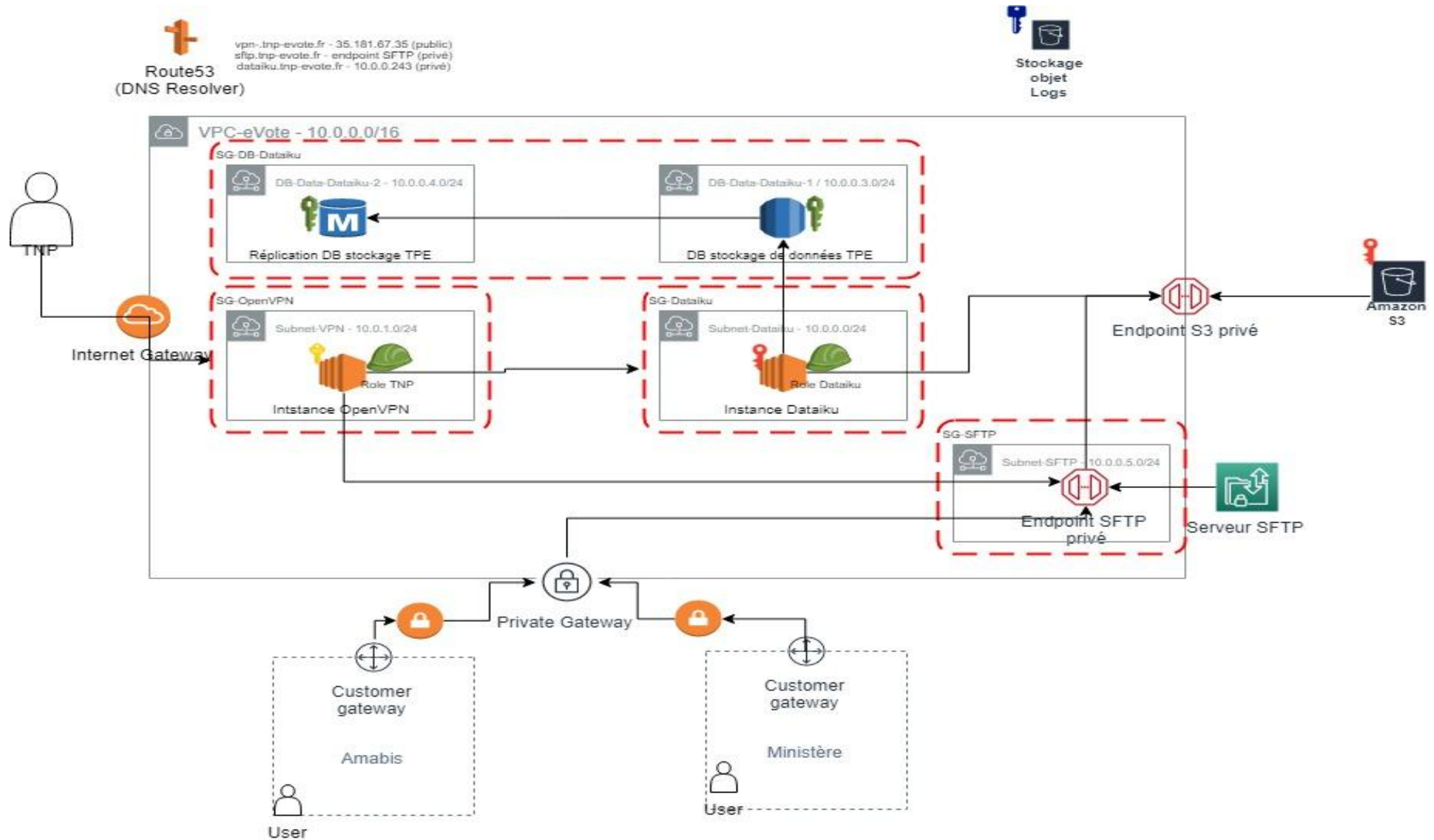
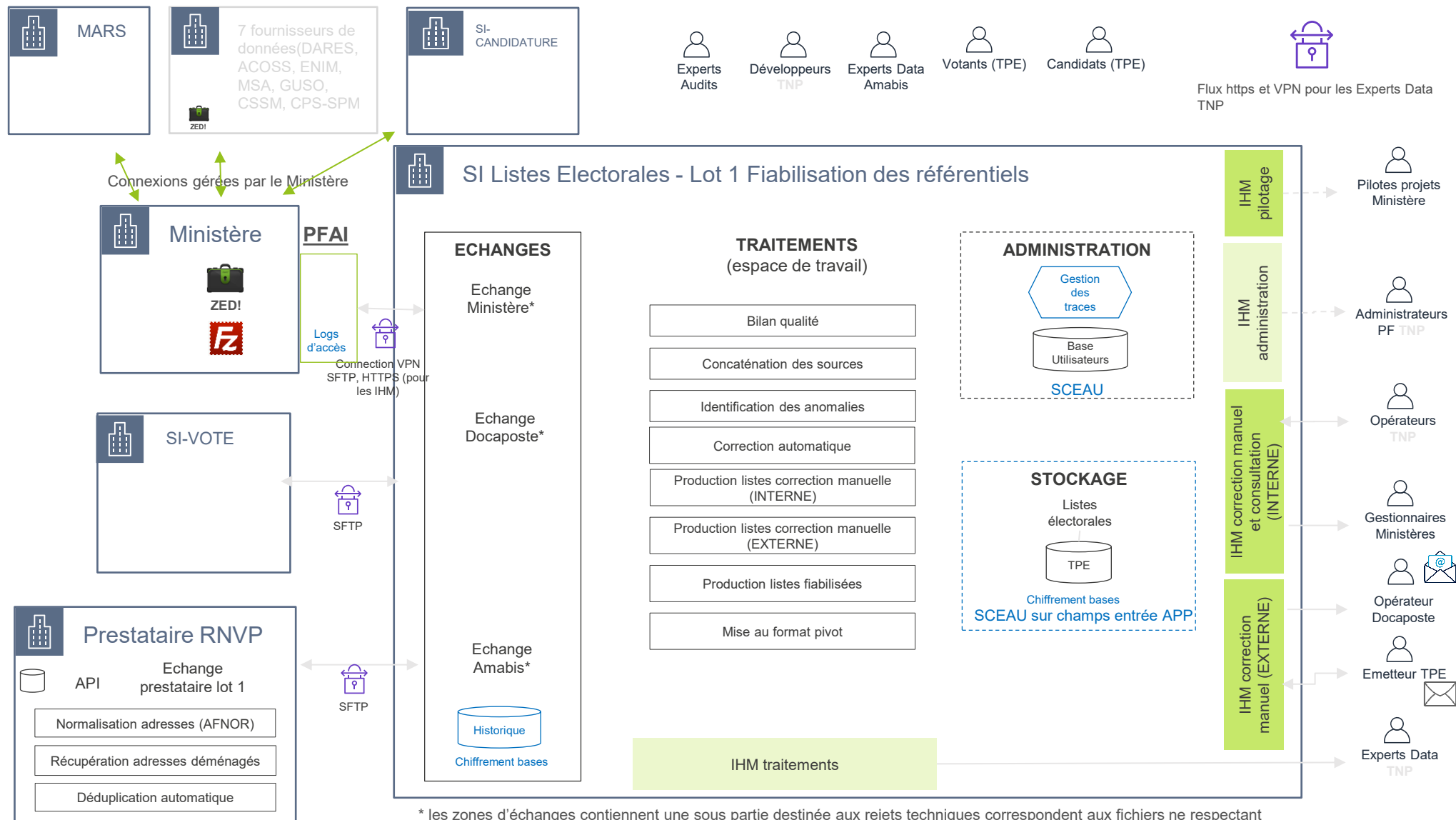


