

Ressource - Cahier des charges E6 (SISR)

I. Caractéristiques

La plateforme prends la forme d'une infrastructure présentée à l'examen.

Celle-ci devra :

- être accessible au jury qui disposera des fiches descriptives normalisées et des comptes en permettant l'accès.
- contenir les éléments obligatoires définis dans le cahier des charges suivant
- contenir 2 projets différents (préparer également des évolutions possibles)
- contenir à l'avance les sources de l'ensemble des outils et produits nécessaires à la réalisation des projets.

Il faudra également fournir les documents demandés plus loin.

Concernant la forme, aucune obligation n'est mentionnée. L'accès proxmox est fourni mais un étudiant peut sur le principe présenter sa propre infrastructure.

Aucune limitation concernant les systèmes, logiciels présentés.

II. Cahier des charges

Info : La plupart des points obligatoires évoqués dans ce chapitre sont cumulatifs, aussi une solution Active directory avec deux contrôleurs de domaines couvrira par exemple à la fois

le "service d'authentification", la "solution garantissant la continuité d'un service" et la "solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion.

Conseil : Comme vous n'êtes pas limités dans la forme, faites avec les solutions sur lesquelles vous vous sentez le plus à l'aise.

2.1 Éléments obligatoires communs aux deux options

Description	Exemples
Un service d'authentification pour les utilisateurs internes et externes à l'organisation	Active directory, Samba, Keycloak...
Un SGBD	Souvent un serveur mariaDB qui supportera les DB de GLPI et de la solution de supervision. <i>Attention : il faudra à minima connaître la structure de vos bases et tables et faire des requêtes SQL basiques.</i>
Un accès sécurisé à internet	La plupart du temps un squid sur votre pfsense / OPNsense
Un environnement de travail collaboratif	exchange, zimbra, nextcloud, ...
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel opensource.	Minimum un serveur windows et un serveur sur une distribution unix de votre choix (debian, ubuntu, centOS, redhat, etc...)
Une solution de sauvegarde	Veeam backup, proxmox backup, veeam agent, altaro, etc... <i>Attention : il faudra être capable de restaurer de la donnée.</i>
Des ressources dont l'accès est sécurisé et soumis à habilitation	Tout est valide tant qu'il y a un système de permission. Cela peut être par exemple un serveur de fichier.
Deux types de terminaux, dont un mobile	Difficilement réalisable dans un cadre virtualisé, cela sera pris en compte. Un poste client simulant un pc portable sera suffisant.

2.2 Outils pour la gestion de la sécurité

Description	Exemples
Gestion des incidents	GLPI, OS Ticket, etc...
Détection / prévention des intrusions	SNORT sur pfsense
Chiffrement	VPN, ou HTTPS (sur reverse proxy par exemple)
Analyse du trafic	nTOPng, wireshark

2.3 Eléments obligatoires propre à l'option SISR

Description	Exemples
Un réseau comportant plusieurs périmètres de sécurité	à minima un réseau local et une DMZ.
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en terme de sécurité et de haute disponibilité	
Un logiciel d'analyse de trames	wireshark sur toute les machines
Un logiciel de gestion des configurations	agent GLPI inventory sur les serveurs, WSUS, foreman, ...
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	mRemoteNG, WAC, RSAT, ...
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes.	Zabbix, nagios, ...
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externe (type internet ou extranet)	VPN
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Mettre des serveurs en HA --> failover
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	Mettre des serveurs en HA --> loadbalancing

2.4 Éléments au choix

Info : Parmi les 4 proposition suivantes, en choisir au moins une.

Description	Exemples
Une solution permettant la connexion sécurisée entre deux sites distants	VPN ipSec
Une solution permettant le déploiement des solutions technique d'accès	WDS, Foreman
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting	Scripts powershell pour l'automatisation de tâches
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	par exemple, activer les audits de connexions active directory et avoir des sondes permettant de relever les tentatives en échec, alerter. Ou faire de l'analyse de fichiers journaux avec splunk.

Conseil : Voici une liste de produits que vous pouvez implémenter dans la plateforme. Il s'agit de propositions / pistes de réflexions. Ne vous y limitez pas et faites des recherches sur le sujet afin de proposer vos produits !

Catalogue de produits

III. Préparation du dossier

Le dossier devra contenir les éléments suivants :

- Un schéma d'architecture contenant les réseaux, hôtes, IP.

- Une fiche avec les Logins et mots de passe
- Des fiches descriptives remplies donc le modèle est fourni en annexe

IV. Déroulé de l'examen

Attention : Les dossiers des plateformes sont à remettre 10 jours avant l'examen. L'accès aux plateformes sera également scellé.

L'examen se déroule en 2 phases :

1. Phase d'étude
2. Phase de réalisation technique

4.1 Phase d'étude

Au début de cette phase, l'examineur remettra au candidat un dossier d'expression du besoin basé sur l'un des deux projets préparé.

30 minutes de préparation :

- Prendre connaissance du dossier et préparer l'entretien
- Interpréter le dossier pour en dégager une analyse du besoin
- Préparer une architecture technique

20 minutes d'entretien :

Suite à la réflexion menée lors de la préparation, il faudra présenter les éléments suivants :

- de présenter l'analyse et l'interprétation de l'expression des besoins ;
- de proposer des spécifications techniques et le choix des outils les plus adaptés pour la réalisation attendue ;
- de présenter et de justifier la démarche envisagée pour répondre aux besoins exprimés.

Lors de cette première phase, la commission d'interrogation peut être amenée à proposer à la personne candidate un ajustement de la démarche à mettre en œuvre.

4.2 Phase de réalisation

Une fois la solution choisie et les ajustements faits.

1 heure de préparation :

- Réaliser en autonomie le projet ainsi que les ajustements demandés.
- Vérifier le bon fonctionnement de la plateforme.

20 minutes d'entretien :

Au terme de la préparation, la commission procède à la recette de la solution et mène un entretien d'explicitation :

- à partir de l'environnement de travail mis à sa disposition, la personne candidate présente sa solution et tous les éléments nécessaires pour justifier la conformité de sa production aux exigences de la demande ;
- la commission questionne ensuite la personne candidate et vérifie l'opérationnalité de la solution, la pertinence des outils utilisés et de la démarche suivie.

Revision #2

Created 2026-07-17 14:28:40 UTC by Olivier

Updated 2026-07-17 14:29:42 UTC by Olivier