

# **Serveur de surveillance UXP 2.10**

**Guide d'installation et de configuration**

UXP-IG-MS

# Table des matières

---

|  |           |
|--|-----------|
| <b>Notes de mise à jour de la dernière version du Serveur de surveillance UXP</b>  | <b>1</b>  |
| <b>1. Introduction</b>   | <b>2</b>  |
| 1.1. Vue d'ensemble  | 2         |
| 1.2. Public cible  | 2         |
| 1.3. Références  | 2         |
| 1.4. Surveillance des serveurs de sécurité   | 4         |
| 1.5. Surveillance des serveurs de registre   | 6         |
| 1.6. Aperçu de la procédure de configuration                                       | 7         |
| <b>2. Configuration du client de surveillance centralisé</b>                       | <b>9</b>  |
| 2.1. Configuration du client de surveillance centralisé sur le Serveur de registre | 9         |
| <b>3. Installer le serveur de surveillance</b>                                     | <b>11</b> |
| 3.1. Configuration requise   | 11        |
| 3.2. Informations requises   | 13        |
| 3.3. Installer les paquets Serveur de surveillance UXP                             | 13        |
| 3.4. Installer la licence  | 14        |
| 3.5. Ajouter une ancre de configuration au Serveur de surveillance                 | 14        |
| 3.6. Connecter le serveur de surveillance au serveur de sécurité du client         | 15        |
| 3.6.1. Configurer la connexion sur le serveur de surveillance                      | 15        |
| 3.6.2. Configurer la connexion sur le Serveur de sécurité                          | 17        |
| 3.7. Vérifications après l'installation  | 17        |
| <b>4. Accorder l'accès aux données de surveillance du serveur de registre</b>      | <b>18</b> |
| <b>5. Configurer Zabbix</b>  | <b>19</b> |
| 5.1. Installer Zabbix  | 19        |
| 5.1.1. Installer un serveur Zabbix unique  | 20        |
| 5.1.2. Installer Zabbix dans une configuration HA native                           | 23        |
| Installer le serveur de base de données  | 23        |
| Installer un nœud du serveur Zabbix  | 24        |
| 5.2. Connecter Zabbix au Serveur de surveillance                                   | 27        |
| 5.3. Configurer l'API de configuration Zabbix                                      | 28        |
| 5.4. Configurer les hôtes surveillés sur Zabbix                                    | 31        |
| 5.4.1. Modèle Zabbix : Serveur de sécurité UXP par MS                              | 33        |

|   |           |
|---|-----------|
| 5.4.2. Modèle Zabbix : Serveur de registre UXP par MS .....   | 36        |
| 5.5. Configurer l'agent Zabbix sur les Serveurs de registre .....   | 37        |
| 5.5.1. Installer et configurer l'agent Zabbix .....   | 37        |
| <b>6. Configurer Elasticsearch et Kibana .....</b>  | <b>39</b> |
| 6.1. Document de données opérationnelles dans Elasticsearch .....   | 39        |
| 6.2. Document sur les statistiques des données opérationnelles dans Elasticsearch.....                              | 42        |
| 6.3. Installer Elasticsearch et Kibana .....  | 42        |
| 6.3.1. Chiffrement du trafic entre le navigateur Web et Kibana .....  | 46        |
| 6.3.2. Installer une grappe Elasticsearch à plusieurs nœuds .....   | 47        |
| 6.4. Connecter Elasticsearch au Serveur de surveillance .....   | 49        |
| 6.4.1. Créer un utilisateur Elasticsearch pour le serveur de surveillance .....                                     | 50        |
| 6.4.2. Configuration du serveur de surveillance .....   | 51        |
| 6.4.3. Utiliser une grappe Elasticsearch à plusieurs nœuds.....   | 55        |
| 6.5. Configurer Kibana pour l'analyse.....  | 56        |
| 6.5.1. Créer une vue de données pour les données opérationnelles / statistiques de<br>données opérationnelles ..... | 56        |
| 6.5.2. Exemple de tableaux de bord .....  | 57        |
| 6.5.3. Autres exemples de visualisation.....  | 58        |
| <b>7. Notifications par e-mail .....</b>  | <b>60</b> |
| <b>8. Haute disponibilité du serveur de surveillance .....</b>  | <b>61</b> |
| 8.1. Ajouter un nœud de serveur de surveillance supplémentaire .....  | 62        |
| 8.2. Supprimer un nœud de serveur de surveillance .....   | 63        |
| 8.3. Changer l'adresse d'un nœud de serveur de surveillance .....   | 64        |
| <b>9. Maintenance .....</b>   | <b>66</b> |
| 9.1. Remplacement des certificats TLS .....   | 66        |
| 9.1.1. Générer un nouveau certificat TLS pour le serveur de surveillance.....                                       | 67        |
| 9.1.2. Générer un nouveau certificat TLS pour le serveur Elasticsearch.....   | 67        |
| 9.2. Changer les intervalles d'interrogation des données de surveillance .....                                      | 68        |
| 9.3. Activer/désactiver la collecte de données de surveillance opérationnelle ou de ses<br>statistiques .....       | 68        |
| 9.4. Changer la période statistique des données de surveillance opérationnelle .....                                | 69        |
| 9.5. Gérer l'inclusion/exclusion des données et statistiques de surveillance opérationnelle ..                      | 69        |
| 9.6. Changer le ou les destinataires des notifications par e-mail .....   | 70        |
| 9.7. Changer le nom de la grappe de serveurs de surveillance .....  | 70        |

|   |           |
|---|-----------|
| 9.8. Configurer la grappe Zabbix .....  | 70        |
| 9.8.1. Ajouter un nœud Zabbix supplémentaire .....                                  | 70        |
| 9.8.2. Supprimer un nœud Zabbix .....   | 70        |
| 9.8.3. Désactiver la grappe HA .....  | 72        |
| 9.8.4. Changer l'adresse d'un nœud Zabbix .....                                     | 72        |
| 9.9. Configurer la grappe Elasticsearch .....                                       | 73        |
| 9.9.1. Ajouter un nœud Elasticsearch supplémentaire .....                           | 73        |
| 9.9.2. Supprimer un nœud Elasticsearch .....  | 74        |
| 9.9.3. Changer l'adresse d'un nœud Elasticsearch .....                              | 76        |
| <b>10. Dépannage .....</b>  | <b>79</b> |
| 10.1. Fichiers journaux .....   | 79        |
| 10.1.1. Configuration des paramètres de journalisation des composants .....         | 79        |
| 10.2. Recharger le serveur de surveillance .....                                    | 80        |
| 10.3. Changer la configuration des agents de surveillance .....                     | 80        |
| 10.4. Vérification de l'envoi des e-mails .....                                     | 80        |
| 10.5. La configuration du serveur Zabbix n'est pas valide .....                     | 81        |
| 10.6. Spam dans les journaux Zabbix : Le prétraitement a échoué pour .....          | 81        |
| 10.7. Identifier le nœud maître du serveur de surveillance pour Zabbix .....        | 81        |
| 10.8. Identifier le nœud maître du serveur de surveillance pour Elasticsearch ..... | 82        |
| <b>11. Migration .....</b>  | <b>83</b> |
| 11.1. Migration de la version 2.9 à la version 2.10 .....                           | 83        |
| 11.2. Migration de la version 2.7 à la version 2.9 .....                            | 83        |
| 11.3. Migration vers la version 2.7 .....   | 86        |
| <b>Annexe A: Notes de mise à jour du Serveur de surveillance UXP .....</b>          | <b>87</b> |

# Notes de mise à jour de la dernière version du Serveur de surveillance UXP

---

## 2.10.0 (11.2025)

- Les versions 9.x d'Elasticsearch et de Kibana sont désormais prises en charge.
- La prise en charge d'Elasticsearch et de Kibana 7.x a été entièrement supprimée.
- La propriété système `opdata-stats-period-seconds` dans `monitoring-server.ini` applique désormais des règles de validation plus strictes.
- Un nouveau paramètre de configuration, `enable_update_existing_triggers`, a été ajouté à `monitor-agent.ini`. Cela permet d'activer ou de désactiver les mises à jour des déclencheurs existants dans les modèles Zabbix UXP, ce qui permet d'éviter les écrasements involontaires.
- Le déclencheur Zabbix `Global configuration is expiring` s'active désormais 24 heures avant l'expiration de la configuration.
- Java Runtime Environment est mis à jour vers la version 21. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Diverses corrections et améliorations mineures ont été apportées.

Pour toutes les notes de mise à jour du Serveur de surveillance UXP, voir l'[Annexe](#).

# 1. Introduction

---

## 1.1. Vue d'ensemble

Ce guide décrit les tâches liées à l'installation du Serveur de surveillance UXP. En outre, il décrit la configuration qui doit être effectuée pour que le serveur de surveillance collecte et transmette les données de surveillance environnementale des serveurs de sécurité et des serveurs de registre à Zabbix, ainsi que les données de surveillance opérationnelle des serveurs de sécurité au serveur Elasticsearch (ES).

L'installation et la configuration automatique du serveur Zabbix sont décrites dans la section [Configurer Zabbix](#).

Pour visualiser les statistiques des demandes des serveurs de sécurité, reportez-vous à la section [Configurer Elasticsearch et Kibana](#) qui contient des guides d'installation ainsi que des exemples de configuration pour le serveur Elasticsearch et Kibana.

## 1.2. Public cible

Ce guide s'adresse aux administrateurs système responsables de la surveillance d'une instance UXP.

Ce document est destiné aux lecteurs ayant une connaissance moyenne de la gestion des serveurs Linux, des réseaux informatiques et des principes de fonctionnement de la technologie UXP.

Des connaissances de base de la solution de surveillance distribuée Zabbix ainsi que des outils d'analyse de données Elasticsearch et Kibana sont nécessaires. Reportez-vous aux sections correspondantes de la documentation de Zabbix [\[Zabbix\]](#), Elasticsearch et Kibana [\[Elastic\]](#).

## 1.3. Références

- [DATE-TIME-FORMATTER] DateFormatter (Java SE 21 & JDK 21)  
<https://docs.oracle.com/en/java/javase/21/docs/api/java.base/java/time/format/DateTimeFormatter.html>
- [\[Elastic\]](#) Elastic Docs | Elastic,  
<https://www.elastic.co/docs>
- [\[Elastic-Roles\]](#) Rôles des utilisateurs | Guide Elasticsearch,  
<https://www.elastic.co/docs/deploy-manage/users-roles/cluster-or-deployment-auth/user-roles>
- [\[Elastic-Cluster\]](#) Ajouter et supprimer des nœuds Elasticsearch | Guide Elasticsearch,  
<https://www.elastic.co/docs/deploy-manage/maintenance/add-and-remove-elasticsearch-nodes>

- [Elastic-Heap] Configuration des paramètres importants | Guide Elasticsearch, <https://www.elastic.co/docs/deploy-manage/deploy/self-managed/important-settings-configuration#heap-size-settings>
- [Elastic-Security] Fonctionnalités de sécurité de la grappe ou du déploiement | Guide Elasticsearch, <https://www.elastic.co/docs/deploy-manage/security#cluster-or-deployment-security-features>
- [Elastic-Upgrade-9.x] Mise à niveau du déploiement ou de la grappe | Guide Elasticsearch [9.0+], <https://www.elastic.co/docs/deploy-manage/upgrade/deployment-or-cluster>
- [LOGBACK-PATTERNS] Documentation de Logback. Chapitre 6 : Mises en page — Conversion Tableau Word, <https://logback.qos.ch/manual/layouts.html#conversionWord>
- [NGINX] Nginx – Équilibreur de charge haute performance, serveur Web, & Reverse Proxy, <http://nginx.org/>
- [Postfix] La page d'accueil de Postfix, <http://www.postfix.org/>
- [Time-Zones] Liste des fuseaux horaires pris en charge, <http://php.net/manual/en/timezones.php>
- [UXP-PR-MESS] Cybernetica AS. Protocole de message UXP v4.0 : Spécifications techniques. Identifiant du document : UXP-PR-MESS
- [UXP-PR-MON] Cybernetica AS. Protocole de surveillance UXP : Spécifications techniques. Identifiant du document : UXP-PR-MON
- [UXP-SYSPAR-MS] Cybernetica AS. Serveur de surveillance UXP : Paramètres du système. Identifiant du document : UXP-SYSPAR-MS
- [UXP-UG-PMA] Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA
- [UXP-UG-RS] Cybernetica AS. Serveur de registre UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-RS
- [UXP-UG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-SS
- [UXP-UPG-UB22] Cybernetica AS. Mise à jour des serveurs UXP d'Ubuntu 20.04 vers Ubuntu 22.04. Identifiant du document : UXP-UPG-UB22
- [UXP-UPG-UB24] Cybernetica AS. Mise à jour des serveurs UXP d'Ubuntu 22.04 vers Ubuntu 24.04. Identifiant du document : UXP-UPG-UB24
- [Zabbix] Documentation Zabbix, <https://www.zabbix.com/manuals>
- [Zabbix-Frontend] Manuel Zabbix, Installation de l'interface Web, <https://www.zabbix.com/documentation/7.0/en/manual/installation/frontend>
- [Zabbix-HA] Manuel Zabbix, Haute disponibilité,

<https://www.zabbix.com/documentation/7.0/en/manual/concepts/server/ha>

- [Zabbix-Install] Télécharger et installer Zabbix,  
<https://www.zabbix.com/download>
- [Zabbix-Requirements] Manuel Zabbix, Configuration requise  
<https://www.zabbix.com/documentation/7.0/en/manual/installation/requirements#database-size>
- [Zabbix-Upgrade-7.0] Manuel Zabbix, 7 Procédure de mise à niveau,  
<https://www.zabbix.com/documentation/7.0/en/manual/installation/upgrade>

## 1.4. Surveillance des serveurs de sécurité

La solution de surveillance UXP permet d'accéder facilement aux informations suivantes.

### Données de surveillance environnementale

Informations sur l'état du serveur de sécurité. Par exemple, la consommation de mémoire, les versions des paquets, l'utilisation du processeur et les statistiques des demandes réussies et échouées traitées par les serveurs de sécurité.

### Données de surveillance opérationnelle

Informations sur les demandes traitées par le serveur de sécurité. Il s'agit de données telles que l'identifiant de la demande, l'identifiant du client, l'identifiant du service, divers attributs lus à partir de l'en-tête du message SOAP ou des en-têtes HTTP (REST), l'horodatage de la demande et de la réponse, la taille de la demande, etc.

### Statistiques des données de surveillance opérationnelle

Statistiques calculées sur la base des données de surveillance opérationnelle. Les statistiques représentent le nombre total de transactions et le nombre de transactions réussies pour chaque combinaison unique d'identifiant et de type de serveur de sécurité, d'identifiant client et d'identifiant de service pour une période donnée.

La figure 1 présente les composants de la solution de surveillance.



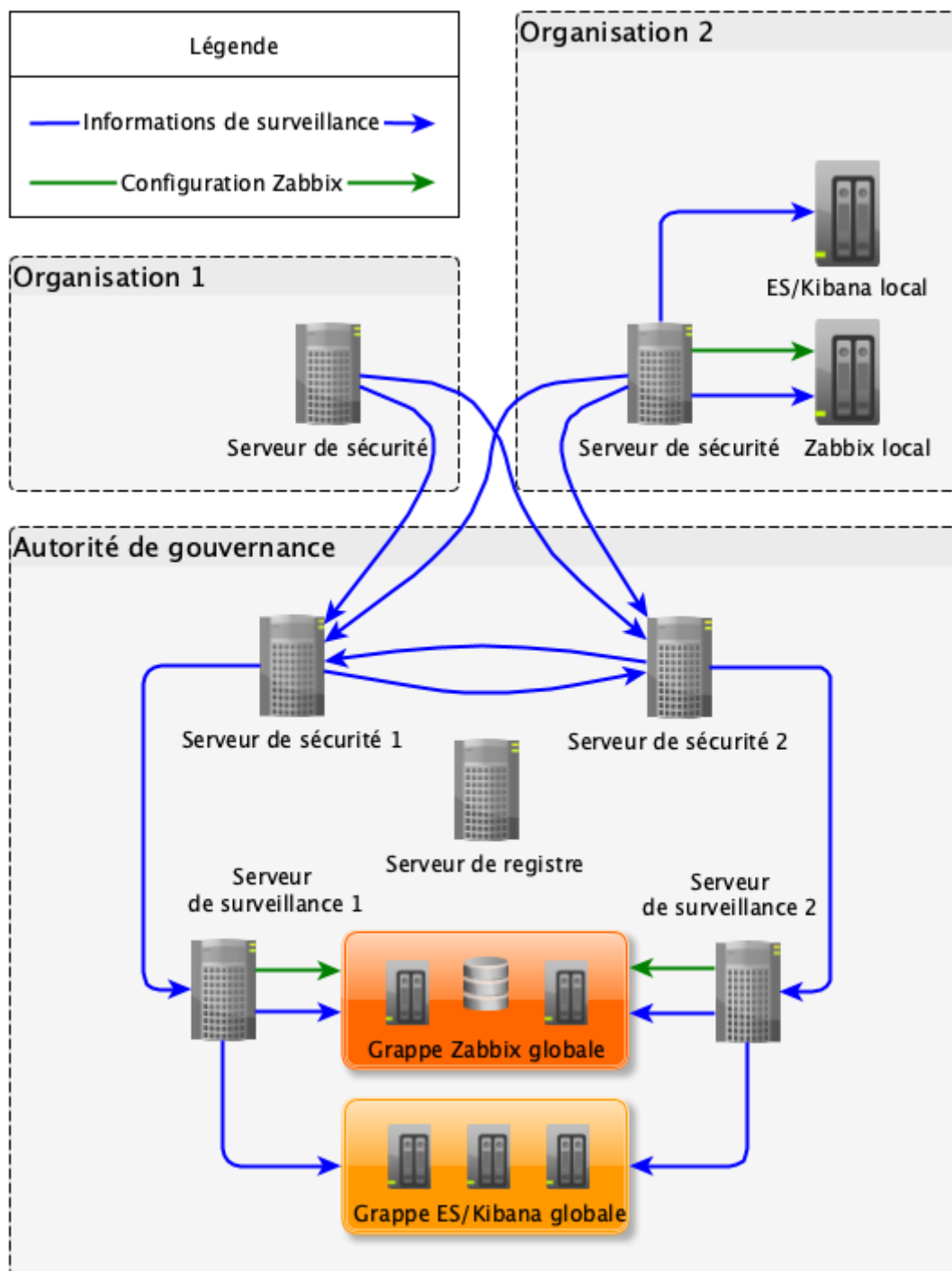


Figure 1. La solution de surveillance des serveurs de sécurité UXP

Dans une instance UXP, la surveillance peut s'effectuer à deux niveaux : organisationnel et central.

1. Au niveau organisationnel (local), un module complémentaire de serveur de sécurité envoie ses informations de surveillance environnementale à Zabbix configuré localement et ses données de surveillance opérationnelle à Elasticsearch configuré localement (flèches bleues correspondantes sur le diagramme).

2. Au niveau central (global), l'administrateur du serveur de registre peut installer un ou plusieurs serveurs de surveillance (grappe) qui collectent les informations provenant des serveurs de sécurité (flèches bleues correspondantes sur le schéma). Le serveur de surveillance utilise son propre serveur de sécurité et le client enregistré (appelé client de surveillance centralisé) qui s'y trouve pour faciliter les demandes de surveillance. Le serveur de surveillance transmet les informations de surveillance environnementale collectées à Zabbix (grappe) et les données de surveillance opérationnelle et leurs statistiques à Elasticsearch (grappe) (flèches bleues correspondantes sur le diagramme).

Les informations relatives au client de surveillance centralisé sont introduites dans le serveur de registre et sont distribuées via la configuration globale à tous les serveurs de sécurité et à tous les serveurs de surveillance.

La communication entre le serveur de sécurité du client de surveillance centralisé et le serveur de surveillance doit être configurée pour utiliser HTTPS. Le serveur de sécurité et le serveur de surveillance utilisent leurs certificats TLS internes, distribués manuellement à l'autre partie, pour s'authentifier l'un l'autre. L'authentification est effectuée tant côté client que côté serveur.

Le module complémentaire du serveur de sécurité et le serveur de surveillance ont tous deux la capacité de configurer automatiquement les entités surveillées dans Zabbix, ce qui élimine la nécessité d'une configuration manuelle (flèches vertes sur le diagramme).

Les services de surveillance sont mis en œuvre sur le serveur de sécurité en tant que services UXP standards. Les spécifications détaillées du protocole de surveillance et du protocole de message UXP figurent dans [\[UXP-PR-MON\]](#) et [\[UXP-PR-MESS\]](#).



Pour plus d'informations sur la configuration de la surveillance locale du serveur de sécurité, voir le guide correspondant [\[UXP-UG-PMA\]](#).

## 1.5. Surveillance des serveurs de registre

La solution de surveillance UXP permet d'accéder facilement aux données suivantes.

### Données de surveillance environnementale

Informations sur l'état du serveur de registre. Par exemple, la consommation de mémoire, l'utilisation du processeur et l'espace disque.

### Données de surveillance UXP

Informations spécifiques à UXP. Par exemple, les données relatives à la configuration globale et à la licence UXP.

La figure 2 présente les composants de la solution de surveillance.

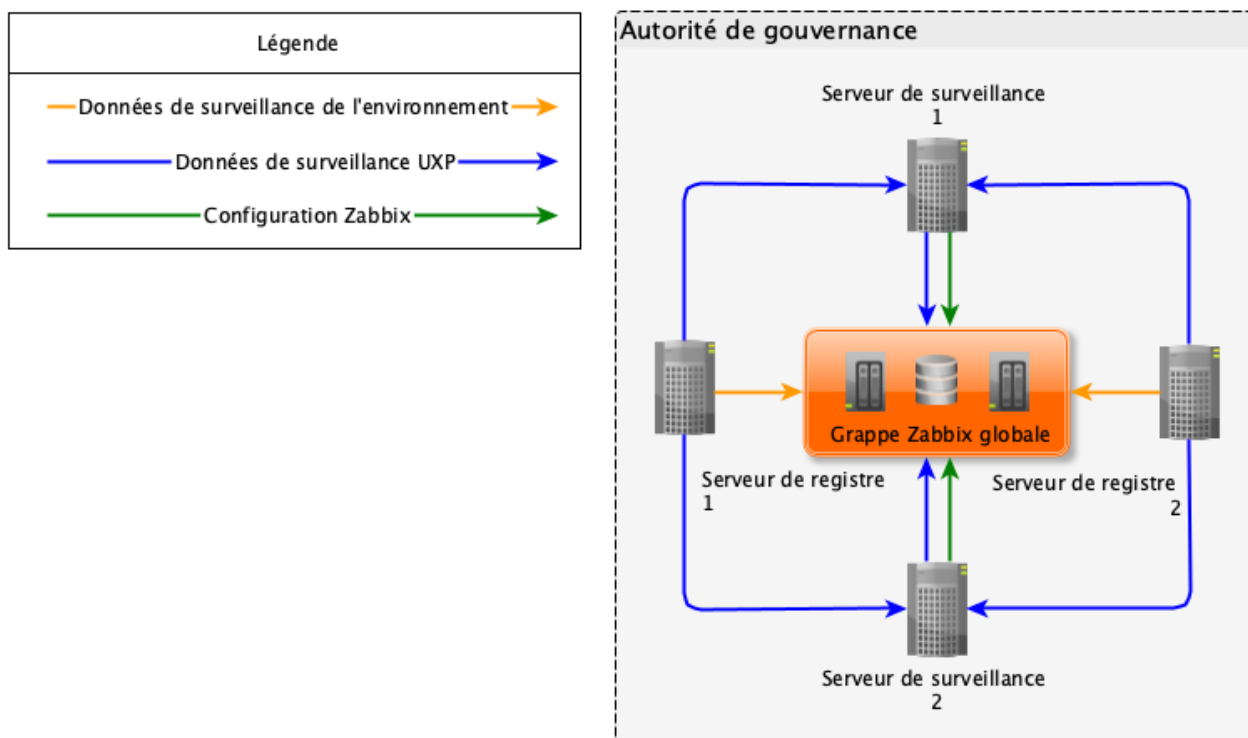


Figure 2. La solution de surveillance du serveur de registre UXP

L'autorité de gouvernance surveille ses serveurs de registre (grappe) en installant un ou plusieurs serveurs de surveillance (grappe) qui collectent des données de surveillance spécifiques à UXP à partir des serveurs de registre via HTTPS (voir les flèches bleues dans le diagramme). Ici, l'authentification HTTPS n'est effectuée ni du côté du client, ni du côté du serveur.

Le serveur de surveillance transmet les données collectées au serveur Zabbix (grappe) (voir les flèches bleues dans le diagramme).

Le serveur Zabbix (grappe) collecte les données de surveillance environnementale des serveurs de registres directement via l'agent Zabbix installé sur les serveurs de registres (voir les flèches orange dans le diagramme).

Le module complémentaire du serveur de sécurité et le serveur de surveillance ont tous deux la capacité de configurer automatiquement les entités surveillées sur Zabbix, ce qui élimine la nécessité d'une configuration manuelle (flèches vertes sur le diagramme).

## 1.6. Aperçu de la procédure de configuration

Le diagramme donne un aperçu des étapes à suivre pour configurer un serveur de surveillance pleinement fonctionnel et le connecter aux serveurs Zabbix et Elasticsearch utilisés pour surveiller et visualiser les informations collectées.

