





DAT	Document d'Architecture Technique	 e.santé Occitanie <small>Connecter pour mieux soigner</small>	 cegedim.cloud
Version : 0.3			

---

# ESANTE OCCITANIE – TUCSV2

---

DAT	Document d'Architecture Technique	 
Version : 0.3		

- APPROBATION

PROPRIETE	
Nom de la Plateforme	SIU 2 / TUCS V2
Client	ESanté Occitanie

	AUTEUR	APPROBATEUR	SECURITE*
Prénom / Nom	xxxxx		
Rôle	xxxxx		
Date	20/02/2024		



\* The Security Officer in charge of the document's validation depends on the platform's responsible/owner. Either Cegedim.cloud's or the Business Unit's Security Officer.

- VERSION DU DOCUMENT



VERSION	DATE	AUTEUR	REMARQUE
0.1	20/02/2024	xxxxx	Première version suite reversibilité hébergement (Ecritel)
0.2	29/07/2024	xxxxx	Détails du RACI et middleware
0.3	23/12/2025	xxxxx	Mise à jour du document

- DOCUMENT DE REFERENCE

REFERENCE	AUTEUR	LIEN

DAT	Document d'Architecture Technique		
Version : 0.3			

1	RESUME.....	4
2	CONTACTS .....	5
2.1	PROPRIETAIRE DE LA PLATEFORME .....	5
2.2	CONTACTS CEDEDIM.CLOUD.....	5
3	INTRODUCTION .....	6
3.1	OBJECTIF DE CE DOCUMENT.....	6
4	SCHEMA D'ARCHITECTURE .....	7
4.1	DETAILS DE LA CONFIGURATION DES VLAN .....	8
4.2	INTERCONNEXION .....	8
5	RACI DE LA PLATEFORME.....	9
5.1	RACI.....	9
6	DESCRIPTION DE LA CONFIGURATION STANDARD DES SERVEURS .....	10
6.1	SERVEURS APPLICATIFS.....	10
6.2	SERVEUR BASE DE DONNEES .....	12
SECURITE	.....	13
6.3	AUTHENTIFICATION.....	13
6.1	AUTORISATION.....	13
6.2	LOG MANAGEMENT (GESTION DES JOURNAUX).....	13
6.3	PATCH MANAGEMENT .....	13
6.4	SERVICE CONTINUITY / DISASTER RECOVERY PLAN .....	13
7	INDICATEURS CLÉS DE PERFORMANCE.....	14
7.1	DISPONIBILITE & CAPACITE .....	14
8	CONFIGURATION RESEAU .....	15
8.1	MATRICE DES PORTS .....	15
8.2	LISTE DES HOTES AUTORISES SUR LE PROXY .....	15
8.3	LOAD BALANCERS .....	16
9	MAINTENANCE.....	17
9.1	SAUVEGARDE DES DONNEES .....	17
9.1.1	Sauvegarde: règles et définition .....	17
9.2	LISTE D' EXCLUSION .....	17
9.3	SUPERVISION .....	17
10	GLOSSAIRE.....	18
11	HISTORIQUE DES VERSIONS .....	19

DAT	Document d'Architecture Technique	 
Version : 0.3		

## 1. RESUME

Ce document décrit la plate-forme pour l'hébergement des applications « Système d'Information des Urgences » (SIU2) du périmètre.

## 2. CONTACTS

### 1.1 PROPRIETAIRE DE LA PLATEFORME



☐ Cegedim.cloud

☒ ESante Occitanie

Prénom / Nom	Position / Details
XXXXX	Chef de Projet SI
XXXXX	Ingénieur Technique
XXXXX	Responsable d'équipe
XXXXX	Responsable de pôle

### 1.2 CONTACTS CEGEDIM.CLOUD

CEGEDIM.CLOUD		
Prénom / Nom	Position / Details	Rôle
XXXXX	Cloud Builder	Intégrateur système
XXXXX	SDM	Suivi Client
XXXXX	Chefferie Projet	Suivi Projet

