

# Cahier Des Charges (CDC)

du projet

## Gestion Centralisée de logs

### Responsabilité documentaire

Action	NOM Prénom	Fonction	Date	Signature
Approuvé par		Client	11/03/2023	
Rédigé par	ChefProjet1	ChefProjet1	10/03/2023	

BTS CIEL_IR	Référence : CDC Révision : 1 – 10/03/2023	1/10
-------------	--	------

## Suivi des révisions documentaires

Indice	Date	Nature de la révision
1	12/03/2023	Première publication

## Documents de références

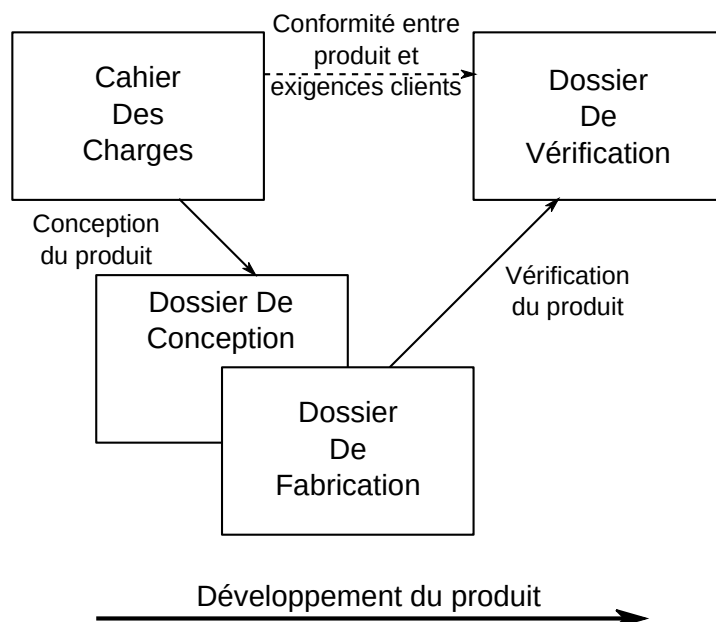
Sigle	Référence	Titre	Rév.	Origine

## Table des matières

<b>1. Nature du document.....</b>	<b>3</b>
<b>2. Présentation du produit à développer.....</b>	<b>4</b>
2.1. Objectif.....	4
2.2. Sitographie :.....	4
<b>3. Exigences client du produit à développer.....</b>	<b>6</b>
3.1. REQ001.REQ003 : Monitorer le poste.....	8
3.2. REQ001.REQ002 : Surveiller le SI.....	9
3.3. REQ001.REQ004 : DevSecOps.....	9

# 1. Nature du document

Ce document est un cahier des charges et a pour but de décrire l'ensemble des exigences client relatives au développement du produit.



**Figure 1: Arborescence documentaire.**

La figure 1 présente le cycle de développement du produit et les documents associés, conformément à la norme de qualité ISO9001. L'axe principal de cette norme est la « *satisfaction client* » et a pour but de garantir la conformité du produit ainsi que la tenue des coûts et délais de développement.

Le *Cahier Des Charges* (CDC) est rédigé par le client et approuvé par le fournisseur. Il regroupe l'ensemble des exigences auxquelles le produit doit répondre.

Le *Dossier De Conception* (DDC) est rédigé par le fournisseur et approuvé par le client. Ce dossier présente l'architecture fonctionnelle du produit développé, le dimensionnement des différents blocs fonctionnels le constituant et les résultats de leur simulation.

Le *Dossier De Vérification* (DDV) est rédigé par le fournisseur et approuvé par le client. Il décrit la manière de vérifier le bon fonctionnement du produit développé et synthétise les résultats des essais réalisés.

## 2. Présentation du produit à développer

### 2.1. Objectif

L'objectif de ce projet est de concevoir et de réaliser un programme de Gestion centralisée de logs.

Sur un poste de travail, les actions de l'utilisateur et/ou des événements systèmes génèrent énormément de logs.

L'entreprise XYZ, de part son segment de marché, est exposée fortement au risque cyber. Le RSSI souhaite mettre en place une politique stricte de sécurité basée sur la règle du moindre privilège ou « least privilege ».

Pour que l'ensemble des collaborateurs adhèrent à cette politique de sécurité, le RSSI souhaite que l'outil de **Gestion Centralisée de logs** leur permettent de prendre conscience des contraintes de sécurité.

Pour cela, le RSSI veut développer une application capable de **trier, visualiser, enregistrer** et **centraliser** les logs du PC des collaborateurs.

Chacun des utilisateurs pourra visualiser les logs importants de son poste de travail, le RSSI lui aura accès à une remontée des logs pour une surveillance centralisée.

Après une étude des produits existant sur le marché, le client ne souhaite pas les utiliser mais préfère une nouvelle application répondant à ces besoins.

Le client a fait un appel d'offre public, notre société a répondu et remporté celui-ci.