Les étapes à effectuer sur le serveur de registre, le serveur de sécurité, Zabbix et

Elasticsearch/Kibana sont marquées par les icônes : (SR), (SS), (Z) et (E/K), respectivement. Toutes les autres étapes s'appliquent au serveur de surveillance.

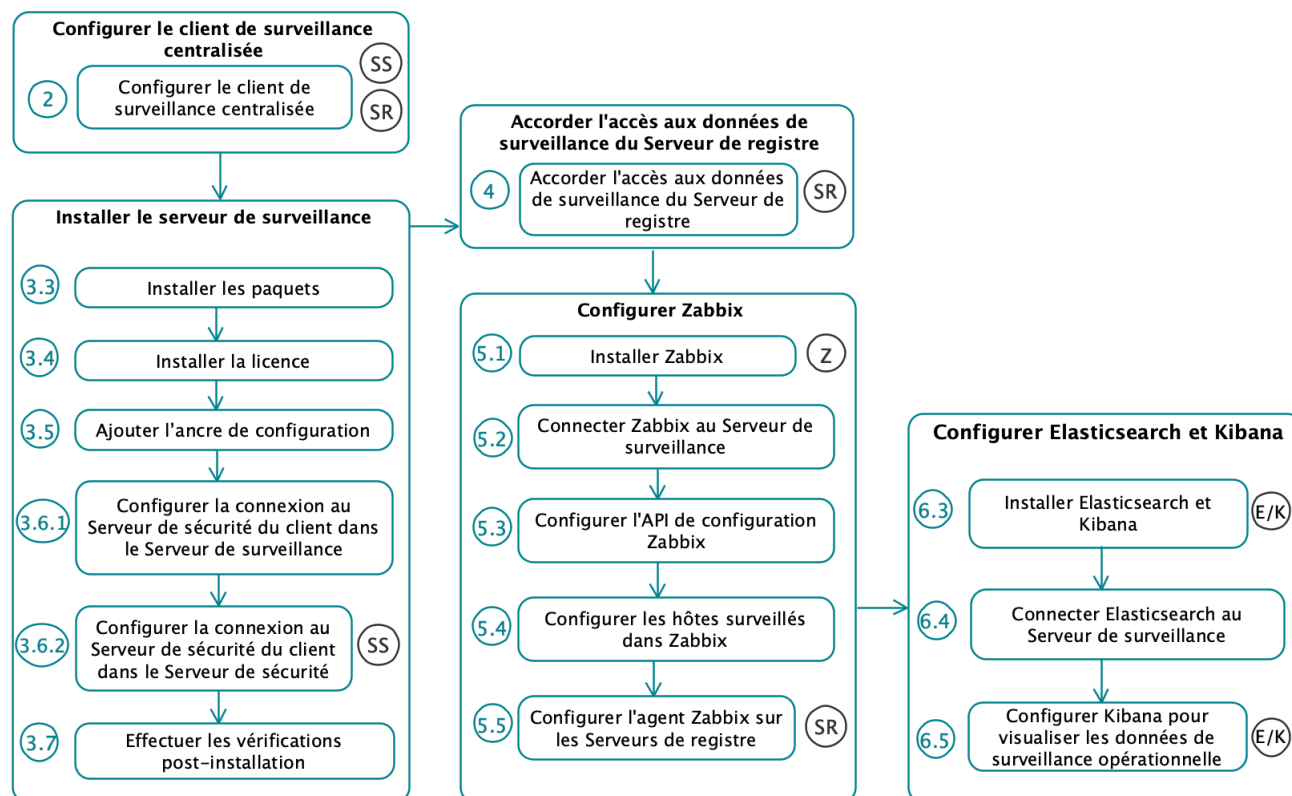


Figure 3. Étapes nécessaires à l'installation et à la configuration d'un Serveur de surveillance UXP

## 2. Configuration du client de surveillance centralisé

Le serveur de surveillance collecte les données de surveillance en envoyant des demandes à son serveur de sécurité en tant que système d'information client, au nom d'un client qui a été ajouté au serveur de sécurité et configuré comme client de surveillance centralisé sur le serveur de registre.

Il est recommandé d'ajouter un nouveau client dédié uniquement à la surveillance centralisée au sein du serveur de sécurité du serveur de surveillance, plutôt que d'utiliser un client existant. Reportez-vous à la section « Ajout d'un client de serveur de sécurité » du guide d'utilisation du Serveur de sécurité [UXP-UG-SS] pour obtenir des instructions sur l'ajout d'un nouveau client de serveur de sécurité, au nom duquel le serveur de surveillance effectuera des demandes de surveillance.



Il est fortement recommandé de configurer le type de connexion entre le serveur de sécurité et le système d'information client sur HTTPS pour le client de surveillance centralisé. Cela empêche les membres UXP non autorisés d'envoyer des messages de surveillance.

**En tant qu'administrateur du serveur de sécurité, sur le serveur de sécurité**

1. Accédez à **SERVICES** → **Clients du serveur de sécurité**, puis cliquez sur le bouton **Systèmes d'information pour le client de surveillance centralisé**.
2. Accédez à **TYPE DE CONNEXION POUR LES SYSTÈMES D'INFORMATION DU CLIENT DU SERVICE**, sélectionnez **HTTPS**, puis cliquez sur **ENREGISTRER**.



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), ajoutez le même client de surveillance centralisé au serveur de sécurité de chaque nœud, en vous assurant que le type correct de connexion est configuré.

### 2.1. Configuration du client de surveillance centralisé sur le Serveur de registre

Le client de surveillance centralisé doit être configuré dans la partie configuration de surveillance de la configuration globale sur le serveur de registre, afin que toutes les parties soient informées de l'existence de ce client spécifique.

La configuration de la surveillance est téléchargée sur le serveur de registre sous la forme du fichier XML `monitoring-params.xml`, qui doit respecter le schéma disponible à l'adresse `http://<registry-server>/monitoring-conf.xsd`, (où `<registry-server>` est l'adresse du serveur de registre).

## En tant qu'administrateur du serveur de registre, créez et téléchargez la configuration de surveillance

1. Dans l'interface utilisateur du serveur de registre, accédez à **Gestion** → **Configuration globale** → **ÉLÉMENTS DE CONFIGURATION**.



Si le serveur de registre dispose déjà d'un fichier `monitoring-params.xml` dans la liste des éléments de la configuration globale, vous pouvez le télécharger et le modifier si nécessaire.

2. Créez un fichier de configuration de surveillance, `monitoring-params.xml`, sur l'ordinateur où vous exécutez l'interface utilisateur du serveur de registre, similaire à l'exemple de configuration :

```
<?xml version="1.0"?>
<tns:conf xmlns:id="http://x-road.eu/xsd/identifiers"
  xmlns:tns="http://x-road.eu/xsd/xroad.xsd">
  <monitoringClient>
    <monitoringClientId id:objectType="SUBSYSTEM">
      <id:xRoadInstance>UXP</id:xRoadInstance>
      <id:memberClass>GOV</id:memberClass>
      <id:memberCode>MANAGEMENT</id:memberCode>
      <id:subsystemCode>MONITORING</id:subsystemCode>
    </monitoringClientId>
  </monitoringClient>
</tns:conf>
```

Remplacez les valeurs des éléments `xRoadInstance`, `memberClass`, `memberCode` et `subsystemCode` (parties de l'identifiant client) dans le fichier de configuration en fonction de l'identifiant du client de surveillance centralisé.



Pour afficher les parties correspondantes de l'instance, de la classe, du code et du sous-système de l'identifiant du client, connectez-vous au serveur de sécurité en tant qu'administrateur du serveur de sécurité. Accédez à **SERVICES** → **Clients du serveur de sécurité** et cliquez sur le bouton Détails du client de surveillance centralisé.

3. Sur la carte **ÉLÉMENTS DE CONFIGURATION**, téléchargez le fichier `monitoring-params.xml` créé en cliquant sur **Télécharger**.

Les informations relatives au client de surveillance centralisé autorisé à recevoir les données de surveillance sont maintenant distribuées aux serveurs de sécurité par le biais de la configuration globale.

## 3. Installer le serveur de surveillance

---

### 3.1. Configuration requise

#### Plates-formes prises en charge

Le système d'exploitation recommandé est **Ubuntu Server 24.04 Long-Term Support (LTS)** sur une plate-forme **64 bits**.

Le logiciel Serveur de surveillance UXP peut être installé à la fois sur du matériel physique et virtualisé (pour ce dernier, Xen et Oracle VirtualBox ont été testés).

Le serveur de surveillance est compatible avec les **Serveurs de registre UXP** et **Serveurs de sécurité UXP** version **1.17** et supérieure. Toutefois, la collecte de statistiques sur les données de surveillance opérationnelle n'est prise en charge par le serveur de sécurité qu'à partir de la version **1.22**.

Le logiciel du serveur de surveillance a été testé et son fonctionnement a été confirmé avec :

- Zabbix versions 6.0 LTS et 7.0 LTS,
- Elasticsearch/Kibana versions 8.x et 9.x.



Le Serveur de surveillance UXP n'est pas compatible avec :

- Zabbix 5.0 et versions antérieures.
- Elasticsearch/Kibana 7.x et versions antérieures.



Zabbix 6.0 LTS est obsolète. Pour maintenir la compatibilité avec le serveur de surveillance, il est recommandé de passer à Zabbix 7.0 LTS.

#### Paramètres matériels minimaux recommandés

- En général, le matériel du serveur (carte mère, processeur, cartes d'interface réseau, système de stockage) doit être compatible avec Ubuntu 24.04 ou Ubuntu 22.04 LTS ;
- Processeur Intel, AMD ou compatible 64 bits double cœur ; la prise en charge du jeu d'instructions AES est fortement recommandée ;
- 2 Go de RAM ;
- 10 Go d'espace sur le disque dur
- Carte d'interface réseau 100 Mbps.

#### Paramètres matériels recommandés

- En général, le matériel du serveur (carte mère, processeur, cartes d'interface réseau, système de stockage) doit être compatible avec Ubuntu 24.04 ou Ubuntu 22.04 LTS ;
- Processeur Intel, AMD ou compatible 64 bits quadricœur ; la prise en charge du jeu d'instructions AES est fortement recommandée ;

- 4 Go de RAM ;
- 15 Go d'espace sur le disque dur
- Carte d'interface réseau 1 Gbps.

### Paramètres logiciels requis

- Un système d'exploitation Ubuntu 24.04 ou 22.04 LTS x86-64 installé et configuré ;
- si le serveur de surveillance est séparé des autres réseaux par un pare-feu et/ou un NAT, les connexions nécessaires depuis le serveur de surveillance doivent être autorisées (voir les ports utilisés dans le tableau suivant) ;
- par défaut, le serveur de surveillance tentera de se connecter aux serveurs de sécurité, aux serveurs de registre, ainsi qu'aux serveurs Zabbix et Elasticsearch en utilisant les valeurs de port par défaut (voir les ports utilisés dans le tableau suivant). Toute configuration à distance différente de la configuration par défaut doit être spécifiée dans la configuration du serveur de surveillance (voir [Serveur de sécurité UXP : Guide de l'utilisateur](#) et Sections [Configurer Zabbix](#), [Configurer Elasticsearch](#) et [Kibana](#)).

Si le serveur de surveillance est installé sur la même machine qu'un serveur Zabbix ou Elasticsearch, assurez-vous qu'il n'y a pas de conflit de port. Il appartient à l'administrateur de reconnaître ces conflits et de les résoudre en modifiant les configurations appropriées.



L'activation des services supplémentaires nécessaires au fonctionnement et à la gestion du système d'exploitation (tels que DNS, NTP et SSH) n'entre pas dans le cadre de ce guide.

### Ports requis pour les connexions sortantes depuis le serveur de surveillance

| Port (TCP) | Objectif  | Portée du réseau |
|------------|---|------------------|
| 80         | Demande de configuration globale à partir d'un serveur de registre ;<br>Extraction des données de surveillance via le serveur de sécurité de gestion (uniquement nécessaire si HTTP est utilisé pour cette connexion) | PRIVÉ            |
| 8080       | Configuration automatique du serveur Zabbix   | PRIVÉ            |
| 4001       | Demande de données de surveillance aux serveurs de registre   | PRIVÉ            |
| 443        | Extraction des données de surveillance via le serveur de sécurité de gestion (uniquement nécessaire si HTTPS est utilisé pour cette connexion)  | PRIVÉ            |
| 10051      | Transmission des données de surveillance aux serveurs Zabbix  | PRIVÉ            |
| 9200       | Transmission des données de surveillance au serveur Elasticsearch   | PRIVÉ            |



La liste des connexions sortantes requises ne comprend que les ports spécifiques connus d'UXP. Les ports requis pour des services supplémentaires tels que DNS, NTP,



SSH ne sont pas couverts.

La portée du réseau spécifie si le port doit être visible uniquement au sein du réseau PRIVÉ (par exemple, au sein de votre organisation) ou si les ports doivent être visibles par le réseau PUBLIC (Internet). Le masquage des ports utilisés uniquement pour les communications au sein du réseau privé de votre organisation réduit le risque d'attaques de sécurité en provenance du réseau public.

## 3.2. Informations requises

Déterminez les informations suivantes avant l'installation.

### Informations fournies par l'autorité de gouvernance

- le nom d'utilisateur et le mot de passe du dépôt logiciel UXP ;
- Une licence Serveur de surveillance UXP,
- le fichier d'ancrage de la configuration globale ainsi que le hachage et la fonction de hachage de l'ancre.

## 3.3. Installer les paquets Serveur de surveillance UXP

Pour installer le logiciel Serveur de surveillance UXP sur Ubuntu, suivez les étapes suivantes :

1. Ajoutez la clé de signature du dépôt des paquets UXP au répertoire `/usr/share/keyrings` :

```
curl https://repo.cyber.ee/uxp/pub.gpg | gpg --dearmor | \
sudo tee /usr/share/keyrings/uxp-pub.gpg >/dev/null
```

2. Ajoutez l'URL du dépôt des paquets UXP et l'emplacement de la clé de signature au fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/ stable main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Ajoutez les informations d'authentification du dépôt UXP au fichier `/etc/apt/auth.conf.d/uxp.conf` :

```
machine repo.cyber.ee
  login <repo-username>
  password <repo-password>
```

4. Exécutez les commandes suivantes pour installer les paquets Serveur de surveillance UXP :

```
sudo apt update
sudo apt install uxp-monitoring-server
```

5. Le serveur de surveillance dépend du serveur de messagerie Postfix (voir la section [Notifications par e-mail](#)). Lors de la configuration de Postfix, choisissez le type général de la configuration du courrier comme Internet Site (le courrier est envoyé directement par SMTP). Reportez-vous au guide Postfix [\[Postfix\]](#) pour configurer correctement le relayage du courrier électronique.

## 3.4. Installer la licence

Serveur de surveillance UXP ne fonctionne pas sans licence valide.

1. Enregistrez la licence Serveur de surveillance UXP sous `/etc/uxp/monitoring-server/license.lic`.
2. Changez le propriétaire et le groupe du fichier `license.lic` :

```
sudo chown root:uxp /etc/uxp/monitoring-server/license.lic
```

3. Modifiez les autorisations du fichier `license.lic` :

```
sudo chmod 640 /etc/uxp/monitoring-server/license.lic
```

## 3.5. Ajouter une ancre de configuration au Serveur de surveillance

L'ancre de configuration est un fichier qui contient des informations utilisées pour télécharger périodiquement la configuration globale signée à partir du serveur de registre et pour vérifier la signature de la configuration téléchargée. L'ancre de configuration est fournie par l'autorité de gouvernance.



Veuillez vérifier que la valeur de hachage de l'ancre correspond à la valeur de hachage publiée par l'autorité de gouvernance.

Par exemple, utilisez le programme en ligne de commande `sha256sum`, `sha384sum` ou `sha512sum` conformément à l'algorithme de valeur de hachage publié pour calculer la valeur de hachage de l'ancre :

```
sha256sum ./configuration-anchor.xml
```

Si vous disposez de droits d'administration sur le serveur de registre UXP, vous pouvez télécharger l'ancre de configuration à partir de celui-ci (voir [\[UXP-UG-RS\]](#)).

1. Enregistrez le fichier d'ancrage sous `/etc/uxp/configuration-anchor.xml` sur le serveur de surveillance.
2. Changez le propriétaire et le groupe du fichier `configuration-anchor.xml` :

```
sudo chown root:uxp /etc/uxp/configuration-anchor.xml
```

### 3. Modifiez les autorisations du fichier `configuration-anchor.xml` :

```
sudo chmod 640 /etc/uxp/configuration-anchor.xml
```

### 4. Redémarrez le service `uxp-confclient` pour forcer le téléchargement de la configuration globale immédiatement (sinon attendez environ 1 minute) :

```
sudo systemctl restart uxp-confclient
```

Le serveur de surveillance télécharge alors périodiquement la configuration globale à partir du serveur de registre afin d'établir une liste des serveurs de sécurité qu'il surveillera.

La liste des serveurs de registre à surveiller est tirée de l'ancre de configuration, qui contient toutes les adresses des serveurs de registre de l'instance UXP.

## 3.6. Connecter le serveur de surveillance au serveur de sécurité du client



Il est fortement recommandé de configurer le type de connexion entre le serveur de sécurité et le système d'information client sur HTTPS pour le client de surveillance centralisé. Cela empêche les membres UXP non autorisés d'envoyer des messages de surveillance.

La configuration de la connexion pour le client de surveillance centralisé sur le serveur de sécurité et le serveur de surveillance doit être configurée de manière cohérente.

### 3.6.1. Configurer la connexion sur le serveur de surveillance



Une description détaillée des paramètres système du serveur de surveillance et de la manière de les modifier est disponible dans [\[UXP-SYSPAR-MS\]](#).

Les paramètres système par défaut du serveur de surveillance se trouvent dans le fichier de configuration `/etc/uxp/conf.d/monitoring-server.ini`. Pour écraser une valeur, il faut la placer dans `/etc/uxp/conf.d/local.ini` sous la section `[monitoring-server]`. Par exemple :

```
[monitoring-server]
security-server-tls-cert-file=/etc/uxp/ssl/security-server.crt
```

Le serveur de surveillance peut utiliser le protocole HTTP ou HTTPS pour communiquer avec le serveur de sécurité. Le protocole HTTPS doit être utilisé dans la plupart des cas. Le protocole HTTPS est particulièrement recommandé s'il n'est pas possible de fournir un segment de réseau séparé pour la communication entre le serveur de surveillance et le serveur de sécurité. Dans ce cas, HTTPS garantit que des méthodes cryptographiques sont

utilisées pour protéger la communication contre d'éventuelles écoutes et interceptions. De plus, l'utilisation du protocole HTTPS empêche les membres UXP non autorisés d'envoyer des messages de surveillance.

### Configurez la connexion au serveur de sécurité en effectuant les étapes suivantes

1. Définissez le protocole de communication (HTTP ou HTTPS) à l'aide du paramètre système `security-server-scheme` (HTTPS par défaut).
2. Réglez le port de connexion à l'aide du paramètre système `security-server-port`. La connexion HTTP est fixée par défaut à 80 et la connexion HTTPS à 443.
3. Dans le cas de HTTPS :
  - a. En tant qu'administrateur du serveur de sécurité, exportez le certificat TLS interne du serveur de sécurité (au format PEM ou DER) à partir du serveur de sécurité en naviguant vers **GESTION** → **Clés et certificats** → **CERTIFICATS TLS INTERNES**, puis en cliquant sur le bouton Exporter le certificat pour le certificat marqué comme IN USE.
  - b. Copiez le fichier de certificat exporté depuis l'ordinateur local vers le serveur de surveillance dans le répertoire `/etc/uxp/ssl` sous le nom `security-server.crt`.
  - c. Modifiez le propriétaire, le groupe et les autorisations du fichier sur le serveur de surveillance :

```
sudo chown root:uxp /etc/uxp/ssl/security-server.crt
sudo chmod 640 /etc/uxp/ssl/security-server.crt
```



Si vous utilisez un nom de fichier autre que `security-server.crt`, définissez le paramètre `security-server-tls-cert-file` sur le chemin absolu du fichier de certificat (par exemple, `/etc/uxp/ssl/<TLS_CERTIFICATE_FILE_NAME>`).

### 4. Redémarrez le serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)) ou lorsque le client de surveillance centralisé est enregistré sur plusieurs serveurs de sécurité, configurez l'identifiant du serveur de sécurité à utiliser (une concaténation de l'identifiant du propriétaire et le code du serveur) dans la configuration du serveur de surveillance. Réglez les paramètres système `security-server-member-class`, `security-server-member-code`, et `security-server-server-code` en conséquence. Les éléments requis de l'identifiant du serveur de sécurité s'affichent dans la boîte de dialogue de connexion au serveur de sécurité.



Pour utiliser une autre adresse que celle du serveur de sécurité de la configuration globale, configurez le paramètre système `security-server-address`. Si le paramètre système `notification-email` est également configuré, les paramètres

de l'identifiant du serveur de sécurité utilisé doivent être configurés pour obtenir l'identifiant correct.

### 3.6.2. Configurer la connexion sur le Serveur de sécurité

En tant qu'administrateur du serveur de sécurité, configurez le client de surveillance centralisé sur le serveur de sécurité.

1. Accédez à **SERVICES** → **Clients du serveur de sécurité**, puis cliquez sur le bouton **Systèmes d'information pour le client de surveillance centralisé**.
2. Assurez-vous que le type de connexion pour le système d'information du client de service est cohérent avec le type de connexion précédemment configuré sur le serveur de surveillance.
3. Dans le cas de HTTPS :
  - a. Téléchargez le fichier du certificat TLS du serveur de surveillance (situé à `/etc/uxp/ssl/monitoring-server.crt` sur le serveur de surveillance) sur l'ordinateur local où vous exécutez l'interface utilisateur du serveur de sécurité.
  - b. Sur le serveur de sécurité, accédez à **CERTIFICATS TLS INTERNES DES SYSTÈMES D'INFORMATION** et cliquez sur **AJOUTER** pour télécharger le certificat TLS du serveur de surveillance.

### 3.7. Vérifications après l'installation

L'installation est réussie si les services `uxp-confclient` et `uxp-monitoring-server` sont démarrés.