Architecture globale eVote





* les zones d'échanges contiennent une sous partie destinée aux rejets techniques correspondent aux fichiers ne respectant pas le format pivot défini, ou n'ayant pas pu être décryptés avec ZED!

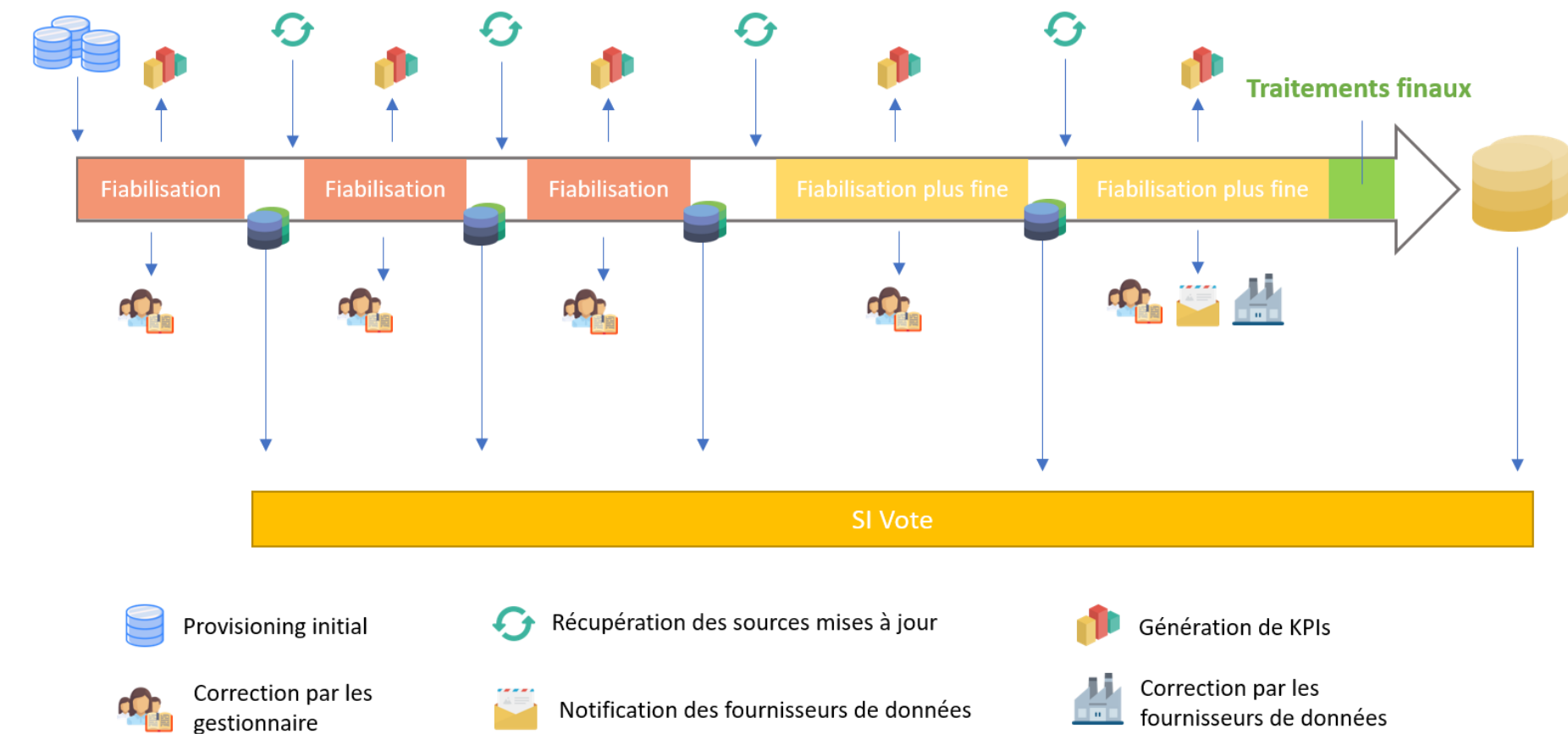
Démarche globale de fiabilisation des listes électorales

V-1.0 vendredi 11 Octobre 2019



- Pour chaque élection une liste fiabilisée sera produite par TNP.
- Des outils de fiabilisation standards et spécifiques pourront être utilisés à cet effet.
- L'expert indépendant s'assurera de la conformité de l'ensemble du système pour permettre son homologation

Démarche globale de fiabilisation



Les spécifications SI Liste électorale 2024

- ▶ **2 Data Centers français distincts (sécurité et de disponibilité), les data centers et les flux sensibles seront localisés en France.**
- ▶ Tous les serveurs connectés au réseau WAN ont un accès restreint et strictement limité par l'utilisation d'un pare-feu. Ils ne sont accessibles que de notre réseau interne par un mot de passe personnel, régulièrement modifié.
- ▶ Toutes les communications s'effectuent via un **tunnel chiffré (VPN)** ou une **liaison SSL** sur réseau public (en sus des divers protocoles applicatifs pouvant être utilisés et définis au niveau de chaque projet).
- ▶ La mise en place de chaque projet s'accompagne d'une mise en œuvre d'une brique de supervision spécifique à la **sécurité des données** (audit des accès, sauvegarde et archivage des données, gestion de la purge, confidentialité et **respect des obligations CNIL**).
- ▶ Un cloisonnement du projet est établi en termes de gestion de droits et de ressources.
- ▶ Les échanges entre l'Application Base Clients et le Service Qualité des données seront réalisés via une **connexion OpenSSH**.
- ▶ Les systèmes sont basés sur Linux.
- ▶ Tout accès à nos serveurs est tracé. Les technologies de virtualisation mises en œuvre facilitent le cloisonnement technique et fonctionnel des différents serveurs et applications. Il en est de même pour leur exploitation et la gestion des incidents.