DAT	Document d'Architecture Technique	 
Version : 0.3		

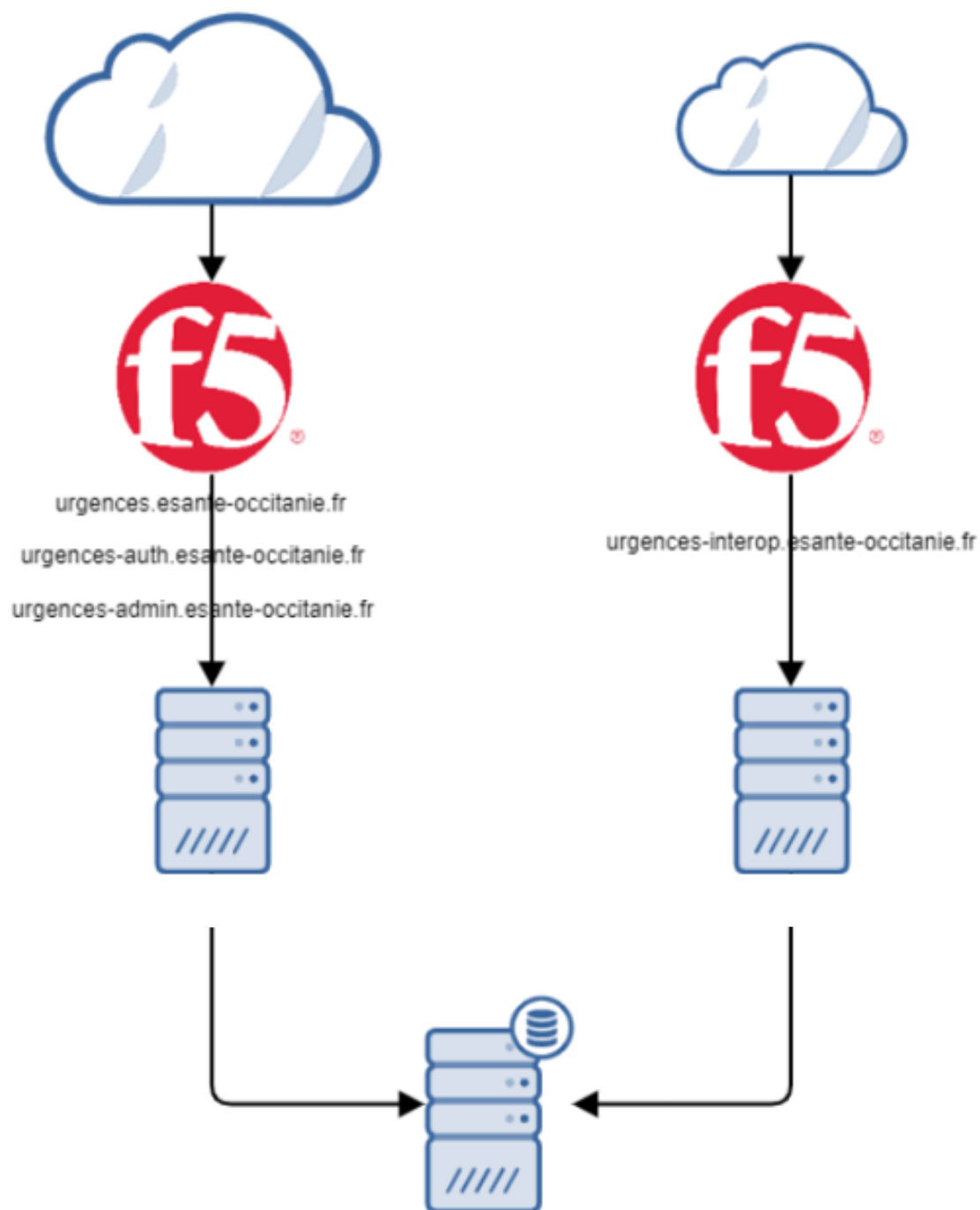
### 3. INTRODUCTION



#### 1.3 OBJECTIF DE CE DOCUMENT

Ce document décrit l'infrastructure en place hébergeant la plateforme SIU 2 d'Esante Occitanie.

## 4. SCHEMA D'ARCHITECTURE

Schéma d'architecture logique



DAT	Document d'Architecture Technique	 
Version : 0.3		

#### 1.4 DETAILS DE LA CONFIGURATION DES VLAN

NOM	ROLE	DETAILS
HT_3494_PROD_FRONT_SIU2_ESO	Zone réseau hébergeant le service applicatif - frontend de production	
HT_3495_PROD_BACK_SIU2_ESO	Zone réseau hébergeant le service Base de données de production	
HT_3496_QA_FRONT_SIU2_ESO	Zone réseau hébergeant le service applicatif - frontend de non production	
HT_3497_QA_BACK_SIU2_ESO	Zone réseau hébergeant le service Base de données de non production	

#### 1.5 INTERCONNEXION

Accès à gitlab.com en https via proxy



## 5. RACI DE LA PLATEFORME

### 1.6 RACI



Le RACI ci-dessous définit les rôles et responsabilités des différents acteurs pour un projet et/ou pendant l'exploitation en cours.