1. Utilisez la commande suivante pour vérifier si les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service uxp-*
```

|  |        |        |         |                                 |
|--|--------|--------|---------|---------------------------------|
| <code>uxp-confclient.service</code>        | loaded | active | running | UXP Global Configuration Client |
| <code>uxp-monitoring-server.service</code> | loaded | active | running | UXP Monitoring Server           |



Le service `uxp-monitoring-server` n'est pas dans l'état `active` et `running` tant que la configuration globale n'a pas été téléchargée par le service `uxp-confclient` et que la licence n'a pas été vérifiée et validée (voir section [Ajouter une ancre de configuration au Serveur de surveillance](#)).

Si le serveur de surveillance a démarré correctement, le fichier `/var/log/uxp/monitoring_server.log` contient une entrée similaire à :

```
[main] INFO e.c.u.m.MonitoringServerMain - STARTUP - Monitoring Server started successfully
```

## 4. Accorder l'accès aux données de surveillance du serveur de registre

Le serveur de registre partage ses données de surveillance spécifiques à UXP via HTTPS par l'intermédiaire de Nginx [\[NGINX\]](#). Les droits d'accès aux données de surveillance sont accordés en fonction de l'adresse IP.

En tant qu'administrateur du serveur de registre, accordez des droits d'accès au serveur de surveillance en ajoutant son adresse IP au fichier de configuration Nginx `/etc/uxp/nginx/monitoring-access-list`. Par exemple :

```
allow 127.0.0.1;  
allow 192.168.1.100;
```

Chaque déclaration `allow` doit se terminer par un point-virgule.



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), incluez les adresses IP de tous les nœuds dans la configuration Nginx.

Après avoir apporté des modifications à la configuration `nginx`, vous devez recharger celle-ci :

```
sudo systemctl reload nginx
```



En cas d'utilisation d'une grappe de serveurs de registre, assurez-vous que ces modifications sont appliquées à tous les nœuds de la grappe.

## 5. Configurer Zabbix

### 5.1. Installer Zabbix

Installez la version appropriée de Zabbix (version 7.0 LTS) ou utilisez une version existante pour transférer les données de surveillance collectées vers Zabbix afin de centraliser l'analyse, les alertes et les rapports.

Vous pouvez utiliser un serveur Zabbix unique ou sa solution de haute disponibilité (HA) [\[Zabbix-HA\]](#), en fonction de l'ampleur de votre déploiement et de vos exigences en matière de fiabilité et de tolérance aux pannes. Dans le mode Zabbix HA, plusieurs serveurs Zabbix sont exécutés en tant que nœuds d'une grappe et ils utilisent la même base de données. Pendant qu'un serveur Zabbix de la grappe est actif, d'autres sont en attente, prêts à prendre le relais si nécessaire.

Si vous souhaitez utiliser une instance existante de Zabbix, assurez-vous qu'elle répond à la configuration requise décrite ci-dessous. Dans ce cas, ignorez cette section et poursuivez la configuration décrite dans la section [Connecter Zabbix au Serveur de surveillance](#).

#### Paramètres système requis pour le serveur Zabbix 7.0 LTS

- **Système d'exploitation Ubuntu 24.04 ou 22.04 Long-Term Support (LTS)** sur une plate-forme **64 bits** ;
- 2 Go de RAM ;
- 20 Go d'espace sur le disque dur.

La taille de la base de données Zabbix dépend principalement des variables ci-dessous, qui définissent la quantité de données historiques stockées :

- le nombre de valeurs traitées par seconde (NVPS),
- paramètres du gestionnaire domestique pour l'historique,
- paramètres du gestionnaire domestique pour les tendances,
- paramètres du gestionnaire domestique pour les événements.



Actuellement, les modèles Zabbix pour le serveur de sécurité (UXP Security Server by MS) et le serveur de registre (UXP Registry Server by MS) comportent respectivement 58 et 3 éléments (piégés). L'intervalle par défaut pour la collecte et l'envoi des données de surveillance est de 180 secondes pour les serveurs de sécurité (configuré par le paramètre `envdata-polling-interval-seconds`) et de 60 secondes pour les serveurs de registre (configuré par le paramètre `registry-server-monitoring-data-polling-interval-seconds`), c'est-à-dire que le NVPS pour le serveur de sécurité est  $58 / 180 = 0.32$  et pour le serveur de registre  $3 / 60 = 0.05$  (au total  $0.32 + 0.05 = 0.37$ ).

Par défaut, Zabbix conserve les valeurs pendant 90 jours, soit  $(90 * 24 * 3600) * 0.37 = 2.877.120$ , soit environ 2,88 millions de valeurs (2,5 millions pour le serveur

de sécurité et 0,38 million pour le serveur de registre).

En fonction du moteur de base de données utilisé et du type de valeurs reçues (flottants, entiers, chaînes, fichiers journaux, etc.), l'espace disque nécessaire à la conservation d'une seule valeur peut varier de 40 octets à plusieurs centaines d'octets. Normalement, il s'agit d'environ 90 octets par valeur pour les éléments numériques. Il est impossible de prévoir avec exactitude la taille des valeurs des éléments de texte/journal, mais vous pouvez vous attendre à environ 500 octets par valeur. Pour simplifier, nous supposons que chaque valeur de chaîne a une taille de 90 octets.

Le modèle de serveur de sécurité contient actuellement 46 valeurs numériques et 12 valeurs de chaînes de caractères (principalement des versions de paquets). Dans ce cas, cela signifie que 2,5 millions de valeurs nécessiteront  $2.5M * 90\text{bytes} = 225\text{MB}$  d'espace disque. Le modèle pour le serveur de registre a actuellement 3 valeurs numériques, c'est-à-dire qu'il nécessite  $0.38M * 90\text{bytes} = 34\text{MB}$ . Au total  $225\text{MB} + 34\text{MB} = 259\text{MB}$ .

Zabbix conserve un ensemble de valeurs max/min/moyenne/nombre d'une durée de 1 heure pour chaque élément du tableau des tendances, par défaut pendant 1 an. Dans ce cas, cela signifie que  $58 + 3$  éléments nécessitent  $61 * (24 * 365) * 90\text{bytes} = 48\text{MB}$  (46 Mo + 2 Mo) d'espace disque.

Chaque événement Zabbix nécessite environ 250 octets et un événement récupéré 80 octets d'espace disque. Il est difficile d'estimer le nombre d'événements générés quotidiennement par Zabbix. Par défaut, Zabbix conserve les événements pendant 1 an. Dans le pire des cas, en supposant un événement par seconde, cela nécessiterait environ 10 Go d'espace disque :  $(365 * 24 * 3600) * (250\text{bytes} + 80\text{bytes})$ .

L'espace disque total requis peut donc être calculé comme suit :

Configuration (normalement 10 Mo ou moins) + Historique + Tendances + Événements

Dans ce cas, l'espace disque total requis est de  $10\text{MB} + 259\text{MB} + 48\text{MB} + 10\text{GB} = 11\text{GB}$ . En général, le calcul est  $10\text{MB} + S * (225\text{MB} + 46\text{MB}) + R * (34\text{MB} + 2\text{MB}) + 10\text{GB}$ , où S est le nombre de serveurs de sécurité et R le nombre de serveurs de registre. Par exemple, une instance comportant 100 serveurs de sécurité et 2 serveurs de registre nécessite 40 Go d'espace disque.

Reportez-vous au manuel de Zabbix [\[Zabbix-Requirements\]](#) pour obtenir des informations détaillées sur l'espace disque requis.

Reportez-vous à la section [Installer un serveur Zabbix unique](#) pour installer un serveur Zabbix unique, ou reportez-vous à la section [Installer Zabbix dans une configuration HA native](#) pour installer Zabbix dans une configuration HA native.



Il est recommandé d'installer Zabbix sur un serveur distinct de celui qui exécute le serveur de surveillance.

### 5.1.1. Installer un serveur Zabbix unique



## Installez Zabbix 7.0 LTS à partir des paquets en utilisant la ligne de commande

### 1. Installez le paquet de configuration du dépôt Zabbix :

#### ◦ Ubuntu 24.04 LTS

```
wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/\
zabbix-release_7.0-2+ubuntu24.04_all.deb

sudo dpkg -i zabbix-release_7.0-2+ubuntu24.04_all.deb
```

#### ◦ Ubuntu 22.04 LTS

```
wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/\
zabbix-release_7.0-2+ubuntu22.04_all.deb

sudo dpkg -i zabbix-release_7.0-2+ubuntu22.04_all.deb
```

### 2. Installez la locale en\_US.UTF-8 :

```
sudo apt update
sudo apt install locales

sudo locale-gen en_US.UTF-8
sudo update-locale
```

### 3. Installez les paquets Zabbix server, frontend, nginx-conf et agent avec le support PostgreSQL (l'ajout de apache2-bin- sautera les paquets apache qui sont par ailleurs automatiquement installés) :

#### ◦ Ubuntu 24.04 LTS

```
sudo apt install nano postgresql zabbix-server-pgsql zabbix-frontend-php \
php8.3-pgsql zabbix-nginx-conf apache2-bin- zabbix-sql-scripts zabbix-agent
```

#### ◦ Ubuntu 22.04 LTS

```
sudo apt install nano postgresql zabbix-server-pgsql zabbix-frontend-php \
php8.1-pgsql zabbix-nginx-conf apache2-bin- zabbix-sql-scripts zabbix-agent
```

### 4. Créez une base de données pour le serveur Zabbix (entrez un mot de passe pour l'utilisateur de la base de données Zabbix et mémorisez-le pour plus tard) :

```
sudo -i -u postgres createuser --pwprompt zabbix
sudo -i -u postgres createdb -O zabbix zabbix
```

### 5. Importez le schéma et les données initiales dans la base de données :

```
zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | \
sudo -u zabbix psql zabbix
```

## 6. Modifiez la configuration de la base de données du serveur Zabbix :

```
sudo nano /etc/zabbix/zabbix_server.conf
```

Décommentez le paramètre `DBPassword` et ajoutez le mot de passe que vous avez créé :

```
DBPassword=my-password
```

## 7. Modifiez le fichier de configuration Nginx :

```
sudo nano /etc/zabbix/nginx.conf
```

Décommentez les directives `listen` et `server_name`, modifiez-les selon vos besoins :

```
listen 8080;
server_name my-zabbix-server-name;
```

## 8. Facultatif : Supprimez le lien symbolique vers la configuration par défaut de Nginx, puisque le fichier de configuration de Zabbix Nginx est situé ailleurs. **NB !** Obligatoire si vous avez configuré la directive `listen` sur 80 à l'étape précédente :

```
sudo rm -f /etc/nginx/sites-enabled/default
```

## 9. Activez et démarrez les processus zabbix, nginx et php :

### • Ubuntu 24.04 LTS

```
sudo systemctl enable zabbix-server zabbix-agent nginx php8.3-fpm
sudo systemctl restart zabbix-server zabbix-agent nginx php8.3-fpm
```

### • Ubuntu 22.04 LTS

```
sudo systemctl enable zabbix-server zabbix-agent nginx php8.1-fpm
sudo systemctl restart zabbix-server zabbix-agent nginx php8.1-fpm
```

## Terminez la configuration du frontend Zabbix en utilisant l'interface utilisateur Zabbix

1. Ouvrez la page d'installation de Zabbix dans le navigateur, ajoutez le numéro de port correct si vous avez remplacé 8080 par quelque chose d'autre dans la configuration nginx `http://<your-zabbix-server>:8080/`.
2. Sur la page **Welcome**, cliquez sur **Next step**.
3. Sur la page **Check of pre-requisites**, cliquez sur **Next step**.
4. Sur la page **Configure DB connection**, vérifiez que le type de base de données est PostgreSQL, saisissez le mot de passe de l'utilisateur de la base de données zabbix, et cliquez sur **Next step**.
5. Sur la page **Settings**, sélectionnez le bon fuseau horaire par défaut et cliquez sur **Next step**.

6. Sur la page **Pre-installation summary**, cliquez sur **Next step**.
7. Sur la page **Install**, cliquez sur **Finish** pour terminer l'installation.

### Modifiez le mot de passe par défaut de l'interface utilisateur Zabbix à l'aide de l'interface utilisateur Zabbix

1. Connectez-vous à l'interface Zabbix en utilisant les informations d'identification par défaut : nom d'utilisateur `Admin` et mot de passe `zabbix`.
2. Dans le menu **Users**, sélectionnez **Users** et cliquez sur l'utilisateur `Admin`.
3. Cliquez sur **Change password** et saisissez un nouveau mot de passe sécurisé.
4. Cliquez sur **Update** pour accepter les modifications.

L'installation du serveur Zabbix est terminée. Passez à la section [Connecter Zabbix au Serveur de surveillance](#) pour obtenir des instructions sur la configuration du serveur de surveillance afin qu'il se connecte au serveur Zabbix.



Reportez-vous à la documentation en ligne de Zabbix [\[Zabbix-Frontend\]](#) pour obtenir des informations plus détaillées sur la configuration du frontend de Zabbix.

## 5.1.2. Installer Zabbix dans une configuration HA native

En mode Zabbix HA, plusieurs serveurs Zabbix sont exécutés en tant que nœuds d'une grappe et ils utilisent le même serveur de base de données.

### Installer le serveur de base de données

#### Installez le serveur de base de données PostgreSQL à partir des paquets en utilisant la ligne de commande

1. Installez le paquet de configuration du dépôt Zabbix en effectuant la première étape de la section précédente [Installer un serveur Zabbix unique](#).
2. Installez le serveur PostgreSQL et les scripts SQL Zabbix nécessaires :

```
sudo apt update
sudo apt install nano postgresql zabbix-sql-scripts
```

3. Créez une base de données pour le serveur Zabbix (entrez un mot de passe pour l'utilisateur de la base de données Zabbix `zabbix` et mémorisez-le pour plus tard) :

```
sudo -i -u postgres createuser --pwprompt zabbix
sudo -i -u postgres createdb -O zabbix zabbix
```

4. Importez le schéma et les données initiales dans la base de données (saisir le mot de passe de l'utilisateur de la base de données `zabbix`) :

```
zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | \
sudo -i -u postgres psql -h 0 -U zabbix -d zabbix -W
```

5. Configurez PostgreSQL pour écouter sur toutes les IP en éditant la configuration de `postgresql.conf` :

```
sudo nano /etc/postgresql/<version>/main/postgresql.conf
```

Décommentez le paramètre `listen_addresses` et fixez la valeur à `'*'` :

```
listen_addresses = '*'
```

6. Configurez l'authentification du client en modifiant la configuration de `pg_hba.conf` :

```
sudo nano /etc/postgresql/<version>/main/pg_hba.conf
```

Ajoutez la ligne suivante à la fin du fichier pour **chaque nœud du serveur Zabbix**, où `<zabbix-node-address>` est le nom d'hôte (qui se résout en adresse IP via DNS), ou l'adresse IP et un masque CIDR du nœud :

```
host      zabbix      zabbix      <zabbix-node-address>      scram-sha-256
```

7. Redémarrez le service `postgresql` :

```
sudo systemctl restart postgresql
```

L'installation du serveur de base de données Zabbix est terminée.

## Installer un nœud du serveur Zabbix

Installez le nœud du serveur Zabbix à partir des paquets à l'aide de la ligne de commande

1. Installez le paquet de configuration du dépôt Zabbix en effectuant la première étape de la section précédente [Installer un serveur Zabbix unique](#).
2. Installez la locale `en_US.UTF-8` :

```
sudo apt update
sudo apt install locales

sudo locale-gen en_US.UTF-8
sudo update-locale
```

3. Installez les paquets Zabbix server, frontend, nginx-conf et agent avec le support PostgreSQL (l'ajout de `apache2-bin` sautera les paquets apache qui sont par ailleurs automatiquement installés) :

- Ubuntu 24.04 LTS

```
sudo apt install nano zabbix-server-psql zabbix-frontend-php \
php8.3-psql zabbix-nginx-conf apache2-bin zabbix-agent
```

- Ubuntu 22.04 LTS

```
sudo apt install nano zabbix-server-pgsql zabbix-frontend-php \
php8.1-pgsql zabbix-nginx-conf apache2-bin- zabbix-agent
```

#### 4. Modifiez la configuration du serveur Zabbix :

```
sudo nano /etc/zabbix/zabbix_server.conf
```

- a. Décommentez le paramètre `DBHost` et définissez l'adresse IP ou le nom d'hôte (qui se résout en adresse IP via DNS) du serveur de base de données :

```
DBHost=<database-server-address>
```

- b. Décommentez le paramètre `DBPassword` et définissez le mot de passe que vous avez créé pour l'utilisateur de la base de données `zabbix` :

```
DBPassword=*****
```

- c. Décommentez le paramètre `HANodeName` et définissez l'identifiant **unique** du nœud, par exemple `zabbix-node-1` :

```
HANodeName=zabbix-node-1
```

- d. Décommentez le paramètre `NodeAddress` et définissez l'adresse qui sera utilisée par le frontend Zabbix pour se connecter au nœud du serveur actif. `NodeAddress` doit correspondre à l'adresse IP ou au nom d'hôte (qui se résout en adresse IP via DNS) du serveur Zabbix concerné.

```
NodeAddress=<zabbix-node-1-address>
```

#### 5. Modifiez le fichier de configuration Nginx :

```
sudo nano /etc/zabbix/nginx.conf
```

Décommentez les directives `listen` et `server_name`, modifiez-les selon vos besoins :

```
listen 8080;
server_name my-zabbix-server-name;
```

6. Facultatif : Supprimez le lien symbolique vers la configuration par défaut de Nginx, puisque le fichier de configuration de Zabbix Nginx est situé ailleurs. **NB !** Obligatoire si vous avez configuré la directive `listen` sur 80 à l'étape précédente :

```
sudo rm -f /etc/nginx/sites-enabled/default
```

#### 7. Activez et démarrez les processus `zabbix`, `nginx` et `php` :

- Ubuntu 24.04 LTS

```
sudo systemctl enable zabbix-server zabbix-agent nginx php8.3-fpm
sudo systemctl restart zabbix-server zabbix-agent nginx php8.3-fpm
```

- Ubuntu 22.04 LTS

```
sudo systemctl enable zabbix-server zabbix-agent nginx php8.1-fpm
sudo systemctl restart zabbix-server zabbix-agent nginx php8.1-fpm
```

## Terminez la configuration du frontend du nœud Zabbix à l'aide de l'interface utilisateur Zabbix

1. Ouvrez la page d'installation de Zabbix dans le navigateur, ajoutez le numéro de port correct si vous avez remplacé 8080 par quelque chose d'autre dans la configuration nginx `http://<your-zabbix-server>:8080/`.
2. Sur la page **Welcome**, cliquez sur **Next step**.
3. Sur la page **Check of pre-requisites**, cliquez sur **Next step**.
4. Sur la page **Configure DB connection**, vérifiez que le type de base de données est PostgreSQL, entrez l'hôte de la base de données, entrez le mot de passe de l'utilisateur de la base de données zabbix, et cliquez sur **Next step**.
5. Sur la page **Settings**, sélectionnez le bon fuseau horaire par défaut et cliquez sur **Next step**.
6. Sur la page **Pre-installation summary**, cliquez sur **Next step**.
7. Sur la page **Install**, cliquez sur **Finish** pour terminer l'installation.

## Modifiez le mot de passe par défaut de l'interface utilisateur Zabbix à l'aide de l'interface utilisateur Zabbix

1. Connectez-vous à l'interface Zabbix en utilisant les informations d'identification par défaut : nom d'utilisateur Admin et mot de passe zabbix.
2. Dans le menu **Users**, sélectionnez **Users** et cliquez sur l'utilisateur Admin.
3. Cliquez sur **Change password** et saisissez un nouveau mot de passe sécurisé.
4. Cliquez sur **Update** pour accepter les modifications.

L'installation du nœud Zabbix est terminée.



Installez le(s) nœud(s) supplémentaire(s) en suivant les étapes précédentes, à l'exception de l'étape de modification du mot de passe par défaut de l'interface utilisateur Zabbix.

Enfin, vérifiez l'état de la grappe Zabbix en exécutant la commande suivante sur les nœuds Zabbix. Si le nœud est actif, il affiche l'état de la grappe. S'il n'est pas actif, répétez la commande sur un autre nœud :

```
sudo zabbix_server -R ha_status
```

Passez aux sections suivantes pour obtenir des instructions sur la configuration du serveur

de surveillance afin qu'il se connecte au serveur Zabbix.

## 5.2. Connecter Zabbix au Serveur de surveillance

Pour permettre la transmission des informations de surveillance à un serveur Zabbix, modifiez le fichier de configuration `/etc/uxp/monitor-agent.ini` sur le serveur de surveillance, en ajoutant une entrée similaire à :

```
[zabbix-1]
address = 192.168.56.101
```

La section `[zabbix-<suffix>]` définit une station de surveillance Zabbix, où le nom de la section a un préfixe obligatoire – `zabbix`, et `<suffix>` doit être une chaîne de caractères unique parmi les autres sections Zabbix.

Le tableau suivant donne un aperçu des champs de configuration possibles pour la connexion de la section Zabbix. Notez que les champs sans valeur par défaut doivent être explicitement définis.

Tableau 1. Paramètres pour la connexion Zabbix

| Champ                           | Valeur par défaut | Explication   |
|---------------------------------|-------------------|---|
| <code>address</code>            |                   | Nom d'hôte du serveur Zabbix (résolu en adresse IP via DNS) ou adresse IP.  |
| <code>port</code>               | 10051             | Port sur lequel le serveur Zabbix écoute les informations de surveillance.  |
| <code>cluster-nodes^[1]^</code> | Liste vide        | Liste séparée par des virgules des noms de section pour les nœuds supplémentaires de la grappe HA native de Zabbix. |

`^[1]^` Si la grappe HA native de Zabbix est utilisée, ajoutez une nouvelle section de configuration pour chaque nœud de la grappe supplémentaire similaire à :



Les nœuds de la grappe Zabbix configurés comme nœuds supplémentaires dans le paramètre `cluster-nodes` n'ont pas d'importance.

```
[zabbix-1]
; ...

cluster-nodes = node-2-for-zabbix-1, node-3-for-zabbix-1

[node-2-for-zabbix-1]
address = 192.168.56.102

[node-3-for-zabbix-1]
address = 192.168.56.103
```

Le tableau suivant donne un aperçu des champs de configuration possibles pour la section du nœud supplémentaire de la grappe. Notez que les champs sans valeur par défaut doivent être explicitement définis.

Tableau 2. Paramètres pour les nœuds supplémentaires dans la grappe Zabbix Native HA

| Champ   | Valeur par défaut | Explication  |
|---------|-------------------|--|
| address |                   | Nom d'hôte du nœud (résolu en adresse IP via DNS) ou adresse IP. |
| port    | 10051             | Port où le nœud écoute les informations de surveillance.         |



Assurez-vous que tous les nœuds de la grappe Zabbix sont accessibles sur le réseau afin d'optimiser les performances et la fiabilité du système de surveillance.

Si le nœud Zabbix actuellement actif est inaccessible, le serveur de surveillance ne parviendra pas à transmettre les données à la grappe Zabbix. Dans le cas d'une grappe de serveurs de surveillance, si le nœud maître du serveur de surveillance pour Zabbix ne peut pas atteindre le nœud actif de Zabbix, un autre nœud de serveur de surveillance tentera d'assumer le rôle de maître pour Zabbix (voir [Haute disponibilité du serveur de surveillance](#)). Toutefois, si tous les autres nœuds du serveur de surveillance sont hors service en même temps, la transmission des données vers la grappe Zabbix échouera.

Avant que le serveur de surveillance puisse interagir avec le Zabbix connecté, l'accès à l'API de configuration de Zabbix doit être correctement configuré. Passez à la section suivante, [Configurer l'API de configuration Zabbix](#), pour continuer à modifier le fichier de configuration.



Les modifications apportées au fichier de configuration `/etc/uxp/monitor-agent.ini` prennent effet après le rechargement de la configuration du serveur de surveillance. Pour ce faire, exécutez la commande suivante sur le serveur de surveillance :

```
sudo reload-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), connectez le ou les nœuds supplémentaires du serveur de surveillance au même Zabbix.

## 5.3. Configurer l'API de configuration Zabbix

Le serveur de surveillance utilise l'API de configuration Zabbix pour activer sa fonctionnalité HA native et pour configurer les hôtes surveillés sur Zabbix.

Pour créer un utilisateur Zabbix pour le client API de configuration avec les privilèges requis sur Zabbix, et pour configurer cet utilisateur ainsi que le point de terminaison API sur le



serveur de surveillance, procédez comme suit :

### Créez un utilisateur Zabbix pour l'accès client à l'API à l'aide de l'interface utilisateur Zabbix

1. Créez un groupe d'hôtes, tel que `uxp-security-servers`, pour le(s) serveur(s) de sécurité en sélectionnant **Data collection** → **Host groups** → **Create host group**.
2. Créez un groupe d'hôtes, tel que `uxp-registry-servers`, pour le(s) serveur(s) de registre en sélectionnant **Data collection** → **Host groups** → **Create host group**.
3. Créez un groupe d'hôtes système UXP MS clusters en sélectionnant **Data collection** → **Host groups** → **Create host group**.
4. Créez un groupe d'utilisateurs en sélectionnant **Users** → **User groups** → **Create user group**.
  - a. Saisissez un nom de groupe, par exemple `UXP Monitoring Servers`.
  - b. Sélectionnez `Disabled` pour **Frontend access**.
  - c. Dans l'onglet **Template permissions**, cliquez sur le lien **Add** et sélectionnez le groupe de modèles `Templates/Applications`. Choisissez les permissions `Read-write`.
  - d. Sur le même onglet, cliquez sur le lien **Add** et sélectionnez le groupe de modèles `Templates/Operating systems`. Choisissez les permissions `Read`.
  - e. Dans l'onglet **Host permissions**, cliquez sur le lien **Add** et sélectionnez les groupes d'hôtes des serveurs de sécurité et des serveurs de registre créés précédemment, ainsi que le groupe d'hôtes `UXP MS clusters`. Choisissez les permissions `Read-write`.
  - f. Cliquez enfin sur **Add**.
5. Créez un utilisateur en sélectionnant **Users** → **Users** → **Create user**.
  - a. Saisissez un nom d'utilisateur, par exemple `uxp-ms`.
  - b. Sélectionnez un groupe précédemment créé dans la rubrique **Groups**.
  - c. Saisissez un mot de passe.
  - d. Dans l'onglet **Permissions**, sélectionnez `Admin role` pour le **Role**.
  - e. Cliquez enfin sur **Add**.

### Configurez l'API de configuration Zabbix sur le serveur de surveillance

Modifiez le fichier de configuration `/etc/uxp/monitor-agent.ini` sur le serveur de surveillance, en ajoutant une entrée similaire à :

```
[zabbix-1]
; ...

conf_api_port = 8080
conf_api_path = /api_jsonrpc.php
username = uxp-ms
password = *****
```

Le tableau suivant donne un aperçu des champs de configuration possibles pour l'API de

configuration de Zabbix. Notez que les champs sans valeur par défaut doivent être explicitement définis.

