kaspersky

Kaspersky Automated Security Awareness Platform On-Premise – Instructions d'installation

Version de l'application : 1.1.0

kaspersky

Cher utilisateur, Chère utilisatrice,

Nous vous remercions de nous confier vos besoins en matière de sécurité. Nous espérons que ce document vous aidera à utiliser le produit et répondra à la plupart de vos questions.

Date de révision du document : 12 mars 2024

https://www.kaspersky.fr
https://support.kaspersky.fr

À propos de Kaspersky https://www.kaspersky.fr/about/company

kaspersky

Contenu

À propos de la plateforme ASAP On-Premise

Kaspersky Automated Security Awareness Platform On-Premise (ci-après également dénommé « ASAP On-Premise » et « ASAP ») est une plateforme de formation sur laquelle les utilisateurs peuvent découvrir les règles de conformité en matière de sécurité de l'information, se renseigner sur les menaces qui les attendent dans leurs activités quotidiennes, et acquérir de l'expérience à l'aide d'exemples pratiques.

La formation permet de développer en détail toutes les connaissances et compétences nécessaires. La formation complète comprend l'assimilation et la consolidation de plus de 350 compétences élémentaires.

La formation est divisée en unités. Chaque unité de formation se concentre sur un thème particulier à un niveau de difficulté correspondant au programme. Les unités de formation contiennent plusieurs cours d'une durée moyenne de 5 à 10 minutes chacun, qui sont ensuite approfondis par des répétitions, des tests et des simulations d'attaques de phishing pendant la formation sur les chapitres (le cas échéant).

Dans cette section

Kit de distribution

Le kit de distribution comprend les fichiers suivants :

- Archive pour l'installation des modules ASAP On-Premise
- Fichiers contenant des informations sur la version (notes de version) en russe et en anglais

Configuration matérielle et logicielle requise

* - dernière version du logiciel au lancement d'ASAP.

Configuration logicielle requise pour les utilisateurs finaux de la plateforme

Les systèmes d'exploitation suivants sont pris en charge :

- Ordinateurs de bureau :
  - Windows 10
  - Windows 7
  - Mac OS*
- Appareils mobiles :

- iOS (dernière version)
- Android version 5 ou version ultérieure

L'un des navigateurs suivants doit être installé sur l'ordinateur pour que l'interface Web fonctionne :

- Ordinateurs de bureau :
  - Microsoft Edge*
  - Mozilla Firefox*
  - Google Chrome*
  - Safari pour MacOS*
- Appareils mobiles :
  - Safari (iOS)
  - Google Chrome (Android)

Configuration matérielle requise pour les utilisateurs finaux de la plateforme

- Processeur de 1 GHz
- 1 Go de RAM
- Bande passante réseau : 1 Mo/s
- 20 Mo d'espace disque

Configuration logicielle requise pour les administrateurs d'ASAP

Les systèmes d'exploitation suivants sont pris en charge :

- Ordinateurs de bureau :
  - Windows 10
  - Windows 7
  - Mac OS*

L'un des navigateurs suivants doit être installé sur l'ordinateur pour que l'interface Web fonctionne :

- Ordinateurs de bureau :
  - Microsoft Edge*
  - Mozilla Firefox*
  - Google Chrome*
  - Safari pour MacOS*

Pour traiter les emails de la plateforme, l'un des clients de messagerie suivants doit être installé sur l'ordinateur :

- MS Outlook version 2010 ou version ultérieure (Windows, macOS).

Configuration matérielle requise pour les administrateurs d'ASAP

- Processeur de 1.5 GHz
- 2 Go de RAM
- Bande passante réseau : 1 Mo/s

- 20 Mo d'espace disque

Configuration matérielle recommandée pour un déploiement sur site d'ASAP

La solution est déployée en tant que cluster k3s sur 1 nœud. Vous pouvez ajouter des ressources complémentaires à chaque module (cœurs de processeur, mémoire vive) et les répartir sur plusieurs serveurs pour augmenter les performances générales.

Configuration matérielle et logicielle requise :

- Processeur Intel ou AMD avec prise en charge de SSE 4.2, au moins 8 cœurs et 16 threads.
- 16 Go de RAM.
- 300 Go d'espace libre sur le disque SSD.
- Système d'exploitation Linux : Rocky Linux (RHEL) 8.5 et versions ultérieures.
- Le SWAP est désactivé.

kaspersky

Licences

Cette section contient les informations de base sur l'octroi de licences pour la plateforme ASAP On-Premise. Pour en savoir plus sur l'octroi de licences pour la plateforme, consultez l'Aide.

Dans cette section

À propos du Contrat de licence

Contrat de licence : un accord juridique entre vous et AO Kaspersky Lab, qui stipule les conditions dans lesquelles vous pouvez utiliser l'application.

Lisez attentivement les conditions du Contrat de licence avant de commencer à utiliser l'application.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final dans le document CLUF_<localization language> disponible dans le kit de distribution de la plateforme. Une fois que la plateforme est installée, le Contrat de licence utilisateur final est également placé dans le dossier /opt/kaspersky/ASAP/CLUF.

