asalae

Pré-requis d'installation

Version 3.0

Libriciel SCOP

Document

Auteur	Sébastien PICARD	***Date de diffusion***	22/10/2024
Chef de projet	Florent VEYRES	***N° de version***	3.0

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Sébastien PICARD	Création de la documentation	22/10/2024

Licence

Table des matières

1. LISTE DES SYSTÈMES D'EXPLOITATION SUPPORTÉS

OS	Statut	Commentaires
Ubuntu >= 24.04 LTS x64	**Supporté**	Version Asalae 3 - OS de référence
RHEL x64	**Supporté**	version en cours de support par RedHat

- Les OS DEBIAN ne sont pas supportés,
- Les versions NON LTS d'Ubuntu Server ne sont pas supportées,
- À ce jour, les versions clone de RHEL ne sont pas supportées.

2. DIMENSIONNEMENT ET RESSOURCES

Le dimensionnement disque peut être effectué sur une unique partition ou via disque /volume séparé suivant le contexte d'utilisation.

Nous conseillons fortement le formatage en LVM afin de pouvoir augmenter à chaud l'espace disque et de s'inspirer du schéma de partitionnement indiqué dans le tableau suivant :

Indicateurs	Ressources test	Ressources production	Commentaires
Espace disque système (racine)	~50 Go	~100 Go	L'espace disque contiendra : L'OS, les logs, les sources de l'application, la base de données PostgreSQL
Espace disque échanges (/data)	XXX Go	XXX Go	Espace tampon pour la réception des transferts entrants **
Espace disque données (/data-archives)	XXX Go	XXX Go	Volume(s) d'archives
CPU	2	4	Indicateurs conseillés
RAM	8 Go	16G	Indicateurs conseillés (en prod un espace de swap de 8G peut être alloué si 8G de RAM disponible)

> ** Taille estimée à 3X le volume de données à envoyer au SAE.

> En cas d'usage intensif du SAE notamment avec des flux de plusieurs centaines de Go, les ressources RAM seront à augmenter.

> En cas d'utilisation du SAE en mode multi-services d'archives (mutualisé) il conviendra d'adopter les pré-requis de production pour les instances de test et d'optimiser le dimensionnement.

> Le dimensionnement de l'espace de stockage /data-archives est éminemment dépendant du(es) type(s) de flux archivé(s), de la taille des fichiers et de leur nombre !

NB 1 : En cas de partition /var distincte de la partition racine, prévoir de provisionner 20 Go (Images docker et logs système)

NB 2 : En cas de partition /tmp distincte de la partition racine, prévoir de provisionner 5 Go

2.1. Volumes de stockage

Asalae est compatible avec une utilisation de volumes de stockage filesystem et S3 (Objet).

- Le type de disque doit être sécurisé et évolutif, disque virtuel ou volume sur baie de stockage type SAN (RDM, etc.),
- Le volume local doit être accessible par le serveur applicatif, il peut s'agir de n'importe quel volume (EXT4/XFS),
- Les volumes NFS sont **PROSCRITS** suite à plusieurs retours d'utilisation problématiques provenant de sources diverses (serveur, client, options de montage, etc.).

La technologie de stockage Objet S3 étant un standard, nous avons qualifié néanmoins certains produits proposant cette API afin de qualifier l'ensemble de nos fonctionnalités, notamment l'upload multipart.

Le connecteur est qualifié pour :

- Minio,
- OVH (Swift et OpenIO),
- Scaleway,
- Scality,
- CEPH (RedHat),
- Isilon (DELL),
- NetAPP StorageGrid = qualifié NetAPP OnTAP = non compatible.

2.2. Dimensionnement optimisé

Suivant le contexte d'utilisation (mutualisant, versements volumineux), il sera possible via le tableau ci dessous de dimensionner plus précisément le SAE.

Les volumes d'archives sont à dimensionner en rapport avec la typologie et taille des versements qui seront envoyés au SAE.

Le répertoire /data désigne **uniquement l'espace disque occupé par les fichiers des transferts** et il ne comprend pas le répertoire temporaire qui accueille les fichiers des transferts le temps du téléchargement.

Rétention des transferts	Volume des transferts/jour	Taille disponible /data
7 jours	500 Mo	4,5 Go
7 jours	1 Go	9 Go
7 jours	5 Go	45 Go
1 jour	500 Mo	1,5 Go
1 jour	1 Go	3 Go
1 jour	5 Go	15 Go

Notes :

- le calcul de la place disponible tient compte d'une journée supplémentaire de sécurité,
- le répertoire temporaire doit être dimensionné en fonction de la taille maximum des transferts.

3. COMMUNICATION RÉSEAU

Voici la liste des ports utilisés en entrée et sortie :

Protocole	Commentaires
HTTP port 80 TCP	redirection vers HTTPS
HTTPS port 443 TCP	Accès utilisateur et réception des flux depuis le TDT ou autre service versant

Certaines ressources doivent être accessibles depuis internet.

