

RECSI

Référentiel de Conception des Systèmes d'Information

Version 2025.3

ADEME - DETSI

Version 2025.3 du 07 juillet 2025

Sommaire

1. Préambule	5
2. Précautions de lecture	7
3. Environnements techniques	8
4. Socles techniques	9
4.1 Bases de Données	9
5. Plateformes et Socles Logiciels	10
6. Solutions techniques	11
7. Règles de développement	12
7.1 Gestion des ports	12
7.2 Envoi de mails	12
7.3 Configuration	12
7.4 Version du site	13
7.5 PHP et les shorttags	13
7.6 Webservices	13
7.7 Stockage des éléments liés à la BDD	13
7.8 Logs	14
8. Briques logicielles	15
9. Composants applicatifs	16
9.1 Animations et widgets	16
9.2 Mise à jour de composants	16
9.3 Génération de PDF	16
9.4 Librairies graphiques	16
9.5 Fédération d'authentification et d'identification	16
9.6 Captcha	16
9.7 Moteurs de recherche	17
9.8 Cartographie	17
9.9 Management et développement d'interfaces (API)	17
9.10 Boutiques en ligne	18
10. Optimisations techniques pour le référencement naturel (SEO) et l'expérience utilisateur	19
11. Suivi statistiques (outils de mesure d'audience et gestion des cookies)	24
12. Chartes graphiques	27
12.1 Ressources	27
13. Numérique responsable	28
14. Politique de sécurité	29
14.1 [OBL] L'application doit pouvoir fonctionner derrière le pare feu applicatif "Cloudflare"	29

14.2	[OBL] Suivi et détection des failles de sécurité	29
14.3	[PRECO] Scripts	29
14.4	Certificat (https)	30
14.5	Authentification	30
14.6	Entrées / Sorties	30
14.7	Fermeture automatique des sessions	31
14.8	Désactivation des comptes par défaut	31
14.9	Tests	31
14.10	Mises à jour	31
15.	Réglementation	32
16.	RGPD - Données personnelles	33
17.	Accessibilité Numérique	35
18.	Livrables	36
19.	Dématérialisation “administrative” (process internes, documents à valeur juridique)	38
19.1	Signature électronique	38
19.2	GED (Gestion Électronique des Documents) / ECM (gestion de contenu d’entreprise) :	38
19.3	SAE (Système d’Archivage Électronique) :	38
19.4	Orchestracteur de processus multi-acteurs et multi-flux :	38
20.	Processus de déploiement	39
21.	Versions des composants applicatifs	44
21.1	Versions des composants applicatifs	44
21.2	Poste Utilisateur	44
22.	Anciennes versions du RECSI	46
23.	Annexes	47
23.1	Liste des annexes disponibles :	47
24.	Annexes	48
24.1	Modèles de conception fonctionnelle	48
25.	Pages de supervision et de validation d’installation	49
25.1	Préambule	49
25.2	Contenu de la réponse	49
25.3	Rubriques	49
25.4	Paramètres de la requête	50
25.5	Contenu de la réponse	51
25.6	Exemples pour une API	54
25.7	Exemples pour le front d'une application	60
26.	Annexes	69
26.1	Recommandations Sécurité	69
27.	Guides Devops	73

28. Mentions Légales	74
29. Politique de protection des données personnelles	75
30. Politique des cookies	76
31. Hébergement - Accords de niveau de service	77
31.1 SLA sur les classes de criticité des applications	77
31.2 Taux de disponibilité sur la plateforme	77
31.3 SLA sur les tickets	78
31.4 SLA sur les environnements conteneurisés	79



RECSI - Référentiel de Conception des Systèmes d'Informations

Info : Le PDF de cette version du site est disponible à [cet emplacement](#).

Info : L'accès au site en ligne (dernière version applicable) est protégé par login et mot de passe. Faire une demande au Pôle Infrastructure Numérique de l'ADEME pour en disposer.

Important - 1

Les nouvelles applications devront être conformes aux spécifications liées à la nouvelle infrastructure d'hébergement d'applications modernes en mode DEVOPS en cloud dont l'infogérance sera déléguée à un prestataire (Kaliop/DRI), à savoir :

- Cloud
- Respect des bonnes pratiques et process DEVOPS accompagné par la société ayant en charge l'exécution de l'infogérance,
- Kubernetes
- Docker
- Gitlab.com

Les applications opérées en production chez l'hébergeur historique (DRI) sont basées sur ces technologies :

- Gitlab de l'ADEME: git.ademe.fr
- Docker
- Docker swarm
- Les applications déployées dans l'environnement 'legacy' ayant pour vocation à migrer vers le cloud tel que décrit ci-dessus, le prestataire TMA devra s'assurer (s'engager à ce) que son application puisse migrer. Il devra également s'assurer qu'elle soit prise en charge à moindre coût par le prestataire ayant en charge l'infogérance des applications en cloud.

1. Préambule

Ce référentiel a pour objet de préciser les normes, technologies et recommandations que doivent satisfaire les produits développés pour le compte de l'ADEME. Le respect de ce référentiel permet à la DETSI et à Digital&Co. de garantir l'intégration, la maintenabilité, la sécurité et la cohérence de ces produits.

Digital & Co est un service de l'ADEME en charge de l'expérience utilisateurs, des statistiques, de la charte graphique web, de l'accessibilité numérique, du référencement naturel et plus globalement, le service offre de manière générale un accompagnement webmarketing au sein de l'agence

Ce référentiel concerne les développements des produits à destination des cibles de l'ADEME (entreprises, collectivités, particuliers et la recherche).

Ce référentiel est surtout un outil de dialogue entre la DETSI, Digital&Co, les Maîtrises d'Ouvrages et les prestataires sur toutes les phases du processus numérique. Il évolue régulièrement, notamment pour intégrer des évolutions liées à la sécurité ou aux composants d'architecture.



2. Précautions de lecture

Les briques applicatives, les composants logiciels, les environnements d'exécution, les exigences sont dénommés "références" dans le reste du document. Ces références sont décrites dans les chapitres présentés par la suite. Les références sont précédées d'un sigle caractérisant leur statut :

Signes utilisés

[PRECO] Préconisation

[INFO] Information

[PRIO] Choix à privilégier

[DMD] Choix à valider par la DETSI et/ou par Digital&Co

[OBL] Obligatoire

Les références régies par des versions sont décrites au dernier chapitre de ce document : [Versions des Références](#).

3. Environnements techniques

[PRIO] Toute nouvelle application doit être cloud-native.

[OBL] Conteneurisation des applications Les applications doivent être livrées sous le format d'un conteneur sous technologie Docker. Les processus de déploiement sont décrits au niveau des annexes.

[DMD] Si la conteneurisation des applications n'est pas possible, il conviendra de le spécifier et dans cas l'utilisation de VM sera possible à titre dérogatoire.

[DMD] Hébergement IAAS : l'utilisation d'un hébergement IaaS devra être justifié avant son implémentation.

[PRIO] Tous les environnements sont hébergés par l'ADEME.

[PRIO] Par défaut l'ADEME met à disposition 4 environnements : • Intégration : Dédié à l'équipe de développement de l'application • Recette : Permet de faire les tests fonctionnels • Pré-Production : Pour les tests de déploiement et la reproduction des anomalies de production • Production

[DMD] Des environnements supplémentaires peuvent être mis à disposition. Il y a 2 types d'environnements : • Hors Production (comme l'intégration, la recette ou la préproduction) • Production pour avoir par exemple 2 versions du site en production

4. Socles techniques

[OBL] Image de référence : usage de l'image de référence Docker mise à disposition par l'ADEME.

4.1 Bases de Données

[OBL] Le nom de la base de données ne doit pas figurer dans les scripts de création de la base de données.

[OBL] Tous les paramètres de connexion aux bases de données doivent être définis dans un seul et même fichier (serveur, utilisateur, mot de passe...).

[OBL] Ces spécificités d'architecture, comme le modèle de données, **doivent être documentés dans le DAT**.

[OBL] La base de données est séparée du serveur applicatif

[OBL] Utiliser des services de base de données managées proposés

- **[PRIO]** MySQL
- **[DMD]** PostgreSQL
- **[DMD]** SQL Server ou autre moteur BDaaS disponible

5. Plateformes et Socles Logiciels

[PRIO] Evaluer en priorité la possibilité d'utiliser le service « Sites-faciles ».

[DMD] PAD Drupal

Le CMS Drupal est une réponse à des besoins en fonctionnalités de communication assez étoffées (Newsletter, pop-in, sondage, flux Rss, ...). Les fonctionnalités et l'ergonomie communément utilisées à l'ADEME sont packagées dans un PAD Drupal (Package ADEME Drupal). Le PAD bénéficie d'un déploiement rapide, d'évolutions et corrections communes à l'ensemble de l'ADEME.

[OBL] L'ensemble des déploiements doit être effectué via Drush et le module features.

[DMD] Drupal

Le CMS Drupal est une réponse à des besoins en fonctionnalités de communication assez étoffées et communes pour des sites de communication (Newsletter, pop-in, sondage, flux Rss, ...). Si pour des besoins spécifiques le CMS Drupal doit être étayé d'une part minime de développements spécifiques (IFrame, Cartographie avancée, ...), le CMS natif Drupal sera privilégié.

[OBL] L'ensemble des déploiements doit être effectué via Drush et le module features.

[OBL] Pour toute application ayant un Back-office (Wordpress, Drupal, ...)

Pour toute nouvelle application, il est obligatoire de fournir à production@ademe.fr un accès en mode administration (via un canal sécurisé).

[OBL] L'url et les identifiants par défaut d'administration sont interdits

[DMD] WordPress

La solution WordPress est privilégiée pour des besoins en fonctionnalités simples de communication descendante (articles, documents, moteur de recherche, formulaire de contact, réseaux sociaux, ...).

[DMD] Autre CMS (Strapi, etc.)

6. Solutions techniques

[OBL] Langages actuels bénéficiant d'une TMA dans les marchés ADEME ainsi que d'une communauté active.

- Exemples non exhaustifs : JS et déclinaisons, PHP, Python

7. Règles de développement

7.1 Gestion des ports

[OBL] L'application devra être développée afin de :

- Pouvoir être exécutée sur un port différent des ports 80, 8080, 443
- L'accès à la base de données MySQL devra pouvoir être faite sur un numéro de port différent que celui par défaut (3306).

7.2 Envoi de mails

[OBL] L'envoi des mails doit se faire sur le port 25 (protocole SMTP) vers un serveur de mails relais.

[OBL] La désactivation de l'envoi de mail ou la redirection des emails vers une adresse mail unique devra pouvoir être possible via un fichier de configuration cf ci-après paragraphe 'Configuration', ceci afin d'éviter tout risque d'envoi de mails intempestifs lors des phases de recettes.

[PRIO] Concernant les campagnes d'e-mailing et les newsletters, l'ADEME met à disposition un outil permettant de gérer les envois de mails massifs de manière efficace. Cet outil permet la professionnalisation des campagnes d'e-mailing (gestion des listes de destinataires, rapports statistiques...) tout en centralisant les données.

@ Contactez le service Digital&Co de l'ADEME pour toute campagne d'e-mailing.

[OBL] E-mailing : L'envoi d'e-mails devra être conforme au RGPD.

[OBL] Newsletter et abonnements électroniques : l'inscription à une newsletter est une collecte de données personnelles, puisque l'adresse email de l'abonné est stockée et utilisée par le diffuseur de la newsletter. Elle est donc soumise à l'article 32 de la Loi Informatique et Libertés, qui précise que l'utilisateur doit être informé :

- de l'identité du responsable du traitement ou de son représentant ; de l'identité de l'expéditeur ;
- de la finalité du traitement (ex. gestion de fichiers spectateurs, diffusion...) ;
- du caractère obligatoire ou facultatif des informations collectées ; des destinataires de ces informations ;
- des conséquences éventuelles d'un défaut de réponse ;
- de l'existence de droits pour les personnes fichées et auprès de qui les faire valoir ; des transmissions envisagées.

Chaque newsletter doit inclure un ou plusieurs liens vers les mentions légales relatives aux informations personnelles de vos abonnés.

Le désabonnement ou la modification des coordonnées : selon l'article L34-5 du Code des postes et des communications électroniques, vous êtes tenu d'indiquer les coordonnées auxquelles le destinataire peut demander le désabonnement de votre newsletter.

Concrètement, vous devez faire apparaître un lien de désabonnement dans le footer (le pied de page) de la newsletter.

Obligations d'affichage et textes à insérer disponibles sur l'intrADEME, dans la rubrique dédiée au [RGPD](#) (voir la fiche pratique « Newsletter »).

7.3 Configuration

[OBL] Les fichiers de configuration de l'application devront clairement être précisés dans la documentation d'installation. Ces fichiers de configuration devront à minima permettre de définir certains paramètres de l'application tels que les envois de mail en fonction du type d'environnement (production ou intégration), cet environnement étant obligatoirement défini dans le virtualhost. Chaque application dispose de son propre virtualhost dédié et ce même si celle-ci est hébergé sur un serveur [VM] mutualisé

Les variables PHP étant communes à l'ensemble des applications hébergées par le serveur Apache, toute variable devant être modifiée devra être précisée afin de l'inclure dans le virtualhost dédié à l'application (par exemple : `PHP_value upload_max_filesize...`).

Utilisation de Javascript

Dans le cas du développement d'un Widget ou d'une animation HTML, les éléments suivants doivent être pris en compte pour une intégration réussie dans les sites de l'ADEME :

1. Si l'animation reste relativement simple, il est préférable de ne pas utiliser les librairies jQuery mais du Javascript pur.
2. Si l'animation nécessite l'utilisation de jQuery, il est important d'éviter les problèmes de conflits entre les librairies JQuery Ademe et celles de l'animation. Pour cela vérifier si jQuery est déjà chargé par le site. Si ce n'est pas le cas, charger la version jQuery du widget, sinon activer le mode "no conflict".

Utilisation des CSS

Il est préférable d'utiliser l'héritage de classe et définir uniquement les éléments au sein d'un conteneur défini, afin d'éviter de parasiter les classes déjà potentiellement existantes.

Dans tous les cas

Il est important de palier aux erreurs de type "cross-domain". Enfin, il est important de détecter le device en cours. En effet, sur mobile le comportement est souvent différent. Il peut être intéressant de proposer l'ouverture de l'animation dans une nouvelle fenêtre.

Cas particulier de Ademe.fr

Dans le cas particulier du site Ademe.fr, les librairies JQuery sont chargées en fin de chargement des pages. La nouvelle animation doit donc être chargée dans la page uniquement lorsque l'ensemble de la page Ademe.fr est construite dans le navigateur. Pour cela, le chargement de l'animation peut être effectué depuis l'action "onLoad".

[OBL] Les spécificités d'architecture, comme l'usage de services externes, doivent être documentés dans le DAT.

7.4 Version du site

[OBL] La version du site doit être directement intégrée dans le bas de page à droite. Le numéro de version doit être défini dans l'un des fichiers de configuration voire dans la base de données.

7.5 PHP et les shorttags

[OBL] L'ADEME n'autorise pas les short tags PHP. Cette contrainte est à prendre en compte dans les développements PHP et donc Drupal.

7.6 Webservices

[OBL] Les webservices développés pour l'ADEME doivent s'appuyer au maximum sur les technologies REST et JSON.

[OBL] Ces spécificités d'architecture, comme l'usage de services externes, doivent être documentés dans le DAT.

7.7 Stockage des éléments liés à la BDD

[OBL] La définition du schéma de la base de données et des éventuelles procédures stockées, index, triggers etc... doivent être stockées au niveau du projet GIT ADEME, soit en étant intégrées directement au code de l'applicatif en cas de gestion automatique, soit de façon manuelle. Plus généralement, tous les éléments nécessaires à l'initialisation d'une base de données fonctionnelle doivent être disponibles au niveau du projet GIT.

7.8 Logs

[OBL] Le prestataire portera une attention particulière aux logs générés par l'application pour qu'ils soient exploitables sur les différents environnements. Ils doivent être suffisamment concis pour retrouver l'information utile et suffisamment détaillés pour analyser les erreurs.

