

Serveur de sécurité UXP 1.25

**Configuration de la surveillance du Serveur de sécurité
UXP-UG-PMA**

Table des matières

1. Introduction	1
1.1. Vue d'ensemble	1
1.2. Public cible	1
1.3. Références	1
2. Surveillance des serveurs de sécurité UXP	3
2.1. Types de données de surveillance	3
2.2. Niveaux de surveillance	3
2.3. Contrôle d'accès aux données de surveillance	5
2.3.1. Droits d'accès aux données de surveillance environnementale	5
2.3.2. Droits d'accès aux données de surveillance opérationnelle et à leurs statistiques	6
2.3.3. Droits d'accès aux données d'état de santé	6
2.4. Utilisations des services de surveillance	6
2.5. Ports par défaut pour la surveillance	6
2.6. Versions testées de Zabbix et Elasticsearch	7
3. Surveillance environnementale	9
3.1. Paramètres système requis pour le serveur Zabbix	9
3.2. Installer Zabbix	10
3.2.1. Installer un seul serveur Zabbix	10
3.2.2. Installer Zabbix dans une configuration HA native	13
Installer le serveur de base de données	13
Installer un nœud du serveur Zabbix	14
3.3. Connecter Zabbix à l'agent de surveillance proxy	17
3.4. Configurer l'hôte du serveur de sécurité Zabbix	18
3.4.1. Configuration via le configurateur Zabbix natif UXP	18
3.4.2. Configuration via Zabbix Discovery	20
3.4.3. Modèle Zabbix : Serveur de sécurité UXP par PMA	22
4. Surveillance opérationnelle	27
4.1. Configurer la surveillance opérationnelle	27
4.1.1. Arrêt de la collecte des données opérationnelles	27
4.1.2. Modification de l'intervalle de nettoyage de la base de données	27
5. Configurer Elasticsearch et Kibana	29

5.1. Document de données opérationnelles dans Elasticsearch	29
5.2. Installer Elasticsearch et Kibana	31
5.2.1. Chiffrement du trafic entre le navigateur Web et Kibana	34
5.2.2. Installer une grappe Elasticsearch à plusieurs nœuds	36
5.3. Connecter Elasticsearch à l'Agent de surveillance proxy	38
5.3.1. Créer un utilisateur Elasticsearch pour l'agent de surveillance Proxy	38
5.3.2. Configurer l'agent de surveillance Proxy	39
5.3.3. Utiliser un cluster Elasticsearch à plusieurs nœuds	41
5.3.4. Remplacer le certificat TLS du client Elasticsearch	42
5.4. Configurer Kibana pour l'analyse	44
5.4.1. Créer une vue de données pour les données opérationnelles	44
5.4.2. Exemple de tableau de bord	45
5.4.3. Autres exemples de visualisation	46
6. Maintenance	48
6.1. Configurer la grappe Zabbix	48
6.1.1. Ajout d'un nœud Zabbix supplémentaire	48
6.1.2. Supprimer un nœud Zabbix	48
6.1.3. Désactiver la grappe HA	49
6.1.4. Changer l'adresse d'un nœud Zabbix	49
6.2. Configurer une grappe Elasticsearch	50
6.2.1. Ajouter un nœud Elasticsearch supplémentaire	50
6.2.2. Supprimer un nœud Elasticsearch	51
6.2.3. Changer l'adresse d'un nœud Elasticsearch	53
7. Dépannage	56
7.1. Fichier journal	56
7.2. Recharger l'agent de surveillance Proxy	56
7.3. Modifier la configuration de l'agent de surveillance proxy	56
7.4. Spam dans les journaux Zabbix : Le prétraitement a échoué pour	56

1. Introduction

1.1. Vue d'ensemble

Ce guide d'utilisation décrit comment configurer la surveillance des serveurs de sécurité au niveau organisationnel. Le guide comprend des instructions sur la manière d'envoyer les données de surveillance collectées aux serveurs Zabbix et Elasticsearch pour un traitement et une visualisation ultérieurs.

La surveillance est assurée par le module complémentaire Agent de surveillance de proxy (PMA). Le module complémentaire PMA est installé lors de l'installation du serveur de sécurité et ne nécessite aucune autre installation.



Si vous devez configurer la surveillance au niveau central, en utilisant un serveur de surveillance, reportez-vous au Guide d'installation et de configuration du Serveur de surveillance UXP [UXP-IG-MS].

1.2. Public cible

Ce guide s'adresse aux administrateurs système responsables de la surveillance des serveurs de sécurité UXP au sein d'une organisation.

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.

Une connaissance de base de la solution de surveillance distribuée Zabbix ainsi que des outils d'analyse de données Elasticsearch et Kibana est requise. Reportez-vous aux sections correspondantes de la documentation de [Zabbix](#) [Zabbix], [Elasticsearch](#) et [Kibana](#) [Elastic].