Périmètre	BUILD	RUN
<b>Hyperviseur</b>	Cegedim.Cloud	Cegedim.Cloud
<b>Socle Système</b>	Cegedim.Cloud	Cegedim.Cloud
<b>Supervision</b>	Cegedim.Cloud	Cegedim.Cloud
<b>Sauvegardes</b>	Cegedim.Cloud	Cegedim.Cloud
<b>Docker</b>	Cegedim.Cloud	Cegedim.Cloud
<b>Base de données Containerisée</b>	E SANTE OCCITANIE / TMA	E SANTE OCCITANIE / TMA
<b>Périmètre applicatif</b>	E SANTE OCCITANIE / TMA	E SANTE OCCITANIE / TMA
<b>Gestion des certificats – let's encrypt (urgences-*.esante-occitanie.fr)</b>	E SANTE OCCITANIE / TMA	E SANTE OCCITANIE / TMA

## 6. DESCRIPTION DE LA CONFIGURATION STANDARD DES SERVEURS

### 1.7 SERVEURS APPLICATIFS

Name	xxxxx
Description/ Fonction	<i>Serveur Applicatif (docker) servant urgences.esante-occitanie.fr</i>
Datacenter :	xxxxx
Type :	Virtuel
Système d'exploitation et version:	<i>Debian 10</i>
Architecture :	<i>64 bits</i>
Nombre de processeurs :	<i>6 (6 Coeurs – 1 Sockets)</i>
Taille de la mémoire:	<i>16Gb</i>
configuration LAN par défaut:	<i>XX.XX.XX.43/27 – vnic 10Gb</i>
Configuration SAN par défaut:	<i>Datastore VMWare -&gt; SAN Baie Flash</i>
Lecteurs, partitions et tailles :	<i>30 Gb</i>
OS -> Licence	<i>N/A</i>

DAT	Document d'Architecture Technique	 
Version : 0.3		

Name	xxxxx
Description/ Fonction	<i>Serveur Applicatif (docker) servant urgences-interop.esante-occitanie.fr</i>
Datacenter :	xxxxx
Type :	Virtuel
Système d'exploitation et version:	<i>Debian 10</i>
Architecture :	<i>64 bits</i>
Nombre de processeurs :	<i>4 (4 Coeurs – 1 Sockets)</i>
Taille de la mémoire:	<i>16Gb</i>
configuration LAN par défaut:	<i>XX.XX.XX.44/27 – vnic 10Gb</i>
configuration SAN par défaut:	<i>Datastore VMWare -&gt; SAN Baie Flash</i>
Lecteurs, partitions et tailles :	<i>30 Gb → /</i> <i>125Gb → /mnt</i>
OS -> Licence	N/A

## 1.8 SERVEUR BASE DE DONNEES

Name	xxxxx
Description/ Fonction	<i>Serveur Base de données (docker)</i>
Datacenter :	xxxxx
Type :	Virtuel
Système d'exploitation et version:	<i>Debian 10</i>
Architecture :	<i>64 bits</i>
Nombre de processeurs :	<i>6 (6 Coeurs – 1 Sockets)</i>
Taille de la mémoire:	<i>64Gb</i>
configuration LAN par défaut:	<i>XX.XX.XX.75/27 – vnic 10Gb</i>
configuration SAN par défaut:	<i>Datastore VMWare -&gt; SAN Baie Flash</i>
Lecteurs, partitions et tailles :	<i>30 Gb → /</i> <i>383Gb → /mnt</i>
OS -> Licence	<i>N/A</i>

## 7. SECURITE

☒ Compatible avec les standards (Si oui, aller au paragraphe § 7.4)

☐ Spécifique (Si oui, suivre les paragraphes §7.1 to 7.3)

### 1.9 AUTHENTIFICATION

*L'authentification se fait via l'authentification par Active Directory sur le domaine cegedim.hds*

### 1.1 AUTORISATION

Présentation des autorisations pour chacun des rôles

ROLE	PERMISSIONS
Administrator	Accès complets aux machines (sudo ALL)
User	Accès en lecture aux machines

Matrice d'autorisation (qui a quel rôle ?). A noter : Une autorisation basée sur l'utilisation des groupes est recommandée (RBAC : Role Based Access Control).