[INFO] Les logs des composants techniques (base de données, ...) sont automatiquement remontés par l'hébergeur de l'application dans l'outil de gestion des logs.

7.8.1 - Niveau :

[OBL] Chaque log produit sera caractérisé par son niveau. Chaque environnement choisira de tracer le niveau de log correspondant à ses besoins selon sur les quatre niveaux suivants :

- ERROR
- WARN
- INFO
- DEBUG

En fonction de la nature des environnements, il devra être possible de définir le niveau de logs produits afin d'optimiser leur exploitation.

7.8.2 - Format :

Un seul format peut être utilisé afin qu'une centralisation de l'ensemble des logs puissent être réalisés pour faciliter leur exploitation.

[OBL] L'ensemble des logs doivent être redirigés vers les sorties standards « stdout » et « stderr ».

7.8.3 - Structure :

Dans le cadre de l'utilisation de log, différentes informations doivent composer la log afin de faciliter leur exploitation :

[OBL]

- message : contenu explicite du log.

[PRIO]

- taskName : Nom principal de traitement/fonction produisant la log. Cette notion permettra d'identifier rapidement la brique fonctionnelle qui a produit ce message.
- status : permet de préciser le résultat du traitement (OK/KO).
- elapsed : durée du traitement ayant généré cette log.

[INFO]

- idUser : identifiant de l'utilisateur applicatif qui a produit ce log.
- correlationID : identifiant de chainage qui permet de regrouper différents logs produits lors d'un même traitement.
- subTaskName : nom secondaire de traitement/fonction produisant la log. Ce nom permet d'identifier de manière plus précise le déclencheur du log.

8. Briques logicielles

- **[PRIO]** Frameworks Symfony
- **[DMD]** Frameworks Zend
- **[DMD]** Frameworks AngularJS
- **[DMD]** NodeJS
- **[INFO]** Frameworks JQuery
- **[INFO]** Frameworks Bootstrap
- **[PRECO]** OPcache

Des briques logicielles telles l'extension **OPcache** (<http://php.net/manual/fr/book.opcache.php>, remplaçante d'APC depuis la version 5.5.0) sont recommandées. Celle-ci permet de mettre en cache mémoire le code PHP ainsi que certaines requêtes SQL.

- **[PRIO]** InnoDB

Le gestionnaire de table utilisé par défaut doit être InnoDB.

- **[DMD]** MyIsam

Pour répondre à des besoins spécifiques de performance, le moteur MyIsam est toléré.

- **[OBL]** API PDO

Dans la mesure du possible des couches d'abstraction doivent être utilisées pour accéder aux données. C'est par exemple l'utilisation de l'API PDO en PHP.

9. Composants applicatifs

9.1 Animations et widgets

[OBL] Les animations Flash ne sont pas autorisées. Les animations doivent être réalisées à l'aide de la technologie HTML5, SVG ou de technologies Javascript.

9.2 Mise à jour de composants

[OBL] L'hébergeur fera une maj auto des composants lors d'une maj mineure sans demande de validation de la part l'équipe projet.

9.3 Génération de PDF

[INFO] L'ADEME dispose d'un générateur de PDF mutualisé ne donnant plus satisfaction (incompatibilité technique, solution non maintenue). Faute d'alternative, dans le cas où l'application doit produire des PDF, il n'est plus impératif de passer par ce serveur mutualisé.

@ Contactez l'aMOA projet du "Pôle Projets" pour obtenir les informations d'utilisation de ce générateur.

[OBL] Les spécificités d'architecture, comme l'usage de services externes, doivent être documentés dans le DAT.

9.4 Librairies graphiques

[OBL] Pour la génération de graphiques statistiques, les développements doivent s'appuyer sur la librairie Google Charts (<https://developers.google.com/chart/>).

[PRECO] Si les graphiques comportent des données personnelles, commerciales ou industrielles, cette librairie graphique n'est pas recommandée.

9.5 Fédération d'authentification et d'identification

[PRIO] Keycloak fournit un Service de Gestion de l'Identité & de l'Authentification qui a pour but de gérer le cycle de vie des identités numériques des utilisateurs des applications Ademe.

C'est une solution 100% Opensource.

Keycloak met à disposition plusieurs méthodes d'authentification de type WebSSO : l'ensemble de ces solutions repose sur le principe de délégation de l'authentification qui n'est plus à la charge de l'application. Une relation de confiance est mise en place entre l'application et la solution d'authentification.

- **[PRIO]** OpenID Connect
- **[INFO]** OAuth 2
- **[INFO]** SAML 2

Les règles de gestion et de mise en place sont disponibles dans l'espace documentaire.

9.6 Captcha

[OBL] Respect du RGPD, Remplacement du CAPTCHA reCAPTCHA (GOOGLE) par Orange live Identity qui a pour caractéristiques principales :

- Conformité RGPD • Souveraineté. Solutions développées et hébergées par Orange Business en France
- Solution monitorée, mise à disposition de statistiques • Mise à disposition de plugins Wordpress, DRUPAL • Compatible avec les langages de développement tels que : Java, PHP

Pour implémenter le Orange live Identity, merci de vous rapprocher de la [DETSI](#).

Un document d'accompagnement à la mise en place de cette solution est disponible à cet emplacement : [Lien](#)

9.7 Moteurs de recherche

[OBL] L'ADEME utilise les moteurs de recherche SolR ou Elasticsearch.

@ Contactez l'aMOA projet du "Pôle Projets" pour toute installation d'un moteur de recherche sur une application.

[OBL] Les moteurs de recherche sont déployés sous forme de container Docker. Le candidat indiquera clairement la version du moteur de recherche retenue et fournira les fichiers de configuration.

9.8 Cartographie

L'ADEME utilise plusieurs systèmes de cartographie :

- **[DMD]** OpenStreetMap pour des cartographies simples. Google Maps n'est pas autorisé.
- **[DMD]** Power BI : Cet outil propose des datavisualisations cartographiques, en particulier en utilisant le composant [Azure Maps](#), qui est utilisé à l'ADEME en association avec les [ressources SIG](#) qui figurent sur le portail interne des données ADEME. Les rapports Power BI peuvent être embarqués via des liens ou iframes, ou pilotés par API (Power BI Embedded) pour des besoins plus fins.
- **[DMD]** Data Fair : cet outil utilisé pour la publication des jeux de données de l'ADEME (<https://data.ademe.fr/>) propose aussi plusieurs [datavisualisations cartographiques](#) pouvant être embarquées dans des iframes.

[OBL] Ces spécificités d'architecture, comme l'usage de services externes, doivent être documentés dans le DAT.

[INFO] Les outils de bureautique que nous conseillons également aux utilisateurs sont Excel pour la réalisation rapide de cartes simples et QGIS qui s'adresse davantage à des géomaticiens pour la réalisation de cartes personnalisées.

Contact ADEME sur les sujets cartographie : Patrice PILLET ([DETSI](#))

9.9 Management et développement d'interfaces (API)

Toute interopérabilité interne ou externe doit être évaluée et validée par l'équipe API Management pour privilégier, autant que pertinent, la réutilisation des développements, leur sécurisation leur supervision et la réduction des adhérences et au travers de Mulesoft.

L'ADEME utilise l'outil Mulesoft.

Cas d'usage Mulesoft :

- Toutes les interfaces inter-applicatives pérennes pour lesquelles il n'existe pas de système point à point supervisé en standard. Cela concerne toutes les applications ADEME que les utilisateurs soient internes ou externes et qu'il s'agisse d'un développement spécifique ou d'un progiciel, sauf, pour les progiciels lorsque ceux-ci fournissent nativement un système d'interfaces point à point supervisé.
- Toutes les publications d'API vers l'externe qui ne disposent pas de couche de sécurisation et dont on souhaite maîtriser la supervision et /ou le versionning.

[OBL] Toute application proposant un service de mise à disposition de données Via API, doit mettre en place un "rate limit" permettant de protéger l'infrastructure de publication de données.

9.10 Boutiques en ligne

[OBL] L'utilisation du CMS PrestaShop (application Web open source permettant de créer une boutique en ligne) n'est pas autorisée.

10. Optimisations techniques pour le référencement naturel (SEO) et l'expérience utilisateur

Contact

Personnes référentes à contacter au sein du service Digital&CO de l'ADEME :

- Sophie EVEN – Chef de Projets Webmarketing – Sophie.even@ademe.fr
- Estelle RIBOT – Coordinatrice du Pôle Web – Estelle.ribot@ademe.fr

Le socle technique d'un site est l'épine dorsale du référencement naturel. L'application des bonnes pratiques suivantes devra obligatoirement être prise en compte par le prestataire technique (MOE).

Le prestataire technique devra appliquer ces règles standards et être force de conseils pour proposer d'autres axes d'optimisation technique en faveur du référencement naturel.

[PRIO] Conception mobile first

La conception mobile doit prévaloir dans toutes les phases du projet de manière à maximiser l'expérience utilisateur et l'optimisation des performances mobiles. La version mobile d'un site web est celle qui est explorée en priorité par les robots.

Le site doit donc être pensé selon les règles "Mobile First" de Google :

- Pas de programmation superflue
- Une performance maximale sur tous les terminaux
- Un accès rapide aux informations
- Un design adapté aux écrans des smartphones
- Pas de grandes images et de fonctions inutiles
- Des codes sources optimisés
- Optimisations des images et des ressources Javascript et CSS

Si le mobile first ne peut pas être priorisé pour un projet, le prestataire technique devra livrer une solution responsive pour adapter l'ensemble des contenus à la navigation sur smartphone. L'ergonomie et les performances techniques devront être maximisées et optimisées sur les différents navigateurs Internet.

[OBL] Navigateurs Internet

Sauf indications précisées directement dans le cahier des charges la liste des navigateurs pour lesquels la compatibilité de tous les développements devra être assurée à 100% sera établie dès la conception en fonction des cibles de l'application. Les navigateurs utilisés par nos cibles sont cités au chapitre [Version des références](#).

Pour les autres navigateurs, il est demandé au prestataire technique de s'assurer que les fonctions principales de l'application soient opérationnelles.

[OBL] Fil d'ariane et menu de navigation

Le prestataire technique devra intégrer un fil d'ariane sur le site pour faciliter la navigation des utilisateurs et l'exploration du site par les robots des moteurs de recherche.

Les sites développés sous Wordpress et Drupal devront s'appuyer sur les systèmes proposés nativement par les CMS en lien avec la gestion dynamique du menu.

Le fil d'ariane doit être affiché en haut de la page sous le menu de navigation, comme indiqué dans la charte graphique web.

Le menu de navigation doit être administrable en backoffice et généré automatiquement pour les sites développés sous Wordpress ou Drupal. L'accès à l'administration du menu doit être accessible aux contributeurs.

[OBL] Balisage sémantique

Le balisage des pages et des contenus doit être effectué selon les règles de l'art.

Quelques règles à respecter :

- Ne pas intégrer de H1 sur les logos
- La balise H1 doit présenter l'objectif de la page pour les utilisateurs, elle doit comporter le mot clé principal du sujet présenté. Pour une page d'accueil ou une page de type « Hub » il s'agira de présenter la raison d'être du site ou de la rubrique et les services proposés aux visiteurs.
- Respecter la hiérarchisation des titres (H1, H2, H3, H4...) et des sections pour structurer les pages et leurs contenus.
- Ne pas utiliser le balisage sémantique pour gérer des contraintes de webdesign. Le balisage sémantique doit être réservé à la structuration des contenus du site. Des styles CSS similaires aux titres peuvent être créés pour traiter les aspects de mise en forme purement esthétiques.
- Ajouter des balises alt (texte alternatif) sur des images à valeur informative (règle similaire au RGAA). Cette option doit être accessible en backoffice.
- Les balises title, méta title et méta description doivent figurer sur toutes les pages du site, dans la partie <head></head> L'administration de ces balises doit être possible en backoffice pour tous les contributeurs. Le nombre limite de caractères doit être respecté pour optimiser l'affichage des résultats sur les moteurs de recherche.
- La balise title doit reprendre le titre de la page (ce titre est visible dans l'onglet du navigateur, il doit contenir le mot clé principal de la page). Aperçu de la balise : <title></title>
- La méta title doit contenir le titre et/ou l'objectif de la page de façon claire et pertinente aux utilisateurs pour les inciter au clic (ce titre est repris dans les résultats des moteurs de recherche, il doit contenir le mot clé principal de la page). Aperçu de la balise : <meta title=" " />
- La méta description doit résumer les contenus / services de la page pour les utilisateurs (cette description est reprise dans les résultats des moteurs de recherche, elle doit contenir le mot clé principal de la page). Aperçu de la balise : <meta description=" " />
- Les balises suivantes devront également être administrables pour chaque page :
 - Balise d'indexation <meta name="robots" content=" ">
 - Balise d'url de référence SEO <link rel="canonical" href=" " />
 - Balise linguistique <link rel="alternate" hreflang=" " href=" " />

[PRIO] Plugins et modules à installer en backoffice pour le SEO

- Module / Plugin SEOPress pour paramétrer les balises SEO de toutes les pages en backoffice
- Module / Plugin pour optimiser la mise cache et la minification des ressources (images, JS, CSS..) en backoffice
- Module / Plugin pour gérer les redirections 301 et 302 en backoffice
- Module / Plugin pour gérer la réécriture des urls en backoffice

[PRIO] Microdonnées

Pour améliorer l'indexation et l'affichage de nos pages dans les premiers résultats des moteurs de recherche, le prestataire pourra avoir recours à l'intégration de données structurées avec le balisage JSON-LD.

Ces microdonnées sont interprétées par les robots pour enrichir l'apparence des résultats et inciter davantage au clic (featured snippets : sitelinks, recommandations étoiles, prix, informations sur l'auteur d'un article, etc...).

Découvrir [l'outil de balisage de Google](#).

[PRIO] Les liens d'ancrage dans les titres et sous-titres

Le prestataire en charge du webmastering éditorial pourra intégrer des liens d'ancrage dans les titres et sous-titres d'une page web pour améliorer l'expérience utilisateur et à faciliter la génération des « featured snippets » sur les résultats des moteurs de recherches.

Le choix des ID d'ancrage devra être pertinent, riche en mots-clés et indiquer aux internautes et aux moteurs de recherche le contenu de chaque section.

Etapes à suivre pour ajouter un lien d'ancrage HTML :

1. Attribuer l'attribut ID avec la balise <a>

Nous pouvons attacher un ID à un titre avec la balise <a> selon un processus similaire à celui utilisé pour créer des hyperliens.

Supposons que nous ayons créé une page web sur les solutions de référencement et que nous souhaitions ajouter un lien vers une section sur le SEO. Nous créons un titre de deuxième niveau pour la section, puis nous ajoutons un lien d'ancrage avec la balise <a> :

- <Anchor Text/><h2>SEO</h2>

Nous pouvons également inclure l'ID d'ancrage dans la balise de titre :

- <Anchor Text/><h2 id="SEO">Section name</h2>

Pour ajouter un ID d'ancrage à une image, incluez-le dans la balise d'image HTML en tant qu'attribut :

- <Anchor Text/>

2. Ajouter l'attribut d'ID à un lien HTML

Pour créer le lien d'ancrage, vous utiliserez l'attribut href. Toutefois, au lieu d'ajouter un lien vers une page web, vous utiliserez l'ID d'ancrage avec le signe dièse (#) :

- <Anchor Text/>SEO Section

Au clic sur le lien l'utilisateur sera directement redirigé vers la section ciblée sur la page.

[OBL] URL rewriting

Le principe de la réécriture d'url est de mettre en place un système pour interpréter les formats d'adresse des pages web dynamiques. Le système devra permettre de définir des URLs explicites et pertinentes pour les utilisateurs, en cohérence avec l'arborescence du site.

Cette action permettra de renforcer la sécurité du site en masquant les noms des variables passées dans l'url. Les règles de réécriture devront être accessibles et modifiables en backoffice. Pour les CMS Wordpress et Drupal le prestataire devra utiliser les modules standards disponibles.