1.3. Références

- [CRON] Expression CRON de Quartz Scheduler, <http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html>
- [DATE-TIME-FORMATTER] DateTimeFormatter (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>
- [Time-Zones] Liste des fuseaux horaires pris en charge, <http://php.net/manual/en/timezones.php>
- [UXP-IG-MS] Cybernetica AS. Serveur de surveillance UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-MS
- [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-UG-SSHA] Cybernetica AS. Serveur de sécurité UXP : Configuration de la haute disponibilité et de l'équilibrage de la charge. Identifiant du document : UXP-UG-SSHA
- [Zabbix] Documentation Zabbix, <http://www.zabbix.com/documentation.php>
- [Zabbix-Discovery] Manuel Zabbix, Découverte, <https://www.zabbix.com/documentation/7.0/en/manual/discovery>
- [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-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 jour, <https://www.zabbix.com/documentation/7.0/en/manual/installation/upgrade>

2. Surveillance des serveurs de sécurité UXP

2.1. Types de données de surveillance

Le serveur de sécurité génère quatre types de données de surveillance.

Données de surveillance environnementale

Informations sur l'état du serveur de sécurité. Par exemple, la consommation de mémoire, l'utilisation du processeur, les versions des paquets, etc.

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.

Données sur la santé

Statistiques basées sur les données de surveillance environnementale et opérationnelle. Par exemple, l'heure de la dernière demande réussie et le nombre de demandes infructueuses.

2.2. Niveaux de surveillance

Dans une instance UXP, la surveillance peut s'effectuer à deux niveaux : organisationnel et central. La figure 1 présente les composants de la solution de surveillance UXP.

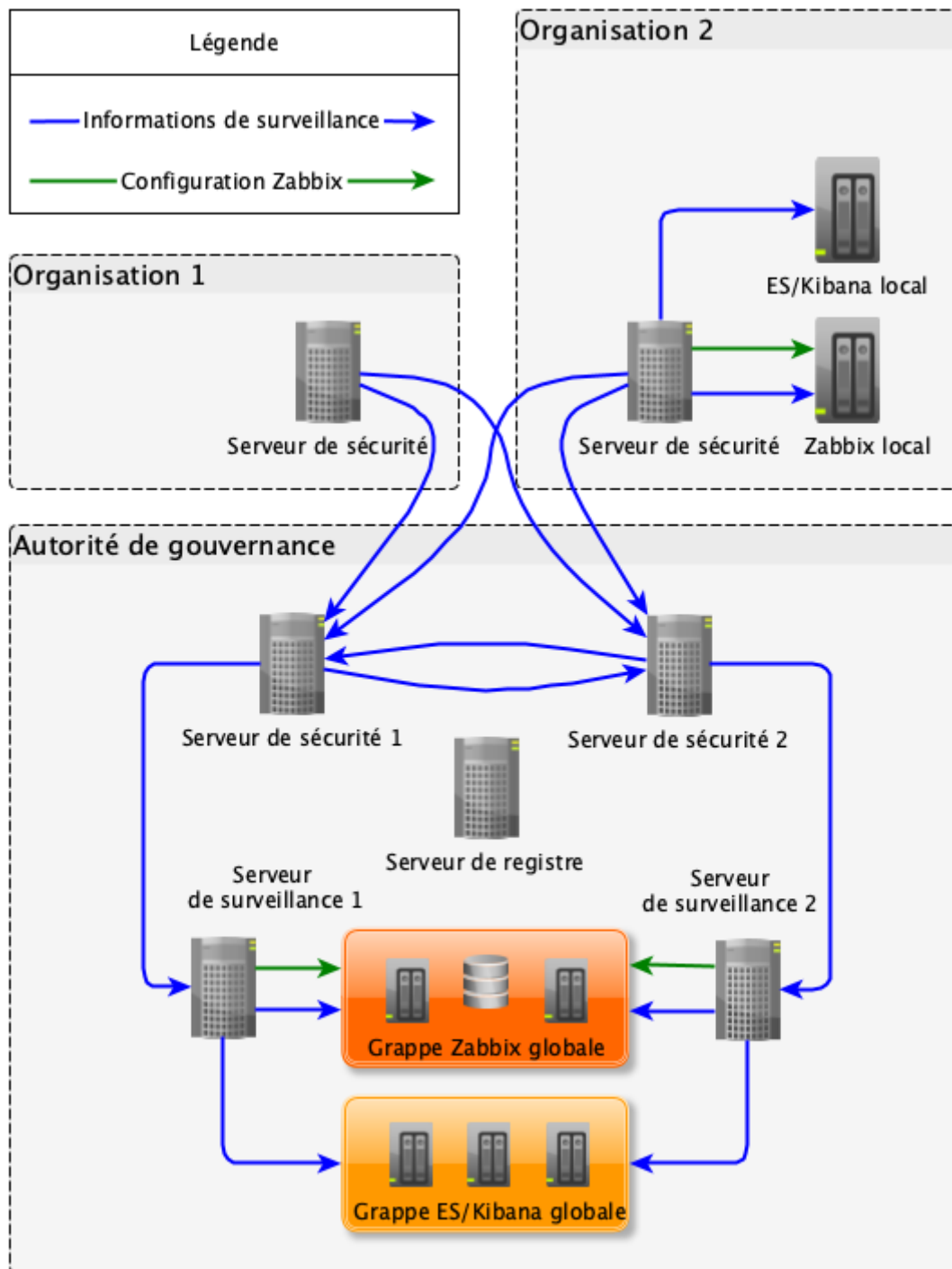


Figure 1. La solution de surveillance UXP

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 central) 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 central de surveillance 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 central de surveillance et le serveur de surveillance doit être configurée pour utiliser HTTPS. Le serveur de sécurité et le serveur de surveillance utilisent tous deux leurs certificats TLS internes qui sont distribués manuellement à chacune des parties. L'authentification se fait à la fois du côté du client et du côté du serveur.