En confirmant que vous acceptez le Contrat de licence utilisateur final lors de votre inscription sur la plateforme, vous acceptez également les conditions du Contrat de licence utilisateur final. Si vous n'acceptez pas les conditions du Contrat de licence utilisateur final, vous devez arrêter votre inscription et vous ne pouvez pas utiliser le programme.

À propos des licences

Licence : un droit limité dans le temps d'utiliser l'application, qui vous est fourni dans le cadre du Contrat de licence.

La licence comprend le droit de recevoir les types de services suivants :

- utiliser l'application conformément aux conditions du Contrat de licence.
- obtenir une assistance technique.

Le volume des services rendus et la période d'utilisation de l'application dépendent du type de licence utilisé pour activer l'application.

Voici les types de licences disponibles :

- *Essai* : une licence gratuite destinée à donner la possibilité d'évaluer l'application.

  Une licence d'essai est de courte durée. Dès que la licence expire, toutes les fonctionnalités de la plateforme Kaspersky Automated Security Awareness sont désactivées. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

  Vous ne pouvez activer l'application sous une licence d'essai qu'une seule fois.

- *Commercial* : une licence payante fournie lors de l'achat de l'application.

  À l'expiration d'une licence commerciale, le programme cesse de remplir ses fonctions. Pour continuer à utiliser la plateforme Kaspersky Automated Security Awareness avec un accès complet à ses fonctionnalités, vous devez renouveler votre licence commerciale.

  Nous vous recommandons de renouveler votre licence au plus tard à sa date d'expiration afin d'éviter toute interruption de service.

À propos du certificat de licence

Certificat de licence : un document que vous recevez avec un fichier de clé ou un code d'activation.

Le Certificat de licence contient les informations suivantes sur la licence fournie :

- la clé de licence ou le numéro de commande
- des informations sur l'utilisateur à qui la licence est fournie
- des informations concernant l'application qui peut être activée à l'aide de la licence fournie
- la limite du nombre d'emplacements de licence (par exemple, le nombre d'appareils sur lesquels vous pouvez utiliser l'application dans le cadre de la licence fournie)
- la date du début de la durée de validité de la licence
- la date de la fin de la durée de validité de la licence
- le type de licence

À propos du fichier clé

Le *fichier clé* est un fichier portant l'extension clé fourni par Kaspersky. Le fichier clé permet d'ajouter la clé de licence qui active l'application.

Le fichier clé est envoyé par email à l'adresse que vous avez fournie après avoir acheté une licence ASAP ou demandé une version d'essai d'ASAP.

Aucune connexion aux serveurs d'activation de Kaspersky n'est requise pour activer l'application à l'aide du fichier clé.

Si vous supprimez accidentellement la clé, elle peut être restaurée. Vous pouvez avoir besoin du fichier clé pour vous inscrire à Kaspersky CompanyAccount, par exemple.

Pour restaurer le fichier clé, vous devez exécuter l'une des actions suivantes :

- Prise de contact avec le vendeur de la licence
- Obtenez un fichier clé sur le site Internet de Kaspersky https://keyfile.kaspersky.com/fr/ grâce à un code d'activation spécifique.

Achat d'une licence

Pour acheter des licences, vous pouvez contacter les partenaires de AO Kaspersky Lab ou les filiales locales de l'entreprise. https://partnersearch.kaspersky.com/?b2bUne liste des partenaires de votre région est disponible sur le site https://partnersearch.kaspersky.com/?b2b

Les partenaires peuvent également fournir des informations et du matériel supplémentaires concernant la plateforme, des informations concernant les prix et les promotions, etc. Un lien vers la page de recherche des entreprises partenaires autorisées est également disponible dans l'interface Web du programme, dans la section **Licences et entreprises**.

À propos du traitement des données

Toutes les données requises pour Kaspersky Automated Security Awareness Platform (ASAP) sont stockées et traitées par l'organisation dont le serveur héberge la plateforme. Aucune donnée n'est transmise à Kaspersky pendant le fonctionnement d'ASAP.

Pendant son fonctionnement, ASAP enregistre les données suivantes sur l'appareil sur lequel la plateforme est installée :

- Identifiants des employés et des entreprises, enregistrements dans la base de données, administrateurs d'entreprise, entreprises achetant la licence, groupe de formation d'employés utilisé pour la synchronisation dans le cloud, diapositives des supports de formation et campagnes de phishing.
- Données relatives à la synchronisation et à l'intégration effectuées via des systèmes externes (SCIM, OPEN API, LOCAL AD, OUTLOOK PLUGIN (alarme anti-phishing)) et résultats de cette synchronisation ; adresse email des utilisateurs, appels aux utilisateurs et données des utilisateurs saisies par l'administrateur.
- Données relatives à l'entreprise formant ses employés à Kaspersky Automated Security Awareness Platform, y compris domaine de l'entreprise (afin que tous les utilisateurs avec une adresse email se trouvant dans ce domaine puissent être ajoutés aux campagnes de phishing sans être informés du début de la formation) et informations sur l'administrateur.
- Données relatives aux licences et à leur durée de validité ainsi qu'au nombre d'employés en formation.
- Données relatives aux campagnes de phishing, aux employés et aux résultats des contrôles, informations sur les emails identifiés comme étant du phishing par les utilisateurs et adresses email des utilisateurs.
- Données relatives à la formation des employés de l'entreprise, aux unités terminées, aux certificats obtenus et aux paramètres de formation.
- Informations internes nécessaires au bon fonctionnement du système.