Tableau 3. Paramètres du configurateur Zabbix

| Champ         | Valeur par défaut | Explication  |
|---------------|-------------------|--|
| conf_api_path | /api_jsonrpc.php  | Chemin de l'API de configuration de Zabbix.  |
| conf_api_port | 8080              | Port de l'API de configuration de Zabbix.  |
| username      |                   | Nom d'utilisateur de l'API de configuration de Zabbix.<br><br><div>L'utilisateur doit être du type Super admin ou Admin avec l'autorisation Read-write pour les groupes d'hôtes configurés des serveurs de sécurité et des serveurs de registre, ainsi que pour le groupe d'hôtes du système UXP MS clusters. En outre, l'utilisateur doit avoir l'autorisation Read-write pour le groupe de modèles Templates/Applications et l'autorisation Read pour le groupe de modèles Templates/Operating systems.</div> |
| password      |                   | Mot de passe de l'utilisateur de l'API de configuration de Zabbix.   |



Les modifications apportées au fichier de configuration `/etc/uxp/monitor-agent.ini` prennent effet après le rechargement de la configuration du serveur de surveillance. Pour ce faire, exécutez la commande suivante sur le serveur de surveillance :

```
sudo reload-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), configurez le ou les nœuds supplémentaires du serveur de surveillance de la même manière en utilisant la même API de configuration.

Avant que le serveur Zabbix connecté puisse recevoir des données de surveillance, les hôtes surveillés et leurs entités doivent être correctement configurés sur le serveur Zabbix. Passez à la section suivante, [Configurer les hôtes surveillés sur Zabbix](#), pour continuer à modifier le fichier de configuration.

## 5.4. Configurer les hôtes surveillés sur Zabbix

Assurez-vous que les hôtes du serveur de sécurité et du serveur de registre et leurs entités de surveillance sont correctement configurés sur le serveur Zabbix.

Le serveur de surveillance comprend une fonctionnalité permettant de configurer les hôtes surveillés sur le serveur Zabbix par l'intermédiaire de l'API Zabbix. Au cours de ce processus, le serveur de surveillance crée sur le serveur Zabbix un groupe d'hôtes pour les serveurs de sécurité et un autre pour les serveurs de registre. Il ajoute ensuite les serveurs de sécurité trouvés dans la configuration globale et les serveurs de registre trouvés dans l'ancre de configuration à leurs groupes respectifs. En outre, il importe le modèle UXP Security Server by MS et le modèle UXP Registry Server by MS, tous deux situés dans `/usr/share/uxp/templates/zabbix`, sur le serveur Zabbix et les lie aux hôtes respectifs nouvellement ajoutés.

En option, le serveur de surveillance peut être configuré pour nettoyer sur Zabbix tous les serveurs obsolètes (ceux qui ne figurent pas dans la configuration globale ou dans l'ancre de configuration).

Au lancement, le serveur de surveillance tente de configurer le serveur Zabbix. Si la configuration échoue (par exemple, si Zabbix est hors service), le serveur de surveillance réessaiera périodiquement la configuration jusqu'à ce qu'elle aboutisse.

Pour activer le configurateur Zabbix, procédez comme suit :

### Configurez le configurateur Zabbix sur le serveur de surveillance

Modifiez le fichier de configuration `/etc/uxp/monitor-agent.ini` sur le serveur de surveillance, en ajoutant une entrée similaire à :

```
[zabbix-1]

; ...

enable_configurator = true
host_group = uxp-security-servers

enable_registry_servers_configurator = true
registry_servers_group = uxp-registry-servers
enable_registry_servers_os_linux_template = true
```

Le tableau suivant donne un aperçu des champs de configuration possibles pour le configurateur Zabbix. Notez que les champs sans valeur par défaut doivent être explicitement définis.

Tableau 4. Paramètres du configurateur Zabbix

| Champ   | Valeur par défaut    | Explication  |
|---|----------------------|--|
| enable_configurator   | true                 | Active/désactive la configuration automatique des serveurs de sécurité sur le serveur Zabbix.  |
| host_group ^[1]^  | uxp-security-servers | Nom du groupe d'hôtes qui contiendra les serveurs de sécurité gérés automatiquement.   |
| <div>  <p>L'utilisateur de l'API de configuration Zabbix doit avoir l'autorisation Read-write pour le groupe d'hôtes des serveurs de sécurité configurés.</p> </div>   |                      |  |
| enable_update_existing_triggers ^[1][2]^  | true                 | Active/désactive la mise à jour des déclencheurs existants (potentiellement écrasés) des modèles Zabbix UXP. Réglez ce paramètre sur false si vous souhaitez conserver les déclencheurs qui ont été modifiés manuellement dans Zabbix. |
| enable_cleanup ^[1]^  | false                | Active/désactive la suppression des serveurs de sécurité retirés du groupe d'hôtes.  |
| enable_registry_servers_configurator  | true                 | Active/désactive la configuration automatique des serveurs de registre sur le serveur Zabbix.  |
| registry_servers_group ^[2]^  | uxp-registry-servers | Nom du groupe d'hôtes qui contiendra les serveurs de registre gérés automatiquement.   |
| <div>  <p>L'utilisateur de l'API de configuration Zabbix doit avoir l'autorisation Read-write pour le groupe d'hôtes des serveurs de registre configurés.</p> </div> |                      |  |
| enable_registry_server_os_linux_template ^[2]^  | false                | Si true, le modèle officiel Zabbix Linux by Zabbix agent sera lié aux hôtes du serveur de registre ajoutés.  |
| enable_registry_server_cleanup ^[2]^  | false                | Active/désactive la suppression des serveurs de registre retirés du groupe d'hôtes.  |

^[1]^ L'option n'est effective que si enable\_configurator = true.

^[2]^ L'option n'est effective que si enable\_registry\_servers\_configurator = true.

Après avoir mis à jour la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```

Enfin, vérifiez dans l'interface utilisateur Zabbix que les hôtes du serveur de sécurité et du serveur de registre ont été créés et que les données de surveillance sont bien reçues en accédant à **Monitoring** → **Latest data**.



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), configurez le ou les nœuds supplémentaires du serveur de surveillance de la même manière.

### 5.4.1. Modèle Zabbix : Serveur de sécurité UXP par MS

Le modèle Security Server by MS, situé sur le serveur de surveillance /usr/share/uxp/templates/zabbix/7.0/template\_app\_uxp\_security\_server\_by\_ms.yaml, fournit les éléments de surveillance et les déclencheurs suivants :

#### Articles

| Nom   | Description  |
|---|--|
| Authentication certificate expire timestamp | Date d'expiration au plus tôt d'un certificat d'authentification actif et enregistré.  |
| Authentication certificate status not good  | Indique si un certificat d'authentification actif et enregistré a une réponse OCSP avec un état autre que Good.                  |
| CPU idle                                    | Pourcentage d'inactivité du processeur au cours des 15 dernières secondes. Calculé de la même manière que l'utilitaire UNIX top. |
| CPU load average                            | Moyenne de la charge du processeur au cours de la dernière minute.   |
| Disk free                                   | Nombre d'octets disponibles sur la partition où se trouve le répertoire racine.  |
| Disk free in %                              | Le pourcentage d'octets disponibles sur la partition où se trouve le répertoire racine.  |
| Disk total                                  | Taille de la partition où se trouve le répertoire racine.  |
| Java VM operable                            | Indique si la Java VM est opérationnelle.  |
| Memory free                                 | Mémoire libre disponible.  |
| Memory total                                | La taille de la mémoire.   |
| [nginx   postgresql]: status                | État du service [nginx   postgresql].  |

| Nom  | Description  |
|--|--|
| [nginx   postgresql]: uptime   | Temps de fonctionnement du service [nginx   postgresql].   |
| NTP synchronized   | Indique si la synchronisation du temps NTP est active.   |
| Operating system and version   | Système d'exploitation et version.   |
| Signing certificate expire timestamp   | Date d'expiration au plus tôt d'un certificat de signature actif.  |
| Signing certificate OCSP status not good   | Indique si un certificat de signature actif a une réponse OCSP avec un état autre que Good.  |
| Statistics period  | Durée de la période statistique.   |
| Swap free  | Espace swap libre disponible.  |
| Swap total   | La taille du swap.   |
| Traffic inbound  | Le trafic réseau entrant pendant la période de statistiques.   |
| Traffic outbound   | Le trafic réseau sortant pendant la période de statistiques.   |
| Uptime   | Temps de fonctionnement du système.  |
| [uxp-addon-metaservices   uxp-addon-monitor   uxp-addon-pkcs11   uxp-confclient   uxp-identity-provider-rest-api   uxp-proxy   uxp-securityserver-rest-api   uxp-securityserver-ui   uxp-securityserver   uxp-verifier]: version | Version du paquet [uxp-addon-metaservices   uxp-addon-monitor   uxp-addon-pkcs11   uxp-confclient   uxp-identity-provider-rest-api   uxp-proxy   uxp-securityserver-rest-api   uxp-securityserver-ui   uxp-securityserver   uxp-verifier]. |
| [uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api]: status                | État du service [uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api].                 |

| Nom  | Description   |
|--|---|
| <code>[uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api]: uptime</code> | Temps de fonctionnement du service <code>[uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api]</code> . |
| UXP error messages count   | Le nombre de demandes échouées au cours de la période statistique.  |
| UXP error messages count since restart   | Nombre de demandes ayant échoué depuis le redémarrage du serveur de sécurité.   |
| UXP error messages last timestamp  | L'horodatage de la dernière demande qui a échoué.   |
| UXP global configuration download timestamp  | Date du dernier téléchargement de la configuration globale valide.  |
| UXP messages count   | Le nombre de demandes réussies et échouées au cours de la période statistique.  |
| UXP messages count since restart   | Nombre de demandes réussies et échouées depuis le redémarrage du serveur de sécurité.   |
| UXP messages last timestamp  | L'horodatage de la dernière demande (réussie ou échouée).   |
| Virtualization platform  | Le nom de la plate-forme de virtualisation.   |

## Déclencheurs

| Nom   | Description   |
|---|---|
| Authentication certificate expires in less than 30 days       | Alerte lorsqu'un certificat d'authentification actif et enregistré expire dans moins de 30 jours.                         |
| Authentication certificate OCSP response status is not 'Good' | Alerte lorsqu'un certificat d'authentification actif et enregistré reçoit une réponse OCSP dont l'état n'est pas « bon ». |
| Disk free is less than 5%                                     | Alerte lorsque l'espace libre du disque est inférieur à 5 %.  |
| Latest valid GC has been downloaded more than 1 hour ago      | Alerte lorsque la dernière configuration globale valide a été téléchargée il y a plus d'une heure.                        |

| Nom   | Description   |
|---|---|
| Monitoring data is not updated by MS  | Alerte lorsque les données de surveillance ne sont pas mises à jour par le Serveur de surveillance UXP pendant au moins trois périodes consécutives de mise à jour par défaut. La période de mise à jour par défaut est de 3 minutes.                 |
| [nginx   postgresql ] is down   | Alerte lorsque le service [nginx   postgresql] est inactif/mort.  |
| Signing certificate expires in less than 30 days  | Alerte lorsqu'un certificat de signature actif expire dans moins de 30 jours.   |
| Signing certificate OCSP response status is not 'Good'  | Alerte lorsqu'un certificat de signature actif reçoit une réponse OCSP dont l'état n'est pas « bon ».   |
| [uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api] is down | Alerte lorsque le service [uxp-confclient   uxp-identity-provider-rest-api   uxp-messagelog-archiver   uxp-messagelog-timestamper   uxp-monitor   uxp-ocsp-cache   uxp-proxy   uxp-securityserver-rest-api   uxp-verifier-rest-api] est inactif/mort. |
| UXP messages rate exceeds threshold   | Alerte lorsque le taux de messages UXP dépasse le seuil défini de 200 requêtes par seconde au cours de la période statistique.  |

## 5.4.2. Modèle Zabbix : Serveur de registre UXP par MS

Le modèle UXP Registry Server by MS, situé sur le serveur de surveillance /usr/share/uxp/templates/zabbix/7.0/template\_app\_uxp\_registry\_server\_by\_ms.yaml, fournit les éléments de surveillance et les déclencheurs suivants :

### Articles

| Nom                                  | Description  |
|--------------------------------------|--|
| Global configuration available       | Indique si la configuration globale est disponible sur le serveur de registre. |
| Global configuration expiration date | La date d'expiration de la configuration globale.                              |
| License file exists                  | Indique si le fichier de licence existe pour le serveur de registre.           |

### Déclencheurs



| Nom                                     | Description  |
|---|--|
| Global configuration generation stopped | Alerte lorsque la génération de la configuration globale a été arrêtée, c'est-à-dire que la date d'expiration de la configuration globale reste inchangée sur les 5 derniers points de données.  |
| Global configuration is expiring        | Alerte lorsque la configuration globale expire dans moins de 24 heures.  |
| Global configuration is not available   | Alerte lorsque la configuration globale n'est pas disponible, c'est-à-dire que la configuration globale n'est pas disponible sur les 5 derniers points de données.   |
| Monitoring data is not updated by MS    | Alertes lorsque les données de surveillance ne sont pas mises à jour par le Serveur de surveillance UXP pendant au moins trois périodes consécutives de mise à jour par défaut. La période de mise à jour par défaut est de 3 minutes. |

## 5.5. Configurer l'agent Zabbix sur les Serveurs de registre

Pour collecter les données de surveillance environnementale définies dans le modèle natif Zabbix Linux by Zabbix agent à partir des serveurs de registres, vous devez installer et configurer l'agent Zabbix sur chaque serveur de registre. Cet agent répondra aux demandes du serveur Zabbix. Par défaut, l'agent Zabbix écoute les connexions sur le port 10050. Pour des informations détaillées sur la configuration de l'agent Zabbix, reportez-vous à la section correspondante dans la [documentation Zabbix](#).



Assurez-vous que le paramètre `enable_registry_servers_os_linux_template` est défini sur `true` dans le fichier de configuration `/etc/uxp/monitor-agent.ini` sur le serveur de surveillance.

### 5.5.1. Installer et configurer l'agent Zabbix

#### Sur le serveur de registre

1. Installez le paquet de configuration du dépôt Zabbix :
  - Ubuntu 22.04 LTS

```
wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/\
zabbix-release_7.0-2+ubuntu22.04_all.deb

sudo dpkg -i zabbix-release_7.0-2+ubuntu22.04_all.deb
```

2. Mettez à jour la liste des paquets et installez l'agent Zabbix :

```
sudo apt update  
sudo apt install zabbix-agent
```

3. Spécifiez l'adresse IP ou le nom d'hôte (qui se résout en adresse IP via DNS) du serveur Zabbix en définissant le paramètre `Server` dans le fichier de configuration principal de l'agent Zabbix situé sous `/etc/zabbix/zabbix_agentd.conf`:

```
Server=<zabbix-server-name-or-IP>
```



Si vous utilisez la solution de haute disponibilité du serveur Zabbix, assurez-vous que toutes les adresses des nœuds de la grappe sont ajoutées au paramètre `Server`, séparées par des virgules.

4. Redémarrez l'agent Zabbix après avoir modifié la configuration :

```
sudo systemctl restart zabbix-agent
```

Enfin, vérifiez dans l'interface utilisateur Zabbix que les données de surveillance du serveur de registre sont bien reçues en accédant à **Monitoring** → **Latest data**.

## 6. Configurer Elasticsearch et Kibana

Configurez Elasticsearch et Kibana pour stocker, analyser et visualiser les données de surveillance opérationnelle et/ou leurs statistiques provenant des serveurs de sécurité.



Par défaut, la collecte des données de surveillance opérationnelle est activée, tandis que la collecte des statistiques des données de surveillance opérationnelle est désactivée. Toutefois, vous pouvez choisir les données à collecter, le cas échéant. Pour modifier ces paramètres, reportez-vous à la section [Activer/désactiver la collecte de données de surveillance opérationnelle ou de ses statistiques](#).


### 6.1. Document de données opérationnelles dans Elasticsearch

Le serveur de sécurité collecte des données opérationnelles et stocke un enregistrement de données pour chaque message UXP échangé. Le document de données opérationnelles correspondant dans Elasticsearch comporte les champs suivants :

| Champ                          | Type de données | Description  |
|--------------------------------|-----------------|--|
| client_member_class            | keyword         | Classe du membre UXP (client).   |
| client_member_code             | keyword         | Code du membre UXP (client).   |
| client_security_server_address | keyword         | Adresse externe du serveur de sécurité du client (IP ou nom) définie dans la configuration globale.  |
| client_subsystem_code          | keyword         | Code du sous-système du membre UXP (client).   |
| client_xroad_instance          | keyword         | Identifiant de l'instance utilisée par le client.  |
| message_id                     | keyword         | Identifiant unique du message.   |
| message_issue                  | keyword         | Identifiant interne du client d'un fichier ou d'un document lié au service.  |
| message_protocol_version       | keyword         | Version du protocole du message UXP.   |
| message_user_id                | keyword         | Code personnel du client qui a initié la demande.  |
| monitoring_data_ts             | date            | Heure UTC (précision à la seconde près) de réception de l'enregistrement des données opérationnelles par l'agent de surveillance proxy du serveur de sécurité. |
| request_attachment_count       | integer         | Nombre de pièces jointes dans la demande SOAP.   |

| Champ                     | Type de données | Description   |
|---------------------------|-----------------|---|
| request_in_ts             | date            | <ul style="list-style-type: none"> <li>Sur le serveur de sécurité du client : Heure UTC (précision à la milliseconde près) à laquelle la demande a été reçue par le serveur de sécurité du client.</li> <li>Sur le serveur de sécurité du fournisseur de services : Heure UTC (précision à la milliseconde près) à laquelle la demande a été reçue par le serveur de sécurité du fournisseur de services.</li> </ul>  |
| request_mime_size         | long            | Taille du conteneur MIME de la demande SOAP (avec pièces jointes) en octets.  |
| request_out_ts            | date            | <ul style="list-style-type: none"> <li>Sur le serveur de sécurité du client : Heure UTC (précision à la milliseconde près) à laquelle la requête a été envoyée depuis le serveur de sécurité du client vers le serveur de sécurité du fournisseur de services.</li> <li>Sur le serveur de sécurité du fournisseur de services : Heure UTC (précision à la milliseconde près) à laquelle la requête a été envoyée depuis le serveur de sécurité du fournisseur de services.</li> </ul> |
| request_soap_size         | long            | Taille de la demande SOAP / de la charge utile de la demande REST en octets.  |
| response_attachment_count | integer         | Nombre de pièces jointes dans la réponse SOAP.  |
| request_type              | keyword         | Type de demande (SOAP versus REST).   |
| response_in_ts            | date            | <ul style="list-style-type: none"> <li>Sur le serveur de sécurité du client : Heure UTC (précision à la milliseconde près) à laquelle la réponse a été reçue par le serveur de sécurité du client.</li> <li>Sur le serveur de sécurité du fournisseur de services : Heure UTC (précision à la milliseconde près) à laquelle la réponse a été reçue par le serveur de sécurité du fournisseur de services.</li> </ul>  |
| response_mime_size        | long            | Taille du conteneur MIME de la réponse SOAP (avec pièces jointes) en octets.  |

| Champ                           | Type de données | Description  |
|---------------------------------|-----------------|--|
| response_out_ts                 | date            | <ul style="list-style-type: none"> <li>Sur le serveur de sécurité du client : Heure UTC (précision à la milliseconde près) à laquelle la réponse a été envoyée depuis le serveur de sécurité du client vers le système d'information du client.</li> <li>Sur le serveur de sécurité du fournisseur de services : Heure UTC (précision à la milliseconde près) à laquelle la réponse a été envoyée depuis le serveur de sécurité du fournisseur de services.</li> </ul> |
| response_soap_size              | long            | Taille de la réponse SOAP / de la charge utile de la réponse REST en octets.   |
| security_server_internal_ip     | keyword         | Adresse IP interne du serveur de sécurité.   |
| security_server_member_class    | keyword         | Classe membre du membre UXP (propriétaire du serveur de sécurité).   |
| security_server_member_code     | keyword         | Code membre du membre UXP (propriétaire du serveur de sécurité).   |
| security_server_server_code     | keyword         | Code du serveur de sécurité.   |
| security_server_type            | keyword         | Type de serveur de sécurité (Client ou Producer).  |
| security_server_xroad_instance  | keyword         | Identifiant de l'instance utilisée par le serveur de sécurité.   |
| service_code                    | keyword         | Code du service.   |
| service_member_class            | keyword         | Classe membre du membre UXP (fournisseur de services).   |
| service_member_code             | keyword         | Code membre du membre UXP (fournisseur de services).   |
| service_security_server_address | keyword         | Adresse externe du serveur de sécurité du fournisseur de services (IP ou nom) définie dans la configuration globale.   |
| service_subsystem_code          | keyword         | Code sous-système du membre UXP (fournisseur de services).   |
| service_version                 | keyword         | Version du service.  |
| service_xroad_instance          | keyword         | Identifiant de l'instance utilisée par le service.   |
| soap_fault_code                 | keyword         | Code d'erreur SOAP en cas de réception de SoapFault.   |

| Champ  | Type de données | Description   |
|--|-----------------|---|
| soap_fault_string  | keyword         | Raison de l'erreur SOAP dans le cas où SoapFault a été reçu.      |
| succeeded  | boolean         | true, si la médiation de la demande a réussi, false sinon.        |
| <div>  <p>La charge utile de la réponse REST n'est pas analysée, le code d'état HTTP autre que 2XX est considéré comme un échec.</p> </div> |                 |   |
| transaction_id   | keyword         | Identifiant de transaction généré par le Serveur de sécurité UXP. |

## 6.2. Document sur les statistiques des données opérationnelles dans Elasticsearch

Les statistiques sur les données opérationnelles sont calculées par le serveur de sécurité sur la base des données opérationnelles stockées. Le document statistique des données opérationnelles correspondant dans Elasticsearch comporte les champs suivants :

| Champ                   | Type de données | Description  |
|-------------------------|-----------------|--|
| client_id               | keyword         | Identifiant client.  |
| duration                | long            | Durée de la période statistique en secondes.   |
| last_monitoring_data_ts | date            | L'horodatage Unix (en secondes) indique quand l'agent de surveillance proxy a reçu le dernier enregistrement de données opérationnelles utilisé dans le calcul de la période de statistiques actuelle. |
| server_id               | keyword         | Identifiant du serveur de sécurité.  |
| server_type             | keyword         | Type de serveur de sécurité (C – client, P – producteur).  |
| service_id              | keyword         | Identifiant du service.  |
| start_ts                | date            | Heure UTC en secondes à laquelle la période de statistiques a commencé.  |
| succeeded_count         | long            | Nombre de transactions réussies.   |
| total_count             | long            | Nombre total de transactions.  |

## 6.3. Installer Elasticsearch et Kibana

## Paramètres système requis pour le serveur Elasticsearch/Kibana

- Système d'exploitation Ubuntu 24.04 ou 22.04 Long-Term Support (LTS) sur une plateforme 64 bits ;
- 8 Go de RAM ;



Pour les déploiements plus importants, envisagez d'utiliser 64 Go ou plus de RAM.



Par défaut, Elasticsearch définit automatiquement la taille du tas de la JVM en fonction des rôles et de la mémoire totale d'un nœud. L'utilisation du dimensionnement par défaut est recommandée pour la plupart des environnements de production, voir [\[Elastic-Heap\]](#).

- 100 Go d'espace sur le disque dur. Pour les déploiements plus importants, envisagez d'utiliser des disques SSD pour améliorer les performances d'E/S.



Les besoins en stockage dépendent fortement du volume de données que vous envisagez d'indexer et de stocker.

Bien qu'il soit difficile de prévoir la taille exacte des données de surveillance opérationnelle, on estime généralement que chaque million d'enregistrements représente environ 250 Mo. Chaque enregistrement correspond à une seule transaction sur le serveur de sécurité.

L'estimation de la taille exacte des statistiques des données de surveillance opérationnelle est encore plus complexe, car elle dépend de la période de statistiques configurée (par défaut : 15 minutes) et de la distribution des demandes dans le temps. En moyenne, la taille des données est d'environ 70 Mo pour chaque million d'enregistrements. Chaque enregistrement représente entre 1 et N transactions agrégées du serveur de sécurité, N variant en fonction de la durée de la période statistique et de la charge de transactions. Une période statistique plus longue ou un nombre plus élevé de demandes pour la même combinaison unique de client et de service au cours de cette période entraîne l'agrégation d'un plus grand nombre de transactions dans un seul enregistrement statistique.

Utilisez le paquet `uxp-monitor-analytics` pour installer et configurer les paquets Elasticsearch et Kibana avec les paramètres suggérés par défaut pour collecter les données opérationnelles UXP.

Si vous souhaitez configurer le serveur de surveillance pour qu'il communique avec une instance existante d'Elasticsearch, ignorez cette section. Reportez-vous à la section [Connecter Elasticsearch au Serveur de surveillance](#) pour obtenir des instructions sur la configuration.



Il est recommandé d'installer Elasticsearch sur un serveur distinct de celui qui exécute le serveur de surveillance.

Pour installer les logiciels Elasticsearch et Kibana sur Ubuntu, suivez les étapes suivantes :

1. Ajoutez la clé de signature du dépôt UXP au répertoire `/usr/share/keyrings` :

```
curl https://repo.cyber.ee/uxp/pub.gpg | gpg --dearmor | \
sudo tee /usr/share/keyrings/uxp-pub.gpg >/dev/null
```

2. Ajoutez l'URL du dépôt des paquets UXP et l'emplacement de la clé de signature au fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/ stable main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Ajoutez les informations d'authentification du dépôt UXP au fichier `/etc/apt/auth.conf.d/uxp.conf` :

```
machine repo.cyber.ee
  login <repo-username>
  password <repo-password>
```

4. Ajouter la clé de signature du dépôt Elasticsearch au répertoire `/usr/share/keyrings` :

```
curl https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --dearmor | \
sudo tee /usr/share/keyrings/elastic-pub.gpg >/dev/null
```

5. Ajoutez l'URL du dépôt du paquet Elasticsearch 9.x et l'emplacement de la clé de signature à `/etc/apt/sources.list.d/elastic-9.x.list` :



Si Elasticsearch 8.x est installé sur votre système, veuillez consulter les [instructions de mise à niveau vers la](#) version 9.x avant de modifier le dépôt Elasticsearch vers la version 9.x.