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

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).

2.3. Contrôle d'accès aux données de surveillance

Toutes les données de surveillance ne sont pas accessibles de la même manière à tous les clients des services. L'accès aux données de surveillance est contrôlé afin de protéger les informations détaillées relatives à la consommation des services des membres UXP et à l'état de santé des serveurs de sécurité du public. Parallèlement, toutes les données de surveillance sont accessibles au système de surveillance central afin de contrôler l'état de l'instance UXP.



Le propriétaire du serveur de sécurité peut demander un ensemble complet de données de surveillance à son serveur de sécurité. Pour éviter tout accès non autorisé aux données de surveillance, la connexion entre le serveur de sécurité et le système d'information qui demande des informations en tant que propriétaire du serveur de sécurité doit être configurée pour utiliser HTTPS. Cela peut être fait dans l'onglet « Serveurs internes » des détails du propriétaire du serveur de sécurité.

2.3.1. Droits d'accès aux données de surveillance environnementale

- Le client de surveillance central peut recevoir les données de surveillance environnementale provenant de tous les serveurs de sécurité d'une instance UXP. Ce droit est utilisé par le serveur de surveillance pour rassembler les données de surveillance de tous les serveurs de sécurité de l'instance.
- Le propriétaire du serveur de sécurité peut recevoir les données de surveillance environnementale de son propre serveur de sécurité.

2.3.2. Droits d'accès aux données de surveillance opérationnelle et à leurs statistiques

- Le client de surveillance central peut recevoir les données de surveillance opérationnelle et leurs statistiques concernant les demandes traitées par tous les serveurs de sécurité de l'instance UXP. Ce droit est utilisé par le serveur de surveillance pour rassembler les données de surveillance de tous les serveurs de sécurité de l'instance.
- Le propriétaire du serveur de sécurité peut recevoir des données de surveillance opérationnelle et leurs statistiques concernant toutes les demandes traitées par son propre serveur de sécurité.
- Tous les clients du serveur de sécurité peuvent recevoir des données de surveillance opérationnelle et leurs statistiques concernant toutes les demandes, qu'ils jouent le rôle de client de service ou de fournisseur de service. Les clients du service peuvent demander leurs données de surveillance opérationnelle et leurs statistiques à partir de n'importe quel serveur de sécurité de l'instance UXP.

2.3.3. Droits d'accès aux données d'état de santé

- Tous les clients (y compris les propriétaires de serveurs de sécurité et le client de surveillance central) peuvent demander les données d'état de santé de tous les serveurs de sécurité.

2.4. Utilisations des services de surveillance

Les privilèges du client de surveillance central sont utilisés par le serveur de surveillance UXP pour surveiller l'ensemble de l'instance UXP.

Les privilèges du propriétaire du serveur de sécurité et des clients peuvent être utilisés par les membres UXP pour mettre en œuvre leurs propres applications personnalisées qui recueillent et traitent les données de surveillance. Par exemple, dans les cas où les outils de surveillance externes (Zabbix, Elasticsearch/Kibana) pris en charge par défaut par les composants UXP ne sont pas suffisants pour atteindre un certain objectif commercial.

Les détails techniques sur la manière d'utiliser les services de surveillance sont disponibles dans la spécification du protocole de surveillance UXP [\[UXP-PR-MON\]](#).

2.5. Ports par défaut pour la surveillance

Le tableau ci-dessous répertorie les ports par défaut utilisés par le module complémentaire PMA du serveur de sécurité pour recevoir des demandes et se connecter aux serveurs Zabbix et Elasticsearch. Si des ports autres que ceux par défaut sont configurés (voir les sections [Installer Zabbix](#) et [Configurer Elasticsearch et Kibana](#)), utilisez-les à la place de ceux définis dans les tableaux.



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 entrantes au serveur de sécurité

Port (TCP)	Objectif	Portée du réseau
2082	Utilisé pour écouter les demandes de service d'informations d'état. Ceci n'est nécessaire que lorsqu'un équilibreur de charge interne est utilisé pour répartir les demandes entre les nœuds d'une grappe de serveurs de sécurité (voir [UXP-UG-SSHA]).	PRIVÉ

Ports requis pour les connexions sortantes du serveur de sécurité

Port (TCP)	Objectif	Portée du réseau
8080	Utilisé pour la configuration à distance du serveur Zabbix. Ceci n'est nécessaire que lorsque Zabbix est utilisé pour surveiller localement le serveur de sécurité avec le configurateur Zabbix natif UXP.	PRIVÉ
10051	Utilisé pour transmettre les données de surveillance au serveur Zabbix. Cela n'est nécessaire que lorsque Zabbix est utilisé pour surveiller localement le serveur de sécurité.	PRIVÉ
9200	Utilisé pour transmettre les données de surveillance opérationnelle au serveur Elasticsearch (API RESTful). Cela n'est nécessaire que si Elasticsearch est utilisé pour surveiller localement le serveur de sécurité.	PRIVÉ

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 sur 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.

