|  |
| --- |
| Shadow Scan |

Pour projets avec XCL

V2.0

Table des matières

[1 Analyse préliminaire 5](#_Toc188610005)

[1.1 Introduction 5](#_Toc188610006)

[1.2 Objectifs 5](#_Toc188610007)

[1.3 Gestion de projet 5](#_Toc188610008)

[1.4 Planification initiale 6](#_Toc188610009)

[2 Analyse / Conception 7](#_Toc188610010)

[2.1 Contexte produit 7](#_Toc188610011)

[2.2 Contextes techniques 8](#_Toc188610012)

[2.2.1 Opérationnel 8](#_Toc188610013)

[*Placer le produit dans son contexte d’opérations.* 8](#_Toc188610014)

[2.2.2 Validation 8](#_Toc188610015)

[2.2.3 Développement 8](#_Toc188610016)

[2.2.4 Justification des choix 8](#_Toc188610017)

[2.3 Concept 9](#_Toc188610018)

[2.4 Analyse fonctionnelle 10](#_Toc188610019)

[2.5 Stratégie de test 10](#_Toc188610020)

[2.6 Risques techniques 10](#_Toc188610021)

[2.7 Planification 10](#_Toc188610022)

[3 Réalisation 11](#_Toc188610023)

[3.1 Points de design spécifiques 11](#_Toc188610024)

[*3.1.1* *…* 11](#_Toc188610025)

[*3.1.2* *…* 11](#_Toc188610026)

[*3.1.3* *…* 11](#_Toc188610027)

[3.2 Déroulement 11](#_Toc188610028)

[3.2.1 Sprints 11](#_Toc188610029)

[3.2.2 Stories 12](#_Toc188610030)

[~~3.3~~ ~~Dossier de réalisation~~ 12](#_Toc188610031)

[3.4 Mise en place de l’environnement de travail 12](#_Toc188610032)

[3.5 Mise en place de l’environnement de test 12](#_Toc188610033)

[3.6 Déploiement du produit 13](#_Toc188610034)

[3.7 Description des tests effectués 13](#_Toc188610035)

[3.8 Bilan 13](#_Toc188610036)

[3.8.1 Erreurs restantes 13](#_Toc188610037)

[3.8.2 Stories 13](#_Toc188610038)

[3.8.3 Dette technique 13](#_Toc188610039)

[3.9 Recours à l’intelligence artificielle 13](#_Toc188610040)

[3.10 Liste des documents fournis 14](#_Toc188610041)

[4 Conclusions 14](#_Toc188610042)

[5 Annexes 15](#_Toc188610043)

[5.1 Résumé du rapport du TPI / version succincte de la documentation 15](#_Toc188610044)

[5.2 Sources – Bibliographie 15](#_Toc188610045)

[5.3 Journal de travail 15](#_Toc188610046)

[~~5.4~~ ~~Manuel d'Installation~~ 15](#_Toc188610047)

[5.5 Manuel d'Utilisation 15](#_Toc188610048)

[5.6 Archives du projet 15](#_Toc188610049)

*NOTE L’INTENTION DES UTILISATEURS DE CE CANEVAS :*  
*Toutes les parties en italiques sont là pour aider à comprendre ce qu’il faut mettre dans cette partie du document. Elles n’ont donc aucune raison d’être dans le document final.*

*De plus, en fonction du type de projet, il est tout à fait possible que certains chapitres ou paragraphes n’aient aucun sens. Dans ce cas il est recommandé de les retirer du document pour éviter de l’alourdir inutilement.*

# Analyse préliminaire

## Introduction

Le but de ce projet est de créer un moyen de monitorer les accès à certaines ressources sur les post des élèves.

Lors d’un test ou un travail le prof va pouvoir définir une liste de ressource interdites (site web, app, fichiers).

Si durant la durée du test ou du travail un élève outrepasse les limitations, il en sera notifié et le prof aussi sans que rien se passe. Le but est seulement de vérifier ce qui se passe et non de l’empêcher.

## Objectifs

Objectifs de formation :

Le but de ce projet est de se préparer au TPI, se remettre dans le bain du fonctionnement des projet et de prendre connaissance de la grille d’évaluation du TPI.

Objectifs du produit :

Le but du produit est de pouvoir créer une liste de ressource interdites, de lancer une vérification sur ces ressource interdite.

D’être informé si une de ces ressources est utilisée (notifications des deux côtés : prof et élève)

## Gestion de projet

Gestion du projet avec IceScrum. Donc le projet sera un projet agile.