GROUP	ROLE
G_ESANTEOCCITANIE_SIU2_RW	Administrator
G_MYIT_PAASDebian_Admins	Administrator
G_ESANTEOCCITANIE_SIU2_R	User

### 1.2 LOG MANAGEMENT (GESTION DES JOURNAUX)

Les évènements système sont récupéré via la solution SIAM Splunk, ils ne sont accessibles que par les équipes d'exploitation et sécurité de Cegedim.Cloud

### 1.3 PATCH MANAGEMENT

Décrire le cycle de vie des correctifs et des mises à niveau.



☒ Patch management standard

☐ Patch management spécifique : Description

### 1.4 SERVICE CONTINUITY / DISASTER RECOVERY PLAN

Conforme au PAS et PAQ du Marché Esante Occitanie - à préciser

RECOVERY TYPE	DURATION (IN HOURS)
RPO	2H
RTO	4H

DAT	Document d'Architecture Technique	 
Version : 0.3		

## 8. INDICATEURS CLÉS DE PERFORMANCE

### 1.5 DISPONIBILITE & CAPACITE

Taux de disponibilité attendu (en %) :

Perspectives de croissance du stockage

## 9. CONFIGURATION RESEAU

### 1.1 MATRICE DES PORTS

Groupe	Membre	Description
<b>g-eso-siu2-app-prod</b>	xx.xx.xx.43 (petesosiuweb01) xx.xx.xx.44 (petesosiuweb02)	Serveurs Applicatifs Frontaux
<b>g-eso-siu2-db-prod</b>	xx.xx.xx.75 (petesosiubdd01)	Serveur base de données
<b>g-eso-siu2-prod</b>	g-eso-siu2-app-prod g-eso-siu2-db-prod	

SOURCE	DESTINATION	PORT	DESCRIPTION
g-eso-siu2-app-prod	g-eso-siu2-db-prod	3306/TCP	MySQL
g-eso-git-ci-agent	g-eso-pass-app-vip-prod	443/TCP	Accès Service Applicatifs interne

### 1.2 LISTE DES HOTES AUTORISES SUR LE PROXY

Hote	Statut
Dev.azure.com	Autorisé
Management.core.windows.net	Autorisé
vstsagentpackage.azureedge.net	Autorisé

### 1.3 LOAD BALANCERS

Hôte	IP	Configuration
<b>Urgences.esante-occitanie.fr / urgences-admin.esante-occitanie / urgences-auth.esante-occitanie.fr</b>	xx.xx.xx.69	Load Balancer niveau 4 sur les ports 443 et 80 (pas de gestion de certificats)
<b>Urgences-interop.esante-occitanie.fr</b>	xx.xx.xx.78	Load Balancer niveau 4 sur les ports 443 et 80 (pas de gestion de certificats)



## 10. MAINTENANCE

### 1.4 SAUVEGARDE DES DONNEES

- ☐ Compatible avec les standards (Si oui, aller au paragraphe § 9.2)
- ☒ Spécifique (Si oui, suivre les paragraphes §9.1.1 jusqu'à 9.1.2)

#### 1.4.1 Sauvegarde : règles et définition

Les Sauvegardes sont effectuées au niveau de l'hyperviseur par la solution de sauvegarde Rubrik :

Fréquence	Rétention
Sauvegarde Quotidienne	93 Jours

### 1.5 LISTE D'EXCLUSION

SERVEUR	PATH	FILES OR DIRECTORY

### 1.6 SUPERVISION

Description du monitoring de base appliqué.

SERVER NAME	CONDITIONS FOR SUCCESS / FAILURE OF AUDIT

## 11. GLOSSAIRE

NOM	DESCRIPTION

12. HISTORIQUE DES VERSIONS

VERSION	DATE	AUTEUR	CHANGEMENT
0.1	2023-09-15	xxxxx	Création du document
0.2	29/07/2024	xxxxx	Détails du RACI et middleware
0.3	23/12/2025	xxxxx	Mise à jour du document