kaspersky

Préparation de l'installation

Pour installer la plateforme, il convient de sélectionner un serveur distinct sur lequel aucune autre application ne sera installée.

Créez un domaine pour la plateforme ASAP On-Premise :

1. Dans le réseau de votre organisation, enregistrez un nom de domaine pour la plateforme.
   Le nom de domaine doit être au format suivant :

   `*.<domain>.<region>`

   Exemple : `*.kasap-domain.fr`
2. Créez deux enregistrements A pour l'adresse IP de votre serveur :
   - domaine

     Exemple : « kasap-domain.fr » dans A « 10.10.11.23 »
   - *.domain

     Exemple : « kasap-domain.fr » dans A « 10.10.11.23 »
3. Émettez un certificat SSL wildcard pour le domaine de la plateforme avec les paramètres suivants :
   - Nom de l'objet : `*.<domaine>.<région>`

     Exemple : `*.kasap-domain.fr`
   - Nom alternatif : `asap-cdn.minio.<domaine>.<région>`

     Exemple : `asap-cdn.minio.kasap-domain.fr`
   - Le certificat doit être émis au format CRT.
4. Ajoutez les certificats racine de l'autorité de certification du domaine aux certificats de confiance sur le serveur sur lequel vous souhaitez installer la plateforme. Cette opération peut être effectuée, par exemple, à l'aide des commandes suivantes :

   ```
   sudo
   cp <your_certificate_for_the_certificate_authority_of_the_main_domain>
   /etc/pki/ca-trust/source/anchors/

   sudo update-ca-trust
   ```

Configuration des règles de traitement des domaines de phishing

Lors des campagnes anti-phishing, les utilisateurs recevront des emails contenant des liens vers un portail local de phishing, et la plateforme suivra les mouvements des utilisateurs vers ce portail. Pour rendre cette session de formation aussi crédible que possible, les domaines de phishing doivent être enregistrés sur le serveur DNS de votre organisation, et des certificats doivent être émis :

1. Sur le serveur DNS de votre organisation, créez une stratégie pour les machines des utilisateurs, selon laquelle les enregistrements A pour les domaines listés ci-dessous seront réglés sur une adresse locale liée à l'adresse IP sur laquelle vous voulez déployer la plateforme ASAP On-Premise.
2. Émettez un certificat SSL pour le domaine kasperskygroup.com, avec une liste de noms alternatifs de sujet (SAN) pour les domaines de phishing listés ci-dessous.

Si, pour une raison quelconque, il vous est impossible d'émettre un tel certificat partagé dans votre organisation, il convient d'émettre un certificat distinct pour chaque domaine et de placer ces certificats sur le serveur de la plateforme dans le répertoire phishing_certificates. De plus, lors du déploiement de la plateforme (voir la section « Installation de la plateforme », page 13), vous devrez répondre `non` lorsque l'assistant d'installation vous demandera si un certificat partagé est disponible pour les domaines du portail de phishing.

Liste des domaines de phishing :

- accommodationstravel.com
- avviso-archiviazione.it
- bestjobs.solutions
- blockchain-info.live
- business-information.me
- business-information.store
- corp-email.info
- correo-interno.es
- courrier-interne.fr
- delivery-post.me
- docs-edit.online
- e-calendario.es
- ecalendar.ws
- events-calendar.site
- events-calendar.today
- free-clinics.co
- google-calendar.com
- install-soft.me
- internal-mail.com
- interne-mail.de
- justmailweb.com
- kasperskygroup.com
- kreditbezahlen.de
- lkea.enligne
- marketingservice.today
- medcenter.world
- medical-help.social
- mydeliverypost.com

- official-inbox.com
- official-law.site
- parties.agency
- paybill.email
- posta-interna.it
- postelivraison.fr
- postoffice.one
- share-to.me
- shop-delivery.store
- soft-exchange.com
- state-official.info
- stop-covid.center
- storagealert.work
- taxpay365.com
- thedeliverypost.com
- top-programme.de
- vosmarchandises.fr

Configurer l'accès au serveur de messagerie SMTP

1. Assurez-vous que le serveur de messagerie SMTP est disponible sur le port 587.

   Les connexions au serveur de messagerie sont chiffrées à l'aide du protocole STARTTLS, et il est recommandé d'utiliser le protocole TLS 1.2 ou une version ultérieure.