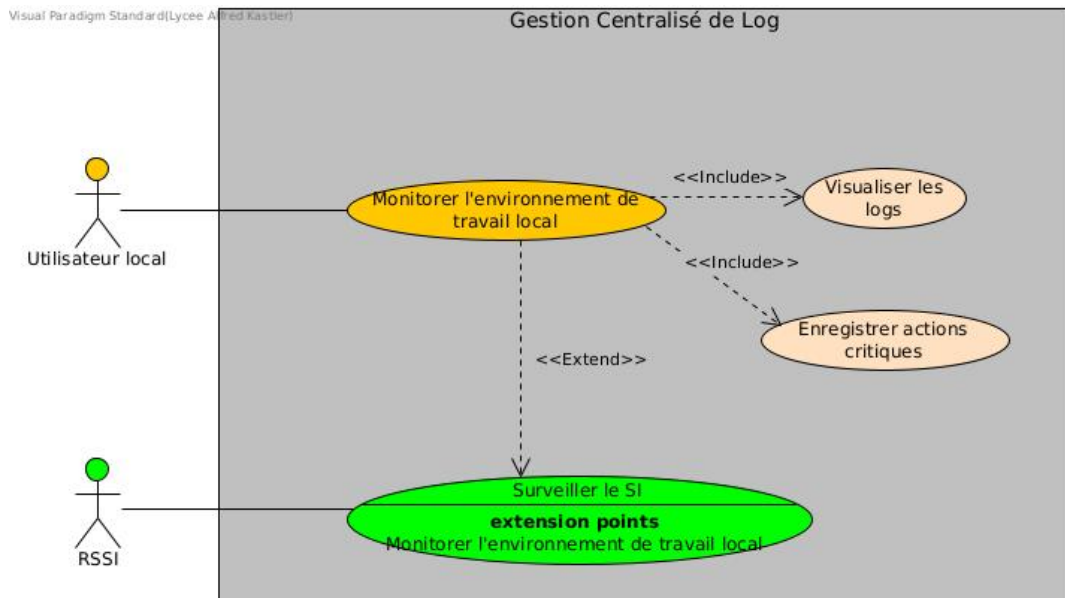
### 2.2. Sitographie :

<https://sematext.com/blog/linux-logs/>

<https://stackify.com/linux-logs/>

Le diagramme des cas d'utilisations ci-dessous décrit les fonctionnalités attendues du produit.

**Figure 2 : diagramme des cas d'utilisations**



### UC Monitorer l'environnement de travail local

Cela consiste à sélectionner, visualiser et enregistrer les actions de l'utilisateur du poste concernant les services critiques de la machine de travail.

Ce cas d'utilisation est détaillé dans les deux UC inclus, « Visualiser les logs » et « Enregistrer Actions Critiques »

### UC Visualiser les logs

Les logs seront visualisés en temps réel par l'utilisateur du poste

### UC Enregistrer Actions Critiques

En plus d'être visualisés, certains logs critiques seront enregistrés pour une exploitation ultérieure.

### UC Surveiller le SI

Les logs seront transmis à un serveur distant pour exploitation par le RSSI (Responsable de la Sécurité du Système d'Information)

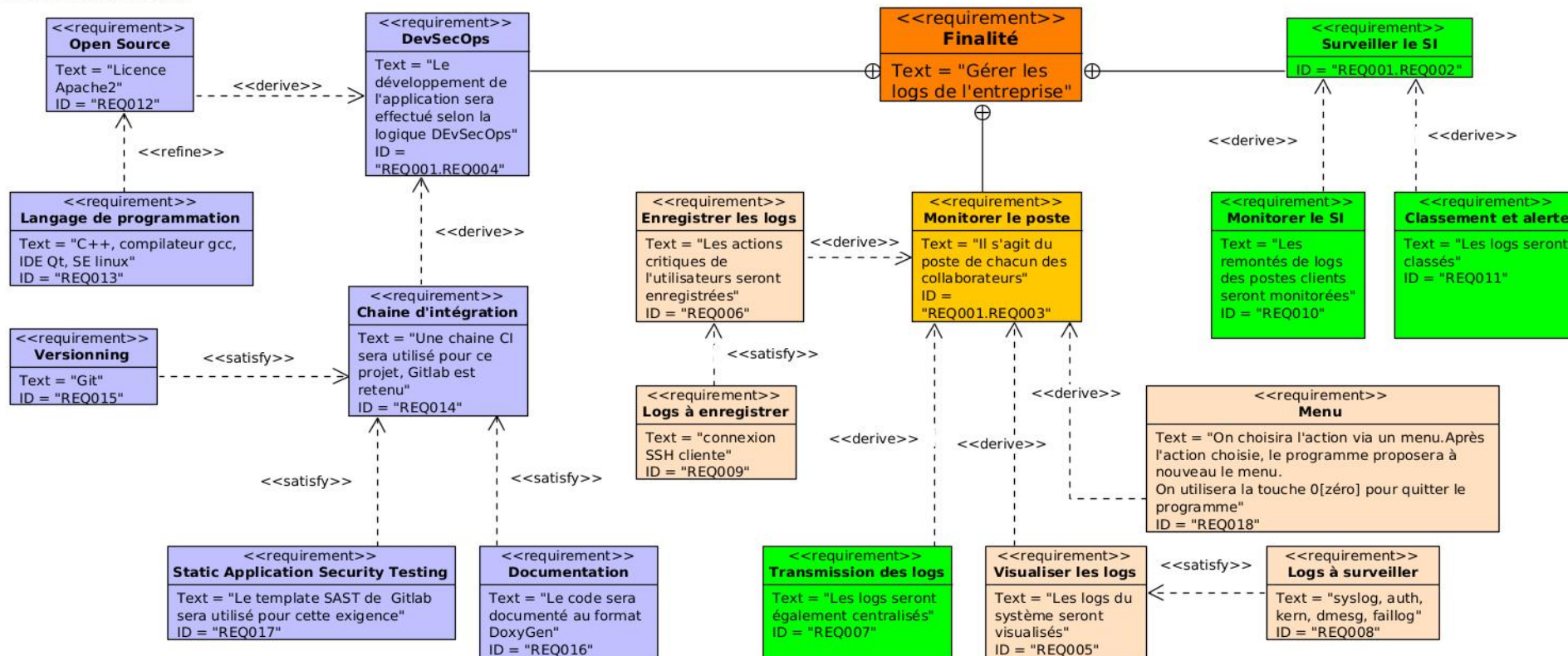
### 3. Exigences client du produit à développer