- ▶ Le prestataire lot 1 s'engage à prendre toutes les mesures nécessaires afin de protéger les données et tout support informatique les contenant contre le vol, la copie ou la destruction accidentelle.
- ▶ **Le prestataire lot 1 prend à sa charge la disponibilité et l'administration de l'infrastructure nécessaire côté serveur : matériel serveur, OS, lignes télécoms sortantes.**
- ▶ Afin de garantir une protection des **données personnelles** maximale, seront mis en œuvre :
 - Chiffrement des bases à l'aide d'algorithmes réputés « forts »
 - Chiffrement des flux : utilisation de TLS 1.2, TLS 1.3, gestion des certificats à l'aide d'un module de sécurité
 - Chiffrement des fichiers de données en transfert avec l'outil Zed!
 - Système d'authentification renforcée en suivant les standards et recommandations
 - Respect des normes et règles définies par le CNIL et la loi RGPD (Règlement général sur la protection des données)
- ▶ **L'auditabilité** du système sera assurée par la **mise en place d'outils de journalisation sur l'ensemble des actions effectuées sur le serveur**, tout respectant les pratiques de sécurité lors de son implémentation (pas de données sensibles dans les logs, ...)
- ▶ **L'exactitude des informations** sera assurée par :
 - L'intégrité des flux garantie par des mécanismes classiques (TLS, codes correcteurs, ...)
 - L'encapsulation des données transmises avec l'outil Zed!
 - L'utilisation d'algorithmes de chiffrement « forts » dans un HSM (Hardware Security Module)
- ▶ Protection contre les **menaces** :
 - Mise en place des briques de sécurité : WAF (Web Application Firewall), anti-DDoS (Distributed Denial of Service), anti-malware, Pare-feu, anti-virus, monitoring, ...
 - Respect des bonnes pratiques en matière de développement Web (OWASP Open Web Application Project)
 - Mécanismes anti-spam pour les inscriptions
- ▶ Les exigences **d'accessibilité** seront respectées lors du développement,
 - un audit pour avoir le label AccessiWeb pourra être initié.