2.6. Versions testées de Zabbix et Elasticsearch

PMA a été testé et confirmé comme fonctionnant avec :

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



PMA 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 PMA, il est

recommandé d'effectuer une mise à jour vers Zabbix 7.0 LTS.

3. Surveillance environnementale

PMA collecte périodiquement les données environnementales du serveur de sécurité (par défaut, toutes les 15 secondes) et les met en mémoire.

Transmettez les données collectées à Zabbix pour une analyse, des alertes et des rapports centralisés. Pour cela, installez le logiciel Zabbix approprié (version 7.0 LTS) ou utilisez un logiciel existant, et configurez-le avec PMA.

Vous pouvez utiliser un seul serveur Zabbix 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 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 dans la section suivante. Ensuite, ignorez la section [Installer Zabbix](#) et poursuivez avec la configuration décrite dans la section [Connecter Zabbix à l'agent de surveillance proxy](#). Sinon, passez à la section [Installer Zabbix](#) pour installer un serveur Zabbix répondant à la configuration requise.

3.1. Paramètres système requis pour le serveur Zabbix

- Système d'exploitation Ubuntu 24.04 ou 22.04 Long-Term Support (LTS) sur une plateforme 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 suivantes, 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, le modèle Zabbix pour le serveur de sécurité UXP Security Server by PMA comporte 62 éléments (piégés). L'intervalle par défaut pour l'envoi des données de surveillance (configuré par le paramètre `zabbix-send-interval-seconds` dans `/etc/uxp/conf.d/addons/proxy-monitor-agent.ini`) est de 180 secondes, c'est-à-dire que le NVPS du serveur de sécurité est $62/180 = 0.34$.

Par défaut, Zabbix conserve les valeurs pendant 90 jours, soit $(90 * 24 * 3600) * 0.34 = 2.643.840$, ou environ 2,64 millions de valeurs.

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 50 valeurs numériques et 12 valeurs de chaînes de caractères (principalement des versions de paquets). Dans ce cas, cela signifie que 2,64 millions de valeurs nécessiteront $2.64M * 90bytes = 230MB$ d'espace disque.

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 62 éléments nécessitent $62 * (24 * 365) * 90bytes = 49MB$ 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 : $(365 * 24 * 3600) * (250bytes + 80bytes)$.

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 $10MB + 230MB + 49MB + 10GB = 11GB$.

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

3.2. Installer Zabbix



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

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

3.2.1. Installer un seul serveur Zabbix

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**, choisissez **Users** et cliquez sur 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 à l'agent de surveillance proxy](#) pour obtenir des instructions sur la configuration de PMA 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.

3.2.2. Installer Zabbix dans une configuration HA native

En mode Zabbix HA, plusieurs serveurs Zabbix sont exécutés en tant que nœuds dans une grappe et 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 seul serveur Zabbix](#).
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 seul serveur Zabbix](#).
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-pgsql zabbix-frontend-php \
php8.3-pgsql 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**, choisissez **Users** et cliquez sur 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 de PMA afin

qu'il se connecte au serveur Zabbix.

3.3. Connecter Zabbix à l'agent de surveillance proxy

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 sécurité, 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.

Avant que le serveur Zabbix connecté puisse recevoir des données de surveillance, les hôtes surveillés et leurs entités doivent être configurés correctement sur le serveur Zabbix. Passez à la section suivante, [Configurer l'hôte du serveur de sécurité 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 de PMA. Pour ce faire, exécutez la commande suivante sur le serveur de sécurité :

```
sudo reload-monitor-agent
```

3.4. Configurer l'hôte du serveur de sécurité Zabbix

Assurez-vous que l'hôte du serveur de sécurité et ses entités de surveillance sont correctement configurés sur le serveur Zabbix. Vous avez deux options : utiliser soit le configurateur Zabbix natif UXP, soit la solution de découverte native de Zabbix [\[Zabbix-Discovery\]](#).

Après la configuration, vérifiez dans l'interface utilisateur Zabbix que l'hôte du serveur de sécurité a été créé et que les données de surveillance sont reçues en naviguant vers **Monitoring** → **Latest data**.

3.4.1. Configuration via le configurateur Zabbix natif UXP

PMA comprend une fonctionnalité permettant de configurer l'hôte du serveur de sécurité sur le serveur Zabbix par l'intermédiaire de l'API Zabbix. Au cours de ce processus, PMA crée un groupe d'hôtes sur le serveur Zabbix et ajoute à ce groupe l'hôte du serveur de sécurité sur lequel il s'exécute. En outre, PMA importe le modèle UXP Security Server by PMA, qui est le modèle de serveur de sécurité pour Zabbix 7.0 (situé dans le répertoire `/usr/share/uxp/templates/zabbix`), sur le serveur Zabbix et le lie à l'hôte nouvellement ajouté.