Il sera séparé en sprints de 2 semaines, 3 au total.

Les sprints reviews seront faite avec le project owner (le chef de projet).

Des user stories sont attachée à chaque sprint.

À chaque début de journée je fait un Meeting.

## Planification initiale

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Sprint 1 | | | | | | | | | |
|  |  |
| 27.01.2024 -> 07.02.2024 | |  |  |  |  |  |  |  |  |  |  |
|  | Etablir la connexion gRPC entre les clients (prof et élève) | | | | | | | |  |
|  |  |  |  |
| Semaine 5->6 | |  |  |  |  |  |  |  |  |  |  |
|  | lire / modifier / exporter / importer une bibliothèque sur le pc prof | | | | | | | |  |
|  |  |  |  |
| ~43.5 H | |  |  |  |  |  |  |  |  |  |  |
|  | lire / modifier / exporter / importer sous liste sur le pc prof | | | | | | | |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Sprint 2 | | | | | | | | | |
| 10.02.2024 -> 21.02.2024 | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | Détection des post allumés et si l'agent est allumé | | | | | | | |  |
| Semaine 7->8 | |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | Scan de l'utilisation de ressource interdites | | | | | | | |  |
| ~43.5 H | |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Sprint 3 | | | | | | | | | |
|  |  |
| 24.02.2024 -> 07.03.2024 | |  |  |  |  |  |  |  |  |  |  |
|  | Envoyer des infos depuis le client (élève) au prof | | | | | | | |  |
|  |  |  |  |
| Semaine 9->10 | |  |  |  |  |  |  |  |  |  |  |
|  | Début / fin du mode test | | | | | | | |  |
|  |  |  |  |
| ~43.5 H | |  |  |  |  |  |  |  |  |  |  |
|  | Lire les dépassements après le test (prof) | | | | | | | |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

# Analyse / Conception

## Contexte produit



Ce programme est un program desktop.

Le but est que le poste du professeur puisse définir des ressources interdites, sites web, application, fichiers, et qu’il soit notifier si un des post client (élève) utilise une ressource interdite.

## Contextes techniques

### Opérationnel

L’environnement se présente comme ceci :

Il y a une salle avec des postes fixes sous Windows 10 ou 11, normalement 16, les élèves utilisent ces postes.

Le prof lui a son ordinateur portable également sous Windows 10 ou 11, il a le client installé.

### Validation

Les postes élèves seront simulés par des laptops avec des comptes admin locaux.

Sur ces postes le programme de scan sera lancé à la main ou comme service et le port 55052 sera ouvert.

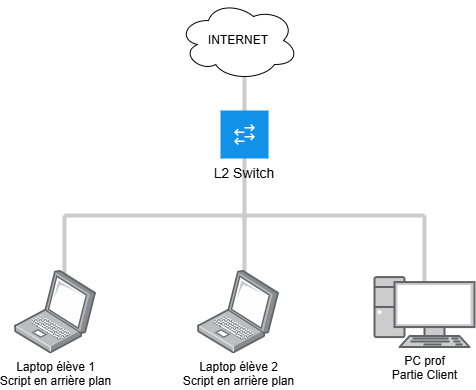
Le poste prof sera simulé par une toure de la salle.

Sur se poste on lancera l’interface au début du test, le port 55052 sera ouvert.

Toutes ces machines se trouveront sur le réseau bleu avec une connexion internet.

Toutes les machines sont dans le même sous réseau, car le prof doit pouvoir pinger les machines élèves.

Au démarrage du test on lance en premier la partie sur les portables, donc la partie de scan des élèves. Ensuite, on lance la partie graphique sur le pc du prof.

**

### Développement

Le post maitre est un post fix avec le port 55052 ouvert et 0 droits admins

Le post client (élève) est un laptop avec un compte admin local (Shadow) qui permet d’exécuter le coté client comme un simple programme.

### Justification des choix

Laptop pour le dev car on a besoin des droits admins

Finalement le but est que le prof (la console, la partie de monitoring) puisse monitorer les post des élèves avec le moins d’efforts possible donc il faut que la partie client soit automatique d’où le service qui démarrera automatiquement et le prof s’y connectera et le scan pourra commencer.

## Concept



Il y aura trois programmes différents :

* L’interface du côté du prof
* L’application en cmd du côté du prof
* L’application en cmd du côté de l’élève

Les deux applications consoles ne sont pas accessible au prof et au élèves.