```
echo "deb [signed-by=/usr/share/keyrings/elastic-pub.gpg] \
https://artifacts.elastic.co/packages/9.x/apt stable main" | \
sudo tee /etc/apt/sources.list.d/elastic-9.x.list
```

6. Exécutez les commandes suivantes pour installer le paquet Analyse des données de surveillance UXP. Cette commande installera les paquets `elasticsearch` et `kibana` sur votre système :

```
sudo apt update
sudo apt install uxp-monitor-analytics
```

Les services `elasticsearch` et `kibana` seront activés et démarrés automatiquement.

7. Assurez-vous que le fichier de configuration Elasticsearch `/etc/elasticsearch/elasticsearch.yml` contient les entrées suivantes ajoutées par le paquet `uxp-monitor-analytics` :



```
cluster.name: uxp
node.name: ${HOSTNAME}
network.host: 0.0.0.0
```

8. Pour modifier le mot de passe généré pour le superutilisateur intégré de `elastic`, exécutez la commande suivante :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic -i
```

9. Par défaut, le serveur Kibana se lie à `localhost`, ce qui signifie que les machines distantes ne peuvent pas se connecter. Pour autoriser les connexions d'utilisateurs distants, modifiez le fichier `/etc/kibana/kibana.yml`. Décommentez le paramètre `server.host` et définissez sa valeur de `localhost` à une adresse IP non bloquée :

```
server.host: 0.0.0.0
```

10. Redémarrez les services après les changements de configuration :

```
sudo systemctl restart elasticsearch kibana
```

11. Assurez-vous que l'interface utilisateur (UI) de Kibana à l'adresse `http://<server-address>:5601/` est accessible dans un navigateur Web.
12. Générez un jeton d'inscription pour l'instance Kibana en exécutant la commande suivante :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

13. Dans l'interface utilisateur Kibana, collez le jeton d'inscription généré à partir du terminal et cliquez sur **Configure Elastic**.
14. Obtenez le code de vérification de Kibana en exécutant la commande suivante :

```
sudo /usr/share/kibana/bin/kibana-verification-code
```

15. Dans l'interface utilisateur de Kibana, collez le code de vérification du terminal et cliquez sur **Verify**.
16. Connectez-vous à l'interface utilisateur Kibana en tant qu'utilisateur `elastic` en utilisant le mot de passe précédemment généré ou mis à jour. Si la boîte de dialogue **Welcome to Elastic** s'affiche, cliquez sur **Explore on my own** pour continuer.



À partir de la version 8.x, Elasticsearch utilise par défaut HTTPS pour les communications sécurisées, à la fois pour son API et pour le trafic interne entre nœuds (les paramètres sont écrits sur le site `/etc/elasticsearch/elasticsearch.yml`). De plus, l'authentification de base est activée par défaut. Cependant, la connexion à Kibana se fait par défaut en HTTP pour des raisons de simplicité lors de la configuration initiale.

Nous recommandons de configurer la connexion entre Kibana et le navigateur Web pour utiliser HTTPS au lieu de HTTP par défaut (voir la section [Chiffrement du trafic entre](#)

le navigateur Web et Kibana).

Reportez-vous à la documentation [\[Elastic-Security\]](#) pour obtenir des informations plus détaillées.



Pour garantir la redondance et la disponibilité du serveur Elasticsearch, vous pouvez utiliser une grappe Elasticsearch avec plusieurs nœuds (voir la section [Installer une grappe Elasticsearch à plusieurs nœuds](#)).

Reportez-vous à la documentation [\[Elastic-Cluster\]](#) pour obtenir des informations plus détaillées.

### 6.3.1. Chiffrement du trafic entre le navigateur Web et Kibana

Pour configurer une connexion HTTPS entre le navigateur Web et Kibana, obtenez d'abord un certificat TLS valide pour le serveur Kibana.

Utilisez une autorité de certification de confiance ou l'autorité de certification interne de votre organisation pour signer le certificat TLS.

Vous pouvez créer une CSR à l'aide de l'outil `elasticsearch-certutil` sur le serveur Elasticsearch/Kibana en exécutant une commande similaire à la suivante, où `--name` spécifie le nom de la demande de certificat à générer, tandis que `--dns` et `--ip` spécifient facultativement une liste de noms DNS et d'adresses IP séparés par des virgules, respectivement, pour le Nom alternatif du sujet (SAN) :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-certutil csr \
--name kibana-server --dns <server-DNS-address> --ip <server-IP-address>
```



Vous pouvez également créer un certificat TLS auto-signé en exécutant une commande similaire à la suivante, où `--name` spécifie le nom du certificat à générer, `--days` définit la validité du certificat en jours, et `--dns` et `--ip` définissent éventuellement des listes de noms DNS et d'adresses IP pour le SAN :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-certutil cert \
--pem --self-signed --name kibana-server --dns <server-DNS-address> \
--ip <server-IP-address> --days 3650
```

Par défaut, les fichiers des clés et des certificats générés (`kibana-server.key` et `kibana-server.crt`) sont regroupés dans le fichier `/usr/share/elasticsearch/certificate-bundle.zip`. Vous pouvez extraire ces fichiers dans le répertoire `./kibana-server` en exécutant la commande suivante :

```
sudo unzip /usr/share/elasticsearch/certificate-bundle.zip
```

Effectuez ensuite les étapes suivantes sur le serveur Kibana :

1. Copiez les fichiers de certificats TLS et de clés privées obtenus, tels que `kibana-server.crt` et `kibana-server.key`, dans le répertoire `/etc/kibana/` du serveur Kibana. Si vous avez généré des certificats avec `elasticsearch-certutil`, déplacez les fichiers générés en exécutant la commande suivante :

```
sudo mv ./kibana-server/kibana-server.* /etc/kibana/
```

2. Définissez la propriété et les autorisations correctes pour ces fichiers en exécutant les commandes suivantes :

```
sudo bash -c 'chown root:kibana /etc/kibana/kibana-server.*'
sudo bash -c 'chmod 640 /etc/kibana/kibana-server.*'
```

3. Sur le serveur Kibana, ajoutez les lignes suivantes à `/etc/kibana/kibana.yml` pour activer TLS pour les connexions entrantes et spécifier les chemins d'accès au certificat du serveur et à la clé privée non chiffrée :

```
server.ssl.enabled: true
server.ssl.certificate: /etc/kibana/kibana-server.crt
server.ssl.key: /etc/kibana/kibana-server.key
```

4. Redémarrez Kibana en exécutant la commande suivante :

```
sudo systemctl restart kibana
```



Après avoir effectué ces modifications, vous devez toujours accéder à Kibana via HTTPS. Par exemple, `https://<server-address>:5601/`.

### 6.3.2. Installer une grappe Elasticsearch à plusieurs nœuds

Pour garantir la redondance et la disponibilité du serveur Elasticsearch, envisagez d'utiliser une grappe Elasticsearch avec plusieurs nœuds.

Lorsque vous démarrez une instance d'Elasticsearch, vous démarrez un nœud. Une grappe Elasticsearch est un groupe de nœuds ayant le même attribut `cluster.name`. Lorsque des nœuds rejoignent ou quittent une grappe, celle-ci se réorganise automatiquement pour répartir uniformément les données entre les nœuds disponibles. Si vous exécutez une seule instance d'Elasticsearch, vous disposez d'une grappe composée d'un seul nœud.



La documentation d'Elasticsearch recommande généralement d'avoir au moins trois nœuds éligibles au statut de maître (par défaut) dans un environnement de production.

Elasticsearch utilise le quorum pour assurer la haute disponibilité et la cohérence de l'état de la grappe. Le quorum est le nombre minimum de nœuds éligibles au statut de maître (la moitié du nombre total de nœuds, plus un) qui doivent se mettre d'accord sur les modifications de l'état de la grappe (par exemple, ajout/suppression de nœuds, création/suppression d'index). Cela évite les scénarios de « split-brain », dans lesquels

plusieurs nœuds assument le rôle de maître en raison d'un partitionnement du réseau.

Pour garantir que la grappe reste disponible, vous ne devez pas arrêter la moitié ou plus des nœuds éligibles au statut de maître en même temps. Tant que plus de la moitié des nœuds sont disponibles, la grappe peut continuer à fonctionner normalement.

Voir [\[Elastic-Cluster\]](#) pour des informations plus détaillées.

Pour inscrire un nœud supplémentaire sur votre grappe, procédez comme suit :

1. Sur le nouveau nœud, configurez le dépôt de paquets en effectuant les étapes 1 à 5 de la section [Installer Elasticsearch et Kibana](#).
2. Installez uniquement le paquet `elasticsearch` en exécutant les commandes suivantes :

```
sudo apt update
sudo apt install elasticsearch
```

3. Créez un jeton d'inscription avec l'outil `elasticsearch-create-enrollment-token` sur **n'importe quel nœud existant** de votre grappe en exécutant la commande suivante :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node
```

4. Sur le nouveau nœud, utilisez le jeton d'inscription généré pour le reconfigurer en exécutant la commande suivante :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-reconfigure-node \
--enrollment-token <generated-token>
```



Le mot de passe du superutilisateur intégré à `elastic` est défini sur la même valeur que sur le nœud où le jeton d'inscription a été généré.

5. Ajoutez les entrées suivantes au fichier de configuration `/etc/elasticsearch/elasticsearch.yml` :

```
cluster.name: uxp
node.name: ${HOSTNAME}
network.host: 0.0.0.0
```

6. Mettez à jour la liste `discovery.seed_hosts` dans le fichier de configuration `/etc/elasticsearch/elasticsearch.yml` sur tous les nœuds. Cette liste spécifie les adresses des nœuds éligibles au statut de maître dans la grappe, ce qui permet au nouveau nœud de découvrir les nœuds existants de la grappe et vice versa. Sur les nœuds existants, ajoutez l'adresse du nouveau nœud à la liste. Sur le nouveau nœud, ajoutez les adresses de tous les nœuds existants (si elles n'ont pas déjà été ajoutées automatiquement). Par exemple :

```
discovery.seed_hosts: ["<node1-host>", "<node2-host>"]
```

où `<node1-host>` et `<node2-host>` sont les adresses des autres nœuds de la grappe. Chaque adresse peut être une adresse IP ou un nom d'hôte (qui se résout en adresse IP via DNS). Le port est facultatif et sa valeur par défaut est 9300.

- Redémarrez le service `elasticsearch` sur tous les nœuds en exécutant la commande :

```
sudo systemctl restart elasticsearch
```

- Sur le nouveau nœud, activez le service `elasticsearch` en exécutant la commande :

```
sudo systemctl enable elasticsearch
```

- Vérifiez les nœuds de la grappe dans votre navigateur Web en naviguant vers `https://<added-node-address>:9200/_cat/nodes?v` et en vous authentifiant avec le nom d'utilisateur `elastic` et son mot de passe. Tous les nœuds de la grappe doivent être répertoriés de la manière suivante :

| ip           | heap.percent | ram.percent | cpu | load_1m | load_5m | load_15m | node.role     |
|--------------|--------------|-------------|-----|---------|---------|----------|---------------|
| master name  |              |             |     |         |         |          |               |
| 192.168.56.1 | 44           | 97          | 1   | 0.30    | 0.34    | 0.16     | cdfhilmrstw - |
| my-es-node-1 |              |             |     |         |         |          |               |
| 192.168.56.2 | 26           | 96          | 6   | 0.27    | 0.16    | 0.06     | cdfhilmrstw * |
| my-es-node-2 |              |             |     |         |         |          |               |

- Procédez à l'installation en effectuant les étapes 6 et 9 à 16 de la procédure d'installation, comme indiqué dans la section [Installer Elasticsearch et Kibana](#).
- Configurez une connexion HTTPS entre le navigateur Web et Kibana en suivant les étapes de la section [Chiffrement du trafic entre le navigateur Web et Kibana](#).



Une fois la grappe **multi-nœuds** formée, supprimez le paramètre `cluster.initial_master_nodes` du fichier de configuration `/etc/elasticsearch/elasticsearch.yml` du nœud initial et redémarrez le service `elasticsearch`.

Si vous laissez `cluster.initial_master_nodes` en place une fois que la grappe a été formée, il y a un risque qu'une mauvaise configuration future entraîne le démarrage d'une nouvelle grappe en même temps que la grappe existante. Il peut être impossible de sortir de cette situation sans perdre des données.

## 6.4. Connecter Elasticsearch au Serveur de surveillance

Pour interagir avec Elasticsearch, le serveur de surveillance a besoin d'informations d'authentification, notamment d'un nom d'utilisateur et d'un mot de passe avec les autorisations nécessaires (y compris l'accès aux données de surveillance opérationnelle et aux indices statistiques des données de surveillance opérationnelle décrits à la section [Configuration du serveur de surveillance](#)). Reportez-vous à la section [Créer un utilisateur Elasticsearch pour le serveur de surveillance](#) pour créer un utilisateur Elasticsearch approprié.

s'il n'en existe pas déjà un.

Reportez-vous à la section [Configuration du serveur de surveillance](#) pour obtenir des instructions sur la configuration du serveur de surveillance afin qu'il interagisse avec Elasticsearch.



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), connectez le ou les nœuds supplémentaires du serveur de surveillance à la même grappe Elasticsearch à l'aide des mêmes informations d'identification.

### 6.4.1. Créer un utilisateur Elasticsearch pour le serveur de surveillance

Dans l'interface utilisateur Kibana, connectez-vous en tant que superutilisateur et créez un nouvel utilisateur avec les privilèges minimaux requis pour le serveur de surveillance :



L'utilisateur créé doit avoir au moins :

1. Les privilèges `create_index`, `manage`, `read`, `view_index_metadata` et `write` sur l'index des données de surveillance opérationnelle (par défaut `uxp-request`), sur l'index des statistiques des données de surveillance opérationnelle (par défaut `uxp-stats`) et sur l'index système `uxp_monitoring_server_master_doc` ;
2. le privilège `monitor` de la grappe.

Pour en savoir plus sur l'authentification des utilisateurs et les privilèges, consultez la documentation Elasticsearch [\[Elastic-Roles\]](#).

1. Créez un nouveau rôle pour l'utilisateur pour le serveur de surveillance en naviguant sur **Management** → **Stack Management** → **Security** → **Roles**, puis en cliquant sur **Create role**.
2. Saisissez un nom de rôle (par exemple, `uxp_ms_client`) et une description de rôle (par exemple, `Grants privileges to UXP MS`).
3. Dans la section **Cluster privileges** de la carte **Elasticsearch**, sélectionnez le privilège requis `monitor`.
4. Dans la section **Index privileges** de la carte **Elasticsearch**, entrez les modèles d'index et attribuez les privilèges appropriés :
  - a. Entrez un modèle d'index pour les données de surveillance opérationnelle, tel que `uxp-request*`, puis sélectionnez les privilèges requis : `create_index`, `manage`, `read`, `view_index_metadata` et `write`.



Le caractère générique `*` dans le nom de l'index permet d'accéder à plusieurs index qui suivent un modèle de dénomination, généralement utilisé pour répartir les données dans des index distincts.

- b. Continuez à ajouter les mêmes privilèges pour l'index des statistiques des données de surveillance opérationnelle, tel que `uxp-stats*`, et pour l'index du système

`uxp_monitoring_server_master_doc`. Cliquez sur **Add index privilege** pour obtenir une autre ligne d'entrée.

c. Cliquez enfin sur **Create role**.

5. Créez un nouvel utilisateur en naviguant dans **Management** → **Stack Management** → **Security** → **Users**, puis en cliquant sur **Create user**.
6. Saisissez un nom d'utilisateur (par exemple, `uxp_ms`), un mot de passe et sélectionnez un rôle précédemment créé, tel que `uxp_ms_client`.
7. Cliquez enfin sur **Create user**.

## 6.4.2. Configuration du serveur de surveillance

Par défaut, le serveur de surveillance est configuré pour collecter des données opérationnelles, tandis que la collecte de statistiques sur les données opérationnelles est désactivée. Toutefois, la collecte de l'un ou l'autre type de données peut être désactivée ou activée (voir la section [Activer/désactiver la collecte de données de surveillance opérationnelle ou de ses statistiques](#)).

L'intervalle de collecte des deux types de données peut également être configuré séparément (voir la section [Changer les intervalles d'interrogation des données de surveillance](#)), de même que la période de statistiques des données opérationnelles (voir la section [Changer la période statistique des données de surveillance opérationnelle](#)).

Sur le serveur de surveillance, activez le transfert des données collectées vers le serveur Elasticsearch cible :

1. Copiez le certificat CA `/etc/elasticsearch/certs/http_ca.crt` du serveur Elasticsearch dans le répertoire `/etc/uxp/ssl` du serveur de surveillance.
2. Définissez la propriété et les autorisations correctes pour ce fichier en exécutant les commandes suivantes :

```
sudo chown root:uxp /etc/uxp/ssl/http_ca.crt
sudo chmod 640 /etc/uxp/ssl/http_ca.crt
```

3. Modifiez le fichier de configuration de `/etc/uxp/monitor-agent.ini` en ajoutant la section suivante `[elasticsearch]` similaire :

```
[elasticsearch]

address = 192.168.56.101
port = 9200
scheme = https
ca-cert-file = /etc/uxp/ssl/http_ca.crt

username = uxp_ms
password = *****

index = uxp-request
stats-index = uxp-stats
```





Par défaut, le serveur de surveillance effectue une vérification du nom d'hôte pour Elasticsearch pendant l'établissement de la connexion TLS.


Le tableau suivant répertorie les champs de configuration possibles de la section Elasticsearch.

Tableau 5. Paramètres d'Elasticsearch

| Champ           | Valeur par défaut | Explication   |
|-----------------|-------------------|---|
| address         |                   | Nom d'hôte (résolu en adresse IP via DNS) ou adresse IP du serveur Elasticsearch. <b>Obligatoire.</b>   |
| port            | 9200              | Le port sur lequel le serveur Elasticsearch écoute les demandes.  |
| scheme          | http              | Le schéma de connexion du client HTTP d'Elasticsearch. Les valeurs possibles sont http et https.  |
| ca-cert-file    |                   | Le nom de fichier (chemin absolu) du certificat de l'autorité de certification d'Elasticsearch (au format PEM ou DER). <b>Obligatoire</b> si le schéma https est utilisé. Le serveur de surveillance a besoin de ce certificat d'autorité de certification pour vérifier le certificat TLS du nœud Elasticsearch lors de l'établissement d'une connexion TLS. |
| verify-hostname | true              | Si le client HTTP Elasticsearch doit vérifier le nom d'hôte du serveur lors de l'établissement d'une connexion TLS dans le cas où le schéma https est utilisé.  |



| Champ                      | Valeur par défaut    | Explication   |
|----------------------------|----------------------|---|
| username                   |                      | <p>Le nom d'utilisateur Elasticsearch pour l'authentification de base. <b>Obligatoire</b> si l'authentification de base est utilisée.</p> <div>  <p>Assurez-vous que l'utilisateur Elasticsearch configuré dispose des privilèges requis pour les index configurés et pour l'index système.</p> </div>   |
| password                   |                      | Le mot de passe de l'utilisateur Elasticsearch pour l'authentification de base. <b>Obligatoire</b> si l'authentification de base est utilisée.  |
| cluster-nodes              | Liste vide           | Liste séparée par des virgules des noms des sections des nœuds de la grappe.  |
| index                      | uxp-request          | <p>Nom de l'index du document de données opérationnelles. Il peut éventuellement contenir un modèle de date pour répartir les données opérationnelles dans des index distincts. Les motifs sont basés sur une simple séquence de lettres et de symboles entourés d'accolades et précédés d'une marque de pourcentage (%{DATE_PATTERN}). Par exemple, uxp-request-%{yyyy.MM.dd}, uxp-request-%{M.y}-opdata, où y représente l'année, M le mois et d le jour du mois. Pour plus d'informations sur la syntaxe des modèles de date, consultez le chapitre « Modèles pour le formatage et l'analyse syntaxique » de la documentation Java <a href="#">[DATE-TIME-FORMATTER]</a>.</p> <div>  <p>Assurez-vous que l'utilisateur Elasticsearch configuré dispose des privilèges requis pour l'index configuré.</p> </div> |
| collection_start_timestamp | 1970-01-01T00:00:00Z | Horodatage (en secondes depuis le début de l'ère Unix ou selon la norme ISO 8601, par exemple « 2018-01-01T00:00:00Z ») de l'enregistrement des données de surveillance opérationnelle à partir duquel la collecte de données commence (facultatif, valeur par défaut : 1970-01-01T00:00:00Z).  |

| Champ                            | Valeur par défaut    | Explication  |
|----------------------------------|----------------------|--|
| stats-index                      | uxp-stats            | <p>Nom de l'index du document statistique des données opérationnelles. Il peut éventuellement contenir un modèle de date pour répartir les statistiques de données opérationnelles dans des index distincts. Les motifs sont basés sur une simple séquence de lettres et de symboles entourés d'accolades et précédés d'une marque de pourcentage (<code>%{DATE_PATTERN}</code>). Par exemple, <code>uxp-stats-%{yyyy.MM.dd}</code>, <code>uxp-stats-%{M.y}-data</code>, où <code>y</code> représente l'année, <code>M</code> le mois et <code>d</code> le jour du mois. Pour plus d'informations sur la syntaxe des modèles de date, consultez le chapitre « Modèles pour le formatage et l'analyse syntaxique » de la documentation Java <a href="#">[DATE-TIME-FORMATTER]</a>.</p> <div>  <p>Assurez-vous que l'utilisateur Elasticsearch configuré dispose des privilèges requis pour l'index configuré.</p> </div> |
| stats_collection_start_timestamp | 1970-01-01T00:00:00Z | <p>Horodatage (en secondes depuis le début de l'ère Unix ou selon la norme ISO 8601, par exemple « 2018-01-01T00:00:00Z ») de l'enregistrement des données de surveillance opérationnelle (<code>monitoring_data_ts</code>) à partir duquel la collecte des statistiques commence (facultatif, valeur par défaut : 1970-01-01T00:00:00Z).</p>  |

Après avoir mis à jour la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), connectez chaque nœud du serveur de surveillance au même Elasticsearch à l'aide des mêmes identifiants.



Le serveur de surveillance utilise son certificat TLS auto-signé `/etc/uxp/ssl/elasticsearch.crt` pour établir une connexion sécurisée avec le serveur Elasticsearch.



Le serveur de surveillance créera automatiquement les index configurés (par exemple, `uxp-request`, `uxp-stats`) sur le serveur Elasticsearch lorsqu'il enverra les données de surveillance appropriées pour la première fois.

### 6.4.3. Utiliser une grappe Elasticsearch à plusieurs nœuds

Lorsque vous utilisez une grappe Elasticsearch à plusieurs nœuds, vous pouvez configurer le serveur de surveillance pour qu'il se connecte à plusieurs nœuds Elasticsearch sur la même grappe. Si un nœud devient indisponible, le serveur de surveillance se connectera de manière transparente à un nœud disponible et continuera à fonctionner. Les demandes adressées aux hôtes disponibles seront acheminées selon un principe de chacun son tour.

Chaque nœud supplémentaire doit avoir sa propre section unique avec l'adresse du nœud et le port d'écoute dans le fichier de configuration `/etc/uxp/monitor-agent.ini`. Ces noms de section (séparés par des virgules) doivent être définis comme valeur du champ `cluster-nodes`. Par exemple :



Les nœuds de la grappe Elasticsearch configurés comme nœuds supplémentaires dans le paramètre `cluster-nodes` n'ont pas d'importance.

```
[elasticsearch]
address=192.168.56.1
port=9200

; ...

cluster-nodes=elasticsearch-node-2, elasticsearch-node-3

[elasticsearch-node-2]
address=192.168.56.2
port=9200

[elasticsearch-node-3]
address=192.168.56.3
port=9200
```



Après avoir mis à jour la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), connectez chaque nœud du serveur de surveillance à la même grappe Elasticsearch à l'aide des mêmes identifiants.



Assurez-vous que tous les nœuds configurés de la grappe Elasticsearch sont accessibles sur le réseau afin d'optimiser les performances et la fiabilité du système de surveillance.

Si aucun des nœuds n'est accessible, le serveur de surveillance ne parviendra pas à transmettre les données à la grappe Elasticsearch. Dans le cas d'une grappe de serveurs de surveillance, si le nœud maître du serveur de surveillance pour Elasticsearch ne peut atteindre aucun nœud Elasticsearch, un autre nœud de serveur de surveillance tentera

d'assumer le rôle de maître pour Elasticsearch (voir [Haute disponibilité du serveur de surveillance](#)). Toutefois, si tous les autres nœuds du serveur de surveillance sont hors service en même temps, la transmission des données vers la grappe Elasticsearch échouera.

## 6.5. Configurer Kibana pour l'analyse

Les données opérationnelles et les statistiques sur les données opérationnelles comprennent des enregistrements provenant à la fois des serveurs de sécurité côté client et côté service, représentant la même transaction au sein du système distribué. Si vous comptez les enregistrements dans Kibana, les doublons seront également inclus dans le décompte. Dans le cas des données opérationnelles, vous pouvez éviter les doublons en filtrant les enregistrements pour n'inclure que ceux provenant du serveur de sécurité côté client, c'est-à-dire ceux dont le champ `security_server_type` a la valeur `Client`. Pour les statistiques sur les données opérationnelles, filtrez les enregistrements dont le champ `server_type` a la valeur `C`.

### 6.5.1. Créer une vue de données pour les données opérationnelles / statistiques de données opérationnelles

Les vues de données identifient les données Elasticsearch que vous souhaitez analyser dans Kibana. Elles peuvent cibler un seul index, plusieurs index ou tous les index contenant vos données de surveillance.



Il n'est pas possible de créer une vue de données dans Kibana pour un index qui n'existe pas encore dans Elasticsearch.

Le serveur de surveillance crée ses index configurés dans Elasticsearch lorsqu'il envoie les données de surveillance appropriées pour la première fois. Pour afficher la liste des index existants, accédez à **Management** → **Stack Management** → **Data** → **Index Management** dans l'interface utilisateur Kibana.

Créez une vue de données pour les données opérationnelles et une autre pour les statistiques des données opérationnelles, si les données appropriées sont collectées.