Au lancement, PMA tente de configurer le serveur Zabbix. Si la configuration échoue (par exemple, si Zabbix est en panne), PMA réessaie périodiquement la configuration jusqu'à ce qu'elle réussisse.

Pour activer le configurateur Zabbix, procédez comme suit :

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

1. Créez un groupe d'hôtes pour les serveurs de sécurité en naviguant vers **Data collection** → **Host groups** et en cliquant sur **Create host group**.
 - a. Saisissez un nom de groupe, par exemple `uxp-security-servers`.
 - b. Cliquez enfin sur **Add**.
2. Créez un groupe d'utilisateurs en naviguant vers **Users** → **User groups** et en cliquant sur **Create user group**.
 - a. Saisissez un nom de groupe, par exemple `UXP PMAs`.
 - b. Sélectionnez `Disabled` pour **Frontend access**.
 - c. Dans l'onglet **Template permissions**, cliquez sur le lien **Add** et sélectionnez `Templates/Applications` modèle de groupe. Choisissez les permissions `Read-write`.
 - d. Dans l'onglet **Host permissions**, cliquez sur le lien **Add** et sélectionnez le groupe d'hôtes des serveurs de sécurité créé précédemment. Choisissez les permissions `Read-write`.
 - e. Cliquez enfin sur **Add**.
3. Créez un utilisateur en naviguant vers **Users** → **Users**, et en cliquant sur **Create user**.
 - a. Saisissez un nom d'utilisateur, par exemple `uxp-pma`.
 - 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**.

Configurer Zabbix sur le serveur de sécurité

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

```
[zabbix-1]

; ...



enable_configurator = true
host_group = uxp-security-servers

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

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 3. Paramètres du configurateur Zabbix

Champ	Valeur par défaut	Explication
enable_configurator	true	Active/désactive la configuration automatique du serveur Zabbix.
<div>  Les options suivantes n'ont d'effet que si <code>enable_configurator = true</code>. </div>		
enable_update_existing_triggers	true	Active/désactive la mise à jour des déclencheurs existants (potentiellement écrasés) des modèles Zabbix UXP. Réglez ce paramètre sur <code>false</code> si vous souhaitez conserver les déclencheurs qui ont été modifiés manuellement dans Zabbix.
enable_coexisting_mode	false	Active/désactive le mode coexistant avec le serveur de surveillance UXP. Si le mode coexistant est activé, le nom d'hôte configuré dans Zabbix reçoit le suffixe « <i>(local)</i> ».
<div>  Si le serveur Zabbix configuré est également utilisé par le serveur de surveillance UXP, activez le mode coexistant pour éviter les collisions de configuration. </div>		
username		Nom d'utilisateur Zabbix. Le type d'utilisateur doit être <code>Super admin</code> ou <code>Admin</code> avec des autorisations <code>Read-write</code> pour les serveurs de sécurité configurés et les groupes d'hôtes <code>Templates/Applications</code> .
password		Mot de passe de l'utilisateur de Zabbix.
conf_api_port	8080	Port de l'API de configuration de Zabbix.
conf_api_path	/api_jsonrpc.php	Chemin de l'API de configuration de Zabbix.
host_group	uxp-security-servers	Le groupe d'hôtes dont PMA doit configurer le serveur de sécurité pour qu'il en fasse partie.

Après avoir mis à jour la configuration, rechargez la configuration de PMA en exécutant la commande suivante sur le serveur de sécurité :