Pour les CMS Drupal le prestataire devra configurer le système pour réécrire les urls node.

[OBL] Redirections 301

Dans le cadre d'une refonte de site web impliquant des modifications sur l'architecture du site, des urls ou du nom de domaine, il est attendu qu'un plan de redirections 301 soit établi pour ne pas générer de 404 et rediriger les anciennes url vers les nouvelles urls du site.

La méthodologie de gestion des redirections pourra être réalisée en collaboration les équipes techniques de l'ADEME (DETSI et Digital&CO).

Dans le cadre de l'administration courante du site, l'outil devra prendre en charge la redirection des urls supprimées ou modifiées :

- Depuis le backoffice l'outil devra permettre de renseigner les urls de redirection à la main ou via un système d'import de fichier csv
- Si aucune règle n'est définie par l'administrateur, une redirection automatique devra être créée pour rediriger vers la première page de niveau supérieure (ex : page de rubrique pour un article).

En cas de modification des urls des pages en backoffice, l'outil devra automatiquement détecter les redirections 301 à ajouter au système.

[OBL] Optimisation des performances (Web Core Vitals - Google)

Le prestataire technique devra se référer aux 3 critères « Signaux Web Essentiels » définis par le moteur de recherches Google pour optimiser l'expérience utilisateur sur les pages du site.

La métrique LCP (Largest Contentful Paint) mesure la performance de chargement et indique le temps de rendu du plus grand élément de contenu visible dans la fenêtre du navigateur. **La LCP doit se produire dans les 2,5 secondes** qui suivent le début du chargement de la page.

La métrique FID (First Input Delay) mesure l'interactivité avec l'utilisateur. Il s'agit du temps écoulé entre le moment où un utilisateur interagit pour la première fois avec une page et le moment où le navigateur répond. Pour offrir une bonne expérience à l'utilisateur, **la FID doit être inférieur à 100 millisecondes**.

La métrique CLS (Cumulative Layout Shift) mesure la stabilité visuelle pendant le chargement d'une page. Pour offrir une bonne expérience, les pages doivent maintenir un **CLS inférieur à 0,1**.

De façon générale l'ensemble des ressources de l'application doit être compressé au maximum de manière à optimiser le temps de chargement des pages et maximiser les performances techniques.

Exemples d'optimisations possibles :

- Compression des ressources HTML, CSS, Javascript...
- Optimisation du poids, de la taille et du format des images pour le web (72 dpi). Les dimensions des visuels doivent être adaptés à leur finalité.
- Mise en cache des pages

[En savoir plus sur les Signaux Web Essentiels de Google](#)**[OBL] Fichiers sitemap.xml et plan du site HTML**

Les fichiers sitemap XML sont des cartes numériques qui aident les robots des moteurs recherche à découvrir les pages importantes des sites et leur fréquence de mises à jour.

Les CMS des sites de l'ADEME doivent être configurés de façon à pouvoir générer automatiquement des fichiers sitemap.xml et garantir leur actualisation. Le paramétrage des fichiers sitemap.xml doit rester accessible en backoffice.

Les sites de l'ADEME doivent également proposer un plan du site détaillé à destination des utilisateurs pour qu'ils puissent accéder à l'ensemble des rubriques et sous-rubriques. Le contenu du plan du site doit être mis à jour automatiquement en fonction de l'actualisation du site et de son arborescence. Le Lien hypertexte pour accéder au « Plan du site » doit être intégré dans le pied de page réglementaire comme indique dans la charte graphique web.

[OBL] Fichier Robots.txt

Robots.txt est un fichier texte contenant des instructions destinées aux robots des moteurs de recherche : il leur indique les pages qu'ils peuvent ou ne peuvent pas explorer. Ces instructions sont spécifiées en "autorisant" ou en "interdisant" le comportement de certains robots (ou de tous). La configuration du fichier robots.txt permet d'optimiser le budget crawl, en indexant uniquement les pages stratégiques, et de sécuriser le site en bloquant l'accès à certains répertoires.

L'administration du fichier Robots doit être accessible en backoffice.

Au moment de la mise en production du site, le prestataire technique devra s'assurer que le fichier robots.txt est correctement configuré pour assurer l'indexation du site et bloquer l'accès aux répertoires et pages sensibles. Le fichier robots.txt devra bloquer le référencement des répertoires ou pages suivantes non utiles à l'internaute :

- Répertoires privés, d'installation ou de configuration (exemples : /includes/, /libraries/, /themes/, /misc/, /modules)
- Pages d'administration du site (ex : /admin)
- Pages de confirmation (ex : /confirmation-inscription)
- Pages de taxonomie (ex : /taxonomy)
- Pages des moteurs de recherche « privées (ex : /search/admin, /?q=admin/)
- Fichiers textes et documents téléchargeables (ex : /README.txt)

Important : tous les documents mis disposition sur les sites de l'ADEME (PDF, EXCEL, DOC...) ne doivent pas être indexés sur les moteurs de recherches. Pour optimiser l'acquisition du trafic, il est attendu que les moteurs de recherche référencent uniquement nos pages web. Les documents mis à disposition par l'ADEME doivent être accessibles uniquement via nos pages web.

[OBL] Gestion des erreurs 404

Une page 404 personnalisée devra être développée pour permettre à l'utilisateur de pouvoir se réorienter sur le site en cas d'erreur de navigation. Exemple de services de navigation à proposer aux utilisateurs : liste de liens, moteur de recherche, retour à la page d'accueil.

[OBL] Gestion des erreurs 403

Les pages privées (en accès restreint par un système d'authentification) ne doivent pas être indexées par les moteurs de recherche. Le passage en mode noindex devra être pris en chargement automatiquement par le système.

[OBL] Pages de confirmation des formulaires

Pour chaque page présentant un formulaire (contact, inscription, etc.), la validation du formulaire doit renvoyer l'internaute vers une page de confirmation dédiée (ex: confirmation-inscription, confirmation-envoi-contact, etc.).

[PRIO] URL d'accès

Sauf indication contraire, tout site web de l'Agence doit être accessible via une URL sans le sous domaine « www » uniquement (Exemple : <https://agirpouurlatransition.ademe.fr/> et non pas <https://www.agirpouurlatransition.ademe.fr/>).

Cette recommandation permettra d'éviter les contenus dupliqués (Duplicate Content) et les problèmes de référencements web.

11. Suivi statistiques (outils de mesure d'audience et gestion des cookies)

Contact

Personnes référentes à contacter au sein du service Digital&CO de l'ADEME :

- Sophie EVEN – Chef de Projets Webmarketing – Sophie.even@ademe.fr
- Estelle RIBOT – Coordinatrice du Pôle Web – Estelle.ribot@ademe.fr

[OBL] Définition des indicateurs de performance et des outils de mesure d'audience

Avant le lancement du projet et au plus tard 1 mois avant la mise en production du site Internet : le porteur de projet et/ou l'AMOA devront contacter les personnes référentes chez Digital&Co pour définir les besoins, les objectifs et les indicateurs de performance attendus.

Cette étape permettra à Digital&Co d'anticiper :

- La création du gestionnaire de cookies pour ce site
- La configuration de l'outil de mesure d'audience
- La création d'un éventuel plan de marquage
- La création d'un tableau de bord de suivi statistiques
- La gestion des droits d'accès aux outils

[OBL] Installation du gestionnaire de cookies de l'ADEME (Tarteacitron.io)

Dans le cadre de la mise en conformité RGPD le prestataire technique devra **obligatoirement installer le gestionnaire de cookies de l'ADEME**.

Le paramétrage du gestionnaire cookies pour un site devra être réalisé en amont sur le compte Tarteacitron de l'ADEME. Le prestataire technique pourra ensuite procéder à son intégration sur l'environnement de production. La mise en conformité RGPD prévoit également d'ajouter un lien « Gestion des cookies » dans le pied de page. Ce lien doit permettre d'ouvrir le gestionnaire de cookies du site avec l'ancre de lien : **#tarteacitron**

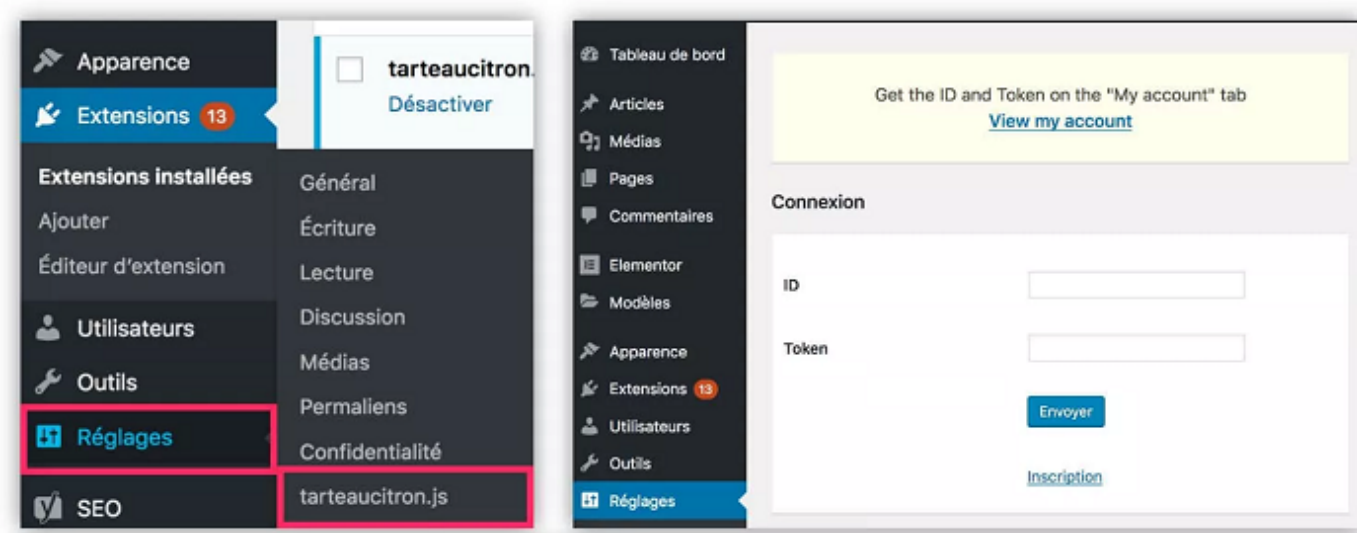
Intégration du gestionnaire de cookies sur un site Wordpress :

Le prestataire technique devra installer l'extension officielle de Tarteacitron.io dans le backoffice et renseigner les identifiants suivants :

UUID : 2df1000bf385655312abede8e30421664e7d594e

Token : contacter Sophie.even@ademe.fr pour obtenir cette clé.

Capture : installation du plugin Tarteacitron.io sur CMS Wordpress

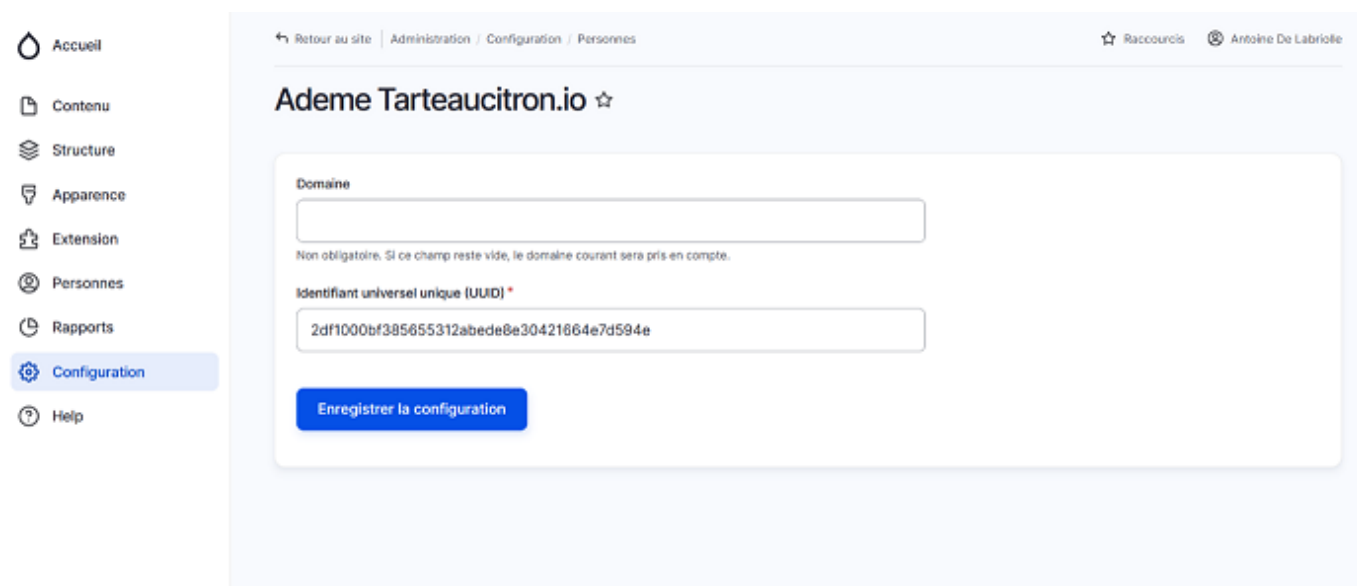


Intégration du gestionnaire de cookies sur un site DRUPAL :

Le prestataire technique devra installer le module de Tarteaucitron.io dans le backoffice et renseigner l'identifiant universel unique (UUID) du compte ADEME.

UUID : 2df1000bf385655312abede8e30421664e7d594e

Capture : installation du module Tarteaucitron.io sur CMS Drupal



Intégration du gestionnaire cookies sur site développé en PHP :

Le prestataire technique devra installer le script suivant dans le code source **juste après la balise d'ouverture <head>** :

```
<script src="https://tarteaucitron.io/load.js?domain=url-de-votre-site.fr&uuid=2df1000bf385655312abede8e30421664e7d594e"></script>
```

Le prestataire technique devra remplacer la valeur **url-de-votre-site.fr** par l'URL du site qui est prévu pour l'environnement de production (sans indiquer le protocole http ou https).

[OBL] Installation et configuration des outils de mesure d'audience

PIANO et EULERIAN sont les 2 solutions de mesure d'audience autorisées par l'ADEME pour suivre les statistiques de ses sites Internet. **L'installation de Google Analytics est désormais interdite à l'ADEME.**

Les outils de mesure d'audience web ne devront pas être installés dans le code source ou directement dans le backoffice du site. Pour tenir compte du consentement des utilisateurs, l'installation devra se faire obligatoirement depuis le gestionnaire de cookies de l'ADEME (Tarteaucitron.io).

[OBL] Intégration d'un bouton opt-out sur la page Politique des cookies

Afin d'assurer la mise en conformité RGPD des outils mesure d'audience qui bénéficient de l'exemption CNIL, il est attendu qu'un bouton opt-out soit ajouté sur la page "Politique des cookies" :

Désactiver les cookies de la mesure d'audience strictement nécessaire

Code HTML à intégrer :

```
<button id="eulerian-optout" class="appeler une classe css bouton existante sur le site">Désactiver les cookies de la mesure d'audience strictement nécessaire</button>
```

(Cf. également l'annexe [Politique des cookies](#), paragraphe 7.1 "Cookies de mesure d'audience").

[OBL] Intégration de Google Tag Manager en dur

Le prestataire technique devra intégrer Google Tag Manager sur le site en dur. Il est attendu que l'ID du GTM soit administrable en backoffice et accessible aux contributeurs de l'ADEME. Contacter Sophie.even@ademe.fr pour obtenir les ID GTM.

[OBL] Le porteur de projet et/ou l'AMOA devront contacter **dès que possible** les personnes référentes chez Digital&Co pour demander la création et la configuration des outils de mesure d'audience. **Un délai d'1 mois est nécessaire** pour traiter cette demande.

12. Chartes graphiques

12.1 Ressources

[OBL] Il existe une [charte graphique commune à tous nos sites web à l'ADEME](#). Si vous n'accédez pas à ce lien, demandez les droits à Digital&Co.

Celle-ci détaille les composants de base à appliquer sur tous les sites et les autres composants communs à appliquer seulement sur les sites qui n'ont pas de dérogation.