Voici la liste des URL utilisées depuis internet pour la phase d'installation :

Ressource	Destination	Protocole	port TCP
Images Docker Asalae	nexus.libriciel.fr	HTTPS	443
Images Docker Asalae	registry.libriciel.fr	HTTPS	443
Images Docker Asalae	hubdocker.libriciel.fr	HTTPS	443
Docker CE	download.docker.com	HTTPS	443
Docker-compose	github.com	HTTPS	443

Voici la liste des URL utilisées depuis internet dans la phase d'exploitation (production) :

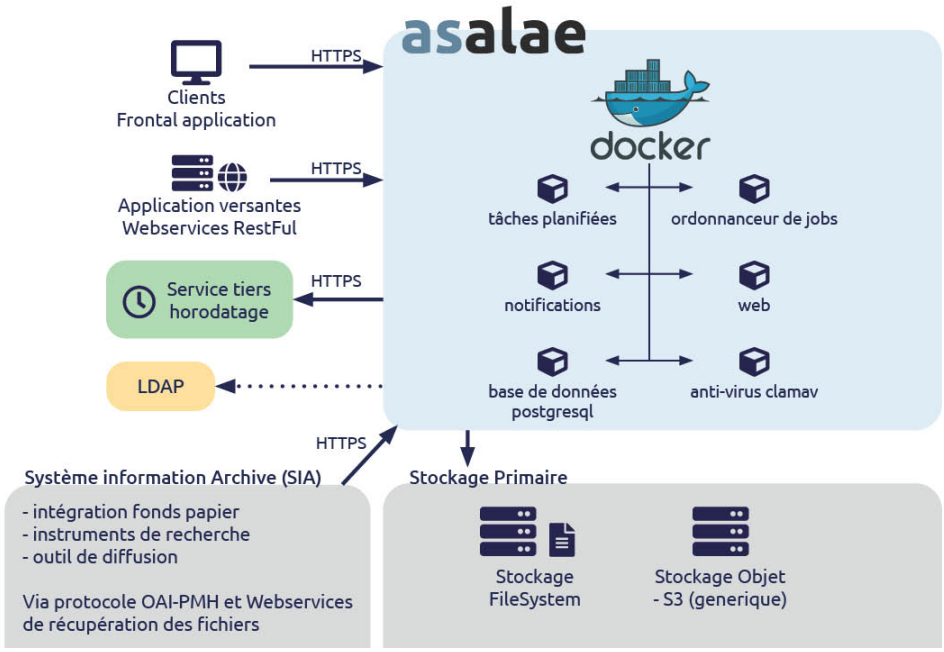
Source	Destination	Protocole	port TCP
Tâche planifiée (entretien Pronom)	Site www.nationalarchives.gov.uk	HTTPS	443
Crontab	Site database.clamav.net	HTTPS	443
asalae	ressources.libriciel.fr	HTTPS	443

> La liste complète des flux réseau est décrite dans la documentation d'exploitation.

4. SCHÉMA D'ARCHITECTURE

Le schéma d'architecture décrit les briques logicielles utilisées.

Toute ces briques doivent être regroupées dans un même serveur, la base de donnée ne contenant qu'une petite partie des meta données, il n'y a aucune plus value à externaliser certaines briques comme la base de données, de plus cela peut entraîner un risque d'intégrité des données en cas de restauration.



Architecture de l'application

Asalae peut être utilisé dans un réseau local, ou être utilisé pour la réception de flux provenant de services versant depuis internet.

L'accès à Asalae s'effectue par navigateur, une URL en domaine ou sous-domaine dédié sera nécessaire, ex **asalae.mondomaine.fr**.

Dans le cas d'un accès nécessaire depuis l'extérieur seront nécessaires :

- Une URL en domaine ou sous-domaine public,
- Les accès aux ports 80 HTTP et 443 HTTPS devront être ouverts depuis l'extérieur du réseau (ex : NAT, reverse proxy).

5. AUTHENTIFICATION SSO

L'Authentification OpenID connect (OIDC) via le protocole `Oauth2` est compatible.

À ce jour seul l'authentification est possible, la création des utilisateurs doit provenir d'une création manuelle ou liaison LDAP.

La configuration s'effectue depuis la console d'administration.

Les informations nécessaires à une mise en place sont :

- Base_url : url avant le `.well-known/openid-configuration` ex : https://portail-sso.collectivite.fr:port/auth/realms/asalae/,
- client_id : ex : asalae,
- client_secret : ex: 132ff39b-xxx-4fa6-xxx-a3ffe63b6b0b,
- username : attribut utilisé pour le login, ex : id.

6. BRIQUES TECHNIQUES

Voici la liste des briques techniques : docker

> Ces briques sont des pré-requis, et seront déployés à l'installation, inutile de procéder à leur mise en place. La liste complète des briques techniques décrite dans la documentation d'exploitation.

7. POSTE CLIENT

7.1. Navigateurs compatibles

Les logiciels produits par Libriciel SCOP sont développés principalement pourGoogle Chrome et Mozilla Firefox

Libriciel SCOP assure la compatibilité de tous ces logiciels avec :

- la dernière version stable de Google Chrome,
- la dernière version de Mozilla Firefox,
- les versions ESR de Mozilla Firefox maintenues par Mozilla.