```
sudo reload-monitor-agent
```

3.4.2. Configuration via Zabbix Discovery

Zabbix Discovery est une fonction qui identifie automatiquement les hôtes sur la base de

critères tels que les plages IP ou les protocoles réseau au sein de votre infrastructure informatique. Lorsqu'elle est déclenchée, cette action de découverte ajoute l'hôte du serveur de sécurité identifié et y associe le modèle UXP Security Server by PMA.

Suivez les étapes ci-dessous pour établir la configuration de l'hôte dans le serveur Zabbix à l'aide de Discovery :

Obtenez le fichier modèle du serveur de sécurité pour Zabbix

1. Copiez le fichier modèle UXP Security Server by PMA `template_app_uxp_security_server_by_pma.yaml` du répertoire `/usr/share/uxp/templates/zabbix/7.0` du serveur de sécurité vers l'ordinateur sur lequel vous exécutez l'interface utilisateur Zabbix.

Dans l'interface utilisateur de Zabbix

2. Importez le modèle UXP Security Server by PMA précédemment copié en naviguant vers **Data collection** → **Templates**, et en cliquant sur **Import**. Choisissez le fichier modèle et cliquez sur **Import**.
3. Créez un groupe d'hôtes pour les serveurs de sécurité découverts en naviguant vers **Data collection** → **Host groups** et en cliquant sur **Create host group**. Saisissez le nom du groupe (par exemple, `uxp-security-servers`) et cliquez sur **Add**.
4. Créez une règle de découverte en naviguant vers **Data collection** → **Discovery**, et en cliquant sur **Create discovery rule**.
 - a. Saisissez le nom de la règle de découverte (par exemple, `Security servers`)
 - b. Saisissez la plage IP correcte pour les serveurs de sécurité.
 - c. Ajoutez un contrôle de découverte en cliquant sur le lien **Add**. Sélectionnez **HTTPS** comme type de contrôle, entrez le port `4000` (le port d'interface utilisateur du serveur de sécurité) et cliquez sur **Add**.
 - d. Pour l'option **Host name**, sélectionnez `DNS name` ou `IP address`.



La valeur de l'option **DNS name** exige que le réseau surveillé utilise des serveurs DNS qui prennent en charge la recherche DNS inversée, ce qui permet de résoudre les adresses IP en noms de domaine.

- e. Cliquez enfin sur **Add**.
5. Créez une action de découverte pour la règle créée en accédant à **Alerts** → **Actions** → **Discovery actions**, et en cliquant sur **Create action**.
 - a. Entrez le nom de l'action (par exemple, `Détection automatique. Serveurs de sécurité`).
 - b. Ajoutez une condition en cliquant sur le lien **Add**.
 - i. Pour le **Type**, sélectionnez `Discovery rule`, pour **Operator**, sélectionnez `equals`, et pour les **Discovery rules**, sélectionnez la règle précédemment créée (par exemple, `Security servers`).
 - ii. Cliquez sur **Add**.

- c. Ajoutez les opérations suivantes en cliquant sur l'onglet **Operations** :
 - i. Cliquez sur le lien **Add**. Sélectionnez Add to host group pour **Operation**, le groupe d'hôtes précédemment créé (par exemple, uxp-security-servers) pour les **Host groups**, et cliquez sur **Add**.
 - ii. Cliquez sur le lien **Add**. Pour **Operation**, sélectionnez Link template, et pour **Templates**, sélectionnez le modèle précédemment importé UXP Security Server by PMA dans le groupe de modèles Templates/Applications. Cliquez sur **Add**.
- d. Cliquez enfin sur **Add**.

Sur le serveur de sécurité

6. Modifiez le fichier de configuration /etc/uxp/monitor-agent.ini pour désactiver le configurateur Zabbix natif UXP et définissez le type de nom d'hôte technique à DNS ou IP conformément à la règle de découverte créée précédemment :

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

enable_configurator = false
technical_host_name_type = DNS
```

Après avoir mis à jour la configuration, rechargez la configuration de PMA en exécutant la commande suivante :

```
sudo reload-monitor-agent
```



Si PMA commence à envoyer des données de surveillance avant que Zabbix ne découvre le serveur de sécurité, des journaux d'avertissement concernant l'échec du traitement de certains paramètres de demande par Zabbix peuvent apparaître dans le fichier proxymonitoragent.log. Il s'agit d'un comportement normal qui s'arrêtera une fois que l'hôte du serveur de sécurité aura été correctement découvert et configuré dans Zabbix.

3.4.3. Modèle Zabbix : Serveur de sécurité UXP par PMA

Le modèle Security Server by PMA, situé sur le serveur de sécurité /usr/share/uxp/templates/zabbix/7.0/template_app_uxp_security_server_by_pma.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.

Nom	Description
Authentication certificate OCSP status not good	Indique si un certificat d'authentification actif et enregistré a une réponse OCSP avec un statut autre que Good.
Authentication certificate usable	Indique si au moins un certificat d'authentification est utilisable.
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.
Global configuration valid	Indique si la configuration globale est valide.
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].
[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.
Security server status	Indique l'état actuel du serveur de sécurité.
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 statut autre que Good.
Software token logged in	Indique si le jeton logiciel de la ou des clés d'authentification est connecté.
Statistics period	Durée de la période statistique.
Swap free	Espace swap libre disponible.
Swap total	La taille du swap.

Nom	Description
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].
[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	Temps de fonctionnement 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].
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.

Nom	Description
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 %.
Global configuration is not valid	Alerte lorsque la configuration globale n'est pas valide.
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.
Monitoring data is not updated by PMA	Alertes lorsque les données de surveillance ne sont pas mises à jour par PMA 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.
Security server is down	Alerte lorsque l'état du serveur de sécurité est DOWN.
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 ».
Software token is not logged in	Alerte lorsque le jeton logiciel de la ou des clés d'authentification n'est pas connecté.

Nom	Description
[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 demandes par seconde au cours de la période statistique.

4. Surveillance opérationnelle

Le serveur de sécurité crée un enregistrement de données de surveillance opérationnelle pour chaque demande UXP échangée. Ces enregistrements sont mis en cache dans le tampon de surveillance opérationnelle basé sur la mémoire et sont ensuite transmis au module complémentaire PMA pour être stockés dans la base de données. Les enregistrements transmis avec succès sont retirés de la mémoire tampon de surveillance opérationnelle.

Pour analyser et visualiser les données opérationnelles, transférez-les depuis PMA vers Elasticsearch. Vous pouvez installer un nouveau serveur Elasticsearch/Kibana ou utiliser un serveur existant. Assurez-vous qu'il est correctement configuré avec PMA (voir section [Configurer Elasticsearch et Kibana](#)).

4.1. Configurer la surveillance opérationnelle

Les valeurs par défaut des paramètres de surveillance opérationnelle ont été choisies pour être suffisantes dans le cas d'une charge moyenne prévue tout en utilisant le matériel minimum recommandé (fichier de configuration `/etc/uxp/conf.d/addons/proxy-monitor-agent.ini`).