Lors de l'importation de l'exemple de tableau de bord ou de visualisations UXP, la vue de données `uxp-visualizations-index` pour le modèle d'index de données opérationnelles `uxp-request*`, avec le champ temporel `request_in_ts` et les champs scriptés supplémentaires requis par les visualisations, est automatiquement créée. Vous pouvez utiliser cette vue de données ou en créer une nouvelle pour explorer les données opérationnelles.

Pour créer une vue de données dans l'interface utilisateur Kibana, procédez comme suit :

1. Accédez à **Management** → **Stack Management** → **Kibana** → **Data Views**, puis cliquez sur **Create data view**.
2. Configurez les champs comme suit :

- a. **Name** – saisissez le nom de la vue de données (par exemple, `uxp-request`, `uxp-stats`).
- b. **Index pattern** – saisissez `uxp-request*` (index des données opérationnelles par défaut) ou `uxp-stats*` (index des statistiques des données opérationnelles par défaut).
- c. **Timestamp field** – choisissez `request_in_ts` pour les données opérationnelles et `start_ts` pour les statistiques des données opérationnelles.

3. Cliquez sur **Save data view to Kibana**.



La vue de données créée peut être utilisée sur n'importe quel nœud Elasticsearch/Kibana au sein de la grappe.

Pour explorer les données opérationnelles stockées et/ou les statistiques relatives aux données opérationnelles, accédez à **Analytics** → **Discover**, puis sélectionnez la vue de données appropriée dans la liste déroulante **Data view**.

## 6.5.2. Exemple de tableaux de bord

Le paquet `uxp-monitor-analytics` fournit des exemples de tableaux de bord `uxp-dashboard.ndjson` ([UXP] Overview) et `uxp-stats-dashboard.ndjson` ([UXP] Stats Overview) situés dans le répertoire `/usr/share/doc/uxp-monitor-analytics/examples/kibana-9.x/dashboards`. Ces tableaux de bord contiennent un ensemble de visualisations différentes (carte thermique, graphiques, affichage numérique, tableaux statistiques, etc.)



Toutes les visualisations de l'exemple de tableau de bord `uxp-dashboard` s'appuient uniquement sur les données opérationnelles et leur modèle d'index `uxp-request*`, tandis que toutes les visualisations de l'exemple de tableau de bord `uxp-stats-dashboard` s'appuient sur les statistiques des données opérationnelles et leur modèle d'index `uxp-stats*`.



Toutes les visualisations des exemples de tableaux de bord incluent des enregistrements provenant à la fois des serveurs de sécurité côté client et côté service. Pour éviter de compter les doublons, filtrez les enregistrements en fonction du type de serveur de sécurité (champ `security_server_type` ou `server_type`, selon le cas).

Pour importer l'exemple d'un tableau de bord sur Kibana, procédez comme suit :

1. Copiez le fichier d'exemple de tableau de bord `uxp-dashboard.ndjson` et/ou `uxp-stats-dashboard.ndjson` depuis le répertoire `/usr/share/doc/uxp-monitor-analytics/examples/kibana-9.x/dashboards` du serveur Kibana vers l'ordinateur local sur lequel vous exécutez l'interface utilisateur Kibana.
2. En tant qu'utilisateur `elastic` dans l'interface utilisateur Kibana :

- a. Naviguez vers **Management** → **Stack Management** → **Kibana** → **Saved Objects** et cliquez sur **Import**.
- b. Sélectionnez le fichier de tableau de bord à importer.
- c. Cliquez enfin sur **Import**, puis sur **Done**.



Lors de l'importation de `uxp-dashboard`, la vue de données `uxp-visualizations-index` pour le modèle d'index de données opérationnelles `uxp-request*`, ainsi que les champs scriptés requis (`timeTotal`, `timeService`, `successfulRequest` et `failedRequest`), sont automatiquement créés. Pour `uxp-stats-dashboard`, la vue de données `uxp-visualizations-stats-index` pour le modèle d'index des statistiques de données opérationnelles `uxp-stats*`, ainsi que le champ scripté requis `failed_count`, sont automatiquement créés.



Si une vue de données en double est configurée sans champs scriptés, certaines visualisations du tableau de bord risquent de ne pas fonctionner. Supprimez la vue de données en double (sans champs scriptés) ou ajoutez les champs scriptés nécessaires à la vue de données en double.



La version actuelle de Kibana utilise la bibliothèque `heatmap charts`, qui ne prend pas en charge les étiquettes verticales, contrairement à la bibliothèque obsolète.

Pour activer les étiquettes verticales dans les visualisations de cartes thermiques, vous pouvez passer à la bibliothèque de cartes thermiques obsolète en suivant les étapes suivantes :

1. Naviguez vers **Management** → **Stack Management** → **Kibana** → **Advanced Settings**.
2. Dans la section **Visualization**, localisez la **Heatmap legacy charts library**.
3. Basculez le paramètre sur **On** et cliquez sur **Save changes**.
4. Cliquez enfin sur **Reload page**.

### 6.5.3. Autres exemples de visualisation

Le paquet `uxp-monitor-analytics` fournit des exemples de visualisation supplémentaires (non inclus dans l'exemple de tableau de bord).



Tous les exemples de visualisation reposent uniquement sur les données opérationnelles et leur schéma d'indexation `uxp-request*`.



Tous les exemples de visualisation incluent des enregistrements provenant à la fois des serveurs de sécurité côté client et côté service. Pour éviter de compter les doublons, filtrez les enregistrements en fonction du type de serveur de sécurité (champ `security_server_type`).

Les visualisations se trouvent dans le répertoire `/usr/share/doc/uxp-monitor-`

analytics/examples/kibana-9.x/visualizations :

- `uxp-message-count-by-security-server.ndjson` – (UXP Message Count by Security Server [UXP]) **visualise la somme totale des messages UXP par serveur de sécurité ;**
- `uxp-message-count-by-security-server-by-service.ndjson` – (UXP Message Count by Security Server by Service [UXP]) **visualise la somme totale des messages UXP par serveur de sécurité et par service ;**
- `succeeded-uxp-message-count-by-service.ndjson` – (Succeeded UXP Message Count by Service [UXP]) **visualise la somme des messages UXP réussis par service.**

Pour importer un exemple de visualisation sur Kibana :

1. Copiez le fichier de visualisation d'exemple souhaité depuis le répertoire du serveur Kibana `/usr/share/doc/uxp-monitor-analytics/examples/kibana-9.x/visualizations` vers l'ordinateur local sur lequel vous exécutez l'interface utilisateur Kibana.
2. En tant qu'utilisateur `elastic` dans l'interface utilisateur Kibana :
  - a. Naviguez vers **Management** → **Stack Management** → **Kibana** → **Saved Objects** et cliquez sur **Import**.
  - b. Sélectionnez le fichier de visualisation à importer.
  - c. Cliquez enfin sur **Import**, puis sur **Done**.



Lors de l'importation de l'exemple de visualisation, la vue de données `uxp-visualizations-index` pour le modèle d'index de données opérationnelles `uxp-request*`, ainsi que les champs scriptés requis (`timeTotal`, `timeService`, `successfulRequest`, et `failedRequest`), sont automatiquement créés.

## 7. Notifications par e-mail

---

Le serveur de surveillance a la capacité d'envoyer des e-mails de notification en cas de défaillance ou de récupération des données de surveillance environnementale demandées au(x) serveur(s) de sécurité.

Tous les serveurs de sécurité qui présentent de nouveaux développements (défaillance ou rétablissement) lors de l'échange des données de surveillance avec le serveur de surveillance seront répertoriés dans un seul e-mail de notification après le cycle de collecte des données de surveillance environnementale.

Le serveur de surveillance envoie des e-mails via le serveur de messagerie Postfix [\[Postfix\]](#) en utilisant la livraison SMTP (Simple Mail Transfer Protocol). Le paquet `postfix` sera installé par défaut en tant que dépendance du paquet `uxp-monitoring-server`. Reportez-vous au guide Postfix [\[Postfix\]](#) pour configurer le relais de messagerie.

Les adresses électroniques des destinataires (séparées par des virgules) peuvent être configurées dans `/etc/uxp/conf.d/local.ini` sous la section `monitoring-server`. Par exemple :

```
[monitoring-server]
notification-email=user-1@example.com, user-2@example.com
```

Après avoir modifié la configuration, redémarrez le serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```



Lors de l'installation de la configuration HA du serveur de surveillance (voir [Haute disponibilité du serveur de surveillance](#)), configurez les notifications par e-mail sur chaque nœud.



## 8. Haute disponibilité du serveur de surveillance

---

Afin d'assurer la collecte ininterrompue des données de surveillance en cas de problèmes de connexion ou de pannes du serveur de surveillance, plusieurs serveurs de surveillance peuvent être utilisés pour assurer une haute disponibilité (HA) native.



Si vous exécutez une seule instance du serveur de surveillance, vous avez une grappe de serveur de surveillance composé d'un seul nœud.

Les serveurs de surveillance forment des grappes distinctes pour la collecte et la transmission des données environnementales à Zabbix, et pour la collecte et la transmission des données opérationnelles à Elasticsearch :

### Grappe pour Zabbix

Tous les serveurs de surveillance configurés avec le même nom de grappe et la même cible Zabbix (grappe) forment automatiquement une grappe pour la collecte des données environnementales. Pendant qu'un nœud de la grappe est actif (nœud maître pour Zabbix), les autres restent en attente, prêts à reprendre la collecte des données environnementales si nécessaire.

Le nœud maître de Zabbix au sein de la grappe est déterminé par un hôte désigné portant le nom de la grappe, configuré dans le groupe d'hôtes Zabbix `UXP MS clusters`. Les nœuds de la grappe surveillent et mettent à jour en permanence l'élément `Node ID` (avec la clé `uxp.ha.node_id`) de l'hôte principal avec son identifiant de nœud respectif, ce qui facilite la détermination du nœud principal pour la période à venir. Par défaut, le nœud conserve son statut de maître pendant 3 minutes jusqu'à ce que ce statut expire, après quoi un autre nœud peut prendre le contrôle. Le paramètre de configuration `master-host-expire-period-seconds`, utilisé pour définir la période d'expiration de l'état du nœud maître, se trouve dans le fichier de configuration `/etc/uxp/conf.d/monitoring-server.ini`. Le délai d'expiration doit être le même pour tous les nœuds de la grappe.

Pour identifier le nœud maître de Zabbix, reportez-vous à la section [Identifier le nœud maître du serveur de surveillance pour Zabbix](#).

### Grappe pour Elasticsearch

Tous les serveurs de surveillance configurés avec le même nom de grappe et la même cible Elasticsearch (grappe) forment automatiquement une grappe pour la collecte des données opérationnelles. Pendant qu'un nœud de la grappe est actif (nœud maître pour Elasticsearch), les autres restent en attente, prêts à reprendre la collecte des données opérationnelles si nécessaire. Tous les nœuds de la grappe devraient utiliser les mêmes noms d'index configurés pour Elasticsearch.

La détermination du nœud principal au sein de la grappe de serveurs de surveillance pour Elasticsearch est facilitée par un document dédié expirant (appelé document principal) stocké dans l'index Elasticsearch `uxp_monitoring_server_master_doc`. Les nœuds de

la grappe surveillent et mettent à jour en permanence le document principal. Le nœud qui a réussi à mettre à jour le document maître devient le nœud maître jusqu'à l'expiration du document. Par défaut, le nœud conserve son statut de maître pendant 10 minutes, après quoi un autre nœud peut prendre le contrôle. Le paramètre de configuration `master-doc-expire-period-seconds`, utilisé pour définir la période d'expiration du document maître, se trouve dans le fichier de configuration `/etc/uxp/conf.d/monitoring-server.ini`.

Pour identifier le nœud maître d'Elasticsearch, reportez-vous à la section [Identifier le nœud maître du serveur de surveillance pour Elasticsearch](#).

Chaque serveur de surveillance doit avoir un nom de grappe configuré et un identifiant de nœud unique (par exemple, UUID) sur cette grappe. Lors de l'installation, les paramètres du serveur de surveillance `cluster-name` et `node-id` sont configurés par défaut en utilisant le nom de la grappe `uxp-ms-cluster` et l'identifiant de nœud unique généré. Ces configurations sont appliquées dans la section `[monitoring-server]` du fichier de configuration `/etc/uxp/conf.d/local.ini`. Par exemple :

```
[monitoring-server]

cluster-name = uxp-ms-cluster
node-id = c5b41dad-52bb-4b8f-9b9f-62b4d9f700ae
```



Pour éviter les enregistrements en double dans Elasticsearch, veillez à ce que les nœuds ayant des noms de grappes différentes ne partagent pas la même cible Elasticsearch et ses noms d'index. Sinon, les données collectées par les nœuds des deux grappes seront stockées dans le même index Elasticsearch, ce qui entraînera une duplication.

Reportez-vous à la section [Changer le nom de la grappe de serveurs de surveillance](#) pour savoir comment modifier le nom de la grappe si nécessaire.



Assurez-vous de l'uniformité entre tous les nœuds de la grappe en vérifiant la cohérence des noms d'index Elasticsearch, ainsi que l'identité des noms de groupes d'hôtes pour les serveurs de sécurité et les serveurs de registre afin de faciliter la configuration du configurateur Zabbix dans le fichier de configuration `/etc/uxp/monitor-agent.ini`.

Tous les nœuds du serveur de surveillance doivent avoir leur propre instance du Serveur de sécurité UXP afin de garantir la disponibilité.

## 8.1. Ajouter un nœud de serveur de surveillance supplémentaire

Pour ajouter un nœud de serveur de surveillance supplémentaire, procédez comme suit :

1. Installez et configurez un nœud de serveur de surveillance supplémentaire comme indiqué à la section [Installer le serveur de surveillance](#).



Au cours de l'installation, le nouveau nœud se voit attribuer un identifiant de nœud unique (spécifié par le paramètre de configuration `node-id`) et le nom de la grappe par défaut `uxp-ms-cluster` (spécifié par le paramètre de configuration `cluster-name`).

2. Accordez l'accès aux données de surveillance du serveur de registre pour le nœud de serveur de surveillance supplémentaire en suivant les étapes décrites dans la section [Accorder l'accès aux données de surveillance du serveur de registre](#).
3. Examinez les changements de configuration effectués précédemment dans le fichier `local.ini` du nœud de serveur de surveillance existant en exécutant la commande suivante :

```
sudo nano /etc/uxp/conf.d/local.ini
```

et écrasez également les paramètres de configuration pertinents sur le nœud de serveur de surveillance supplémentaire. Après avoir modifié la configuration, redémarrez le nœud du serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```

4. Consultez le fichier de configuration `monitor-agent.ini` du nœud de serveur de surveillance existant en exécutant la commande suivante :

```
sudo nano /etc/uxp/monitor-agent.ini
```

et configurez les mêmes serveurs Zabbix et Elasticsearch pour le nœud de serveur de surveillance supplémentaire en suivant les étapes décrites dans les sections [Connecter Zabbix au Serveur de surveillance](#), [Configurer les hôtes surveillés sur Zabbix](#) et [Configuration du serveur de surveillance](#), [Utiliser une grappe Elasticsearch à plusieurs nœuds](#), respectivement.

## 8.2. Supprimer un nœud de serveur de surveillance

Pour supprimer un nœud de serveur de surveillance de la grappe, procédez comme suit :

### Sur le nœud de serveur de surveillance en cours de suppression

1. Arrêtez les services du serveur de surveillance en exécutant les commandes suivantes :

```
sudo systemctl stop uxp-monitoring-server uxp-confclient
sudo systemctl disable uxp-monitoring-server uxp-confclient
```

### En tant qu'administrateur du serveur de registre sur celui-ci (sur chaque nœud dans le cas d'une grappe de serveurs de registre)

1. Révoquez l'accès accordé au nœud de serveur de surveillance supprimé :
  - a. Supprimez le nœud de la ligne `allow <address>` du fichier de configuration de Nginx `monitoring-access-list` :

```
sudo nano /etc/uxp/nginx/monitoring-access-list
```

- b. Rechargez la configuration de Nginx :

```
sudo systemctl reload nginx
```

### En tant qu'administrateur du serveur de sécurité sur le serveur de sécurité du serveur de surveillance

1. Supprimez le certificat TLS du nœud de serveur de surveillance en cours de suppression :
  - a. Accédez à **SERVICES** → **Clients du serveur de sécurité**, puis cliquez sur le bouton Système d'information pour le client de surveillance centralisé.
  - b. Accédez à la section **CERTIFICATS TLS INTERNES DES SYSTÈMES D'INFORMATION** et supprimez le certificat TLS (s'il existe) du nœud du serveur de surveillance supprimé en cliquant sur le bouton Supprimer.

## 8.3. Changer l'adresse d'un nœud de serveur de surveillance

Pour modifier l'adresse IP ou le nom DNS d'un nœud de serveur de surveillance, procédez comme suit.

### Sur le nœud de serveur de surveillance

1. Remplacez les anciens certificats TLS du serveur de surveillance comme décrit dans la section [Remplacement des certificats TLS](#).

### En tant qu'administrateur du serveur de registre sur celui-ci (sur chaque nœud dans le cas d'une grappe de serveurs de registre)

1. Modifiez l'adresse du nœud du serveur de surveillance dans la liste de contrôle d'accès :
  - a. Modifiez la ligne `allow <address>` correspondante dans le fichier de configuration Nginx `monitoring-access-list`:

```
sudo nano /etc/uxp/nginx/monitoring-access-list
```

- b. Rechargez la configuration de Nginx :

```
sudo systemctl reload nginx
```

### En tant qu'administrateur du serveur de sécurité sur le nœud du serveur de surveillance du serveur de sécurité

1. Remplacez l'ancien certificat TLS du nœud du serveur de surveillance, s'il existe :
  - a. Accédez à **SERVICES** → **Clients du serveur de sécurité**, puis cliquez sur le bouton Système d'information pour le client de surveillance centralisé.
  - b. Accédez à la section **CERTIFICATS TLS INTERNES DES SYSTÈMES D'INFORMATION**. Si le certificat TLS du nœud du serveur de surveillance existe :

- i. Supprimez l'ancien certificat TLS en cliquant sur le bouton de suppression correspondant.
- ii. Téléchargez le nouveau fichier de certificat TLS (situé à l'adresse `/etc/uxp/ssl/monitoring-server.crt` sur le nœud du serveur de surveillance) sur l'ordinateur local où vous exécutez l'interface utilisateur du serveur de sécurité.
- iii. Téléchargez le nouveau certificat TLS du nœud du serveur de surveillance en cliquant sur **AJOUTER**.

# 9. Maintenance

## 9.1. Remplacement des certificats TLS

Lors de l'installation, un certificat TLS auto-signé est généré pour le serveur de surveillance. Ce certificat est utilisé pour la communication HTTPS sécurisée avec le serveur de sécurité et se trouve à l'adresse `/etc/uxp/ssl/monitoring-server.crt`. En outre, un certificat TLS auto-signé est généré pour la communication HTTPS avec le serveur Elasticsearch (`/etc/uxp/ssl/elasticsearch.crt`). La durée de validité des deux certificats est de 100 ans.

Voici quelques situations qui nécessitent le remplacement du certificat TLS :

- changement d'hôte ou d'adresse IP du serveur de surveillance ;
- la clé privée du certificat est compromise ;
- le certificat nécessite un nouvel algorithme cryptographique différent.

Pour remplacer le certificat TLS ultérieurement, utilisez la commande `generate-monitoring-server-certificate`.

Utilisation de la commande :

```
Usage: /usr/bin/generate-monitoring-server-certificate [-n <basename>]
<-s "<certificate DN>" | -S> [-a "<subjectAltName>" | -f]
[-H <sha256 | sha512>] [-2 | -3 | -4 | -e <EC>]
```

Generate monitoring server TLS certificate (by default NIST P-256).

OPTIONS:

- `-h` show this message
- `-n` `basename`, like `'monitoring-server'` or `'elasticsearch'`, defaults to `'monitoring-server'`
- `-s` subject, optional. Format `"/C=EE/O=Company/CN=server.name.tld"`
- `-S` fill Subject with `/CN=${HOST}` value
- `-a` subjectAltName, optional. Format `"DNS:serverAlt.name.tld,IP:1.1.1.1,IP:2.2.2.2"`
- `-f` fill subjectAltName automatically from `hostname` and IP addresses
- `-H` hashing algorithm to use `for` the certificate digest, defaults to `sha256`
- `-2` generate 2k RSA key
- `-3` generate 3k RSA key
- `-4` generate 4k RSA key
- `-e` generate EC key. Possible values: `'p256'` (NIST P-256 aka `secp256r1`), `'p384'` (NIST P-384 aka `secp384r1`), `'p521'` (NIST P-521 aka `secp521r1`)



Pour remplacer le certificat sans interrompre le service de surveillance, il est recommandé de remplacer le certificat progressivement. Si l'interruption ne pose pas de

problème, vous pouvez remplacer le certificat immédiatement.



Le mot de passe du fichier P12 généré est le nom de base spécifié.

### 9.1.1. Générer un nouveau certificat TLS pour le serveur de surveillance

1. Générez une nouvelle clé et un nouveau certificat à l'endroit de votre choix.

```
sudo generate-monitoring-server-certificate -S -f
```

Comme la clé et le certificat existent déjà au moment de l'exécution de la commande, une invite demande si l'on veut écraser le fichier existant.

Pour écraser les fichiers existants dans le répertoire `/etc/uxp/ssl/` (méthode de remplacement immédiat), appuyez sur `Y`.

Pour générer les fichiers dans le répertoire de travail actuel, sous les noms `monitoring-server.key`, `monitoring-server.crt`, et `monitoring-server.p12` (méthode de remplacement graduel), appuyez sur n'importe quelle autre touche. Après avoir ajouté le fichier de certificat généré `monitoring-server.crt` à la liste des certificats TLS internes du client de surveillance centralisé sur le serveur de sécurité (voir [\[UXP-UG-SS\]](#)), déplacez les fichiers générés dans le répertoire `/etc/uxp/ssl/` pour remplacer les anciens :

```
sudo mv monitoring-server.* /etc/uxp/ssl/
```

2. Modifiez le propriétaire, le groupe et les autorisations des fichiers copiés :

```
sudo bash -c 'chown root:uxp /etc/uxp/ssl/monitoring-server.*'  
sudo bash -c 'chmod 640 /etc/uxp/ssl/monitoring-server.*'
```

3. Redémarrez le serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```

### 9.1.2. Générer un nouveau certificat TLS pour le serveur Elasticsearch

1. Générez une nouvelle clé et un nouveau certificat à l'endroit de votre choix.

```
sudo generate-monitoring-server-certificate -S -f -n elasticsearch
```

Comme la clé et le certificat existent déjà au moment de l'exécution de la commande, une invite demande si l'on veut écraser le fichier existant.

Pour écraser les fichiers existants dans le répertoire `/etc/uxp/ssl/`, appuyez sur `Y`.

2. Redémarrez le serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```

## 9.2. Changer les intervalles d'interrogation des données de surveillance

Les intervalles d'interrogation des données de surveillance sont définis par les paramètres système dans le fichier de configuration du serveur de surveillance (/etc/uxp/conf.d/monitoring-server.ini).

### Intervalles d'interrogation des serveurs de sécurité

- Pour changer l'intervalle auquel le Serveur de surveillance UXP interroge les données de surveillance environnementale, modifiez la valeur du paramètre système `envdata-polling-interval-seconds`.
- Pour changer l'intervalle auquel le Serveur de surveillance UXP interroge les données de surveillance opérationnelle, modifiez la valeur du paramètre système `opdata-polling-interval-seconds`.
- Pour changer l'intervalle auquel le Serveur de surveillance UXP interroge les statistiques de données de surveillance opérationnelle, modifiez la valeur du paramètre système `opdata-stats-polling-interval-seconds`.

### Intervalle d'interrogation des serveurs de registre

- Pour modifier l'intervalle auquel le Serveur de surveillance UXP interroge les données de surveillance des serveurs de registre, modifiez la valeur du paramètre système `registry-server-monitoring-data-polling-interval-seconds`.

Voir la description détaillée de la modification des valeurs des paramètres système dans [\[UXP-SYSPAR-MS\]](#).

## 9.3. Activer/désactiver la collecte de données de surveillance opérationnelle ou de ses statistiques

L'activation de la collecte des données de surveillance opérationnelle et/ou des statistiques des serveurs de sécurité est définie par les paramètres système dans le fichier de configuration du serveur de surveillance (/etc/uxp/conf.d/monitoring-server.ini).

- Pour activer/désactiver la collecte des données de surveillance opérationnelle, modifiez la valeur du paramètre système `opdata-collection-enabled`.
- Pour activer/désactiver la collecte de statistiques sur les données de surveillance opérationnelle, modifiez la valeur du paramètre système `opdata-stats-collection-enabled`.

Voir la description détaillée de la modification des valeurs des paramètres système dans [\[UXP-SYSPAR-MS\]](#).



## 9.4. Changer la période statistique des données de surveillance opérationnelle

La durée de la période statistique des données de surveillance opérationnelle est définie par un paramètre système dans le fichier de configuration du serveur de surveillance (/etc/uxp/conf.d/monitoring-server.ini).

Pour changer la période des statistiques, modifiez la valeur du paramètre système `opdata-stats-period-seconds`.



Choisissez la valeur avec soin — elle doit diviser 86 400 (24 heures) de manière égale afin de garantir que les périodes des rapports quotidiens et des résumés correspondent correctement.