2. Pour l'authentification sur le serveur de messagerie, vous pouvez utiliser soit un certificat, soit un identifiant et un mot de passe. Vous pouvez sélectionner la méthode d'authentification lors de l'installation.

   Pour l'authentification par certificat, il convient d'abord de configurer le serveur de messagerie en conséquence et de préparer un certificat au format CRT et une clé privée au format KEY.

Vérifier que le serveur dispose d'une connectivité réseau

1. Ouvrez les ports 80, 443, 22 et 587 sur le serveur sur lequel vous souhaitez installer la plateforme.
2. Assurez-vous que le port 22 est utilisé pour une connexion SSH au serveur.

   Lors de l'installation de la plateforme, tous les ports à l'exception des ports 80, 443, 22 et 587 sont fermés, et si une connexion SSH est configurée pour un autre port, elle sera interrompue.

kaspersky

Installation d'ASAP On-Premise

Dans cette section

Installation de la plateforme

► *Pour installer la plateforme ASAP On-Premise, procédez comme suit :*

1. Assurez-vous d'avoir terminé la préparation de l'installation (page 10) et vérifiez que le serveur sur lequel vous souhaitez déployer la plateforme répond à la configuration matérielle et logicielle requise (voir la section « Configuration matérielle et logicielle requise », page 4).
2. Copiez le contenu de l'archive dans le kit de distribution (voir la section « Kit de distribution », page 4) vers le répertoire du serveur sur lequel vous souhaitez déployer la plateforme ASAP On-Premise, puis accédez à ce répertoire.

   > Si vous souhaitez installer la formation en kazakh, définissez la valeur de la variable `CUSTOM_EDUCATION_TOKEN` sur `kz` dans le fichier Helm/.system_env.

3. Exécutez le script install.sh en tant qu'utilisateur doté des privilèges root à l'aide de la commande « install » ou « --install ».

   Exemple de commande : `sudo ./install.sh --install`

   > Afin d'éviter que l'installation ne soit interrompue en cas de fermeture de la session, il est conseillé d'exécuter le script dans un multiplexeur de terminaux tmux ou screen. Par exemple, vous pouvez créer un terminal à l'aide de la commande `sudo tmux new -s kasap`.

   Le script d'installation démarrera. Au cours du processus d'installation, vous devrez répondre aux questions du script ou fournir les données nécessaires à son exécution :

   - **Acceptez-vous les conditions du Contrat de licence utilisateur final (CLUF) ?** (voir la section « À propos du Contrat de licence utilisateur final », page 7) : répondez `oui` si vous acceptez le Contrat de licence utilisateur final.

     Si vous n'acceptez pas le Contrat de licence utilisateur final, répondez `non`. Dans ce cas, le déploiement de la plateforme sera interrompu.

   - **Saisir le domaine sans le '*'** : indiquez le domaine sur lequel vous souhaitez déployer la plateforme ASAP On-Premise.

     Exemple : `kasap-domain.com`

- **Saisir le chemin d'accès au certificat SSL** : indiquez le chemin d'accès au certificat SSL pour le domaine sur lequel la plateforme ASAP On-Premise sera déployée. Le certificat doit être au format CRT.

  Exemple : `certificate/qa-onprem.crt`

- **Saisir le chemin d'accès à la clé SSL** : indiquez le chemin d'accès à la clé du certificat sélectionné à l'étape précédente des instructions.

  Exemple : `certificate/qa-onprem.key`

- **Saisir le chemin d'accès au certificat racine pour le domaine <Domain name>** : indiquez le chemin d'accès au certificat racine pour le domaine sur lequel vous souhaitez déployer ASAP On-Premise. Le certificat doit être au format CRT.

  Exemple : `kasap-domain.com: certificate/root-ca.crt`

- **Saisir une liste de codes de langue séparés par des virgules pour les langues à installer** : indiquez la liste des localisations de la formation qui doivent être installées. Si vous n'entrez pas de codes de langue, la valeur par défaut (« `en,ru` ») est utilisée et les formations en anglais et en russe sont installées.

  Exemple : `en,de,fr`

  Langues disponibles et codes correspondants :

  - English - en
  - Bosanski - bs
  - Català - ca
  - Čeština - cs
  - Dansk - da
  - Deutsch - de
  - Ελληνικά - el
  - Español (España) - es
  - Español (México) - mx
  - Français - fr
  - Hrvatski - hr
  - Italiano - it
  - Қазақша - kk
  - Magyar - hu
  - Nederlands - nl
  - Polski - pl
  - Português (Brasil) - br
  - Português (Portugal) - pt
  - Română - ro
  - Русский - ru
  - Slovenski - sk

- Srpski - sr
- Svenska - sv
- Türkçe - tr
- العربية - ar
- 日本語 - ja
- 漢語 - zh

- **Vous possédez un certificat de phishing** : (Possédez-vous un certificat partagé pour le portail de phishing ?)
  - répondez `oui` si vous avez réussi à configurer un certificat partagé pour le portail de phishing et tous ses domaines. Si vous sélectionnez cette option, vous devrez également indiquer le chemin d'accès et la clé du certificat SSL pour le portail de phishing :
    - **Saisir le chemin d'accès au certificat SSL de phishing** : indiquez le chemin d'accès au certificat SSL partagé pour les domaines de phishing. Le certificat doit être au format CRT.