Pour remplacer les valeurs par défaut, ajoutez `[op-monitor-buffer]` et `[op-monitor]` au fichier `/etc/uxp/conf.d/local.ini` sur le serveur de sécurité et définissez de nouvelles valeurs de paramètres. Pour en savoir plus, consultez les sections suivantes.

4.1.1. Arrêt de la collecte des données opérationnelles



Il n'est PAS recommandé d'arrêter ou de désactiver la collecte des données de surveillance opérationnelle, car celles-ci sont utilisées à des fins de surveillance, pour produire des rapports à l'intention des propriétaires d'entreprises ou sont exigées par les autorités.

Si, pour une raison quelconque, les données opérationnelles ne doivent pas être collectées et transmises à PMA, vous pouvez régler le paramètre de mémoire tampon de surveillance opérationnelle `size` sur 0 (la valeur par défaut est de 20 000 enregistrements) :

```
[op-monitor-buffer]
size = 0
```

Après avoir modifié la configuration, redémarrez le service `uxp-proxy` pour appliquer les changements :

```
sudo systemctl restart uxp-proxy
```

4.1.2. Modification de l'intervalle de nettoyage de la base de données

En fonction de la charge du système et des ressources disponibles, il peut être nécessaire d'ajuster l'intervalle de suppression des anciens enregistrements de la base de données de surveillance opérationnelle.

Pour modifier l'intervalle de suppression, placez les paramètres suivants dans la section `[op-monitor]`.

Modifiez `retain-records-for-days` si l'intervalle de nettoyage est trop court ou trop long. Par exemple, si le disque se remplit avant le nettoyage ou si vous devez conserver les enregistrements pendant une durée supérieure à la durée par défaut de 7 jours.

Le paramètre `clean-interval` (une [expression Cron \[CRON\]](#)) spécifie la fréquence à laquelle le système vérifie si un nettoyage est nécessaire. Si l'intervalle par défaut de 12 heures ne convient pas, ajustez-le selon vos besoins.

Après avoir modifié la configuration, redémarrez le service `uxp-monitor` pour appliquer les changements :

```
sudo systemctl restart uxp-monitor
```

5. Configurer Elasticsearch et Kibana

5.1. Document de données opérationnelles dans Elasticsearch

Le serveur de sécurité collecte des données opérationnelles, un enregistrement de données est stocké (via PMA) pour chaque message UXP transmis. 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 dans PMA.
request_attachment_count	integer	Nombre de pièces jointes dans la demande SOAP.
request_in_ts	date	<ul style="list-style-type: none"> 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. 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.
request_mime_size	long	Taille du conteneur MIME de la demande SOAP (avec pièces jointes) en octets.

Champ	Type de données	Description
request_out_ts	date	<ul style="list-style-type: none"> Sur le serveur de sécurité du client : Heure UTC (précision à la milliseconde près) à laquelle la demande a été envoyée depuis le serveur de sécurité du client vers le serveur de sécurité du fournisseur de services. Sur le serveur de sécurité du fournisseur de services : Heure UTC (précision à la milliseconde près) à laquelle la demande a été envoyée depuis le serveur sécurisé du fournisseur de services.
request_soap_size	long	Taille de la demande SOAP ou 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"> 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. 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.
response_mime_size	long	Taille du conteneur MIME de la réponse SOAP (avec pièces jointes) en octets.
response_out_ts	date	<ul style="list-style-type: none"> 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. 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.
response_soap_size	long	Taille de la réponse SOAP ou 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).

Champ	Type de données	Description
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 (prestataire 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.
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.

5.2. 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 plate-

forme 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 [\[Elastic-Heap\]](#).

- 20 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 à environ 250 Mo pour 1 million d'enregistrements.

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 PMA pour qu'il communique avec une instance existante d'Elasticsearch, ignorez cette section. Reportez-vous à la section [Connecter Elasticsearch à l'Agent de surveillance proxy](#) pour obtenir des instructions sur la configuration.



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

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 du paquet 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/ jammy 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. Ajoutez 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. Sur l'interface utilisateur Kibana, connectez-vous en tant qu'utilisateur `elastic` en utilisant le mot de passe précédemment généré ou modifié.



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.

5.2.1. 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 de clés et de 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/`.

5.2.2. 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. 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 précédente [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-here>
```



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.

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

```
sudo systemctl restart elasticsearch
```

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