Par exemple : 900 (15 min), 1 800 (30 min), 3 600 (1 heure), 14 400 (4 heures)...

La valeur minimale autorisée est de 30 secondes. La valeur maximale autorisée est de 86 400 secondes (24 heures).

Voir la description détaillée de la modification des valeurs des paramètres système dans [\[UXP-SYSPAR-MS\]](#).

## 9.5. Gérer l'inclusion/exclusion des données et statistiques de surveillance opérationnelle

Par défaut, le serveur de surveillance exclut du stockage sur Elasticsearch les données de surveillance opérationnelle et les statistiques relatives aux services de gestion, aux méta-services et aux demandes de surveillance, afin de réduire l'empreinte numérique et d'éviter d'inonder le magasin de données avec un trafic interne de faible valeur qui rendrait l'analyse des données plus gourmande en ressources.

Si vous souhaitez toujours que ces données soient stockées sur Elasticsearch, remplacez les valeurs par défaut des paramètres système suivants, définis dans la section `[monitoring-server]` dans le fichier `/etc/uxp/conf.d/monitoring-server.ini` :

- `opdata-exclude-management-service-transactions`,
- `opdata-exclude-meta-service-transactions`,
- `opdata-exclude-monitoring-transactions`,
- `opdata-stats-exclude-management-service-transactions`,
- `opdata-stats-exclude-meta-service-transactions`,
- `opdata-stats-exclude-monitoring-transactions`.

Voir la description détaillée de la modification des valeurs des paramètres système dans [\[UXP-SYSPAR-MS\]](#).

## 9.6. Changer le ou les destinataires des notifications par e-mail

Pour changer le ou les destinataires des notifications par e-mail, modifiez la valeur du paramètre système `notification-email`.

Voir la description détaillée de la modification des valeurs des paramètres système dans [\[UXP-SYSPAR-MS\]](#).

## 9.7. Changer le nom de la grappe de serveurs de surveillance

Pour changer le nom de la grappe du serveur de surveillance :

1. arrêtez le serveur de surveillance sur tous les autres nœuds de la grappe ;
2. changez la valeur du paramètre `cluster-name` dans le fichier de configuration `/etc/uxp/conf.d/local.ini` ;
3. redémarrez le serveur de surveillance :

```
sudo systemctl restart uxp-monitoring-server
```

4. modifiez le paramètre `cluster-name` sur tous les autres nœuds et redémarrez le serveur de surveillance.

## 9.8. Configurer la grappe Zabbix

### 9.8.1. Ajouter un nœud Zabbix supplémentaire

Pour ajouter un nœud Zabbix supplémentaire, procédez comme suit :

1. Sur le serveur de registre (sur chaque nœud dans le cas d'une grappe de serveurs de registre), configurez la nouvelle adresse du nœud Zabbix pour l'agent Zabbix (s'il est installé) en suivant les étapes 3 et 4 décrites dans la section [Installer et configurer l'agent Zabbix](#).
2. Sur le serveur de base de données Zabbix, configurez l'authentification du client pour le nouveau nœud en effectuant les étapes 6 et 7 décrites dans la section [Installer le serveur de base de données](#).
3. Installez un nœud Zabbix supplémentaire comme indiqué dans la section [Installer un nœud du serveur Zabbix](#), en ignorant l'étape inutile consistant à modifier le mot de passe par défaut de l'interface utilisateur Zabbix.
4. Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance), connectez le nouveau nœud Zabbix comme indiqué dans la section [Connecter Zabbix au Serveur de surveillance](#).

### 9.8.2. Supprimer un nœud Zabbix

Pour supprimer un nœud Zabbix de la grappe, procédez comme suit :

### Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance)

1. Modifiez le fichier de configuration de `monitor-agent.ini` :

```
sudo nano /etc/uxp/monitor-agent.ini
```

en supprimant le nom de la section du nœud du paramètre `cluster-nodes` dans la section Zabbix appropriée. De plus, supprimez la section correspondante du nœud restant. Si le nœud est configuré en dehors de la liste `cluster-nodes` (en utilisant le paramètre `address` directement dans la section Zabbix), mettez à jour le paramètre `address` pour qu'il corresponde à l'adresse d'un autre nœud dans la liste `cluster-nodes`, puis supprimez le nom de sa section de la liste `cluster-nodes` et supprimez la section de nœud restante correspondante.

2. Après avoir modifié la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```

### Sur le nœud Zabbix en cours de suppression

1. Arrêtez les services Zabbix en exécutant les commandes suivantes :

- Ubuntu 24.04 LTS

```
sudo systemctl stop zabbix-server zabbix-agent nginx php8.3-fpm
sudo systemctl disable zabbix-server zabbix-agent nginx php8.3-fpm
```

- Ubuntu 22.04 LTS

```
sudo systemctl stop zabbix-server zabbix-agent nginx php8.1-fpm
sudo systemctl disable zabbix-server zabbix-agent nginx php8.1-fpm
```

### Sur le serveur de base de données Zabbix

1. Supprimez la ligne d'authentification du client pour le nœud dans le fichier de configuration `pg_hba.conf` :

```
sudo nano /etc/postgresql/<version>/main/pg_hba.conf
```

2. Redémarrez le service `postgresql` :

```
sudo systemctl restart postgresql
```

### Sur le serveur de registre (sur chaque nœud dans le cas d'une grappe de serveurs de registre), si l'agent Zabbix est installé

1. Supprimez l'adresse du nœud de la liste spécifiée dans le paramètre `Server` du fichier de configuration de l'agent Zabbix `zabbix_agentd.conf` :

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

2. Redémarrez l'agent Zabbix après avoir modifié la configuration :

```
sudo systemctl restart zabbix-agent
```

### 9.8.3. Désactiver la grappe HA

Si une grappe Zabbix à nœud unique subsiste, vous pouvez désactiver la grappe HA en suivant ces étapes :

#### Sur le nœud Zabbix

1. Commentez le paramètre `HANodeName` dans le fichier de configuration `zabbix_server.conf` :

```
sudo nano /etc/zabbix/zabbix_server.conf
```

par exemple :

```
# HANodeName=zabbix-node-1
```

2. Redémarrez le serveur Zabbix (il démarrera en mode autonome) :

```
sudo systemctl restart zabbix-server
```

### 9.8.4. Changer l'adresse d'un nœud Zabbix

Pour modifier l'adresse IP ou le nom DNS d'un nœud Zabbix, procédez comme suit :

**Sur le serveur de registre (sur chaque nœud dans le cas d'une grappe de serveurs de registre), si l'agent Zabbix est installé**

1. Mettez à jour l'adresse du nœud dans la liste spécifiée par le paramètre `Server` dans le fichier de configuration de l'agent Zabbix `zabbix_agentd.conf` :

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

2. Redémarrez l'agent Zabbix :

```
sudo systemctl restart zabbix-agent
```

#### Sur le serveur de base de données Zabbix

1. Modifiez la ligne d'authentification du client en mettant à jour l'adresse du nœud dans le fichier de configuration `pg_hba.conf` :

```
sudo nano /etc/postgresql/<version>/main/pg_hba.conf
```

2. Redémarrez le service `postgresql` :

```
sudo systemctl restart postgresql
```

### Sur le nœud Zabbix dont l'adresse est modifiée

1. Mettez à jour le paramètre `NodeAddress` dans le fichier de configuration `zabbix_server.conf` :

```
sudo nano /etc/zabbix/zabbix_server.conf
```

2. Mettez à jour le paramètre `server_name` (s'il est défini) dans le fichier de configuration `nginx.conf` :

```
sudo nano /etc/zabbix/nginx.conf
```

3. Redémarrez les services Zabbix en exécutant la commande suivante :

- Ubuntu 24.04 LTS

```
sudo systemctl restart zabbix-server zabbix-agent nginx php8.3-fpm
```

- Ubuntu 22.04 LTS

```
sudo systemctl restart zabbix-server zabbix-agent nginx php8.1-fpm
```

4. Enfin, vérifiez l'état de la grappe Zabbix en exécutant la commande suivante sur les nœuds Zabbix. Si le nœud est actif, il affiche l'état de la grappe. S'il n'est pas actif, répétez la commande sur un autre nœud :

```
sudo zabbix_server -R ha_status
```

### Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance)

1. Mettez à jour l'adresse du nœud Zabbix (spécifiée dans le paramètre `address`) dans la section Zabbix appropriée ou dans la section référencée par le paramètre `cluster-nodes` dans le fichier de configuration `monitor-agent.ini` :

```
sudo nano /etc/uxp/monitor-agent.ini
```

2. Après avoir modifié la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```

## 9.9. Configurer la grappe Elasticsearch

### 9.9.1. Ajouter un nœud Elasticsearch supplémentaire

Pour ajouter un nœud Elasticsearch supplémentaire, procédez comme suit :

1. Inscrivez un nœud Elasticsearch supplémentaire en suivant les étapes décrites dans la section [Installer une grappe Elasticsearch à plusieurs nœuds](#).
2. Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance), connectez le nouveau nœud Elasticsearch comme indiqué dans la section [Utiliser une grappe Elasticsearch à plusieurs nœuds](#).

## 9.9.2. Supprimer un nœud Elasticsearch



Tant qu'il y a au **moins trois** nœuds éligibles au titre de maître sur la grappe, il est généralement préférable de retirer les nœuds un par un, en laissant suffisamment de temps à la grappe pour ajuster automatiquement la configuration de vote et adapter le niveau de tolérance aux fautes au nouvel ensemble de nœuds, c'est-à-dire pour rééquilibrer correctement les tessons qui se trouvaient sur le nœud retiré avant d'envisager le retrait d'un autre nœud.

Vous pouvez consulter une liste détaillée des nœuds contenant des tessons spécifiques en visitant l'URL : `https://<elastic-node-address>:9200/_cat/shards?v`. Ouvrez cette URL dans votre navigateur Web et connectez-vous en utilisant les informations d'identification de l'utilisateur `elastic`. Assurez-vous que les tessons ont été réalloués à partir du nœud précédemment supprimé en vérifiant qu'aucun tesson n'est affecté au nom du nœud supprimé.

S'il ne reste que **deux** nœuds éligibles au rôle de maître, aucun des deux nœuds ne peut être supprimé en toute sécurité, car ils sont tous deux nécessaires pour garantir la fiabilité du processus. Pour supprimer l'un de ces nœuds, vous devez d'abord informer Elasticsearch qu'il ne doit pas faire partie de la configuration de vote et que le pouvoir de vote doit être attribué à l'autre nœud. Vous pouvez alors mettre hors ligne le nœud exclu sans empêcher l'autre nœud de progresser.

Ajoutez le nœud supprimé à la liste des exclusions de la configuration de vote et attendez jusqu'au délai par défaut de 30 secondes pour que le système reconfigure automatiquement le nœud hors de la configuration de vote, en exécutant la commande suivante sur n'importe quel nœud de la grappe :



```
curl -k -X POST -u elastic \
https://localhost:9200/_cluster/voting_config_exclusions\
?node_names=<node-name>
```

où `<node-name>` est le nom du nœud (valeur du paramètre `node.name` dans la configuration `/etc/elasticsearch/elasticsearch.yml`, par défaut le nom d'hôte) à supprimer.

L'ajout d'une exclusion pour un nœud crée une entrée pour ce nœud dans la liste des exclusions de la configuration de vote, ce qui fait que le système tente automatiquement de reconfigurer la configuration de vote pour supprimer ce nœud et l'empêche de revenir dans la configuration de vote une fois qu'il a été supprimé. La liste actuelle des exclusions est stockée dans l'état de la grappe et peut être consultée comme suit :

```
curl -k -u elastic https://localhost:9200/_cluster/state\
?filter_path=metadata.cluster_coordination.voting_config_exclusions
```

Cette exclusion peut être supprimée après l'arrêt du nœud et son retrait de la grappe.

```
curl -k -X DELETE -u elastic \
https://localhost:9200/_cluster/voting_config_exclusions
```

Pour supprimer un nœud Elasticsearch de la grappe, procédez comme suit :

### Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance)

1. Modifiez le fichier de configuration de `monitor-agent.ini` :

```
sudo nano /etc/uxp/monitor-agent.ini
```

en supprimant le nom de la section du nœud du paramètre `cluster-nodes` dans la section `[elasticsearch]`. De plus, supprimez la section correspondante du nœud restant. Si le nœud est configuré en dehors de la liste `cluster-nodes` (à l'aide du paramètre `address` directement dans la section `[elasticsearch]`), mettez à jour le paramètre `address` pour qu'il corresponde à l'adresse d'un autre nœud de la liste `cluster-nodes`, puis supprimez son nom de section de la liste `cluster-nodes` et supprimez la section de nœud restante correspondante.

2. Après avoir modifié la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```

### Sur le nœud Elasticsearch en cours de suppression

1. Arrêtez les services Elasticsearch et Kibana en exécutant les commandes suivantes :

```
sudo systemctl stop elasticsearch kibana
sudo systemctl disable elasticsearch kibana
```

### Sur tous les autres nœuds Elasticsearch

1. Supprimez l'adresse du nœud en cours de suppression de la liste `discovery.seed_hosts` dans le fichier de configuration `elasticsearch.yml` :

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```



S'il reste une grappe à nœud unique (c'est-à-dire que la liste `discovery.seed_hosts` reste vide), elle remplit toujours la condition de vérification du démarrage en s'assurant qu'au moins l'un des nœuds `discovery.seed_hosts`, `discovery.seed_providers` ou `cluster.initial_master_nodes` est configuré.

2. Après avoir modifié la configuration, redémarrez le service `elasticsearch` :

```
sudo systemctl restart elasticsearch
```

### 9.9.3. Changer l'adresse d'un nœud Elasticsearch

Pour modifier l'adresse IP ou le nom DNS du nœud Elasticsearch, procédez comme suit :

#### Sur le nœud Elasticsearch dont l'adresse est modifiée

1. Générez un nouveau certificat TLS pour les connexions client API HTTP, telles que Kibana et le serveur de surveillance :
  - a. Extrayez la clé privée CA HTTP Elasticsearch du fichier `http.p12` vers un fichier de magasin de clés distinct `http_ca.p12` (si cela n'a pas déjà été fait) :



Utilisez le même mot de passe pour le magasin de clés source et le magasin de clés de destination. Le mot de passe est obtenu en exécutant la commande suivante :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-keystore show \
xpack.security.http.ssl.keystore.secure_password
```

```
sudo /usr/share/elasticsearch/jdk/bin/keytool -importkeystore \
-srckeystore /etc/elasticsearch/certs/http.p12 \
-destkeystore /etc/elasticsearch/certs/http_ca.p12 \
-deststoretype PKCS12 -srcalias http_ca
```

et définissez la propriété et les autorisations correctes pour le fichier `http_ca.p12` en exécutant les commandes suivantes :

```
sudo chown root:elasticsearch /etc/elasticsearch/certs/http_ca.p12
sudo chmod 660 /etc/elasticsearch/certs/http_ca.p12
```

- b. Générez un nouveau certificat TLS API HTTP en exécutant la commande suivante et en répondant aux invites :

```
sudo /usr/share/elasticsearch/bin/elasticsearch-certutil http
```



- Ne générez pas de CSR en entrant `n` ;
- utilisez une autorité de certification existante en saisissant `y` ;
- entrez le chemin d'accès au dépôt de clés de l'autorité de certification `/etc/elasticsearch/certs/http_ca.p12` ;
- entrez le mot de passe de ce magasin de clés ;
- fixez la période de validation des certificats à 100 ans en saisissant `100y` ;
- générez un certificat par nœud en saisissant `y` ;
- entrez le nom du nœud (par exemple, le nom d'hôte) ;
- entrez le(s) nom(s) DNS pour le Nom de sujet alternatif (SAN) ;



- vérifiez ce qui a été saisi et confirmez en saisissant y ;
- entrez la ou les adresses IP pour le SAN ;
- vérifiez ce qui a été saisi et confirmez en saisissant y ;
- ne modifiez aucune option en entrant n ;
- ne générez pas de certificats supplémentaires en saisissant n ;
- entrez le même mot de passe que celui utilisé pour http.p12 pour le nouveau fichier de magasin de clés ;
- générez le fichier d'archive à l'emplacement par défaut en appuyant sur **Entrée**.

- c. Extrayez le nouveau fichier de magasin de clés http.p12 de l'archive /usr/share/elasticsearch/elasticsearch-ssl-http.zip créée et remplacez l'ancien fichier situé dans /etc/elasticsearch/certs/http.p12 par le nouveau fichier en exécutant la commande suivante :

```
sudo unzip -j -o /usr/share/elasticsearch/elasticsearch-ssl-http.zip \
elasticsearch/http.p12 -d /etc/elasticsearch/certs
```

- d. Définissez la propriété et les autorisations correctes pour le fichier http.p12 en exécutant les commandes suivantes :

```
sudo chown root:elasticsearch /etc/elasticsearch/certs/http.p12
sudo chmod 660 /etc/elasticsearch/certs/http.p12
```

- e. Importez la clé privée de l'autorité de certification HTTP (requis par l'outil elasticsearch-create-enrollment-token) de http\_ca.p12 vers le nouveau http.p12 en exécutant la commande suivante :

```
sudo /usr/share/elasticsearch/jdk/bin/keytool -importkeystore \
-srckeystore /etc/elasticsearch/certs/http_ca.p12 \
-destkeystore /etc/elasticsearch/certs/http.p12
```

- f. Enfin, redémarrez le service elasticsearch :

```
sudo systemctl restart elasticsearch
```

2. Mettez à jour l'adresse du nœud dans les paramètres elasticsearch.hosts et xpack.fleet.outputs du fichier de configuration kibana.yml :

```
sudo nano /etc/kibana/kibana.yml
```

3. Obtenez et configurez un nouveau certificat TLS pour Kibana en suivant les étapes décrites dans la section [Chiffrement du trafic entre le navigateur Web et Kibana](#).

## Sur tous les autres nœuds Elasticsearch

1. Mettez à jour l'adresse du nœud dont l'adresse est modifiée dans la liste

`discovery.seed_hosts` du fichier de configuration `elasticsearch.yml` :

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

2. Après avoir modifié la configuration, redémarrez le service `elasticsearch` :

```
sudo systemctl restart elasticsearch
```

3. Vérifiez finalement les nœuds de la grappe dans votre navigateur Web en naviguant vers `https://<node-address>:9200/_cat/nodes?v` et en vous authentifiant avec le nom d'utilisateur `elastic` et son mot de passe. Tous les nœuds de la grappe doivent être répertoriés.

### **Sur le serveur de surveillance (sur chaque nœud dans le cas d'une grappe de serveurs de surveillance)**

1. Mettez à jour l'adresse du nœud Elasticsearch (spécifiée dans le paramètre `address`) dans la section `[elasticsearch]` appropriée ou dans la section référencée par le paramètre `cluster-nodes` dans le fichier de configuration `monitor-agent.ini` :

```
sudo nano /etc/uxp/monitor-agent.ini
```

2. Après avoir modifié la configuration, rechargez le serveur de surveillance :

```
sudo reload-monitoring-server
```

# 10. Dépannage

---

## 10.1. Fichiers journaux

Les fichiers journaux aident à résoudre les erreurs qui surviennent et à détecter d'éventuels comportements inattendus. La lecture des fichiers journaux nécessite des privilèges root.

- Le Serveur de surveillance écrit les journaux dans le fichier `/var/log/uxp/monitoring_server.log`.
- Les enregistrements des activités liées au téléchargement de la configuration globale se trouvent dans le fichier `/var/log/uxp/configuration_client.log`.

Le système **Logback** est utilisé pour la journalisation.

Dans Logback, les niveaux de journalisation sont classés du plus bas au plus élevé en fonction de leur gravité : `TRACE < DEBUG < INFO < WARN < ERROR`.

Notez qu'il n'est pas recommandé de définir un niveau de journalisation inférieur à `INFO` sur les systèmes de production pendant plus longtemps que nécessaire, car la verbosité excessive des niveaux inférieurs peut épuiser les ressources de votre système.

Les paramètres par défaut de la journalisation sont les suivants :

- les enregistrements sont consignés au niveau `INFO` ;
- une nouvelle archive ZIP des enregistrements du journal est créée une fois par jour ou lorsque la taille du fichier journal atteint 100 Mo (`maxFileSize` dans la politique de roulement) ;
- les enregistrements sont conservés pendant 60 jours (`maxHistory`) ou jusqu'à ce que 1 Go d'espace de stockage (`totalSizeCap`) ait été utilisé.

### 10.1.1. Configuration des paramètres de journalisation des composants

Chaque composant UXP possède son propre fichier de configuration **Logback**

| Service               | Fichier de configuration                                   |
|-----------------------|--|
| uxp-monitoring-server | <code>/etc/uxp/conf.d/monitoring-server-logback.xml</code> |
| uxp-confclient        | <code>/etc/uxp/conf.d/confclient-logback.xml</code>        |

Tous les fichiers de configuration de journalisation suivent la même structure générale. Par exemple, pour chaque fichier journal généré par un composant, il existe une section qui configure la politique de stockage des anciens fichiers journaux :

```
<appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${logOutputPath}/monitoring_server.log</file>
  <rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <fileNamePattern>${logOutputPath}/monitoring_server.%d{yyyy-MM-dd}.%i.log.zip</fileNamePattern>
    <!-- each file should be at most 100MB, keep 60 days worth of history, but at
most 1GB -->
    <maxFileSize>100MB</maxFileSize>
    <maxHistory>60</maxHistory>
    <totalSizeCap>1GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%d [%thread] %-5level %logger{36} - %msg%n</pattern>
    <charset>UTF-8</charset>
  </encoder>
</appender>
```

Pour modifier la taille des archives ZIP et la durée de stockage des archives, modifiez les paramètres `maxFileSize`, `maxHistory` et `totalSizeCap` dans la section `rollingPolicy`.

En outre, le paramètre `pattern` décrit le modèle de journalisation utilisé pour les entrées du fichier journal. Elle peut être configurée conformément à [\[LOGBACK-PATTERNS\]](#).

## 10.2. Recharger le serveur de surveillance

La plupart des scénarios dans lesquels le serveur de surveillance ne fonctionne pas comme souhaité peuvent être réparés en rechargeant celui-ci avec la commande :

```
sudo reload-monitoring-server
```

Cette commande permet au serveur de surveillance de lire la configuration des agents de surveillance à partir du fichier de configuration `/etc/uxp/monitor-agent.ini` et de mettre à jour ses composants en fonction des changements détectés. Tous les serveurs Zabbix présents dans la configuration et dont la capacité de reconfiguration automatique est activée seront alors reconfigurés.

## 10.3. Changer la configuration des agents de surveillance

Après avoir modifié le fichier de configuration des agents de surveillance (`/etc/uxp/monitor-agent.ini`), vous devez recharger le serveur de surveillance à l'aide de la commande `sudo reload-monitoring-server`.

## 10.4. Vérification de l'envoi des e-mails

Utilisez la commande Postfix `sendmail` (ou un programme similaire) pour vérifier si le serveur est en mesure d'envoyer des e-mails :

```
echo "Subject: Test email from $HOSTNAME" | sendmail test@example.com
```

Si l'e-mail n'arrive pas, vérifiez le fichier journal de Postfix `/var/log/mail.log` et/ou la configuration :

```
postconf -n
```

Assurez-vous que Postfix est configuré correctement [\[Postfix\]](#).

## 10.5. La configuration du serveur Zabbix n'est pas valide

Si la configuration d'un serveur Zabbix est perdue ou invalide, utilisez la commande `sudo reload-monitoring-server` pour forcer la reconfiguration de celui-ci.

## 10.6. Spam dans les journaux Zabbix : Le prétraitement a échoué pour

Le retrait de nœuds de la grappe Zabbix ou la réactivation du mode HA natif de Zabbix peut entraîner l'inondation du fichier `/var/log/zabbix/zabbix_server.log` par des erreurs répétitives similaires :

```
176787:20250124:140825.445 error reason for "Zabbix
server:zabbix.node.stats[cm69dr64e0001tf6miumuotwy]" changed: Preprocessing failed for:
[{"id":"cm6aoej2v0001e86n3tzttask","name":"zabbix-node-
2","status":3,"lastaccess":1737727704,"add...
```

Pour résoudre ce problème, suivez les étapes suivantes dans l'interface utilisateur de Zabbix :

1. Naviguez vers la **Data collection** → **Hosts** et cliquez sur le lien **Items** sur la ligne hôte Zabbix server.
2. Saisissez `stats` dans le filtre **Key** et cliquez sur **Apply**.
3. Sélectionnez dans la liste tous les éléments `zabbix.node.stats` ayant le statut **Not supported** et supprimez-les en cliquant sur **Delete**.

## 10.7. Identifier le nœud maître du serveur de surveillance pour Zabbix

Pour identifier le nœud maître de Zabbix au sein de la grappe de serveurs de surveillance, accédez à **Monitoring** → **Latest data** dans l'interface utilisateur Zabbix. Localisez l'hôte du nœud maître, nommé d'après le nom de la grappe, situé dans le groupe d'hôtes étiqueté UXP MS clusters. L'élément **Node ID** (avec la clé `uxp.ha.node_id`) dans l'hôte maître contient l'identifiant du dernier nœud maître actuel, tandis que sa valeur **Latest check** indique l'horodatage de la dernière mise à jour de son statut de maître. Par défaut, l'hôte conserve son statut de maître pendant 3 minutes (paramètre de configuration `master-host-expire-period-seconds` dans le fichier de configuration `/etc/uxp/conf.d/monitoring-`

`server.ini`) jusqu'à ce que le statut expire.

## 10.8. Identifier le nœud maître du serveur de surveillance pour Elasticsearch

Pour identifier le nœud maître pour Elasticsearch au sein de la grappe de serveurs de surveillance, accédez à **Analytics** → **Discover** dans l'interface utilisateur Kibana. Sélectionnez la vue de données correspondant à l'index `uxp_monitoring_server_master_doc` pour visualiser le(s) document(s) maître(s). Si la vue de données n'est pas disponible, créez-la d'abord en accédant à **Management** → **Stack Management** → **Kibana** → **Data Views** → **Create data view**.

Il est également possible d'exécuter une demande GET similaire au serveur Elasticsearch pour récupérer et visualiser le(s) document(s) maître(s) :