Les composants de base sont :

- Le bloc-marque de l'Etat
- La typographie
- La palette de couleurs
- Le pied-de-page (footer)
- Le gestionnaire de consentement

Les autres composants communs sont :

- L'en-tête (header)
- Le fil d'Ariane

[DMD]

Les sites pouvant faire l'objet d'une dérogation sont les sites de campagne, en partenariat, les grands programmes et les marques déposées.

Une demande de dérogation doit être adressée **au service Digital&Co**.

Au-delà des éléments cités ci-dessus, il est recommandé d'utiliser le design system de l'Etat : <https://www.systeme-de-design.gouv.fr/>

@ Contactez Marie-Charlotte Deniez, référente charte graphique web, pour plus d'informations.

[OBL] Dans le cas de réalisation d'une charte graphique, les composants graphiques réalisés (exemples : image, logo, feuille de style, etc.) seront fournis par le prestataire.

En plus de ces fichiers, un document dans un format modifiable (exemple : Word) décrira tous les éléments de la charte graphique utilisée (zoning, navigation, logo, dimensions, codes couleurs, polices utilisées, règles d'usage, etc...).

Les fichiers sources de conception graphique devront être mis à disposition de l'ADEME à sa demande.

13. Numérique responsable

[OBL] L'ADEME vérifie le bon respect de ces engagements au travers de l'outil FRUGGR

[OBL] L'ADEME s'engage à réduire l'impact environnemental et améliorer l'impact social de ses services numériques. Le numérique responsable implique donc une démarche responsable tout au long du cycle de vie du produit numérique. Plus d'infos : <https://ecoresponsable.numerique.gouv.fr/>

Les bases de l'écoconception sont attendues tout en laissant la priorité au besoin métier :

Questionnement du besoin métier

Facilitation de la maintenance (technologies standard, modularisation, ...)

Architecture adaptée aux charges attendues et contraintes du produit

[OBL] Dans le but de donner du sens aux actions Numérique Responsable tous les acteurs d'une équipe doivent avoir suivi le MOOC de sensibilisation de l'INR : <https://www.academie-nr.org/sensibilisation/#/>

[OBL] Le Référentiel général d'écoconception de services numériques (RGESN) contient des bonnes pratiques qui doivent être respectées par toutes les équipes <https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>

[OBL] L'ADEME s'est équipé d'un outil qui permet d'objectiver simplement le respect des bonnes pratiques NR : Fruggr. Cet outil produit une note sur 100 points. L'ADEME impose les critères suivants :

Tous les produits ADEME doivent avoir une note minimale de 80 points du 1er jour de mise en production au décommissionnement.

L'ADEME souhaite que les équipes lancent un audit à minima tous les 3 mois.

Pour brancher un produit ADEME à l'outil Fruggr, faire une demande à jean-pascal.martin.ext@ademe.fr copie gildas.falkenstein@ademe.fr

[OBL] les équipes produits devront mettre en oeuvre un plan d'action pour atteindre les 80 points dès lors que leur note est inférieure à 80 pts.

[OBL] Tous les nouveaux sites doivent disposer d'une page qui détaille la démarche d'écoconception mise en place pour que le produit soit le plus sobre possible. Cette page doit être accessible depuis le footer du site comme le prévoit la charte graphique web de l'ADEME.

[RECO] Les équipes qui le souhaitent peuvent obtenir un audit de conformité RGESN réalisé par un prestataire tiers afin de valoriser les actions d'écoconception. Contacter gildas.falkenstein@ademe.fr pour plus de détails.

[RECO] Boîte à outils du numérique responsable pour obtenir des métriques et recommandations de bonnes pratiques : <https://ecoresponsable.numerique.gouv.fr/publications/boite-outils/>

Pour aller plus loin : Consultez la rubrique Numérique du site Communication Responsable de l'ADEME

Pour aller plus loin : suivez le MOOC Numérique Responsable de l'INR <https://www.academie-nr.org/#mooc-nr>

14. Politique de sécurité

14.1 **[OBL]** L'application doit pouvoir fonctionner derrière le pare feu applicatif "Cloudflare"

14.2 **[OBL]** Suivi et détection des failles de sécurité

L'ADEME met en œuvre plusieurs outils visant à analyser et détecter des failles éventuelles de sécurité.

Le niveau de sécurité demandé sera en lien avec le niveau de criticité des applications concernées spécifié par l'ADEME.

Les outils utilisés par l'ADEME sont les suivants :

- **WAF Cloudflare :**

Toute application ouverte à l'externe doit être protégée derrière la suite d'outils proposée par Cloudflare (WAF, etc.) et la recette devra intégrer ces composants.

- **Purplemet :**

Analyse des applications de façon hebdomadaire. Une note de A à F est attribuée à chaque analyse.

Toute application initialement livrée en production devra avoir un score égal à A.

Pour les applications déjà en production, tout score E ou F devra faire l'objet d'un plan d'actions de la part du projet pour revenir à un niveau de sécurité acceptable pour l'ADEME.

Toute vulnérabilité ayant une sévérité critique "critical" ou haute "high" doit être traitée sans délai et un plan d'action doit être transmis à l'ADEME.

Toute vulnérabilité ayant un taux d'exploitabilité (EPSS) supérieur ou égal à 10% doit être traitée sans délai et un plan d'action doit être transmis à l'ADEME.

- **Trivy**

Toute vulnérabilité ayant une sévérité critique "critical" ou haute "high" doit être traitée sans délai et un plan d'action doit être transmis à l'ADEME.

- **WPScan**

Un site WordPress ayant un statut "Vulnérable" doit faire l'objet d'une analyse et d'un plan d'action afin de revenir à un statut "Secure".

[OBL] Tout incident détecté sur une application (lié à l'exploitation d'une vulnérabilité par exemple ou à une fuite de données) doit être immédiatement remonté à l'équipe projet et au RSSI de l'ADEME.

14.3 **[PRECO]** Scripts

[OBL] L'ensemble des informations sensibles (tokens, mdp) ne doit pas être stocké en clair. L'ADEME exige l'utilisation d'un type de stockage sécurisé adéquat (Vault par exemple).

Le compte utilisé par l'application devra disposer des droits minimum strictement nécessaires au bon fonctionnement de celle-ci.

Dans le cas où les procédures/livrables de mises à jour applicatives incluent des scripts SQL de mise à jour de la base de données et doivent être réalisés sur le serveur d'application, un compte MySQL utilisé sera dédié uniquement à cette fonctionnalité.

[OBL] L'application développée devra être exempte de toute faille de sécurité (sql injection, chaînes de connexion à la base de données, fichier contenant un phpinfo ...). Le prestataire veillera notamment à contrôler systématiquement les entrées utilisateurs (URL, champs de formulaires ...).

[OBL] Upload de fichiers

Si l'application permet d'uploader un fichier sur le serveur, l'application devra vérifier le type MIME et l'extension du fichier. Ne pas autoriser tout type de fichier. En cas d'inclusion de fichier, une liste blanche de fichiers pouvant être inclus doit être mise en place.

[OBL] Les fichiers contenant des macro (xlsm, docm par exemple) sont interdits

[INFO] L'ADEME se réserve le droit de réaliser un audit de sécurité sur l'application lui étant livrée par une société tierce.

[OBL] Recommandations Sécurité

Une liste des recommandations Sécurité pour la mise en œuvre d'un site web est précisée au niveau de l'annexe "Recommandations sécurité", disponible à [cet emplacement](#).

Le respect de ces recommandations est obligatoire. Le non respect de certains éléments peut être accepté à titre dérogatoire, sous réserve de justification.

[OBL] Le prestataire se réfèrera aux référentiels suivants pour garantir un niveau de sécurité de l'application développée, répondant à l'état de l'art :

- Référentiel d'exigences de l'ANSSI
- Guides CIS (Center for Internet Security)
- Référentiel Top 10 OWASP
- CVE (Common Vulnerabilities and Exposures)

[PRECO] Le prestataire devra être en capacité de réaliser une analyse de risque permettant d'identifier à la fois les enjeux de sécurité informatique spécifiques à l'application demandée, et le moyens mis en œuvre pour garantir le niveau de sécurité adéquate.

[OBL] Dans le cas où des scripts système doivent être mis en place (ex : un batch), le prestataire devra se mettre en relation avec le "Pôle Projets" le plus tôt possible dans la phase de réalisation.

@ Contactez l'aMOA projet du "Pôle Projets" pour fournir les justifications techniques et fonctionnelles de l'utilité d'un tel script ainsi que la démonstration que le script ne nuit pas à la sécurité des systèmes d'information de l'ADEME.

[PRECO] L'utilisation de la commande PHP exec() est à éviter car non compatible avec les contraintes d'hébergement de l'ADEME.

14.4 Certificat (https)

[OBL] Toutes les applications utiliseront le protocole SSL/HTTPS.

@ Contactez l'aMOA projet du "Pôle Projets" pour les demandes de certificats auprès de l'autorité compétente. Le prestataire doit donc fournir des clés d'authentification temporaires.

14.5 Authentification

[OBL] Utiliser la fédération d'identités ADEME (outil Keycloak, protocole SAML et OAuth).

Les règles de gestion de la Fédération d'Identité, précisant ces principes sont disponibles dans l'espace documentaire.

@ Contactez la DETSI

14.6 Entrées / Sorties

[OBL] @ Contactez l'aMOA projet du "Pôle Projets" si l'application à des interactions avec d'autres systèmes d'information que celui de l'ADEME ou si elle nécessite l'ouverture de connexion particulière.

Le cas typique d'une « entrée »/ « sortie » est la « mise à disposition »/ « l'accès » à un web service. Dans ce cas, le nom du Web Service, son adresse, son port d'écoute et son rôle doivent être définis dans le document d'installation. Un autre exemple est l'utilisation d'outils tels que « RSYNC ».

[OBL] Ces spécificités d'architecture doivent être documentés dans le DAT.

[OBL] Une revue annuelle des comptes d'accès doit être mise en place pour s'assurer que tous les accès à l'application sont légitimes.

14.7 Fermeture automatique des sessions

[OBL] Toute application gérant des sessions utilisateurs doit mettre en œuvre un mécanisme de fermeture de session automatique.

Par défaut, la session de l'utilisateur doit expirer automatiquement après 1 heure d'inactivité.

14.8 Désactivation des comptes par défaut

[OBL] Certains CMS comme Drupal proposent une option du type :

Les visiteurs peuvent créer leur propre compte sans approbation de l'administrateur.

Cette option doit être désactivée et remplacée par une option du type :

Les visiteurs peuvent créer leur propre compte, mais l'approbation d'un administrateur est requise.

14.9 Tests

[INFO] Le "Pôle Projets" utilise régulièrement les outils JMeter et Selenium pour réaliser ses tests. Dans le cas où la MOE dispose de fichiers de tests compatibles, elle est encouragée à les fournir à l'ADEME.

[OBL] La responsabilité et l'outillage des tests figureront dans l'ordre du jour de réunion de lancement du projet.

14.10 Mises à jour

[OBL] L'application doit impérativement être conçue pour supporter les mises à jour de sécurité d'OS et de logiciels. Toutes les mises à jour de sécurité doivent être installées dès que possible.

15. Réglementation

Le contenu des pages règlementaires doit être relu et adapté pour chaque site.

[OBL] Dans le footer, sont obligatoires les mentions suivantes avec accès à des pages dédiées :

- Mentions légales (cf annexe [Mentions Légales](#))
- Politique de protection des données personnelles (Cf. [page dédiée](#))
- Politique des cookies (Cf. [page dédiée](#))
- Gestion des cookies (lien qui permet d'ouvrir la modale de gestion du consentement à tout moment)
- CGU-Conditions générales d'utilisation (uniquement pour les sites de ventes e-commerce)
- Plan du site
- Mention du niveau d'accessibilité comme suit, avec un lien vers la déclaration d'accessibilité (à demander à Marie-Charlotte Deniez ou Estelle Ribot Digital&Co):
- Accessibilité : totalement conforme
- Accessibilité : partiellement conforme
- Accessibilité : non conforme

16. RGPD - Données personnelles

[INFO] Pour s'adapter aux enjeux du numérique et garantir une meilleure maîtrise des données personnelles, l'Europe a mis en œuvre le règlement général sur la protection des données (RGPD ou GDPR), entré en application le 25 mai 2018. À l'ère du numérique, il renforce ainsi le contrôle par le citoyen de l'utilisation qui peut être faite des données le concernant.

Le RGPD encadre le traitement des données personnelles de manière égalitaire sur le territoire de l'Union européenne. Il s'applique à toute organisation, publique ou privée, qui traite des données personnelles pour son compte ou en tant que sous-traitant. Dans ces deux cas, l'ADEME en tant qu'établissement public à caractère industriel et commercial, a des obligations spécifiques pour garantir la protection des données qui lui sont confiées. Les cinq grandes règles de protection des données personnelles sont les suivantes :

- Le principe de finalité : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- Le principe de proportionnalité et de pertinence : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- Le principe d'une durée de conservation limitée : une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
- Le principe de sécurité et de confidentialité : le responsable du fichier doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- Les droits des personnes sur leurs données : droit d'accès, de rectification, d'opposition, à l'effacement - ou "droit à l'oubli", etc.

[OBL] Sur l'intrADEME, il est présenté l'essentiel à connaître sur l'application du RGPD et l'organisation mise en place à l'ADEME pour s'y conformer. Le corpus documentaire est constitué par :

- La mise en œuvre des cookies de navigation (bandeau informatif, acceptation, personnalisation) => Comment mettre en place les cookies ? (Cf. [paragraphe](#) du RECSI)
- La création de formulaires (inscription à un événement ou à une formation, diffusion d'un questionnaire => comment rendre mon formulaire conforme ?
- L'envoi d'e-mailing => Comment faire un emailing conforme ? (Cf. [paragraphe](#) du RECSI)
- L'abonnement et l'envoi à une newsletter régulière => comment faire une newsletter conforme ? (Cf. [paragraphe](#) du RECSI).
- La collecte des données en partenariat (sur un événement, avec des acteurs locaux e.g. Région) => Document en cours de production
- La demande d'inscription des utilisateurs (création de compte utilisateur, mise en place des emails transactionnels avec mot de passe) => Comment faire une création de compte conforme ? (document de travail - actualisation du document à venir) ;
- Le format des emails transactionnels ;
- Les textes réglementaires informatifs à intégrer dans les sites web (en français ou anglais) : mentions légales, politique de protection des données à caractère personnel et politique cookies (Cf. [paragraphe](#) du RECSI).

Les fiches pratiques et techniques constituant le corpus documentaire RGPD sont disponibles sur la [page intrADEME](#) ou via la [page Wiki Redmine](#), accessible sans compte utilisateur.

[INFO] Terminologie :

- **Données personnelles** : Données permettant d'identifier directement ou indirectement (par croisement) une personne physique (nom, prénom, courriel, immatriculation, téléphone, photographie, date de naissance, commune de résidence, empreinte digitale, ...).
- **Données commerciale, industrielle et secret des protégés** : Données s'appliquant à toute personne morale dès lors qu'elle déploie son activité, en tout ou partie, en milieu concurrentiel et dont la communication porterait atteinte au secret en matière commerciale et industrielle (secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles, ...).

[OBL] Dès la phase de spécifications générales (cahier des charges), ces exigences de conception doivent être intégrées pour être précisées et adaptées au projet en phase de spécifications détaillées.

[OBL] Droits de personne physique (données personnelles) ou morale (données commerciale, industrielle et secret des protégés) :

- L'utilisateur doit donner son consentement (acte positif et explicite) pour :
- La collecte et le traitement des données.
- Le partage des données à des tiers
- L'utilisateur doit pouvoir refuser le partage.

Pour respecter le consentement des utilisateurs, quant à l'utilisation des cookies tiers, il est prévu que chaque site intègre l'outil tarteaucitron.io, compte ademe (cf procédure – Mettre lien vers page statistique).

- L'utilisateur doit pouvoir vérifier, modifier et supprimer
- Les données enregistrées
- Les données partagées.
- L'utilisateur doit pouvoir revenir sur son consentement.