Elles sont juste là pour communiquer des informations, au départ la partie du prof dit au côté élève qu’il va la monitorer. Une fois le scan lancé (annoncé par le côté du prof), le côté élève va remonter toutes infractions au côté du prof qui lui à son tour va le remonter à l’interface du prof qui va afficher les informations

## Analyse fonctionnelle

### Détecter les postes d'une salle

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir détecter les postes d'une salle en indiquant le nom de la salle. Je veux savoir si les postes sont allumés, éteint et si l'agent ShadowScan est allumé ou pas. |
| Tests d’acceptance :   |  |  | | --- | --- | | détection des postes | on lance juste la console, 0 machine détecté   Rentrer le nom de la classe dans laquelle on se trouve et appuyer sur le bouton recherche   La liste des machine de la classe apparait et on voit leurs état de connexion (Hors ligne, Allumé, En ligne) | |

### Sélectionner les Pcs à monitorer

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir sélectionner des postes dans la liste des postes détectés que je veux inclure dans le monitoring |
| Tests d'acceptance:   |  |  | | --- | --- | | Sélection des pc à monitorer | On a détecté nos machine via le nom de la salle   on sélectionne via des checkbox des machines qu'on veux monitorer   les machine sélectionnées ont leur textbox chequées | |

### Démarrer/Clôturer une session de monitoring

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir démarrer/clôturer une session de monitoring sur une liste de postes sélectionnés. |
| Tests d'acceptance:   |  |  | | --- | --- | | Lancement de la session | La session est fermée, au moins une machine est sélectionnée   on clique sur le bouton pour commencer le scan   si un dépassement arrive, on en est notifié | | Clôture de la session | La session est ouverte, au moins une machine est sélectionnée   on clique sur le bouton pour fermer le scan   on est plus notifié quand un dépassement arrive | |

### Manager des éléments à la liste de toutes les ressources

(Auteur : Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir ajouter/retirer des ressources (site web, application, fichier) à la liste qui contient toutes les ressources. |
| Tests d’acceptance :   |  |  | | --- | --- | | Ajouter un élément à la liste | On est sur la page pour ajouter un élément à la liste   on ajoute un lien/nom d'application/nom de fichier dans le champ et on appuie sur le bouton ajouter   la ressource est ajoutée à la liste | | Supprimer un élément de la liste | On est sur la page pour ajouter un élément à la liste   on clique sur un lien/nom d'application/nom de fichier dans la liste pour le sélectionner (sélection multiple possible) et on appuie sur le bouton supprimer   la ressource est retirée à la liste | |

### Manager une sous liste de ressource bannies

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir créer une sous liste en sélectionnant certaines ressources bannies. Pouvoir ajouter et retirer des ressources d'une sous liste. |
| Tests d’acceptance :   |  |  | | --- | --- | | Ajouter une ressource | On est sur la page pour ajouter un élément à la liste   on clique sur une ressource dans la liste des ressources et on appuie sur le bouton ajouter (au centre)   la ressource est ajoutée à la liste | | Supprimer une ressource | On est sur la page pour ajouter un élément à la liste   on clique sur une ressource dans la sous liste des ressources et on appuie sur le bouton supprimer (en dessous)   la ressource est supprimée à la liste | |

### Popup quand un dépassement est détecté (prof)

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir recevoir un popup quand un dépassement est détecté sur un des postes monitorés et quel est la ressource interdite. Le popup peut être désactivé depuis le client. |
| Tests d’acceptance :   |  |  | | --- | --- | | Détection d'un dépassement sur le poste d'un élève | on est sur le poste en train de travailler, les notification de l'app sont actives   l'élève se rend sur un site interdit (ex: chatgpt si l'IA est interdite)   un popup Windows nous informe du dépassement avec le nom de la ressource interdite, le nom de la machine et de l'utilisateur | |

### Afficher le Pc en rouge si un dépassement est découvert dessus

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Que quand un dépassement est détecté sur un post, il soit en rouge dans la console et que je puisse cliquer dessus pour avoir un détail de l'infraction. |
| Tests d’acceptance :   |  |  | | --- | --- | | Détection de dépassement | On est sur la page on voit tous les pc monitorés   un dépassement arrive sur un poste (ex site web banni)   le pc sur lequel le dépassement est arrivé, le fond devient rouge pour signaler le problème | |

### Popup quand un dépassement est détecté (élève)

(Auteur: Morgan Dussault)

|  |
| --- |
| En tant qu'utilisateur, je veux : Pouvoir recevoir un popup quand un dépassement est détecté sur mon post et quel est la ressource interdite. Le popup peut être désactivé depuis le client (post prof). |
| Tests d’acceptance :   |  |  | | --- | --- | | Détection de dépassement | On est sur le poste en train de travailler   on se rend sur un site interdit (ex: chatgpt si l'IA est interdite)   un popup Windows nous informe du dépassement avec le nom de la ressource interdite | |

## Stratégie de test

Les postes élèves seront simulés par des laptops avec des comptes admin locaux.