Ce chapitre détaille l'ensemble des exigences client du produit à développer. Chaque exigence est rédigée de manière concise et non ambiguë afin d'être vérifiable explicitement par l'équipe de développement.

Le diagramme des exigences ci-après décrit les exigences attendues par le client

Figure 3 : Diagramme des exigences

Visual Paradigm Standard (Lycee Alfred Kastler)



### **3.1. REQ001.REQ003 : Monitorer le poste**

Les exigences suivantes détaillent cette exigence

#### **Référence de l'exigence id REQ005 : Visualiser les logs**

Les logs sélectionnés et filtrés devront être actifs dans une console et/ou un terminal dédié de l'utilisateur

#### **Référence de l'exigence id REQ 008 : Logs à surveiller**

Les logs à surveiller sont les suivants :

- Demande de droits sudo
- Connexion sur le poste local
- Événement système critique

#### **Référence de l'exigence id REQ 006 : Enregistrer les logs**

En sus d'une surveillance des logs de la REQ 008, certaines commandes devront être enregistrées sur le postes de travail.

#### **Référence de l'exigence id REQ 009 : Logs à enregistrer**

Les connexions SSH clientes seront enregistrées dans un fichier txt qui contiendra les informations suivantes :

- Date de la demande de connexion
- Heure de la demande de connexion
- Nom du poste client
- Nom de l'utilisateur connecté
- SSH : nom de l'utilisateur
- SSH : Adresse ou DNS du serveur
- SSH : Port de connexion

#### **Référence de l'exigence id REQ 007 : Transmission des logs**

Les logs des exigences précédentes seront transmis à un serveur spécifique pour une exploitation centralisée.

BTS CIEL_IR	Référence : _CDC Révision : 1 – /	8/10
-------------	--------------------------------------	------



### Référence de l'exigence id REQ 018 : Menu

On choisira l'action via un menu.

Après l'action choisie, le programme proposera à nouveau le menu.

On utilisera la touche 0[zéro] pour quitter le programme

## 3.2. REQ001.REQ002 : Surveiller le SI

Les exigences suivantes détaillent cette exigence.

### Référence de l'exigence id REQ010 : Monitorer le SI

Le RSSI doit avoir accès à une remontée des logs par poste sur une adresse dédiée et sécurisée.

### Référence de l'exigence id REQ 0011 : Classement et alerte

Les logs seront classés.

## 3.3. REQ001.REQ004 : DevSecOps

Le développement de l'application sera effectué selon la logique DevSecOps. Les exigences ci-dessous détaillent celles-ci dans ce projet.

### Référence de l'exigence id REQ012 : Open Source

Afin de garantir une sécurité de l'exécution du code, le client souhaite avoir accès au code source de l'application qui sera développé sous licence Apache2.

### Référence de l'exigence id REQ 0013 : Langage de programmation

Le client souhaite que l'application soit développée en C++ pour des raisons de performances. La cible est Linux, SE de tous les postes de travail de l'entreprise.

Le chef de projet choisit de développer sous l'IDE QtCreator, avec la chaîne de compilation Cmake.

BTS CIEL_IR	Référence : _CDC Révision : 1 – /	9/10
-------------	--------------------------------------	------

### Référence de l'exigence id REQ 0014 : Chaîne d'intégration

Tous le code produit devra être déposé sur le serveur Gitlab de l'entreprise, un pipeline d'intégration comprenant les étapes de compilation, de tests SAST et de génération automatique de la documentation est défini pour ce projet.

### Référence de l'exigence id REQ 0015 : Versionning

Le code sera versionné avec Git.

### Référence de l'exigence id REQ 0017 : Static Application Security Testing

Le template SAAT de Gitlab sera utilisé pour cette exigence.

### Référence de l'exigence id REQ 0016 : Documentation

Le code sera documenté au format DoxyGen. La documentation sera générée automatiquement.