique n'est pas accessible directement par les utilisateurs.

Chaque brique distante est agrégée au sein d'un cluster pour former, au final, une seule brique.

- Hébergement : dans le datacenter de Toulouse « L'arche de données Francis Sevila » (voir annexe).
- Volumétrie de 1 Po.
Volume alloué à 960 To (une réserve est laissée sur chaque serveur pour pouvoir créer dans le futur et si besoin de nouveaux volumes ou étendre le volume initial /adr).

- Composé de 10 serveurs, 12 disques (7.2K RPM NLSAS de 10To) en RAID6 (tolérance de panne de 2 disques)
- 2 interfaces réseau 10 Gbits/s en agrégation de lien
- GlusterFS (mode distribué)
- Pas d'instantanés (snapshots)
- Accès au stockage : adrtoulouse.ingenum.inra.fr, SSH/SFTP

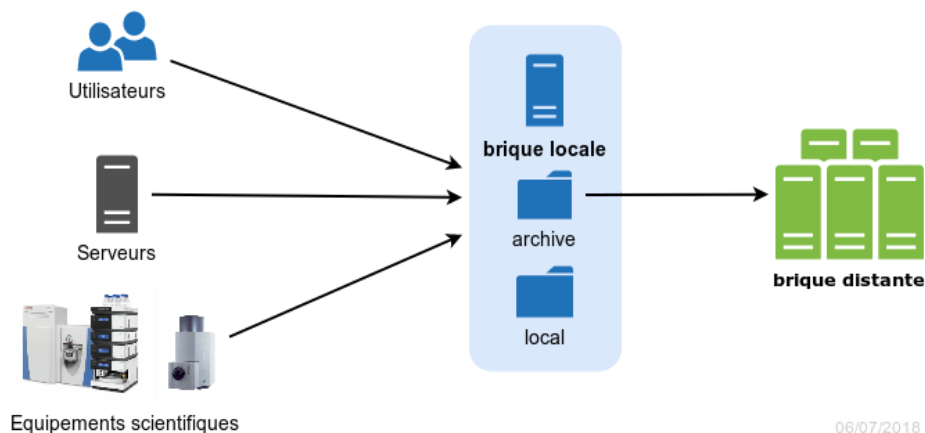


Flux des données

Les données sont déposées via SFTP (i.e. connexion chiffrée) sur la brique locale par les utilisateurs locaux ou par des machines (serveurs, équipements de laboratoires).

Depuis la brique locale, suivant le dossier utilisé:

- Les données dans le dossier local/ ne sont pas répliquées
- Les données dans le dossier archive/ sont répliquées au travers d'une connexion SSH (i.e. chiffrée) sur la brique distante.



06/07/2018

Durée de conservation des données

Associée à la garantie des serveurs. Une fois la garantie arrivée à terme, à charge du contributeur de renouveler l'équipement ou la maintenance. Dans le cas où le contributeur ne renouvelle pas, la récupération des données est à sa charge avant décommissionnement. Il peut soit récupérer ses serveurs (qui ne pourront plus être hébergés dans les DC INRA sans maintenance associée) ou faire le choix de les céder à ADR (qui peut choisir d'étendre la maintenance si c'est encore possible).

- 1ère vague d'achat (2017): Matériel garanti 5 ans jusqu'en juin 2022 (expiration le 05-07-2022) - garantie étendue jusqu'en fin 2024
- 2ème vague d'achat (2018): Matériel garanti 7 ans jusqu'en juin 2025
- 3ème vague d'achat (2020) : Matériel garanti 7 ans jusqu'en juin 2027

Coût de la solution

On peut se donner un ordre d'idée du coût de la solution, sans compter les ressources humaines:

- Une "brique" (locale ou distante) coûte environ 10000 € HT, avec une garantie sur 7 ans, fournissant environ 100 To utile
- Hébergement de la brique: 750 € HT/an (tarification 2017 datacenter INRA)

L'investissement de base comporte deux briques: une locale et une distante.

Sur une période de 5 ans, on obtient un coût au To de l'ordre de **~45 € /To /an avec réplication**.

Autres serveurs

Serveur central d'administration - adrmaster.ingenum.inra.fr

Ce serveur supporte plusieurs rôles :

- Serveur de déploiement (Kickstart + Ansible)
- Serveur frontal pour l'administration (connexions autorisées sur l'ensemble des machines ADR depuis ce serveur)
- Gitlab-runner
- Supervision (Nagios)

Caractéristiques :

- Machine virtuelle
4 CPU / 8 Go RAM / Disque système de 40 Go
- Hébergement : infrastructure Proxmox de l'unité Ingenum dans le datacenter « L'arche de données Francis Sevila ».