Le poste prof sera simulé par une toure de la salle.

Toutes ces machines se trouveront sur le réseau bleu avec une connexion internet.

Toutes les machines sont dans le même sous réseau, car le prof doit pouvoir pinger les machines élèves.

Au démarrage du test on lance en premier la partie sur les portables, donc la partie de scan des élèves. Ensuite, on lance la partie graphique sur le pc du prof.

Le post maitre aura le port 55052 ouvert

Le post client aura la partie client du code qui tourne comme service non-stop (démarrage automatique) ou en tant qu’application classique, son port 550522 sera également ouvert.

Voir Section 2.2.2 Validation pour plus de détails

## Risques techniques

Avoir les droits admins pour pouvoir travailler sur le développement du côté élève. Si on ouvre un port ou on ajoute un compte dans les admins locaux, ça ne reste pas par ce qu’une GPO le reset.

# Réalisation

## Points de design spécifiques

***Ce chapitre est constitué de plusieurs sous-chapitre.***

***Chaque sous-chapitre explique un point de design technique particulier, quelque chose que vous avez dû inventer pour répondre au besoin et qui ne peut pas s’expliquer par de simples commentaires dans le code.***

***Il s’agit d’explications techniques sur le fonctionnement du système. Les explications sont appuyées par des diagrammes, ou de très brefs éléments de code.***

***NE PAS mettre ici des pratiques usuelles que tout professionnel de la branche connaît déjà. Par exemple, n’EXPLIQUEZ PAS ICI CE QU’EST LE PATTERN MVC.***

***Exemple (simplifié à l’extrême) : Protection contre des formulaires mal intentionnés ou modifiés***

* ***Au moment de générer le formulaire, le script php :***
  + ***Concatène les noms de tous les champs contenus dans le formulaire***
  + ***Calcule un hash SHA256 de la chaîne obtenue***
  + ***Ajoute un input nommé « CSRF » de type hidden dans le form***
* ***A la réception du POST du fromulaire***
  + ***Concatène les noms des indices de $\_POST***
  + ***Calcule un hash SHA256 de la chaîne obtenue***
  + ***Vérifie que la valeur du champ CSRF correspond***

### *…*

### *…*

### *…*

## Déroulement

### Sprints

Sprint 1 :

Pas de user stories complétées,

La storie « Manager une sous liste de ressource bannies » et « Manager des éléments à la liste de toutes les ressources »

J’ai effectué des recherches sur gRPC.

J’ai eu pas mal de problèmes avec les droits admins sur les posts (ouvrir les ports pour gRPC, installer les mises à jour vscode, installer des versions de .NET)

1 jour d’absence

Besoins des droits admins sur les machines ou l’app est développée

Sprint 2 :

Deux stories réalisées : « Manager une sous liste de ressource bannies » et « Sélectionner les Pcs à monitorer ».

La storie « Manager des éléments à la liste de toutes les ressources » n’a pas été finie car j’ai fait le choix, sans consulter le Product owner, de ne pas ajouter l’option de suppression des ressources

La storie « Détecter les postes d'une salle » est faite en partie, ping les post (ping réseau) et récupère le statu mais ne ping pas gRPC

Manque de communication :

J’ai fait plusieurs choix sans consulter le Product Owner

Le réseau bleu (réseau de dev) est arrivé tardivement ce qui m’a limité dans mes possibilités

Sprint 3 :

***Pour chaque sprint : Résumer le déroulement du sprint, le résultat de sa revue, sa retrospective***

### Stories

Manager une sous liste de ressource bannies :

Tout s’est passé plutôt bien passé, j’ai eu un peut de peine avec l’import du fichier json dans un objet et recréer tableau correspondant pour la modification du fichier (écrase le contenu du fichier quand on fait des modifications)

Sélectionner les Pcs à monitorer :

Tout c’est bien passé, j’ai ajouté l’option pour générer des nom de pc alternatifs et ce sans en parler au Product Owner

***Résumer comment s’est passé la réalisation de chaque story, ses difficultés, les alternatives envisagées mais rejetées, ses surprises, …***