    Exemple : `certificate/phishing.crt`

    - **Saisir le chemin d'accès à la clé SSL de phishing** : indiquez le chemin d'accès à la clé du certificat SSL partagé pour les domaines de phishing.

    Exemple : `certificate/phishing.key`
  - Répondez `non` si vous ne pouvez pas configurer de certificat partagé pour le portail de phishing et si vous devez créer des certificats pour chaque domaine distinct. Si vous sélectionnez cette réponse, assurez-vous que les certificats du portail de phishing pour chaque domaine sont placés dans le répertoire phishing_certificates (voir la section « Préparation de l'installation », page 10).
- **Saisir le nom d'utilisateur pour 'MINIO_LOGIN'** : indiquez le nom sous lequel vous souhaitez pouvoir vous connecter au service MinIO déployé à l'adresse minio-console.%domain_name%.
- **Saisir le mot de passe pour 'MINIO_PASS'** : indiquez le mot de passe pour vous connecter au service MinIO. Le mot de passe doit comporter au moins 8 caractères et contenir au moins une lettre et un chiffre.
- **Saisir le nom d'utilisateur pour 'S3_LOGIN'** : indiquez le nom d'utilisateur pour l'API MinIO à laquelle la plateforme accédera.
- **Saisir le mot de passe pour 'S3_PASS'** : indiquez le mot de passe pour le service API MinIO. Le mot de passe doit comporter au moins 8 caractères et contenir au moins une lettre et un chiffre.
- **Saisir le nom d'utilisateur pour 'MONGO_LOGIN'** : indiquez le nom d'utilisateur pour le service MongoDB.
- **Saisir le mot de passe pour 'MONGO_PASS'** : indiquez le mot de passe pour le service MongoDB. Le mot de passe doit comporter au moins 8 caractères et contenir au moins une lettre et un chiffre.
- **Saisir le nom d'utilisateur pour 'DOCKER_REGISTRY_LOGIN'** : indiquez le nom d'utilisateur pour le service de stockage des images Docker.
- **Saisir le mot de passe pour 'DOCKER_REGISTRY_PASS'** : indiquez le mot de passe pour le service de stockage des images Docker. Le mot de passe doit comporter au moins 8 caractères et contenir au moins une lettre et un chiffre.
- **Saisir l'hôte pour 'SMTP_HOST'** : indiquez le serveur de messagerie de votre organisation.

  Exemple : `mail.kasap-domain.fr`

- **Saisir EMAIL_NOREPLAY pour la vérification** : indiquez l'adresse email à partir de laquelle les notifications ASAP seront envoyées. Les emails envoyés à cette adresse ne seront pas acceptés.

  Exemple : `no-reply@kasap-domain.fr`

- Sélectionnez une option de connexion au serveur de messagerie :
  - Saisissez le chiffre `1` si vous souhaitez utiliser votre identifiant et votre mot de passe pour vous connecter. En sélectionnant cette option, vous devrez également indiquer un identifiant et un mot de passe pour vous connecter au serveur de messagerie :
    - **Saisir SMTP_LOGIN pour la vérification** : indiquez l'adresse email pour l'authentification auprès du serveur de messagerie.

      Exemple : `k3s@kasap-domain.fr`

    - **Saisir le mot de passe pour 'SMTP_PASS'** : indiquez le mot de passe pour l'authentification sur le serveur de messagerie.
  - Saisissez le chiffre `2` si vous souhaitez utiliser un certificat pour vous connecter au serveur de messagerie. Lors de la sélection de cette option, vous devrez également indiquer le chemin d'accès au certificat au format CRT et le chemin d'accès à la clé au format KEY :
    - **Saisir le chemin d'accès au certificat SSL pour le SMTP-relay** : indiquez le chemin d'accès au certificat SSL pour le serveur de messagerie. Le certificat doit être au format CRT.

      Exemple : `certificate/email.crt`

    - **Saisir le chemin d'accès à la clé SSL pour le SMTP-relay** : indiquez le chemin d'accès à la clé du certificat SSL pour le serveur de messagerie.