[OBL] Traitements à mettre en œuvre Du moment qu'un traitement sollicite l'utilisateur pour saisir des informations concernant ses données personnelles telles que définies dans le présent document, l'ADEME se doit de recueillir le consentement explicite de l'utilisateur.

Pour tout complément sur le RGPD :

- Sur le site de la CNIL
- @ Contactez l'ADEME : rgpd@ademe.fr

[INFO] Mise en œuvre de la Loi pour une République Numérique

Loi n°2016-1321 du 7 octobre 2016, dite Loi numérique.

Pour tout complément sur l'opendata à l'ADEME : @ Contactez : laurent.morice@ademe.fr

17. Accessibilité Numérique

[INFO] Les obligations d'accessibilité des sites publics aux personnes en situation de handicap ont été introduites par l'article 47 de la loi du 11 février 2005. Le décret n° 2019-768 du 24 juillet 2019 précise les obligations légales.

En tant qu'opérateur de l'Etat, l'ADEME est soumise à la mise en accessibilité de ses services numériques : sites web internes et externes, applications mobiles, progiciels et matériels numériques urbains (bornes...).

Au-delà de l'obligation légale, l'ADEME s'est dotée d'un plan d'action sur la transition écologique et l'inclusion. Un des axes est l'amélioration de l'accessibilité numérique.

[OBL] Les sites Web et autres produits numériques de l'Agence doivent répondre aux exigences de la [méthode technique du RGAA](#) permettant de vérifier qu'une page web est conforme aux critères pour atteindre une note de 100 % sur le socle technique livré.

En plus de l'obligation de conformité totale au RGAA, chaque service en ligne doit proposer :

- Une [déclaration d'accessibilité](#) ;
- La [mention de la conformité en page d'accueil](#) ;
- Un lien vers le [schéma pluriannuel de mise en accessibilité numérique](#) de l'entité.

Une personne référente formée sur l'accessibilité numérique doit être identifiée côté prestataire et doit pouvoir être mobilisée sur le projet si besoin.

[INFO]

La personne référente chez le prestataire pourra s'appuyer sur la [méthodologie de test](#) et le [kit d'audit](#) proposés sur le site du RGAA pour s'assurer de la qualité et de la conformité de ses livrables.

Le pôle Design des services numériques de l'Etat met à disposition une [sélection d'outils faits maison](#) pour vous accompagner dans l'amélioration de l'accessibilité et du design de vos sites et applications web.

L'outil Fruggr installé sur la plupart des produits numériques de l'ADEME permet de remonter des non-conformités ou des alertes sur la partie RGAA, il conviendra d'apporter les correctifs avant de demander la réalisation d'un audit de contrôle par un prestataire tiers.

La DEMTE met également à disposition de ses collaborateurs une check-list des 12 critères d'accessibilité les plus souvent revenus et facilement remédiables. Un tutoriel e-learning (20 minutes) est également à disposition pour apprendre à évaluer ces 12 critères.

L'ADEME se réserve le droit de réaliser un audit d'accessibilité sur l'application lui étant livrée. Dès lors que l'audit est réalisé, les équipes ont un délai de 3 à 5 mois pour apporter les correctifs prioritaires.

18. Livrables

[OBL] Les livrables validés doivent être déposés et actualisés dans l'espace Jira / Confluence dédié au projet à chaque étape de la vie du projet (conception, réalisation, TMA,...).

- **[OBL]** Les documents d'une application sont :
 - SFG - Spéc. Fonc. Générales
 - SGE - Spéc. Graph. et Ergo.
 - SFD - Spéc. Fonct. Détaillées
 - STD - Spéc. Tech. Détaillées (architecture, composants, modèle de données)
 - MIS - Manuels d'InStallation
 - MEX - Manuel d'EXploitation
 - GUT - Guides Utilisateurs
- **[OBL]** L'ensemble des sources d'une application doivent être déposées dans le dépôt Git ADEME. Doivent y figurer (non exhaustif) :
 - Les scripts de création de base de données ;
 - Packages applicatifs Drupal comprenant :
 - les fichiers constitutifs et déployables de la version de Drupal retenue
 - les fichiers constitutifs et déployables des modules communautaires de Drupal retenus pour le projet
 - Codes sources des développements spécifiques documentés comprenant :
 - le code source de l'application
 - les fichiers et ressources graphiques, constitutifs des interfaces, et leur fichiers projets quand ces ressources sont issues d'une transformation de fichiers sources (exemple: fichiers PSD multi-calque ou autres formats)
 - les feuilles de styles CSS organisant les interfaces graphiques
 - les fichiers de francisation des modules communautaires utilisés
 - la page de test de l'application et le scénario de test
 - le script de mise à jour des droits sur le système de fichiers.
- **[OBL]** Les droits d'auteur de l'ensemble des créations seront cédés à l'ADEME pour toute utilisation ultérieure éventuelle.

[OBL] Page de supervision et de validation d'installation :

Une page de surveillance paramétrable, incluse dans les sources de l'application, doit permettre à l'ADEME, ainsi qu'à la société en charge d'héberger l'application de valider à tout moment que tous les composants techniques nécessaires à l'application soient opérationnels.

Elle devra pouvoir être interfacée avec un outil de supervision de type UptimeRobot, Site24x7, Nagios, Centreon, Zabbix...

Cette page devra également permettre de vérifier l'installation de tous les composants nécessaires à la bonne exécution de l'application livrée.

Le détail d'une page de supervision et de validation d'installation est fourni en [annexe de ce document](#).

[OBL] Opérations de maintenances

Les redirections et autres paramétrages des applications PHP ne doivent pas être effectués directement dans le fichier .htaccess mais doivent être intégrés dans un fichier de configuration Apache.

Cas d'une installation

- **[OBL]** règles générales
- Les applications livrées ne devront être constituées que des stricts codes sources (application + fichiers de paramètres), des scripts de création et d'alimentation de(s) base(s) de données ainsi que de la documentation associée.
- Cette documentation devra permettre aux personnes chargées de l'intégration des livrables (ADEME et hébergeur) d'installer ceux-ci de façon autonome.
- Les documentations et livrables devront être fournis au moins la veille de l'installation.
- Lors de la mise en production, une assistance téléphonique doit être mise en place et disponible pour accompagner nos administrateurs en cas de difficulté.
- En aucun cas, les livrables ne devront comporter les environnements de développement tels que XAMP ou WAMP, ceux-ci ne pouvant être installés sur les serveurs mutualisés.
- **[OBL]** Dans le manuel d'installation des applications de type LAMP, le répertoire dans lequel sera installée l'application (par exemple /var/www) sera nommée DocumentRoot.

[OBL] Toute nouvelle mise en production utilisant le CI/CD devra être précédée d'une information dans le canal Teams du projet. Pour les anciens produits, la demande doit être adressée via Jira vers l'hébergeur avec un délai de prévenance de 6 jours ouvrés.

[INFO] Cas d'une mise à jour

Lors des mises à jour, les fichiers de configuration **ne devront en aucun cas écraser ceux de la plate-forme sur laquelle ils sont installés**. Si les procédures d'installation nécessitent un remplacement de ceux-ci, le prestataire devra disposer des paramètres de la plate-forme de l'ADEME afin de les intégrer dans ses livrables.

[OBL] Accessibilité numérique

Dès lors qu'un audit d'accessibilité numérique est réalisé par l'ADEME, le prestataire devra fournir à la référente accessibilité chez Digital&Co le tableau de suivi des correctifs apportés.

19. Dématérialisation "administrative" (process internes, documents à valeur juridique)

19.1 Signature électronique

- Process de signature interne :
- **[PRIO]** i-Parapheur/Libriciel et certificat RGS** (signature électronique avancée avec certificat qualifié - requis pour marchés publics) > service Saas
- Process de signature externe :
- **[PRIO]** Yousign (signature électronique simple - suffisant pour bénéficiaires des Aides -, application ou API) > service Saas

19.2 GED (Gestion Électronique des Documents) / ECM (gestion de contenu d'entreprise) :

- **[PRIO]** Alfresco (pour gérer et organiser vos informations sous forme de documents électroniques) > tiers hébergeur [ADEME](#)

19.3 SAE (Système d'Archivage Électronique) :

- **[PRIO]** solution basée sur "as@lae"/Libriciel et portée par le Tiers Archiveur "OKANTIS" > service SaaS

19.4 Orchestrateur de processus multi-acteurs et multi-flux :

- **[INFO]** Pastell/Libriciel (interopérabilité entre applications - ex. : OPALE/i-parapheur, dépôt en GED, versement en SAE) > service SaaS

20. Processus de déploiement

[OBL] Les applications hébergées sur l'infrastructure Cloud, ainsi que les applications WordPress devront être prises en charge par la MOE jusqu'à l'environnement de Production inclus. Les applications hébergées sur les anciens socles techniques ne sont pas concernées par cette exigence.

Pour information concernant les applications non hébergées dans le cloud

[PRECO] Environnement de démonstration

L'ADEME préconise de réaliser un test de recevabilité sur un démonstrateur mis à disposition de l'ADEME et de son aMOA par la MOE.

[PRECO] Processus de livraison L'ADEME préconise l'utilisation de l'outil GIT (gestion de versions) sur son serveur git (git.ademe.fr), celui-ci servant de référence pour tous les déploiements sur l'ensemble des environnements.

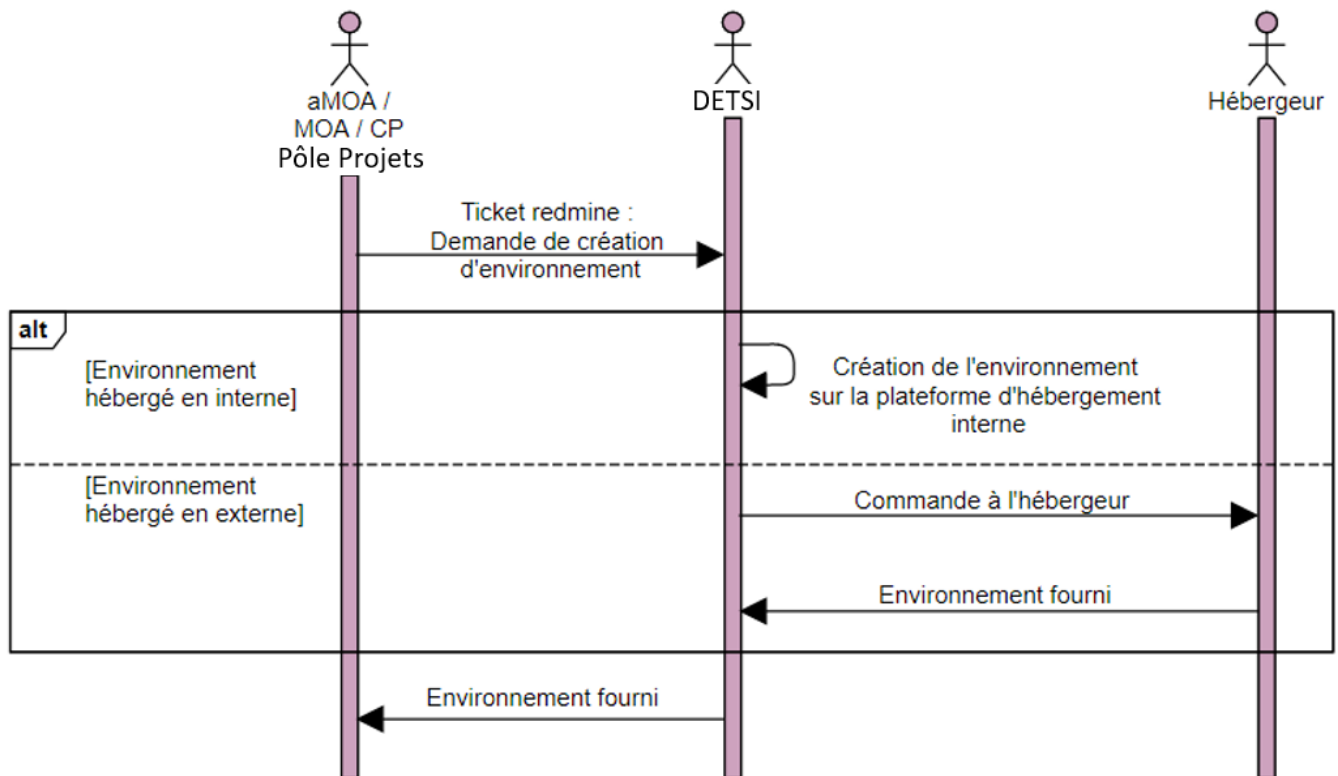
[INFO] 1ère livraison - Création d'un nouvel environnement d'intégration - pré-production ou production

Avant toute première installation sur un environnement d'intégration, de pré-production ou de production, une demande de création d'environnement doit être effectuée sous Redmine 5 semaines avant la première livraison.

L'environnement pourra être hébergé soit sur la plateforme d'hébergement de l'ADEME (hébergement interne), soit par l'hébergeur ADEME (hébergement externe). Seule l'ADEME est habilitée à commander de nouveaux environnement à l'hébergeur, c'est pourquoi dans les deux cas, le ticket Redmine devra être assigné à la DETSI.

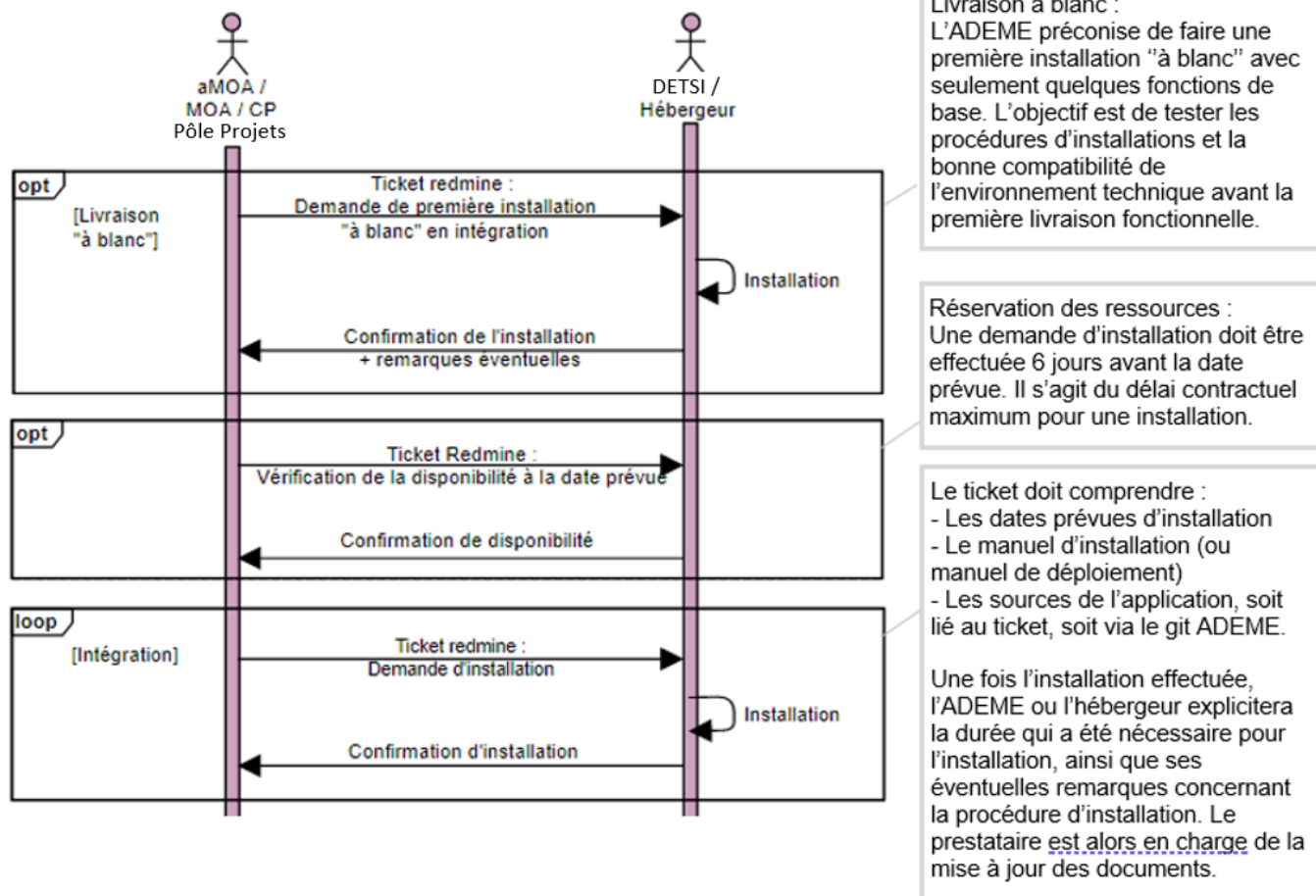
Cet environnement sera le plus proche possible de l'environnement de production envisagé, afin de réduire les risques d'anomalies liés à des versions de composant différentes.