```
http://<elasticsearch-server>:9200/uxp_monitoring_server_master_doc/_search?pretty=true
```

La réponse est similaire à :

```
...
"hits" : [
  {
    "_index" : "uxp_monitoring_server_master_doc",
    "_type" : "_doc",
    "_id" : "f0c40c89f5ec11f42f02e4391398b1b45172b42abfe900b9440600aa05c39733",
    "_score" : 1.0,
    "_source" : {
      "node_id" : "53ed0672-41bc-4ba7-991c-7e3fab099461",
      "expires_ts" : 1581949640445,
      "updated_ts" : 1581949460445
      "cluster_name" : "uxp-ms-cluster"
    }
  }
]
...
```

Dans le document principal, le champ `node_id` indique l'identifiant de l'actuel/du dernier nœud maître de la grappe nommée dans `cluster_name`, tandis que `expires_ts` et `updated_ts` représentent les horodatages UNIX d'expiration et de dernière mise à jour du document (en millisecondes).

# 11. Migration

---

## 11.1. Migration de la version 2.9 à la version 2.10

- La prise en charge d'Elasticsearch et de Kibana 7.x a été complètement supprimée dans cette version. Si vous utilisez encore la version 7.x, mettez les deux à jour vers la version 8.x avant de mettre à jour le serveur de surveillance.
- La propriété système `opdata-stats-period-seconds` dans le fichier de configuration `monitoring-server.ini` a maintenant des règles de validation plus strictes. Ces restrictions garantissent que les statistiques de surveillance opérationnelle sont agrégées sur des périodes cohérentes et alignées :
  - Valeur minimale : 30 secondes.
  - Valeur maximale : 86 400 secondes (24 heures)
  - La valeur configurée doit diviser uniformément 86 400 secondes (24 heures). Cela garantit que la période de statistiques quotidiennes est divisée de manière égale en intervalles entiers.

Si votre serveur de surveillance est configuré pour collecter des statistiques sur les données de surveillance opérationnelle et que vous n'utilisez pas la valeur par défaut de `opdata-stats-period-seconds`, assurez-vous que la valeur configurée est conforme aux restrictions ci-dessus.

- Dans la version 1.25.0 du serveur de registre, la période de validité par défaut de la configuration globale est passée de 10 minutes à 72 heures. En conséquence, le déclencheur Zabbix **La configuration globale arrive à expiration** s'active désormais **24 heures** avant l'expiration de la configuration.

Si vous n'avez pas encore effectué la mise à jour vers le serveur de registre 1.25.0, ce déclencheur peut se déclencher prématurément et générer de fausses alarmes, car l'ancienne fenêtre d'expiration de 10 minutes s'applique toujours. Après la mise à jour vers la version 1.25.0, qui étend la période de validité par défaut à 72 heures, le déclencheur s'activera comme prévu.

## 11.2. Migration de la version 2.7 à la version 2.9

- La plate-forme minimale supportée est maintenant Ubuntu **22.04** LTS. Si votre système d'exploitation est plus ancien, passez à la version 22.04 avant de mettre à jour le logiciel. Suivez les instructions figurant dans [\[UXP-UPG-UB22\]](#).
- La prise en charge de la version **5.0** LTS de Zabbix a été supprimée. Si vous l'utilisez encore, passez à Zabbix 6.0 LTS avant de mettre à jour le logiciel.
- Fichier de configuration `/etc/uxp/monitor-agent.ini` mis à jour :
  - Les valeurs par défaut de `conf_api_path` et `conf_api_port` pour Zabbix ont été remplacées par `/api_jsonrpc.php` et `8080`, respectivement. Si vous utilisiez les

valeurs par défaut précédentes, veuillez à mettre ces paramètres de configuration à jour lors de la fusion du fichier de configuration pendant la mise à jour.

- La valeur par défaut du paramètre `enable_registry_servers_configurator` a été fixée à `true` et des valeurs par défaut ont été ajoutées pour `host_group` et `registry_servers_group` pour Zabbix : `uxp-security-servers` et `uxp-registry-servers`, respectivement. Utilisez les valeurs appropriées lors de la fusion du fichier de configuration `monitoring-agent.ini`.
- `username` et `password` sont désormais toujours requis pour la configuration de l'API Zabbix. En outre, l'utilisateur configuré doit recevoir l'autorisation `Read-write` pour le groupe d'hôtes UXP MS clusters afin de garantir la continuité du fonctionnement.



Avant de mettre à jour le logiciel UXP, consultez la section [Configurer l'API de configuration Zabbix](#) pour vérifier que l'utilisateur Zabbix approprié dispose des privilèges nécessaires. Cette documentation a été développée sur la base de Zabbix 7.0 LTS, et la structure du menu peut différer de celle de la version 6.0 !

- Par défaut, le client HTTP Elasticsearch vérifie désormais le nom d'hôte du serveur Elasticsearch pendant l'établissement de la connexion TLS (lors de l'utilisation du schéma `https`). Si l'adresse Elasticsearch configurée dans `/etc/uxp/monitor-agent.ini` ne correspond pas au nom alternatif du sujet (SAN) dans le certificat TLS de l'API HTTP Elasticsearch, vous disposez des options suivantes :
  - Mettez à jour l'adresse Elasticsearch dans `/etc/uxp/monitor-agent.ini` pour qu'elle corresponde au SAN.
  - Régénérez le certificat de l'API HTTP Elasticsearch avec le SAN correct.
  - Désactivez la vérification du nom d'hôte sur le serveur de surveillance en définissant `verify-hostname=false` dans la section `[elasticsearch]` du fichier de configuration `/etc/uxp/monitor-agent.ini`.
- Amélioration des données de surveillance opérationnelle en faisant la distinction entre les messages SOAP et REST :
  - Introduction d'un nouveau champ, `request_type`, dans le document de données de surveillance opérationnelle pour préciser si une demande est SOAP ou REST.
  - Les données de surveillance reflètent désormais directement les caractéristiques du message REST, plutôt que le message SOAP enveloppant le message REST transmis entre les serveurs de sécurité.
    - Le champ `request_soap_size` représente maintenant la taille de la demande SOAP ou de la charge utile de la demande REST en octets.
    - Le champ `response_soap_size` représente maintenant la taille de la réponse SOAP ou de la charge utile de la réponse REST en octets.
    - Les champs `request_attachment_count` et `response_attachment_count` sont désormais définis sur 0 pour les messages REST (auparavant 1 si le message REST avait une charge utile ajoutée en tant que pièce jointe dans le message SOAP enveloppant).



- Étant donné que la charge utile de la réponse REST n'est pas analysée par le serveur de sécurité, tout code d'état HTTP autre que 2XX est désormais considéré comme un échec, représenté par le champ `succeeded`.

Si nécessaire, mettez à jour vos visualisations de données de surveillance opérationnelle personnalisées dans Kibana.

- Amélioration de la haute disponibilité des serveurs de surveillance. Un nouveau paramètre de configuration, `cluster-name`, a été introduit pour définir la grappe de serveurs de surveillance :
  - Les serveurs de surveillance portant le même nom de grappe et ciblant le même Zabbix (grappe) forment automatiquement une grappe pour la collecte de données environnementales.
  - Les serveurs de surveillance portant le même nom de grappe et ciblant le même Elasticsearch (grappe) forment automatiquement une grappe pour la collecte de données opérationnelles. Tous les nœuds de la grappe doivent utiliser les mêmes noms d'index configurés pour Elasticsearch.

Si aucun Elasticsearch n'est configuré pour le serveur de surveillance lors de la mise à jour, le nom de la grappe est défini comme `uxp-ms-cluster`. Sinon, pour des raisons de compatibilité ascendante, le nom de l'index des données de surveillance opérationnelle est utilisé comme nom de la grappe. Après avoir mis à jour tous les nœuds du serveur de surveillance, vous pouvez renommer la grappe si vous le souhaitez en suivant les étapes de la section [Changer le nom de la grappe de serveurs de surveillance](#).

- Ajout d'une fonctionnalité permettant de collecter des statistiques sur les données de surveillance opérationnelle des serveurs de sécurité par le biais de la nouvelle demande de surveillance `getSecurityServerOperationalDataStats`. Assurez-vous que tous les serveurs de sécurité de la même instance ont été mis à jour vers la version 1.24.0 au moins avant d'activer la collecte de statistiques. Dans le cas contraire, le serveur de surveillance recevra des réponses d'erreur de la part de serveurs de sécurité incompatibles.
- Par défaut, le serveur de surveillance exclut désormais du stockage dans Elasticsearch les données de surveillance opérationnelle et les statistiques relatives aux services de gestion, aux méta-services et aux demandes de surveillance. Toutefois, lors d'une mise à jour du logiciel, les valeurs par défaut des paramètres de configuration pertinents sont écrasées pour assurer la compatibilité ascendante, de sorte que ces données continueront d'être stockées à moins d'être reconfigurées manuellement. Reportez-vous à la section [Gérer l'inclusion/exclusion des données et statistiques de surveillance opérationnelle](#) pour obtenir des informations détaillées.



Après avoir mis à jour les paquets du serveur de surveillance, il est recommandé de :

- Mettre à jour le serveur de surveillance vers Ubuntu **24.04** LTS. Suivez les instructions figurant dans [\[UXP-UPG-UB24\]](#).
- Mettre Zabbix à jour avec la version **7.0** LTS, car Zabbix 6.0 LTS est maintenant déprécié et son support sera supprimé dans une prochaine version. Suivez les instructions figurant dans [\[Zabbix-Upgrade-7.0\]](#).

- Mettre Elasticsearch/Kibana à jour avec la version **8.x**, si nécessaire, car la version 7.x est désormais obsolète et sa prise en charge sera supprimée dans une prochaine version. Suivez les instructions figurant dans [\[Elastic-Upgrade-8.18\]](#).

## 11.3. Migration vers la version 2.7

- Remplacement du client Java High Level REST d'Elasticsearch obsolète par le client Java API.

Mettre au moins à jour Elasticsearch vers la version **7.17** pour être compatible avec le client API Java.

- Les modèles Zabbix sont désormais utilisés pour configurer les serveurs de sécurité vers Zabbix.



La migration vers les modèles supprime tous les anciens serveurs de sécurité (basés sur le groupe d'hôtes configuré et la configuration globale UXP) configurés dans Zabbix. Créez une sauvegarde de Zabbix si nécessaire.

Si plusieurs serveurs de surveillance (configuration à haute disponibilité) configurent les hôtes du serveur de sécurité sur le même Zabbix, définissez la valeur du paramètre `enable_configurator` sur `false` dans le fichier de configuration `/etc/uxp/monitor-agent.ini` des autres serveurs de surveillance correspondants et rechargez leur configuration avant de mettre à jour le premier serveur de surveillance qui configure Zabbix. Après avoir mis à jour les autres serveurs, modifiez la valeur du paramètre correspondant et rechargez à nouveau les serveurs. Cela garantit que, pendant la mise à jour, les serveurs non mis à jour ne reconfigurent pas les hôtes du serveur de sécurité supprimé vers Zabbix d'une manière démodée.

- Le modèle Zabbix pour les hôtes du serveur de registre a été renommé et amélioré.



La migration de l'ancien modèle du serveur de registre `Template UXP Registry Server` vers le nouveau modèle supprime tous les éléments de l'ancien modèle des hôtes du serveur de registre configurés dans Zabbix. Créez une sauvegarde de Zabbix si nécessaire.

Si plusieurs serveurs de surveillance (configuration à haute disponibilité) configurent les hôtes du serveur de registre sur le même Zabbix, définissez la valeur du paramètre `enable_registry_servers_configurator` sur `false` dans le fichier de configuration `/etc/uxp/monitor-agent.ini` des autres serveurs de surveillance correspondants et rechargez leur configuration avant de mettre à jour le premier serveur de surveillance qui configure Zabbix. Après avoir mis à jour les autres serveurs, modifiez la valeur du paramètre correspondant et rechargez à nouveau les serveurs. Cela garantit que, lors de la mise à jour, les serveurs non mis à jour ne reconfigurent pas les hôtes du serveur de registre à l'aide de l'ancien modèle.

# Annexe A: Notes de mise à jour du Serveur de surveillance UXP

---

## 2.10.0 (11.2025)

- Les versions 9.x d'Elasticsearch et de Kibana sont désormais prises en charge.
- La prise en charge d'Elasticsearch et de Kibana 7.x a été entièrement supprimée.
- La propriété système `opdata-stats-period-seconds` dans `monitoring-server.ini` applique désormais des règles de validation plus strictes.
- Un nouveau paramètre de configuration, `enable_update_existing_triggers`, a été ajouté à `monitor-agent.ini`. Cela permet d'activer ou de désactiver les mises à jour des déclencheurs existants dans les modèles Zabbix UXP, ce qui permet d'éviter les écrasements involontaires.
- Le déclencheur Zabbix `Global configuration is expiring` s'active désormais 24 heures avant l'expiration de la configuration.
- Java Runtime Environment est mis à jour vers la version 21. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Diverses corrections et améliorations mineures ont été apportées.

## 2.9.0 (09.2025)

- Ubuntu 24.04 LTS est désormais une plate-forme prise en charge (et recommandée). Consultez le guide de mise à jour d'Ubuntu UXP-UPG-UB24.
- Zabbix 7.0 LTS est maintenant pris en charge. Celle de Zabbix 6.0 LTS est obsolète et sera supprimée dans une prochaine version.
- La prise en charge de la version 7.x d'Elasticsearch/Kibana est obsolète et sera supprimée dans une prochaine version.
- Ajout de nouveaux paramètres de configuration pour le serveur de surveillance : `elasticsearch-client-connect-timeout-seconds` et `elasticsearch-client-read-timeout-seconds`, permettant de configurer les délais d'expiration de connexion et de lecture du client HTTP Elasticsearch.
- Ajout de valeurs par défaut aux groupes d'hôtes des serveurs de sécurité et des serveurs de registre dans Zabbix : `uxp-security-servers` et `uxp-registry-servers`, respectivement.
- Par défaut, la configuration des serveurs de registre sur Zabbix à l'aide du configurateur Zabbix natif UXP est désormais activée.
- Si Zabbix est configuré sur le serveur de surveillance, le nom d'utilisateur et le mot de passe de l'API de configuration sont désormais toujours requis. En outre, l'utilisateur configuré doit disposer d'une autorisation de lecture-écriture pour le groupe d'hôtes UXP `MS clusters` sur Zabbix afin d'assurer la continuité du fonctionnement.
- Amélioration du modèle Zabbix UXP `Security Server by MS` par l'ajout d'un nouveau

service UXP `uxp-message-log-timestamp`.

- Par défaut, les données de surveillance opérationnelle et les statistiques relatives au service de gestion, au méta-service et aux demandes de surveillance ne sont plus stockées sur Elasticsearch. De nouveaux paramètres de configuration sont introduits pour activer/désactiver cette fonction :
  - `opdata-exclude-management-service-transactions`,
  - `opdata-exclude-meta-service-transactions`,
  - `opdata-exclude-monitoring-transactions`,
  - `opdata-stats-exclude-management-service-transactions`,
  - `opdata-stats-exclude-meta-service-transactions`,
  - `opdata-stats-exclude-monitoring-transactions`.
- Mise à jour des bibliothèques et des composants tiers pour garantir la sécurité du système.
- Diverses corrections et améliorations mineures.

### 2.8.3 (02.2025)

- Ajout de la prise en charge de la grappe HA native Zabbix.
- Suppression de la prise en charge de la version 5.0 LTS de Zabbix.
- Amélioration du modèle UXP Security Server by MS Zabbix :
  - Nouveaux éléments ajoutés :
    - `uxp.certs.auth.expire_timestamp`
    - `uxp.certs.auth.ocsp_not_good`
    - `uxp.certs.sign.expire_timestamp`
    - `uxp.certs.sign.ocsp_not_good`
    - `uxp.gc.download_timestamp`
    - `uxp.proc.uxp_identity_provider_rest_api.status`
    - `uxp.proc.uxp_identity_provider_rest_api.uptime`
    - `uxp.proc.uxp_verifier_rest_api.status`
    - `uxp.proc.uxp_verifier_rest_api.uptime`
    - `uxp.system.sw.uxp_identity_provider_rest_api.version`
    - `uxp.system.jvm.operable`
  - De nouveaux déclencheurs ont été ajoutés :
    - Le certificat d'authentification expire dans moins de 30 jours
    - `L'état de la réponse OCSP du certificat d'authentification n'est pas « Bon »`
    - Le certificat de signature expire dans moins de 30 jours
    - `L'état de la réponse OCSP du certificat de signature n'est pas « Bon »`

- La dernière CG valide a été téléchargée il y a plus d'une heure
- [nginx | postgresql] est en panne
- [uxp-confclient | uxp-identity-provider-rest-api | uxp-messagelog-archiver | uxp-monitor | uxp-ocsp-cache | uxp-proxy | uxp-securityserver-rest-api | uxp-verifier-rest-api] est en panne
- Le taux de messages UXP dépasse le seuil
- **Modèle Zabbix** Serveur de registre UXP par MS amélioré :
  - **Nouveau déclencheur** Les données de surveillance ne sont pas mises à jour par MS ajouté.
- **Mise à jour des valeurs par défaut des paramètres de configuration de Zabbix :**
  - `conf_api_path` : est passé de `/zabbix/api_jsonrpc.php` à `/api_jsonrpc.php`
  - `conf_api_port` : est passé de `80` à `8080`
- **Amélioration de la haute disponibilité du serveur de surveillance :**
  - Tous les serveurs ayant le même nom de grappe et la même instance Zabbix ciblent automatiquement une grappe pour la collecte des données environnementales. Un nœud de la grappe (maître pour Zabbix) collecte les données, tandis que des nœuds de secours peuvent prendre le relais en cas de besoin.
- Amélioration des données de surveillance opérationnelle en faisant la distinction entre les messages SOAP et REST.
- Ajout de la collecte de statistiques sur les données de surveillance opérationnelle.
- Par défaut, le client HTTP Elasticsearch vérifie désormais le nom d'hôte du serveur Elasticsearch pendant l'établissement de la connexion TLS (lors de l'utilisation du schéma `https`).
- La période de validité des certificats TLS internes générés est passée de 20 à 100 ans.
- La plate-forme minimale supportée est maintenant Ubuntu 22.04 LTS.
- Mise à jour des bibliothèques et des composants tiers pour garantir la sécurité du système.
- Diverses corrections et améliorations mineures.

## 2.7.0 (06.2023)



Consultez la section [Migration](#) avant la mise à jour.

- Amélioration de la prise en charge d'Elasticsearch.
  - La version 8.x des outils Elasticsearch et Kibana est désormais prise en charge.
  - Remplacement du client Java High Level REST d'Elasticsearch obsolète par le client Java API.
  - Amélioration des exemples de visualisations et du tableau de bord Kibana.

- Amélioration de la prise en charge de Zabbix.
  - La version 6.0 LTS de Zabbix est désormais prise en charge.
  - L'ancienne version 4.0 LTS de Zabbix n'est plus officiellement prise en charge.
  - Les modèles Zabbix sont désormais utilisés pour configurer les serveurs de sécurité vers Zabbix.
    - Ajout du modèle `Template App UXP Security Server by MS` pour Zabbix 5.0 et `UXP Security Server by MS` pour Zabbix 6.0.
    - Anciennes clés d'objets et certains noms d'objets renommés.
    - Anciens éléments pour les progiciels UXP, états des processus et temps de fonctionnement divisés pour une meilleure convivialité.
    - Ajout d'un nouvel élément calculé `Disque libre en %`.
    - Suppression de l'élément sans valeur `La configuration globale est valide`.
    - Ajout de quelques déclencheurs aux modèles.
  - Amélioration des modèles de serveur de registre Zabbix.
    - Ajout du modèle `Template App UXP Registry Server by MS` pour Zabbix 5.0 et `UXP Registry Server by MS` pour Zabbix 6.0.
    - Suppression de l'ancien modèle Zabbix 4.0 `Template UXP Registry Server`.
    - Anciennes clés d'objets et certains noms d'objets renommés.
- L'historique des journaux système est désormais conservé pendant 60 jours au lieu de 30.
- Java Runtime Environment est mis à jour vers la version 17. Mise à jour d'autres bibliothèques et composants tiers afin de garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

## 2.6.0 (12.2022)

- Ubuntu 22.04 LTS est désormais une plate-forme prise en charge (et recommandée). Ubuntu 20.04 LTS est désormais une plate-forme minimale prise en charge. Consultez le guide de mise à niveau Ubuntu UXP-UPG-UB22.
- Versions des bibliothèques et composants tiers mises à niveau afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

## 2.5.0 (11.2021)



Le serveur de surveillance n'est plus compatible avec l'ancienne version **6.x** d'Elasticsearch.

- Le serveur de surveillance prend désormais en charge la connexion TLS et l'authentification de base avec Elasticsearch.
  - Ajout de nouveaux paramètres pour configurer le serveur de surveillance de manière

sécurisée vers Elasticsearch. Les nouveaux paramètres du fichier `monitor-agent.ini` sont `scheme`, `username`, `password`, `ca-cert-file`, et `verify-hostname`.

- Versions des bibliothèques et composants tiers mises à niveau afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

#### 2.4.1 (10.2021)

- Ajout de nouveaux paramètres de configuration `security-server-verify-hostname` et `registry-server-verify-hostname` pour activer la vérification du nom d'hôte des clients HTTP du serveur de sécurité et du serveur de registre lors de l'établissement d'une connexion TLS.

#### 2.4.0 (05.2021)

- Nouvelle solution de surveillance des serveurs de registre (voir UXP-IG-MS « Surveillance des serveurs de registre »).
  - Les paramètres spécifiques au système d'exploitation et à UXP peuvent être contrôlés.
  - Le serveur de surveillance peut automatiquement configurer Zabbix avec des serveurs de registre en tant qu'hôtes et leur associer les modèles appropriés.
- Le serveur de surveillance peut maintenant utiliser l'adresse IP interne du serveur de sécurité pour la communication (voir le paramètre `security-server-address` dans UXP-SYSPAR-MS).
  - Cela permet d'utiliser l'adresse IP interne du serveur de sécurité (au lieu de l'adresse donnée dans la configuration globale) en connexion avec le serveur de surveillance afin d'éviter le trafic sur le réseau public.
- Les niveaux de journalisation peuvent désormais être modifiés sans redémarrer les services UXP.
  - Cela permet de déboguer dans des environnements réels sans causer de temps d'arrêt.
- Les anciennes versions de Zabbix 2.2 – 2.4, et 3.0 – 3.4 ne sont plus officiellement prises en charge.
- Versions des bibliothèques et composants tiers mises à niveau afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

#### 2.3.0 (09.2020)

- Ajout de la prise en charge des clés EC et des clés RSA plus longues (3072 et 4096 bits) pour le certificat TLS du serveur de surveillance.
- Ajout de la prise en charge de TLS 1.3 (désormais protocole par défaut) entre le serveur de surveillance et le serveur de sécurité. TLS 1.2 est toujours pris en charge pour des raisons de compatibilité ascendante.
- Ubuntu 20.04 LTS est désormais une plate-forme prise en charge (et recommandée). Consultez le guide de mise à jour Ubuntu UXP-UPG-UB20.

- Versions des bibliothèques et composants tiers mises à niveau afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

### **2.2.1 (03.2020)**

- Amélioration du document UXP-IG-MS.

### **2.2 (02.2020)**

- La version 7.x des outils Elasticsearch et Kibana est désormais prise en charge.
- Les grappes Elasticsearch sont prises en charge.
- Ajout de la prise en charge des grappes de serveurs de surveillance. Plusieurs serveurs de surveillance peuvent être configurés pour utiliser la même grappe Elasticsearch.
- Ajout de la prise en charge des notifications par e-mail. Le serveur de surveillance peut désormais envoyer un e-mail en cas d'échec de la collecte des données de surveillance auprès des serveurs de sécurité.
- Ubuntu 18.04 LTS est désormais une plate-forme minimale prise en charge.
- Java Runtime Environment est mis à jour vers la version 11. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Corrections et améliorations mineures.

### **2.1 (08.2019)**

- Corrections et améliorations mineures.
- Mise à jour des bibliothèques tierces.
- Documentation améliorée (UXP-IG-MS).

### **2.0.1 (02.2018)**

- Documentation mise à jour.
- Correction de la collecte des données environnementales et amélioration de la gestion des erreurs.

### **2.0 (12.2018)**

- Lancement initial de la nouvelle architecture de surveillance. Prise en charge d'un nouveau protocole de surveillance (méthode pull au lieu de push, basée sur le protocole de message UXP) et de statistiques détaillées. Pour plus d'informations, consultez la section « Améliorations majeures » de UXP-IG-MS.
- Ubuntu 18.04 LTS est désormais une plate-forme prise en charge (et recommandée).