Diagramme source

Légende

Logo	Service	Usage eVote
	Route53 – Resolver DNS AWS	Route53 – Resolver DNS AWS
	Subnet – Sous-réseau AWS	Route53 – Resolver DNS AWS
	Subnet – Sous-réseau AWS	Route53 – Resolver DNS AWS
	RDS – Base de données MySQL AWS	Route53 – Resolver DNS AWS
	Site-to-Ste VPN – Services de gestion de VPN IpSec Site-to-Site dAWS	Route53 – Resolver DNS AWS
	Roles & Policies – Gestion des droits d’usage de services AWS	Route53 – Resolver DNS AWS
	Endpoints – Points d’accès privés aux services AWS	Route53 – Resolver DNS AWS
	Clés de chiffrements de données – gérées via le service KMSAWS	Route53 – Resolver DNS AWS
	Security Groups – Firewall infra AWS	Route53 – Resolver DNS AWS

VPC et sous-réseaux

→ 2VPC global pour toute l'application

Nom VPC	CIDR	Passerelle Internet	Sous-réseaux associés	Passerelles associées	VPN associés
Evote-tpe-vpc	12.0.0.0/16	Oui	• Evote-tpe-pub-eu • 3 evote-tpe-prv-eu	• Endpoint S3 • Endpoint VPC-MIN	• VPN Client endpoint prestataire lot 1
Evote-min-vpc	10.0.0.0/16	Non		• Endpoint SFTP • Endpoint s3	• VPN Client endpoint Ministère

Security Groups

→ 3Security Groups

Nom	Permissions Inbound	Ports accessibles (Inbound)	Permissions outbound	Ports accessibles (outbound)	Domaine d'application
SG-DB-Dataiku	Security Group Dataiku	3306	Security Group Dataiku	3306	Instance Database Dataiku
Uat-default-vpn-security-group	IP ministere – Ports 443	443	IP Prestataire lot 1 – Ports	*	VPN - Client
SG-SFTP	VPN TPE VPN MIN	22	Security SFTP	*	Serveur SFTP

Instances Compute

→ 2 instances de compute

Nom	CPU	Mémoire	Stockage	Réseau	Sous-réseau associé	Security Group associé	Usage	Adresse IP publique	Adresse IP privée	Politique de backup	Role AWS	Clé de cryptage du volume (AWS KMS)
Dataiku	1	2		Faible à modéré	Subnet-Dataiku	Dataiku-SG-IAC	Instance de traitement de données Ministère	-	10.0.1.136 - dataiku.tnp-evote.fr	None à date (1/J – sur 7 jours)	U-role-iac	Cle-EBS

Bases de données

→ 1 instance MySQL managée et à haute disponibilité

Nom	CPU	Mémoire	Stockage	Réseau	Sous-réseau associé	Security Group associé	Usage	Adresse IP publique	Adresse IP privée	Politique de backup	Role AWS	Clé de cryptage du volume (AWS KMS)
Db-dataiku	1	2		Faible à modéré	- Subnet-DB-Dataiku-1 - Subnet-DB-Dataiku-2	SG-DB-Dataiku	Instance de stockage de données Dataiku	-	-	db-dataiku.cjlox14qnpno.eu-west-3.rds.amazonaws.com	-	Cle-DB-dataiku