      Exemple : `certificate/email.key`

Cette action lancera l'installation d'ASAP On-Premise, qui impliquera un cluster k3s avec tout le contenu et les services nécessaires au bon fonctionnement de la plateforme.

kaspersky

Résultat de l'installation

Une fois l'installation terminée, les services suivants seront créés :

- **Erreur ! La référence du lien hypertexte n'est pas valide.** (par exemple : `https://asap-api.kasap-domain.fr`) : utilisé pour intégrer la plateforme à d'autres solutions via l'API.
- https://app.<domain>.<region> (par exemple : `https://app.kasap-domain.fr`) : utilisé pour se connecter à l'interface Web de la plateforme.
- https://*.<domain>.<region>, par exemple : `https://*.kasap-domain.fr`
- https://cdn.<domain>.<region>, par exemple : `https://cdn.kasap-domain.fr`
- https://test-player.<domain>.<region>, par exemple : `https://test-player.kasap-domain.fr`
- https://minio.<domain>.<region>, par exemple : `https://minio.kasap-domain.fr`
- https://minio-console.<domain>.<region>, par exemple : `https://minio-console.kasap-domain.fr`
- https://asap-cdn.minio.<domain>.<region>, par exemple : `https://asap-cdn.minio.kasap-domain.fr`

Vérification du résultat de l'installation

► *Pour vérifier que la plateforme ASAP On-Premise est correctement installée, procédez comme suit :*

- Accédez à l'URL de connexion de la plateforme (utilisez une URL au format https://app.<domain>.<region>, par exemple `https://app.kasap-domain.fr`) et vérifiez que l'application est disponible : la fenêtre de connexion devrait s'afficher et vous inviter à saisir votre identifiant et votre mot de passe.
- Accédez à l'un des domaines de phishing précédemment configurés et assurez-vous qu'une page 404 s'affiche pour celui-ci (il s'agit d'un comportement normal). De plus, dans le navigateur, dans les paramètres de connexion de la page, dans la section Réseau, assurez-vous que la réponse à la requête /server-list.json contient l'URL au format https://asap-api.<domain>.<region>.

Si ces deux conditions sont remplies, l'installation est conforme.

► *Pour vérifier le fonctionnement de la plateforme ASAP On-Premise, l'administrateur de la plateforme doit :*

1. Accéder à l'URL de connexion de la plateforme (utilisez une URL au format https://app.<domain>.<region>, par exemple `https://app.kasap-domain.fr`).

   La fenêtre de connexion à la plateforme s'ouvre.
2. Cliquer sur le lien **S'inscrire** et terminer le processus d'enregistrement en indiquant son adresse email et son mot de passe.
3. Attendre de recevoir l'email de confirmation de l'enregistrement, puis cliquer sur le lien.

   Une fois l'enregistrement terminé, la page avec le panneau de configuration devrait s'afficher.
4. Accéder à la page **Contenus**, ouvrir n'importe quel cours dans la section **Cours** et s'assurer que le lecteur de test affiche le contenu.

Si toutes les étapes ont pu être finalisées, la plateforme a été correctement installée.

Suppression d'ASAP On-Premise

► *Pour supprimer la plateforme ASAP On-Premise, procédez comme suit :*

1. En tant qu'utilisateur doté des privilèges root, vous devez vous rendre dans le répertoire où le kit de distribution a été copié et décompressé lors de l'installation de la plateforme.
2. Exécutez le script install.sh à l'aide de la commande « uninstall » ou « --uninstall ».

   Exemple : `sudo ./install.sh --uninstall`

L'exécution du script supprimera le cluster k3s sur lequel la plateforme a été installée. Le répertoire de la plateforme, le kit de distribution et les fichiers log doivent être supprimés manuellement.

kaspersky

Mise à jour de la plateforme

Dans cette section

Mise à jour de la version de la plateforme

► *Pour mettre à niveau la plateforme ASAP On-Premise vers la version suivante, procédez comme suit :*

1. Sur le serveur de la plateforme, placez l'image que vous souhaitez utiliser pour mettre à jour la plateforme dans le répertoire kasap_images.
2. Copiez le contenu de l'archive dans le kit de distribution (voir la section « Kit de distribution », page 4) vers le répertoire du serveur sur lequel vous souhaitez déployer la plateforme ASAP On-Premise, puis accédez à ce répertoire.
3. Exécutez le script install.sh en tant qu'utilisateur doté des privilèges root à l'aide de la commande « update » ou « --update ». La procédure de mise à jour d'ASAP On-Premise est semblable à la procédure d'installation (voir la section « Installation d'ASAP On-Premise », page 13).

   Exemple de commande : `sudo ./install.sh --update`
4. Si nécessaire, spécifiez de nouveaux certificats lors de l'installation.

La plateforme sera mise à jour vers la version suivante.

Mise à jour des certificats SSL

Si nécessaire, vous pouvez mettre à jour les certificats SSL utilisés lors de l'installation de la plateforme. Pour ce faire, il convient de lancer la procédure de mise à jour de la plateforme à l'aide de l'image qui a été utilisée pour la première installation de la plateforme. Dans ce cas, les nouveaux certificats doivent être spécifiés lors de l'installation.

► *Pour mettre à jour les certificats SSL pour une plateforme ASAP On-Premise déjà installée, procédez comme suit :*

1. Sur le serveur de la plateforme, placez l'image que vous souhaitez utiliser pour mettre à jour la plateforme dans le répertoire kasap_images.

   Assurez-vous que la version de l'image d'installation d'ASAP On-Premise correspond à la version de la plateforme ASAP On-Premise qui est installée dans votre organisation. Si les versions sont différentes, toutes les données des utilisateurs et tous les résultats d'apprentissage sont perdus pendant la mise à niveau.