Serveur frontal GlusterFS - adrtoulouse.ingenum.inra.fr

Serveur permettant l'accès au volume GlusterFS (ce dernier n'étant accessible que localement).

Le serveur est un client GLusterFS et monte le volume GlusterFS */adr*.

- Machine virtuelle
8 CPU / 16 Go RAM
Disque système de 20 Go (/boot + LVM avec LV root xfs 17Go / + LV swap 1 Go)
1 interface réseau 10 Gbits/s (hérite d'un bond de 2 cartes 10 G, interface "virtio")
- Hébergement : infrastructure Proxmox de l'unité Ingenum dans le datacenter de Toulouse « Arche de données Francis Sevila »

-
- Sauvegardé tous les jours en local sur l'hôte et sur le même disque, via snapshots, rétention de 15 jours

Serveur GitLab - forgemia.inra.fr

La ForgeMIA (<http://forgemia.inra.fr>) est une forge logicielle, sous GitLab, du département de recherche Mathématiques et Informatique Appliquées (MIA) de l'Institut National de Recherche Agronomique (INRA).

Le service est virtualisé sur un serveur hébergé dans le datacenter de Toulouse « L'arche de données Francis Sevila ».

L'administration du serveur est assurée par une équipe composée d'administrateurs systèmes de différentes unités du département MIA en collaboration avec l'Équipe Informatique de Centre de Toulouse. Contact ForgeMIA : support-forgemia@inrae.fr (Christian Poirier, Maurice Baudry)

Nous avons choisi de nous appuyer sur ForgeMIA pour :

- éviter la gestion d'une nouvelle forge (maintenance, mise à jours, etc.),
- GitLab et gitlab-ci (en dernière version),
- l'authentification via la Fédération Éducation - Recherche (RENATER),
- du fait de la présence d'un membre du CT.

Une fois authentifié en utilisant son compte INRAE, il faut demander à un administrateur ADR d'être rattaché à l'équipe AgroDataRing du GitLab.

Rôles et responsabilités

Le partenaire reste le propriétaire et le responsable des données hébergées.

Utilisateur

Les utilisateurs de la solution AgroDataRing sont créés par un administrateur ou le gestionnaire de données.

Leur accès est restreint à la brique locale et les permissions (accès à certains dossiers, lecture, écriture, etc.) sont gérées par le gestionnaire de données ou l'administrateur du site.

Gestionnaire de données (data manager)

Le gestionnaire de données est le responsable des données hébergées et des permissions/droits d'accès pour son site (brique locale).

Ce rôle n'est pas toujours identifié et généralement assumé par l'administrateur local du site.

Administrateur

Les membres du comité technique ont accès à la totalité de l'infrastructure à des fins de maintenance en conditions opérationnelles.

Compte de service

Afin d'automatiser le transfert des données, par exemple pour des machines d'acquisitions, des comptes de services peuvent être créés.

Ces comptes peuvent être créés localement ou via l'AD.

Les comptes de service ou les clés sont alors gérés par l'administrateur local du site et sous sa responsabilité.

Politiques de sécurité, confidentialité et authentification

Dépendantes de la politique de sécurité du système d'information de chaque site.

Règles techniques mises en place :

- Accès administrateurs gérés via Ansible (gestion centralisé des comptes)
Par mots de passe ou par clés SSH.
- Les administrateurs AgroDataRing ont accès à la totalité des serveurs (en tant que root)
- Accès restreints sur chaque site aux utilisateurs enregistrés
- Accès, si possible, limité par adresses IP
- Firewall du serveur activé (firewalld)
- Bannissement des utilisateurs (fail2ban)
- Transferts via connexion chiffrée (SSH/SFTP)

Actuellement, les comptes peuvent être gérés de deux façons :

- via un Active Directory (INRAE, Université, etc.)
 - via des comptes locaux
- Les comptes utilisateurs et les groupes sont déclarés dans un fichier de configuration unique et centralisé sur Ansible.

Autres documentations

Page AgroDataRing

<https://www6.inrae.fr/datapartage/Gerer/Stocker-les-donnees/AgroDataRing>

Portail Data Inrae

<https://data.inra.fr/>

Plan de Gestion de Données (PGD)

Aide à la création: <https://dmp.opidor.fr/>

Réaliser un plan de gestion de données:

<http://doranum.fr/plan-de-gestion-de-donnees-dmp/>

<https://hal-descartes.archives-ouvertes.fr/page/data-management-plan>