Ci-dessous le diagramme résumant les actions attendues :



[INFO] 1er déploiement en recette / intégration

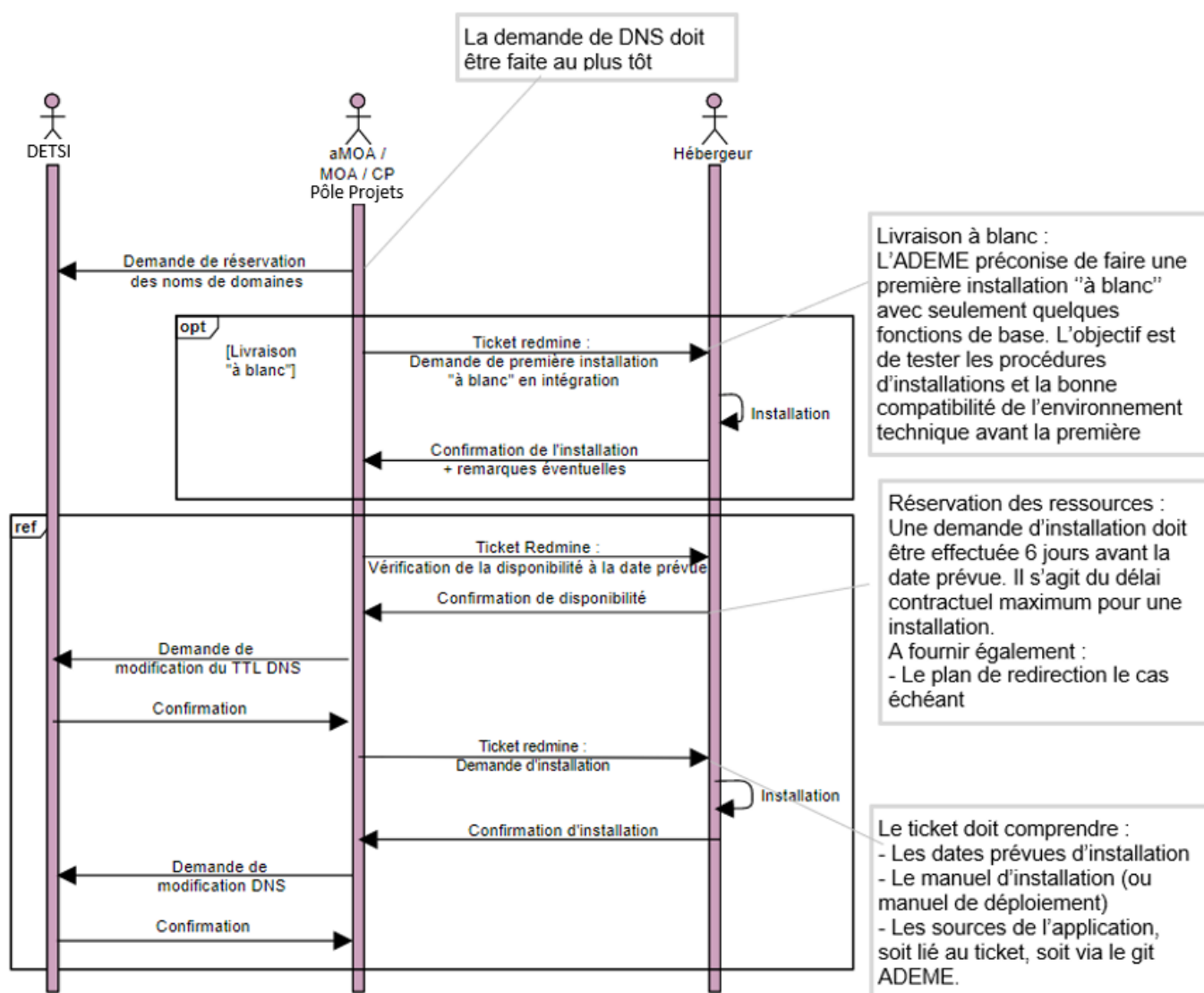
Lorsque les environnements ont été créés, les premières livraisons peuvent être envisagées. Voici le schéma résumant les actions attendues :



[INFO] 1er déploiement en pré-production

Le schéma précédent s'applique aussi bien aux environnements d'intégration que de pré-production. La livraison « à blanc » peut s'effectuer sur les deux environnements en parallèle. Pour la suite, on attendra évidemment la validation de la recette sur l'environnement d'intégration pour lancer une installation en pré-production.

[INFO] 1er déploiement en production

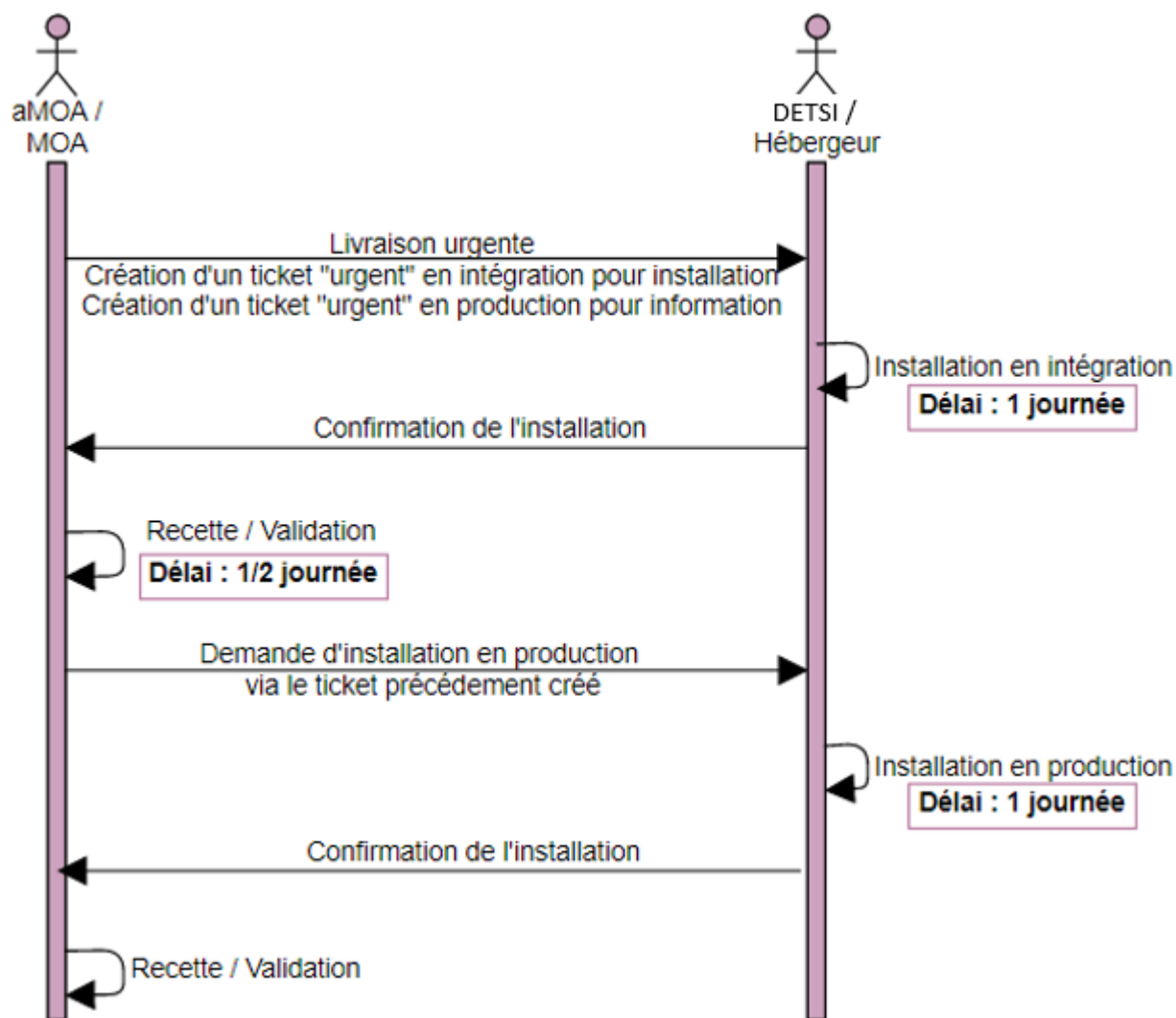


[INFO] Déploiements urgents / Correctifs d'anomalies

Dans le cas de remontée d'anomalies urgentes, les délais peuvent être raccourcis. Une fois le correctif livré par la MOE, la procédure consiste à créer immédiatement deux tickets « urgent » sous Redmine :

- Le 1er à destination de l'intégration, contenant les sources et le manuel de déploiement.
- Le second à destination de la production, afin de les informer de l'arrivée imminente d'une livraison en production. L'objectif est de maximiser les chances de réactivité

L'hébergeur dispose d'un délai d'une journée pour chaque installation. On obtient alors le déroulé suivant pour les anomalies urgentes, partant de la livraison du correctif par la MOE :



****[INFO]** Accès à la plate-forme hébergeant les serveurs de production de l'ADEME ******

Un accès aux serveurs de production (FTP, Base de données,...) pourra exceptionnellement être ouvert et accompagné par l'hébergeur sous certaines conditions. Contacter le Pôle Infra numérique de la DETSI.

[INFO] Guides Devops

Un guide concernant les déploiements Devops sur les environnements de pré-intégration ADEME est disponible à cet [emplacement](#).

Pour les applications hébergées chez DRI (Legacy), un guide Devops générique est également disponible à cet [emplacement](#).

Pour les applications ayant vocation à être hébergées chez Scaleway (sous Kubernetes), un document est en cours de préparation au moment de la validation de cette version du RECSI. Il sera ajouté ultérieurement.

21. Versions des composants applicatifs

Précautions de lecture

Les références ne font pas toutes l'objet d'un versionning, par conséquent la lecture de ce document ne pourra se limiter à ce chapitre.

21.1 Versions des composants applicatifs

Les composants applicatifs doivent évoluer tout au long du projet afin de profiter des dernières mises à jour de sécurité et de maintenance pour ne pas cumuler de dette technique. Les versions des composants applicatifs ne doivent donc pas être figées avant la livraison en recette.

Pour les composants ayant plusieurs types de release, il faudra choisir les versions LTS (Long Term Support). A titre d'information, le site suivant permet de consulter les cycles de vie des principaux composants applicatifs : **<https://endoflife.date/>**.

Dans le cas où la version déterminée par les règles précédentes ne peut pas être appliquée, l'équipe de développement devra en informer l'ensemble du projet et justifier son choix.

Exemples :

- Incompatibilité technique avec la nouvelle version nécessitant des travaux d'adaptation de l'application.
- Mise en place d'une version plus récente que la LTS pour l'utilisation de nouvelles fonctionnalités non présentes dans cette dernière.

Les applications hébergées en mode « cloud » chez Scaleway devront effectuer les montées de versions conformément aux spécifications techniques des bases de données managées indiquées à cet emplacement : **<https://www.scaleway.com/fr/database/>**.

21.2 Poste Utilisateur

Les versions des références indiquées ci-dessous correspondent à celles validées à la date de mise à jour du document.

Sauf indications précisées directement dans le cahier des charges

Système d'exploitation
Windows
APPLE Mac OS
LINUX
IOS
Androïd

Navigateur
Microsoft Internet Explorer
Google Chrome
Mozilla Firefox
Microsoft Edge
Safari

22. Anciennes versions du RECSI



 Les documents pointés par cette page correspondent aux anciennes versions du RECSI.

Version 2023.1 (Mars 2023)

-  [RECSI incluant les annexes](#)

Version 4.2.2 (2020)

-  [RECSI sans les annexes](#)
-  [RECSI incluant les annexes](#)
-  [Annexe Page de validation d'installation](#)
-  [Annexe Page de supervision](#)

23. Annexes

23.1 Liste des annexes disponibles :

- [Modèles de conception fonctionnelle](#)
- [Pages de supervision et de validation d'installation](#)
- [Recommandations sécurité](#)
- [Guides Devops](#)
- [Mentions Légales](#)
- [Politique de protection des données personnelles](#)
- [Politique des cookies](#)
- [Hébergement / niveau de service](#)

24. Annexes

24.1 Modèles de conception fonctionnelle

24.1.1 Préambule

Cette annexe constitue la liste des exigences fonctionnelles de l'ADEME communes à la plupart des projets pilotés par le "Pôle Projets". Elle a pour objectif :

- En phase de consultation des fournisseurs, de donner un maximum de détails fonctionnels aux candidats pour permettre une précision du chiffrage accrue
- En phase de conception du projet, de mutualiser les ateliers de spécifications déjà effectués sur d'autres applications mais concernant les mêmes blocs fonctionnels « génériques ». Sauf demande expresse, seuls les seuils et valeurs par défaut ([PRECO]) pourront être rediscuté-e-s.

Tout comme dans le RECSI, les exigences par défaut décrites ci-après, sont automatiquement remises en cause si une consigne contraire est établie dans le cahier des charges ou durant un atelier de spécification.

24.1.2 Précautions de lecture

Les exigences fonctionnelles décrites dans les chapitres suivants sont précédées d'un sigle caractérisant leur statut :

- **[PRECO]** Préconisation
- **[INFO]** Information
- **[PRIO]** Choix à privilégier
- **[DMD]** Choix à valider par la DETSI
- **[OBL]** Obligatoire

24.1.3 Dépôt de fichiers

La fonction de dépôt de fichier doit présenter :

- **[OBL]** Un bouton « Parcourir » ouvrant une fenêtre modale permettant de naviguer dans le système de fichier de l'utilisateur et permettant d'accéder à tous les types de fichier autorisés dans l'application cible.
- **[OBL]** Un champ « nom du fichier » à caractère obligatoire. Il est composé du titre du fichier et de son extension, sans le chemin complet. Il est récupéré par défaut lors du choix du fichier avec le bouton « Parcourir ». Ce champ n'est pas modifiable directement **[PRECO]** Une limite de 100 caractères est à mettre en place.
- **[PRECO]** Un champ « Description » ou « Intitulé » limité à 100 caractères

Il convient au minimum de fixer des limites pour :

- Les formats de fichiers acceptés.

[PRECO] En fonction du média attendu (image, texte, vidéo, ...) les formats standards sont à privilégier (JPG, PNG, DOC, DOCX, PDF, AVI, WMV, ...) - La taille maximale d'un fichier.

[PRECO] Une limite à 2Mo est à privilégier. A adapter au contexte. - Une taille maximale d'un dossier utilisateur, dans le cas où un utilisateur peut stocker plusieurs documents dans son espace.

[PRECO] Une limite à 64Mo est à privilégier (64 Mo étant la limite de AV-scanner). Consulter la DETSI si la valeur est insuffisante. A adapter au contexte.

25. Pages de supervision et de validation d'installation

25.1 Préambule

Une page de surveillance paramétrable, incluse dans les sources de l'application, doit permettre à l'ADEME, ainsi qu'à la société en charge d'héberger l'application de valider à tout moment que tous les composants techniques nécessaires à l'application soient opérationnels.

Elle devra pouvoir être interfacée avec un outil de supervision de type UptimeRobot, Site24x7, Nagios, Centreon, Zabbix...