2. Copiez le contenu de l'archive dans le kit de distribution (voir la section « Kit de distribution », page 4) dans le répertoire du serveur sur lequel vous souhaitez déployer la plateforme ASAP On-Premise, puis accédez à ce répertoire.

   Dans ce cas, vous devez utiliser le kit de distribution qui a été utilisé pour installer ASAP On-Premise dans votre organisation.

3. Exécutez le script install.sh en tant qu'utilisateur doté des privilèges root à l'aide de la commande « update » ou « --update ». La procédure de mise à jour d'ASAP On-Premise est semblable à la procédure d'installation (voir la section « Installation d'ASAP On-Premise », page 13).

   Exemple de commande : `sudo ./install.sh --update`

4. Spécifiez les nouveaux certificats lors de l'installation.

Les certificats SSL de la plateforme seront mis à jour.

kaspersky

À propos de la copie de sauvegarde

Cette section décrit l'utilisation des copies de sauvegarde de la plateforme ASAP On-Premise, c'est-à-dire leur création et leur déploiement.

Dans cette section

Création d'une copie de sauvegarde

► *Pour créer une copie de sauvegarde des modules de la plateforme, procédez comme suit :*

1. Décompressez l'archive du kit de distribution de la plateforme et accédez au dossier avec son contenu.
2. À l'aide du script backup.sh, créez une copie de sauvegarde du module requis :
   - Exécutez `sudo ./backup.sh --backup full` si vous souhaitez créer une copie de sauvegarde de MongoDB et MinIO.
   - Exécutez `sudo ./backup.sh --backup mongo` si vous souhaitez créer une copie de sauvegarde de MongoDB.
   - Exécutez `sudo ./backup.sh --backup minio` si vous souhaitez créer une copie de sauvegarde de MinIO.
3. Saisissez votre identifiant et votre mot de passe (voir la section « Installation d'ASAP On-Premise », page 13) pour accéder aux modules que vous souhaitez sauvegarder.

Les modules sélectionnés seront sauvegardés.

kaspersky

Déploiement à partir d'une copie de sauvegarde

► *Pour déployer un module à partir d'une copie de sauvegarde créée précédemment, procédez comme suit :*

1. Décompressez l'archive du kit de distribution de la plateforme et accédez au dossier avec son contenu.
2. Utilisez le script backup.sh pour déployer les modules à partir des copies de sauvegarde créées précédemment :
   - Exécutez `sudo ./backup.sh --restore full` si vous souhaitez déployer MongoDB et MinIO.
   - Exécutez `sudo ./backup.sh --restore mongo` si vous souhaitez déployer MongoDB.
   - Exécutez `sudo ./backup.sh --restore minio` si vous souhaitez déployer MinIO.
3. Saisissez votre identifiant et votre mot de passe (voir la section « Installation d'ASAP On-Premise », page 13) pour accéder aux modules que vous souhaitez déployer.

Les modules sont déployés à partir des copies de sauvegarde.

Sources d'informations sur l'application

La page Kaspersky Automated Security Awareness Platform sur le site Web de Kaspersky

Sur la page Kaspersky Automated Security Awareness Platform (https://www.kaspersky.fr/small-to-medium-business-security/security-awareness-platform), vous pouvez consulter des informations générales sur l'application, son fonctionnement et ses fonctionnalités.

La page Kaspersky Automated Security Awareness Platform contient un lien vers la boutique en ligne. C'est ici que vous pouvez acheter ou renouveler l'application.

Discussions concernant les applications Kaspersky sur le Forum

Si votre question ne nécessite pas de réponse immédiate, vous pouvez en discuter avec les experts de Kaspersky et d'autres utilisateurs de notre Forum (https://forum.kaspersky.com/forum/pour-particuliers-66/).

Ici, vous pouvez afficher les sujets existants, laisser vos commentaires ou créer de nouveaux sujets.

kaspersky

Description des scripts d'installation

L'archive dans le kit de distribution comprend les scripts suivants :

- logs.sh : utilisé pour créer manuellement des logs (voir la section « À propos du traitement des données », page 9) de tous les Pods déployés dans le cluster k3s. Ce script doit être exécuté en tant qu'utilisateur avec les privilèges root. Le script démarre sans commandes supplémentaires.

  Exemple d'utilisation : `sudo ./logs.sh`

  > Lors de la suppression de la plateforme (voir la section « Suppression d'ASAP On-Premise », page 19), les logs doivent être supprimés manuellement.

- install.sh : utilisé pour l'installation (voir la section « Installation d'ASAP On-Premise », page 13), la suppression (voir la section « Suppression d'ASAP On-Premise », page 19) et la mise à jour (voir la section « Mise à jour de la plateforme », page 20) des composants du cluster et de la plateforme. Ce script doit être exécuté en tant qu'utilisateur avec les privilèges root.

  Commandes disponibles :

  - install ou --install : utilisé pour installer les modules du cluster et de la plateforme.