## ~~Dossier de réalisation~~

*~~Décrire la réalisation "physique" de votre projet~~*

* *~~les répertoires où le logiciel est installé~~*
* *~~la liste de tous les fichiers et une rapide description de leur contenu (des noms qui parlent !)~~*
* *~~les versions des systèmes d'exploitation et des outils logiciels~~*
* *~~la description exacte du matériel~~*
* *~~le numéro de version de votre produit !~~*
* *~~programmation et scripts: librairies externes, dictionnaire des données, reconstruction du logiciel - cible à partir des sources.~~*

*~~NOTE : Evitez d’inclure les listings des sources, à moins que vous ne désiriez en expliquer une partie vous paraissant importante. Dans ce cas n’incluez que cette partie…~~*

***Ce chapitre est éclaté en trois ci-dessous***

## Mise en place de l’environnement de travail

* ***Comment accéder au code source***
* *la liste de tous les fichiers et une rapide description de leur contenu (des noms qui parlent !)*
* *les versions des systèmes d'exploitation et des outils logiciels*
* *la description exacte du matériel*

***Ce chapitre décrit précisément comment un employé qualifié peut recréer l’environnement dans lequel vous avez effectué ce travail***

## Mise en place de l’environnement de test

* *la liste de tous les fichiers et une rapide description de leur contenu (des noms qui parlent !)*
* *les versions des systèmes d'exploitation et des outils logiciels*
* *la description exacte du matériel*
* ***La marche à suivre pour préparer l’environnement (ne pas oublier les données de test, ainsi que les mots de passe éventuels)***

***Ce chapitre décrit précisément comment un employé qualifié peut recréer le contexte décrit par la stratégie de test***

## Déploiement du produit

* *la liste de tous les fichiers et une rapide description de leur contenu (des noms qui parlent !)*
* *les versions des systèmes d'exploitation et des outils logiciels*
* *la description exacte du matériel*
* ***La marche à suivre pour préparer l’environnement (ne pas oublier les données de test, ainsi que les mots de passe éventuels)***

***Ce chapitre décrit précisément comment un employé qualifié peut mettre votre produit en production***

## Description des tests effectués

*~~Pour chaque partie testée de votre projet, il faut décrire:~~*

* *~~les conditions exactes de chaque test~~*
* *~~les preuves de test (papier ou fichier)~~*
* *~~tests sans preuve: fournir au moins une description~~*

***Reprendre les tests d’acceptance d’IceScrum au moyen de la feuille ad hoc d’IceTools***

## Bilan

### Erreurs restantes

*S'il reste encore des erreurs :*

* *Description détaillée*
* *Conséquences sur l'utilisation du produit*
* *Actions envisagées ou possibles*

### Stories

***Ce qu’on pensait faire vs ce qu’on a fait***

### Dette technique

***Reporter la*** [***dette technique***](https://www.premaccess.com/qu-est-ce-que-dette-technique-comment-la-maitriser/#:~:text=La%20dette%20technique%20survient%20quand,de%20plus%20en%20plus%20fr%C3%A9quents.) ***connue. S’appuyer sur la pratique des // TODO***

## Recours à l’intelligence artificielle

***Comment avez-vous utilisé l’IA dans votre projet.***

***Si vous ne l’avez pas utilisée, pourquoi ?***

***Ce chapitre doit contenir au minimum 200 mots***

## Liste des documents fournis

*Lister les documents fournis au client avec votre produit, en indiquant les numéros de versions*

* *le rapport de projet*
* *le manuel d'Installation (en annexe)*
* *le manuel d'Utilisation avec des exemples graphiques (en annexe)*
* *autres…*

# Conclusions

*Développez en tous cas les points suivants :*

* *Objectifs atteints / non-atteints*
* *Bilan personnel : points positifs / négatifs*
* *Difficultés particulières*
* *Suites possibles pour le projet (évolutions & améliorations)*

# Annexes

## Résumé du rapport du TPI / version succincte de la documentation

## Sources – Bibliographie

*Liste des livres utilisés (Titre, auteur, date), des sites Internet (URL) consultés, des articles (Revue, date, titre, auteur) … Et de toutes les aides externes (noms)*

## Journal de travail

|  |  |  |  |
| --- | --- | --- | --- |
| **~~Date~~** | **~~Durée~~** | **~~Activité~~** | **~~Remarques~~** |
|  |  |  |  |
|  |  |  |  |

***Référence à votre journal de travail (en PDF)***

## ~~Manuel d'Installation~~

## Manuel d'Utilisation

## Archives du projet

*Media, … dans une fourre en plastique*