Pour les applications non conteneurisées, cette page pourra indiquer :

- Si le serveur est correctement configuré conformément aux prérequis.
- Si les droits sur le système de fichiers sont corrects.

Les 2 points ci-dessus sont implicites dans le cas d'une application conteneurisée :

- C'est l'image qui est garante des prérequis nécessaires à l'application.
- C'est au démarrage du conteneur que l'entrypoint doit réaliser les vérifications concernant les permissions.

25.2 Contenu de la réponse

La réponse doit permettre de vérifier rapidement que les fonctionnalités principales du site fonctionnent. Son contenu peut inclure différentes rubriques détaillées dans les paragraphes suivants.

25.3 Rubriques

Une liste non exhaustive de rubriques servira à regrouper les tests (ou sondes) par famille. Certaines rubriques devront obligatoirement être présentes dans la page de surveillance. D'autres rubriques sont optionnelles, en fonction du contexte projet.

Rubriques	Sonde/Test	Présence
Résultats	Statut global à l'instant t. (Tous les éléments « vitaux » sont au statut « OK »).	Obligatoire
Supervision fonctionnelle	Accès à la page d'accueil	Obligatoire
	Accès à une page interne	Obligatoire
	Accès à la base de données	Obligatoire
	Test d'envoi de courriel	Si concerné
	Vérifier que le système d'authentification à l'application est fonctionnel.	Si concerné
	Vérifier que les API ou services sollicités sont opérationnels (Accès SFTP, LDAP, Webservices...)	Si concerné
Supervision batch & crons	Pour chaque batch et cron : - Nom/Libellé - Indicateur(s) - Statut	Si concerné
Configuration et tests serveur	Vérifier que les composants techniques installés sont conformes aux versions minimales requises (Ne pas afficher les versions).	Obligatoire
	Tout autre élément nécessaire à l'installation	Si concerné
	Présence de librairies (non dockerisées).	Si concerné
	Etat d'un démon local	Si concerné
	Ecriture sur disque	Si concerné
	Génération d'un PDF	Si concerné
	Envoi d'un mail	Si concerné
Configuration des droits	Vérifier la présence d'un utilisateur ayant les droits d'admin	Si concerné
	Présence des fichiers et dossiers nécessaires au bon fonctionnement de l'application	Si concerné
	Vérifier l'absence des fichiers et dossiers de travail qui ne doivent pas se retrouver en production (Installation).	Si concerné
	Vérification des droits d'écriture / lecture aux dossiers et fichiers nécessaires au bon fonctionnement de l'application	Si concerné

25.4 Paramètres de la requête

Le paramètre « format » permet de définir le format de la réponse.

Le paramètre « niveau » permet de définir le niveau de détail des tests déclenchés.

Ainsi, il sera possible de couvrir différents cas de figure, par exemple :

- Surveillance périodique type UptimeRobot (Format JSON, niveau de détail 1)
- Vérification visuelle synthétique d'état par les équipes métier (Format HTML, niveau détail 1)
- Vérification visuelle d'état suite à un déploiement (Format HTML, niveau de détail 2)
- Opération manuelle de contrôle (Format JSON, niveau de détail 2).

25.4.1 Paramètre « format »

- Valeurs possibles : JSON, html, texte...

25.4.2 Paramètre « niveau »

Chaque sonde devra définir un niveau à partir duquel elle sera déclenchée.

Ainsi, il sera possible de distinguer des tests « basiques », de niveau 1, effectués par défaut (ex : connexion à la BDD), de tests plus approfondis et donc plus consommateurs en termes de ressources, de niveau 2 ou plus.

Ces derniers ne devront être effectués que ponctuellement, par exemple à l'issue d'une installation ou d'une mise à jour.

Il est de la responsabilité du projet de définir le niveau de chacune des sondes.

- Valeurs possibles : 1, 2, 3...

25.5 Contenu de la réponse

25.5.1 Distinction entre éléments vitaux et non vitaux (optionnelle)

En fonction du contexte projet, il peut être utile de distinguer la surveillance d'éléments vitaux, indispensables au bon fonctionnement du site, avec des éléments nécessitant d'être surveillés mais considérés comme non « vitaux ».

Cette distinction est optionnelle, en fonction des besoins du projet. Si tous éléments sont vitaux, la valeur à mentionner sera « True » (Cf. ci-dessous).

L'indisponibilité de ces éléments non vitaux (par exemple un script de mise à jour périodique de certaines données) permettrait toutefois au site de fonctionner de façon acceptable, même en mode dégradé.

Afin de prendre en compte cette distinction, il est possible d'affiner les contrôles de la page de surveillance de la façon suivante :

25.5.2 Paramètre « vital »

- Composant vital : « True/False », pour prise en compte au niveau de l'alerte globale du site :
- Statut global « OK » si tous les éléments, vitaux et non vitaux, sont OK.
- Statut global « Warning » si tous les éléments vitaux sont OK, et qu'au moins un élément « non-vital » est KO.

25.5.3 Format des données

La page de surveillance comportera autant de sondes (probes) que nécessaire.

[Option] Chaque sonde ne sera testée/affichée que dans le cas où son niveau est supérieur ou égal au paramètre « niveau » passé à la page.

" Sections " (Rubriques) est un tableau clef>valeur avec une clef numérique et une valeur de type string correspondant au nom de la rubrique :

sections : Array

id: Int, id topic => string, nom de la rubrique

probes : Array

Id : Int

title : string, nom de la sonde détaillé [obligatoire]

status, string (OK/KO), état du test [obligatoire]

definition : String, description sommaire du test réalisé [obligatoire]

vital: bool : Définit si le test est vital pour que le site fonctionne ou s'il peut fonctionner en mode dégradé en cas d'erreur sur ce test. [obligatoire].

version: String ou Array of string, Version remontée par la sonde (no d'applicatif, version de librairie présente, version des données...) [facultatif]

messages: Array, Liste des derniers messages remontés par la sonde [facultatif]

id_topic : Int, Id de la rubrique à laquelle rattacher la sonde [obligatoire]

level : int, niveau de détail à partir duquel le test sera effectué, 1 étant le niveau par défaut [obligatoire]

25.5.4 Format de la page

Les formats attendus pour cette page sont les suivants :

- **[OBL]** Une page au format JSON : **Obligatoire**.
- Une page au format texte ou html, permettant une lecture plus accessible à des utilisateurs non techniques : **Facultatif** (En fonction des besoins du projet).

25.5.5 **Résultats**

Statut global :

Lorsque la configuration du serveur correspond à l'attendu, et que l'ensemble des éléments surveillés sont **OK** :

- La page doit retourner le code **200**.
- Au format JSON : La propriété « Status » située à la racine doit mentionner : « OK ».
- Au format html : Le message « **Le site fonctionne** » s'affiche en haut de la page, en **vert**.

Si au moins un élément « vital » est **KO** :

- La page doit retourner le code **503**.
- Au format JSON : La propriété « Status » située à la racine doit mentionner : « KO ».
- Au format html : Le message « **Site KO : Veuillez consulter le détail ci-dessous et corriger les points KO** », s'affiche en haut de la page, en **rouge**.

[OPTION] Si la notion d'éléments « **non vitaux** » est retenue par le projet :

Si les éléments « vitaux » sont OK et au moins un élément « non vital » est KO :

- La page doit retourner le code **520**.
- Au format JSON : La propriété « Status » située à la racine doit mentionner : « WARNING ».
- Au format html : Le message « **WARNING : Certains éléments « non vitaux » sont KO : Veuillez consulter le détail ci-dessous et corriger les points KO** » s'affiche en haut de la page, en **orange**.



En cas de surveillance d'éléments « non-vitaux », 2 alertes distinctes seront mises en place au niveau des outils de supervision :

- Une alerte en cas de dysfonctionnement détecté sur les éléments essentiels.
- Une alerte en cas de dysfonctionnement détecté sur les éléments "non-vitaux".

Statuts détaillés :

Pour chacun des éléments testés, faire apparaître « **OK** » ou « **KO** », en fonction du résultat obtenu.

En cas d'erreur, un message clair (en html), ou la propriété « message » (en JSON), doit apparaître, permettant ainsi l'identification du composant défectueux. Exemples :

- Impossible d'accéder à la base de données
- Impossible d'accéder à l'API https://nom_du_web_service
- Impossible d'accéder à l'antivirus scanner-clamd

25.5.6 URL

Afin de standardiser l'appel aux pages de surveillance, l'url des pages sera du type :

- Pour une API : <https://monapi.ademe.fr/api/vX/health> (X= Numéro de version)
- Pour un site : <https://monapplication.ademe.fr/health>

25.5.7 Sécurité

Cette page de surveillance devant être accessible par des outils tierces tels que 'uptime robot' (<https://uptimerobot.com/>), et pouvant éventuellement exécuter des traitements consommateurs en ressources, elle devra impérativement être sécurisée afin d'éviter toute attaque la ciblant (telle que DDOS) et pouvant impacter la disponibilité de l'application concernée.

2 méthodes sont préconisées par l'ADEME pour sécuriser la page de supervision et de validation d'installation :

Intégration d'un Token : Solution à privilégier.

- Ajout d'un token (fixe) dans les en-têtes (header) : avec token = [token].
- Longueur et complexité du Token : Fonction SHA2, longueur 256 bits.
- Paramétrage du token :
- Pour les applications conteneurisées : A paramétrer en tant que variable CI.
- Pour les applications non conteneurisées : A intégrer dans le fichier de configuration.

Identification par login et mot de passe :

A défaut de Token, la mise en place d'une identification par login et mot de passe est envisageable, sous réserve que la gestion des identifiants soit incluse dans l'application et facilement administrable via une interface ou .htaccess (sous apache).

25.6 Exemples pour une API

Réponse de l'URI /health avec un état " OK " :

Formats	Exemples
API JSON brut "OK"	<pre>{ "status": "OK", "sections": { "0": "Stockage", "1": "Scanners" }, "probes": [{ "title": "Accès R/W au stockage", "definition": "Création dossier dans data_directory : /var/scanner", "status": "OK", "vital": true, "id_section": 0, "level": 1 }, { "title": "scanner-ok", "definition": "Retourne systématiquement OK sans tester de contenu.", "status": "OK", "vital": false, "id_section": 1, "level": 1 }, { "title": "scanner-clamd", "definition": "Teste la chaine retournée par Clamd sur la commande VERSION", "status": "OK", "version": { "engine": "0.105.1", "signatures": { "id": "26686", "date": "Tue Oct 11 10:00:23 2022" } }, "vital": true, "id_section": 1, "level": 1 }], "ok_scanners": 2, "ko_scanners": 0, "duration": { "controller": 10.179996490478516, "request": 10.215044021606445 } }</pre>

Formats	Exemples
API JSON Firefox "OK"	JSONDonnées brutesEn-têtes EnregistrerCopierTout réduireTout développerFiltrer le JSON status:"OK" ▼ sections: 0:"Stockage" 1:"Scanners" ▼ probes: ▼ 0: title:"Accès R/W au stockage" ▼ definition:"Création dossier dans data_directory : /var/scanner" status:"OK" vital:true id_section:0 level:1 ▼ 1: title:"scanner-ok" ▼ definition:"Retourne systématiquement OK sans tester de contenu." status:"OK" vital:false id_section:1 level:1 ▼ 2: title:"scanner-clamd" ▼ definition:"Teste la chaine retournée par Clamd sur la commande VERSION" status:"OK" ▼ version: engine:"0.105.1" ▼ signatures: id:"26686" date:"Tue Oct 11 10:00:23 2022" vital:true id_section:1 level:1 ok_scanners:2 ko_scanners:0 ▼ duration: controller:13.025999069213867 request:13.052940368652344

Réponse de l'URI /health avec un état " KO " :

Formats	Exemples
API JSON brut "KO"	<pre>{ "status": "KO", "sections": { "0": "Stockage", "1": "Scanners" }, "probes": [{ "title": "Accès R/W au stockage", "definition": "Création dossier dans data_directory : /var/scanner", "status": "OK", "vital": true, "id_section": 0, "level": 1 }, { "title": "scanner-ok", "definition": "Retourne systématiquement OK sans tester de contenu.", "status": "OK", "vital": false, "id_section": 1, "level": 1 }, { "title": "scanner-clamd", "status": "ERROR", "data": "gethostbyname(scanner-clamd) failed. Is scanner this started ?", "vital": true, "id_section": 1, "level": 1 }], "ok_scanners": 1, "ko_scanners": 1, "duration": { "controller": 16.412019729614258, "request": 16.4339542388916 } }</pre>

Formats	Exemples
API JSON Firefox "KO"	JSONDonnées brutesEn-têtes EnregistrerCopierTout réduireTout développerFiltrer le JSON status:"KO" ▼ sections: 0:"Stockage" 1:"Scanners" ▼ probes: ▼ 0: title:"Accès R/W au stockage" ▼ definition:"Création dossier dans data_directory : /var/scanner" status:"OK" vital:true id_section:0 level:1 ▼ 1: title:"scanner-ok" ▼ definition:"Retourne systématiquement OK sans tester de contenu." status:"OK" vital:false id_section:1 level:1 ▼ 2: title:"scanner-clamd" status:"ERROR" data:"Connection refused" vital:true id_section:1 level:1 ok_scanners:1 ko_scanners:1 ▼ duration: controller:1007.4470043182373 request:1007.4682235717773

Réponse de l'URI /health avec un état "WARNING" :

Formats	Exemples
API JSON brut "Warning"	<pre>{ "status": "WARNING", "sections": { "0": "Stockage", "1": "Scanners" }, "probes": [{ "title": "Accès R/W au stockage", "definition": "Création dossier dans data_directory : /var/scanner", "status": "OK", "vital": true, "id_section": 0, "level": 1 }, { "title": "scanner-ok", "status": "ERROR", "data": "gethostbyname(scanner-ok) failed. Is scanner this started ?", "vital": false, "id_section": 1, "level": 1 }, { "title": "scanner-clamd", "definition": "Teste la chaine retournée par Clamd sur la commande VERSION", "status": "OK", "version": { "engine": "0.105.1", "signatures": { "id": "26686", "date": "Tue Oct 11 10:00:23 2022" } }, "vital": true, "id_section": 1, "level": 1 }], "ok_scanners": 1, "ko_scanners": 1, "duration": { "controller": 17.21787452697754, "request": 17.24100112915039 } }</pre>

Formats	Exemples
API JSON Firefox "Warning"	JSON Données brutes En-têtes Enregistrer Copier Tout réduire Tout développer  Filtrer le JSON <pre> status: "WARNING" ▼ sections: 0: "Stockage" 1: "Scanners" ▼ probes: ▼ 0: title: "Accès R/W au stockage" ▼ definition: "Création dossier dans data_directory : /var/scanner" status: "OK" vital: true id_section: 0 level: 1 ▼ 1: title: "scanner-ok" status: "ERROR" ▼ data: "gethostbyname(scanner-ok) failed. Is scanner this started ?" vital: false id_section: 1 level: 1 ▼ 2: title: "scanner-clamd" ▼ definition: "Teste la chaine retournée par Clamd sur la commande VERSION" status: "OK" ▼ version: engine: "0.105.1" ▼ signatures: id: "26686" date: "Tue Oct 11 10:00:23 2022" vital: true id_section: 1 level: 1 ok_scanners: 1 ko_scanners: 1 ▼ duration: controller: 16.656875610351562 request: 16.6780948638916 </pre>

25.7 Exemples pour le front d'une application

Page de surveillance/supervision avec un état " OK " :

Formats	Exemples
Front JSON Brut "OK"	<pre> { "status": "OK", "sections": { "1": "Fichiers", "0": "Base de données", "2": "Communication avec les API" }, "probes": [{ "title": "Ecriture cache", "status": "OK", "definition": "Ecrit un fichier dans le répertoire de cache", "vital": false, "level": 2, "id_section": 1 }, { "title": "Ecriture data", "status": "OK", "definition": "Ecrit un fichier dans le répertoire data", "vital": true, "level": 1, "id_section": 1 }, { "title": "Test accès db", "status": "OK", "definition": "Teste le lien avec la base de données (ping)", "vital": true, "level": 1, "id_section": 0 }, { "title": "Test accès api", "status": "OK", "definition": "Teste le lien avec domoticz", "vital": true, "level": 1, "id_section": 2, "message": "Code http: 200 " }] } </pre>