    Paramètres disponibles :

    - fullcontent ou exécution de la commande sans aucun paramètre : si ce paramètre est spécifié, l'installation des modules du cluster et de la plateforme commencera, et l'intégralité du contenu des cours de formation pour toutes les langues sélectionnées sera chargé sur le S3 MinIO.
    - minicontent : si ce paramètre est spécifié, l'installation des modules du cluster et de la plateforme commencera, et seules les formations express en russe seront chargées sur le S3 MinIO. Cette option d'installation peut être utilisée comme installation de démonstration.
    - nocontent : si ce paramètre est spécifié, l'installation des modules du cluster et de la plateforme commencera, mais le contenu des cours de formation ne sera pas chargé sur le S3 MinIO. Cette option d'installation permet de vérifier qu'il est en principe possible de déployer la plateforme sur le serveur et dans l'environnement réseau sélectionnés.
  - uninstall ou --uninstall : utilisé pour supprimer les modules du cluster et de la plateforme.
  - update ou --update : utilisé pour mettre à jour les modules de la plateforme.
  - help ou --help : utilisé pour obtenir de l'aide sur l'exécution du script.

  Exemples d'utilisation :

  - `sudo ./install.sh --install fullcontent` ou `sudo ./install.sh --install` : commande pour un déploiement complet de la plateforme ;
  - `sudo ./install.sh --install minicontent` : commande pour un déploiement de démonstration de la plateforme ;
  - `sudo ./install.sh --update` : commande pour le lancement de la mise à jour des modules de la plateforme ;
  - `sudo ./install.sh --update` ou `sudo ./install.sh` : commande pour l'obtention d'aide sur l'exécution du script.

- backup.sh : utilisé pour créer une copie de sauvegarde des modules du cluster et de la plateforme (voir la section « Création d'une copie de sauvegarde », page 22) et pour déployer la plateforme à partir d'une copie de sauvegarde (voir la section « Déploiement à partir d'une copie de sauvegarde », page22).
  Ce script doit être exécuté en tant qu'utilisateur avec les privilèges root.

  Commandes disponibles :

  - backup ou --backup : utilisé pour créer une copie de sauvegarde du cluster de la plateforme et de ses modules.

    Paramètres disponibles :

    - full : spécifiez ce paramètre pour créer des copies de sauvegarde de la base de données MongoDB et du cluster MinIO S3.
    - mongo : spécifiez cette option pour créer une copie de sauvegarde de la base de données MongoDB.
    - minio : spécifiez ce paramètre pour créer une copie de sauvegarde du cluster MinIO S3.
  - restore ou --restore : utilisé pour déployer un cluster de la plateforme et ses modules à partir d'une copie de sauvegarde.

    Paramètres disponibles :

    - full : si ce paramètre est spécifié, la base de données MongoDB et le cluster MinIO S3 seront déployés à partir d'une copie de sauvegarde.
    - mongo : spécifiez ce paramètre pour déployer également la base de données MongoDB à partir d'une copie de sauvegarde.
    - minio : spécifiez ce paramètre pour déployer le cluster MinIO S3 à partir d'une copie de sauvegarde.

  Exemples d'utilisation :

  - `sudo ./backup.sh --backup full` : commande pour créer une copie de sauvegarde des modules du cluster et de la plateforme ;
  - `sudo ./backup.sh --backup mongo` : commande pour créer une copie de sauvegarde de la base de données MongoDB ;
  - `sudo ./backup.sh --restore minio` : commande pour déployer un cluster à partir d'une copie de sauvegarde.

Informations sur les codes tiers

Les informations sur le code tiers sont contenues dans le fichier LEGAL_NOTICES situé dans le répertoire /opt/kaspersky/ASAP/LEGAL_NOTICES.

Avis relatif aux marques de commerce

Les marques déposées et les marques de service appartiennent à leurs propriétaires respectifs.

AMD est une marque ou une marque déposée d'Advanced Micro Devices, Inc.

Apple, Mac, Mac OS, macOS et Safari sont des marques d'Apple Inc.

iOS est une marque de Cisco Systems, Inc. déposée aux Etats-Unis et aux autres pays, et/ou ses compagnies affiliées.

Docker et le logo Docker sont des marques de commerce ou des marques déposées de Docker, Inc. aux États-Unis et/ou dans d'autres pays. Docker, Inc. et d'autres parties peuvent également avoir des droits sur des marques de commerce décrites par d'autres conditions utilisées dans ce document.

Google, Android, Gmail, Google Apps et Google Chrome sont des marques de Google LLC.

Intel est une marque d'Intel Corporation aux États-Unis et/ou dans d'autres pays.

Linux est la marque de Linus Torvalds aux États-Unis et dans d'autres pays.

Microsoft, Internet Explorer, Microsoft Edge, Office 365, Outlook et Windows sont des marques de commerce de Microsoft Corporation.

Mozilla et Firefox sont des marques de Mozilla Foundation aux États-Unis et dans d'autres pays.

Helm est une marque déposée de Linux Foundation aux États-Unis et dans d'autres pays.