Bien que développés pour les standards du web, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont pas garantis :

- sur d'autres versions de Google Chrome (beta, canary) ou Mozilla Firefox (ESR non maintenues, anciennes versions),
- sur d'autres navigateurs (Microsoft Internet Explorer, Microsoft Edge, Apple Safari, Opera...),
- sur les technologies de bureau à distance (Citrix XenApp, Citrix XenDesktop, Microsoft RDS, Microsoft Terminal Server...), en particulier pour les fonctionnalités de signature électronique.

7.2. Systèmes d'exploitation compatibles

D'une manière générale, Libriciel assure la compatibilité côté client avec la plupart des systèmes d'exploitations grand public maintenus par leurs distributeurs et permettant de faire fonctionner les navigateurs compatibles.

Néanmoins, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont garantis que sur les versions du système Microsoft Windows maintenues par Microsoft à destination des postes clients.

En particulier, les outils de signature (Libersign) ne sont développés que pour Windows sur les architectures Intel x86 et AMD 64 et ne fonctionnent pas avec d'autres systèmes d'exploitation.

7.3. Signature électronique

L'outil de signature (LiberSign2) s'adapte selon le navigateur utilisé :

Pour Mozilla Firefox ou Google Chrome : pas "d'applet JAVA", car une extension de navigateur est utilisée, en liaison avec un "logiciel compagnon".

Le logiciel compagnon est installé dans le répertoire utilisateur, normalement accessible sans droit administrateur.

Remarque pour les postes sous contrainte (avec GPO ou restriction de droit de type Citrix) : le poste utilisateur doit avoir accès au répertoire %LOCALAPPDATA%, directement utilisé par l'extension LiberSign.

Pour Microsoft Internet Explorer 11 : déploiement du plugin JAVA à jour, pour permettre la signature électronique. En l'absence de "magasin d'extensions", le recours au système d'applets JAVA reste obligatoire.

8. ÉCRITURE EN Y OU N

Asalae v3 peut être installée avec une réplication et écriture en Y ou en N.

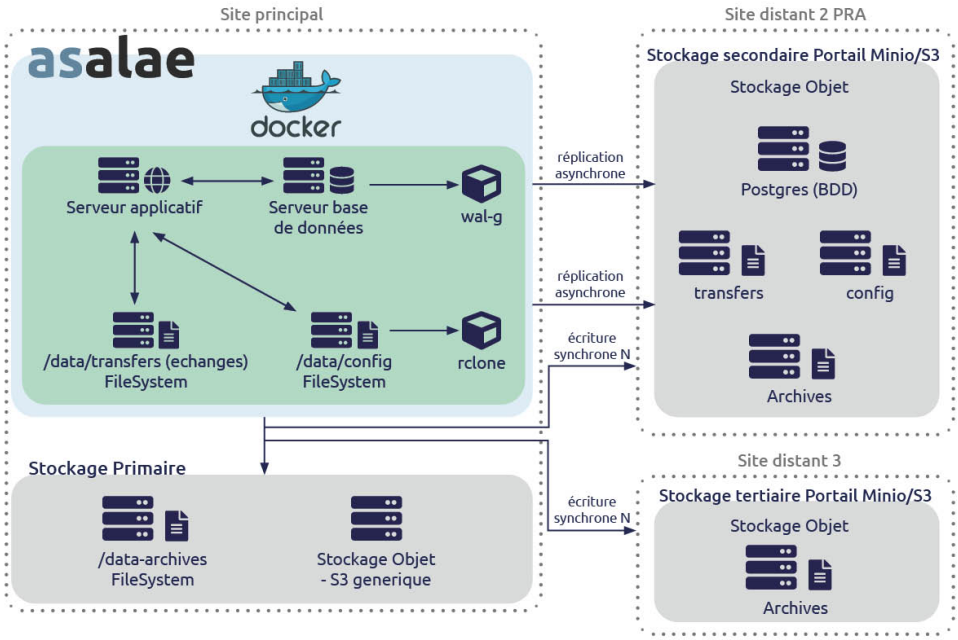
Ces deux composants permettent de mettre en place un plan de reprise d'activité (PRA) qui en cas d'incident majeur permettra de remonter le site primaire à partir des données répliquées. La haute disponibilité ou plan de continuité d'activité (PCA) n'est pas envisagé via la mise en place de cette fonction.

Si votre infrastructure dispose de fonctions de réplication synchrones et idéalement sur deux bâtiments, la mise en réplication n'est pas nécessaire.

L'écriture en N permet d'écrire sur N volumes de stockage identiques la donnée à archiver. Un mécanisme d'accusé de réception permet d'obtenir une cohérence sur ces deux volumes.

Idéalement, un des N volumes doit être local et les autres montés sur le serveur primaire depuis une infrastructure distante.

8.1. schéma d'architecture réplication + écriture en N



Architecture interne