Formats	Exemples
Front JSON Firefox "OK"	JSONDonnées brutesEn-têtes EnregistrerCopierTout réduireTout développer Filtrer le JSON <pre> status: "OK" ▼ sections: 0: "Base de données" 1: "Fichiers" 2: "Communication avec les API" ▼ probes: ▼ 0: title: "Ecriture cache" status: "OK" definition: "Ecrit un fichier dans le répertoire de cache" vital: false level: 2 id_section: 1 ▼ 1: title: "Ecriture data" status: "OK" definition: "Ecrit un fichier dans le répertoire data" vital: true level: 1 id_section: 1 ▼ 2: title: "Test accès db" status: "OK" definition: "Teste le lien avec la base de données (ping)" vital: true level: 1 id_section: 0 ▼ 3: title: "Test accès api" status: "OK" definition: "Teste le lien avec domoticz" vital: true level: 1 id_section: 2 message: "Code http: 200 "</pre>

Formats	Exemples
Front HTML OK	Le site fonctionne. Fichiers • Ecriture cache : OK Ecrit un fichier dans le répertoire de cache • Ecriture data : OK Ecrit un fichier dans le répertoire data Base de données • Test accès db : OK Teste le lien avec la base de données (ping) Communication avec les API • Test accès api : OK Teste le lien avec domoticz Message: Code http: 200

Page de surveillance/supervision avec un état " **KO** " :

Formats	Exemples
Front JSON Brut "KO"	<pre> { "status": "KO", "sections": { "1": "Fichiers", "0": "Base de données", "2": "Communication avec les API" }, "probes": [{ "title": "Ecriture cache", "status": "OK", "definition": "Ecrit un fichier dans le répertoire de cache", "vital": false, "level": 2, "id_section": 1 }, { "title": "Ecriture data", "status": "KO", "definition": "Ecrit un fichier dans le répertoire data", "vital": true, "level": 1, "id_section": 1 }, { "title": "Test accès db", "status": "OK", "definition": "Teste le lien avec la base de données (ping)", "vital": true, "level": 1, "id_section": 0 }, { "title": "Test accès api", "status": "OK", "definition": "Teste le lien avec domoticz", "vital": true, "level": 1, "id_section": 2, "message": "Code http: 200 " }] } </pre>

Formats	Exemples
Front JSON Firefox "KO"	JSON Données brutes En-têtes Enregistrer Copier Tout réduire Tout développer  Filtrer le JSON <pre> status: "KO" ▼ sections: 0: "Base de données" 1: "Fichiers" 2: "Communication avec les API" ▼ probes: ▼ 0: title: "Ecriture cache" status: "OK" definition: "Ecrit un fichier dans le répertoire de cache" vital: false level: 2 id_section: 1 ▼ 1: title: "Ecriture data" status: "KO" definition: "Ecrit un fichier dans le répertoire data" vital: true level: 1 id_section: 1 ▼ 2: title: "Test accès db" status: "OK" definition: "Teste le lien avec la base de données (ping)" vital: true level: 1 id_section: 0 ▼ 3: title: "Test accès api" status: "OK" definition: "Teste le lien avec domoticz" vital: true level: 1 id_section: 2 message: "Code http: 200 "</pre>

Formats	Exemples
Front HTML "KO"	Site KO : Veuillez consulter le détail ci-dessous et corriger les points KO. Fichiers • Ecriture cache : OK Ecrit un fichier dans le répertoire de cache • Ecriture data : KO Ecrit un fichier dans le répertoire data Base de données • Test accès db : OK Teste le lien avec la base de données (ping) Communication avec les API • Test accès api : OK Teste le lien avec domoticz Message: Code http: 200

Page de surveillance/supervision avec un état " **WARNING** " :

Formats	Exemples
Front JSON Brut "Warning"	<pre>{ "status": "WARNING", "sections": { "1": "Fichiers", "0": "Base de données", "2": "Communication avec les API" }, "probes": [{ "title": "Ecriture cache", "status": "KO", "definition": "Ecrit un fichier dans le répertoire de cache", "vital": false, "level": 2, "id_section": 1 }, { "title": "Ecriture data", "status": "OK", "definition": "Ecrit un fichier dans le répertoire data", "vital": true, "level": 1, "id_section": 1 }, { "title": "Test accès db", "status": "OK", "definition": "Teste le lien avec la base de données (ping)", "vital": true, "level": 1, "id_section": 0 }, { "title": "Test accès api", "status": "OK", "definition": "Teste le lien avec domoticz", "vital": true, "level": 1, "id_section": 2, "message": "Code http: 200 " }] }</pre>

Formats	Exemples
Front JSON Firefox "Warning"	JSON Données brutes En-têtes Enregistrer Copier Tout réduire Tout développer  Filtrer le JSON <pre> status: "WARNING" ▼ sections: 0: "Base de données" 1: "Fichiers" 2: "Communication avec les API" ▼ probes: ▼ 0: title: "Ecriture cache" status: "KO" definition: "Ecrit un fichier dans le répertoire de cache" vital: false level: 2 id_section: 1 ▼ 1: title: "Ecriture data" status: "OK" definition: "Ecrit un fichier dans le répertoire data" vital: true level: 1 id_section: 1 ▼ 2: title: "Test accès db" status: "OK" definition: "Teste le lien avec la base de données (ping)" vital: true level: 1 id_section: 0 ▼ 3: title: "Test accès api" status: "OK" definition: "Teste le lien avec domoticz" vital: true level: 1 id_section: 2 message: "Code http: 200 "</pre>

Formats	Exemples
Front HTML "Warning"	WARNING : Certains éléments "non vitaux" sont KO, Veuillez consulter le détail ci-dessous et corriger les points KO. Fichiers • Ecriture cache : KO Ecrit un fichier dans le répertoire de cache • Ecriture data : OK Ecrit un fichier dans le répertoire data Base de données • Test accès db : OK Teste le lien avec la base de données (ping) Communication avec les API • Test accès api : OK Teste le lien avec domoticz Message: Code http: 200

26. Annexes

26.1 Recommandations Sécurité

26.1.1 Recommandations Sécurité pour la mise en œuvre d'un site web :

Le respect de ces recommandations est obligatoire. Le non respect de certains éléments peut être accepté à titre dérogatoire, sous réserve de justification.

La documentation complète concernant les recommandations listées ci-dessous est disponible à [cet emplacement](#).

(**Source** : https://www.ssi.gouv.fr/uploads/2013/05/anssi-guide-recommandations_mise_en_oeuvre_site_web_maitriser_standards_securite_cote_navigateur-v2.0.pdf)

- R1 Mettre en oeuvre TLS à l'état de l'art
- R2 Mettre en oeuvre HSTS
- R3 Surveiller les CT logs
- R4 Utiliser l'API DOM à bon escient
- R5 Dissocier clairement la composition des pages web
- R6 Expliciter la nature d'une ressource avec l'en-tête Content-Type
- R7 Vérifier l'échappement des contenus inclus
- R8 Vérifier la conformité des données issues de sources externes
- R9 Proscrire l'usage de la fonction eval()
- R10 Proscrire l'usage de constructions basées sur l'évaluation de code
- R11 Contrôler l'intégrité des contenus internes
- R12 Contrôler l'intégrité des contenus tiers
- R13 Restreindre les contenus aux ressources fiables
- R14 Mettre en oeuvre CSP par en-tête HTTP
- R14- Mettre en oeuvre CSP par balise meta dans les pages HTML
- R15 Interdire des contenus inline
- R16 Définir la directive default-src
- R17 Utiliser CSP contre le clickjacking
- R18 Utiliser X-Frame-Options contre le clickjacking
- R19 Etudier les risques liés à la collecte de rapports CSP
- R20 Réduire l'impact des requêtes silencieuses via CSP
- R21 Définir la stratégie de construction de l'en-tête Referer
- R22 Modifier ponctuellement l'en-tête Referer
- R23 Ne pas stocker des informations sensibles dans les bases de données locales
- R23- Éviter de stocker des informations sensibles dans les bases de données locales
- R24 Ne pas stocker des informations sensibles dans les bases de données IndexedDB
- R24- Éviter de stocker des informations sensibles dans les bases de données IndexedDB
- R25 Proscrire l'usage de l'API Web SQL Database
- R26 Ne pas stocker d'informations sensibles dans les cookies
- R27 Cloisonner les sessions au moyen de noms de domaine distincts
- R28 Définir le path d'un cookie
- R29 Maîtriser l'accès aux cookies en JavaScript
- R30 Proscrire l'accès en JavaScript à un cookie de session
- R31 Limiter le transit des cookies aux flux sécurisés
- R32 Définir une stratégie stricte d'envoi des cookies en cross-site
- R33 Définir une stratégie stricte d'envoi des cookies de session en cross-site
- R34 Encoder les réponses XMLHttpRequest
- R35 Choisir une API selon sa méthode HTTP
- R36- Utiliser XHR avec la méthode GET sous certaines conditions
- R36 Utiliser XHR avec la méthode POST
- R36+ Utiliser XHR avec la méthode PUT
- R37 Compléter la mise oeuvre de XHR par une configuration CSP
- R38 Protéger les appels XHR par un contrôle anti-CSRF

- R39 Mettre en oeuvre un preflight lors des appels CORS
- R40 Vérifier la valeur de l'Origin lors de la réception d'une requête CORS
- R41 Cloisonner les services web au moyen de noms de domaines distincts
- R42 Éviter l'usage de bibliothèques publiques effectuant des appels CORS.
- R42- Isoler l'utilisation de bibliothèques publiques effectuant des appels CORS.
- R43 Anonymiser le chargement des ressources en cross-origin
- R44 Préférer l'utilisation de l'API Fetch à XMLHttpRequest
- R45 Sécuriser l'ouverture de nouvelles fenêtres
- R46 Définir une stratégie d'ouverture en cross-origin
- R47 Utiliser le mode strict
- R48 Isoler les traitements par Web Workers
- R48+ Isoler les traitements par Web Worker et Origin « data : »
- R49 Formaliser les échanges en utilisant l'API de Message
- R50 Cloisonner les traitements dans des iframes
- R51 Cloisonner les traitements avec une sandbox
- R52 Favoriser la déclaration de sandbox via CSP
- R52+ Cloisonner les traitements par une iframe sur une seconde Origin
- R53 Formaliser les échanges en utilisant l'API de Message
- R54 Définir l'Origin lors de l'utilisation de l'API de Message
- R55 Contrôler l'Origin lors de l'utilisation de l'API de Message
- R56 Compléter la déclaration d'une API de messages par la définition d'une CSP
- R57 Proscrire l'écriture de document.domain
- R58 Proscrire l'usage de JSON-P
- R59 Définir des profils de déploiement spécifiques aux contextes
- R60 Empêcher le déploiement d'un profil non adapté au contexte
- R61 Limiter les composants logiciels tiers
- R62 Maintenir à jour les composants logiciels tiers utilisés
- R63 Ne pas modifier le coeur des composants logiciels tiers utilisés

27. Guides Devops

Guides Devops ADEME disponibles

Guide devops environnement de pré-intégration (ADEME) :

-  [Guide Devops préintégration](#)

Guide devops générique (DRI) :

-  [Guide Devops Générique DRI](#)

28. Mentions Légales

Mentions Légales

-  [Mentions légales \(au 07/07/2023\)](#)

29. Politique de protection des données personnelles

Politique de protection des données personnelles

-  [Politique de protection des données personnelles \(au 07/07/2023\)](#)

30. Politique des cookies

Politique des cookies

-  [Politique des cookies \(au 14/11/2023\)](#)

31. Hébergement - Accords de niveau de service

L'hébergeur est engagé contractuellement avec l'ADEME par un accord de niveau de service (service-level agreement - SLA). Ci-après le détail de ces SLA par catégorie.

31.1 SLA sur les classes de criticité des applications

31.1.1 Accords de niveau de service des applications

Les applications hébergées peuvent être classées en 4 niveaux de criticité selon différents critères qui sont définis par l'ADEME lors de l'élaboration du projet.

- RTO (Recovery Time Objective) ou GTR (Garantie de temps de rétablissement) : délai de reprise de fonctionnement de l'application, exprimé en heures ; ce délai exclut le délai préalable à la restauration parfois nécessaire dans certains cas d'incidents.
- RPO (Recovery Point Objective) : correspond à la perte de données autorisée, exprimée en heures.

Le tableau ci-après décrit pour chaque niveau la plage de surveillance, le RTO/GTR et le RPO :

Classe de criticité	Plage d'ouverture du service sur incidents	RTO / GTR	RPO	Politique de sauvegarde appliquée
C1	7/7 - 24/24	2h	2h	
C2	7/7 - 24/24	4h	8h	
C3	5/7 8h/18h (Jours ouvrés)	24h	24h	
C4	5/7 8h/18h (Jours ouvrés)	48h	24h	

31.2 Taux de disponibilité sur la plateforme

31.2.1 Accords sur le niveau disponibilité de la plateforme

Taux de disponibilité plateforme	Détail	Plage d'ouverture du service	Engagement	Politique de sauvegarde appliquée
Taux de dispo	Datacenter (Climatisation, Electricité, Surface, Accès Réseau Opérateur), <u>MCO</u> des matériels et équipements, des solutions réseaux, des solutions de sécurité, des solutions de stockage et sauvegarde et des hyperviseurs. Services de supervision	7/7 - 24/24	99,95%	4h d'indisponibilité par an, 2 interruptions max. par an

31.3 SLA sur les tickets

31.3.1 Accords de niveau de service des tickets

INCIDENT

Caractérisation des services	Délai de prise en charge	RTO/GTR délai de réalisation	Plage d'ouverture
Critique	15 min	4h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4
Majeur	15 min	24h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4
Mineur	15 min	48h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4

PROBLÈME

Caractérisation des services	Délai de prise en charge	RTO/GTR délai de réalisation	Plage d'ouverture
Critique	15 min	4h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4
Majeur	15 min	24h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4
Mineur	15 min	48h	7/7 24/24 App C1 et C2 5/7 8-18h App C3 et C4

DEMANDE DE SERVICES ET EXÉCUTION DE REQUÊTES

Détail des services	Délai de prise en compte	Délai de réalisation
Demande système simple : arrêt/démarrage VM, application, service	2h	2h
Demande Base de données (arrêt/démarrage instance/base Mysql, Sql server, PostGreSQL, gestion datafiles, arrêt/relance plan de maintenance, rafraichissement d'environnements)	2h	J+1
Demande Middleware (bibliothèques/serveur web/serveur app., docker, symfony, Zend, Drupal, SPIP, Wordpress, Java/Php/.Net/Python)	2h	Cf. SLA par application
Demande d'intégration applicative : installation d'un patch (correctifs)	2h	4h
Demande d'intégration applicative : installation d'une mise à jour simple (fichiers, scripts)	4h	J+2
Demande d'intégration applicative : installation d'une mise à jour simple avec GIT/SVN	4h	J+1
Demande d'intégration applicative : installation d'une mise à jour moyenne (fichiers, scripts, bases de données)	4h	J+3
Demande d'intégration applicative : installation d'une mise à jour urgente	1h	4h
Demande d'intégration applicative : installation d'une nouvelle application	4h	J+4
Patch de sécurité (opération non planifiée)	2h	4h

31.4 SLA sur les environnements conteneurisés

Opération	Délais de prise en compte	Délais de réalisation
Ajout de RAM	15 min	4h – 2h si urgent
Ajout de CPU	15 min	4h – 2h si urgent
Ajout d'un container	15 min	24h
Ajout d'une seconde VM	15 min	24h

Pour l'ajout d'un conteneur ou d'une VM, il faut ajouter à ces temps de mise à disposition, les délais de création d'environnement (1j) ou de MEP applicative (2h si urgent, ou J+1 à J+5 selon environnement et complexité).