```
sudo systemctl enable elasticsearch
```

9. 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							

10. 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](#).

11. 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.

5.3. Connecter Elasticsearch à l'Agent de surveillance proxy

Pour interagir avec Elasticsearch, PMA 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 à l'index des données de surveillance opérationnelle décrit à la section [Configurer l'agent de surveillance Proxy](#)). Reportez-vous à la section [Créer un utilisateur Elasticsearch pour l'agent de surveillance Proxy](#) pour créer un utilisateur Elasticsearch approprié s'il n'en existe pas déjà un.

Reportez-vous à la section [Configurer l'agent de surveillance Proxy](#) pour obtenir des instructions sur la configuration de PMA afin qu'il interagisse avec Elasticsearch.

5.3.1. Créer un utilisateur Elasticsearch pour l'agent de surveillance Proxy

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



L'utilisateur de PMA doit avoir au moins :

1. Privilèges `create_index`, `manage`, `read`, `view_index_metadata` et `write` sur l'index Elasticsearch configuré (par défaut : `uxp-request`) ;
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 PMA en naviguant sur **Management** → **Stack Management** → **Security** → **Roles**, puis en cliquant sur **Create role**.
2. Saisissez un nom de rôle (par exemple, `uxp_pma_client`) et une description de rôle (par exemple, `Grants privileges to UXP PMA`).

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 un modèle d'indexation pour les données de surveillance opérationnelle, tel que `uxp-request*`, puis sélectionnez les privilèges requis : `create_index`, `manage`, `read`, `view_index_metadata` et `write`. Cliquez enfin sur **Create role**.



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.

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_pma`), un mot de passe et sélectionnez un rôle précédemment créé, tel que `uxp_pma_client`.
7. Cliquez enfin sur **Create user**.

5.3.2. Configurer l'agent de surveillance Proxy

Sur le serveur de sécurité, activez la transmission des données de surveillance opérationnelle au 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 sécurité.
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_pma
password = *****

index = uxp-request
```





Par défaut, PMA 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 4. Paramètres d'Elasticsearch

Champ	Valeur par défaut	Explication
address		Nom d'hôte (résolu en adresse IP via DNS) ou adresse IP du serveur Elasticsearch. Obligatoire.
port	9200	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). Obligatoire si le schéma https est utilisé. L'agent de surveillance proxy a besoin de ce certificat CA 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.
username		Le nom d'utilisateur Elasticsearch pour l'authentification de base. Obligatoire si l'authentification de base est utilisée.
		<div>  <p>Assurez-vous que l'utilisateur Elasticsearch configuré dispose des privilèges requis pour l'index configuré.</p> </div>
password		Le mot de passe de l'utilisateur Elasticsearch pour l'authentification de base. Obligatoire 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.

Champ	Valeur par défaut	Explication
index	uxp-request	<p>Nom de l'index du document. 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 (<code>%{DATE_PATTERN}</code>). Par exemple, <code>uxp-%{yyyy.MM.dd}</code>, <code>uxp-%{M.y}-opdata</code>, où y représente l'année, M le mois et d le jour du mois. Pour des informations plus détaillées sur la syntaxe des motifs de date, lisez le chapitre « Patterns for Formatting and Parsing » de la documentation Java [DATE-TIME-FORMATTER].</p> <div>  <p>Assurez-vous que l'utilisateur Elasticsearch configuré dispose des privilèges requis pour l'index configuré.</p> </div>
max_batch_records	1000	L'API bulk d'Elasticsearch permet d'indexer plusieurs documents en une seule demande. Ce paramètre détermine le nombre maximal d'enregistrements de surveillance pour une demande groupée.
collection_start_timestamp	1970-01-01T00:00:00Z	L'horodatage de l'enregistrement de surveillance (en secondes Unix ou ISO 8601, par exemple 2018-01-01T00:00:00Z) à partir duquel la collecte des enregistrements commence.

Après avoir mis à jour la configuration, rechargez la configuration de PMA en exécutant la commande suivante :

```
sudo reload-monitor-agent
```



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



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

5.3.3. Utiliser un cluster Elasticsearch à plusieurs nœuds

Lorsque vous utilisez une grappe Elasticsearch à plusieurs nœuds, vous pouvez configurer PMA pour qu'il se connecte à plusieurs nœuds Elasticsearch sur la même grappe. Si un nœud

devient indisponible, PMA 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 la configuration de PMA en exécutant la commande suivante :

```
sudo reload-monitor-agent
```

5.3.4. Remplacer le certificat TLS du client Elasticsearch

Lors de l'installation du serveur de sécurité, un certificat TLS auto-signé est généré pour le client Elasticsearch utilisé par PMA. Le certificat peut être consulté à l'adresse `/etc/uxp/ssl/elasticsearch.crt` et sa période de validité est de 100 ans.

Voici quelques situations qui nécessitent le remplacement du certificat TLS :

- changement du nom d'hôte ou de l'adresse IP du serveur de sécurité ;
- la clé privée du certificat a été compromise ;
- le certificat nécessite un nouvel algorithme cryptographique différent.

Pour remplacer le certificat TLS ultérieurement, utilisez le script `generate_certificate.sh`.

Utilisation du script :

```
Usage: /usr/share/uxp/scripts/generate_certificate.sh -n <basename>
<-s "<certificate DN>" | -S> [-a "<subjectAltName>" | -f]
[-d <path>] [-p] [-c <path>] [-2 | -3 | -4 | -e <EC> | -w <ED>]

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

OPTIONS:
  -h      show this message
  -n      basename, like 'internal' or 'nginx'
  -d      working/output directory, defaults to /etc/uxp/ssl
  -m      multiple certs generation support (cert is generated to the '<basename>-<epoch-
millis>' subdirectory)
  -f      fill subjectAltName automatically from hostname and IP addresses
  -S      fill Subject with /CN=${HOST} value
  -s      subject, optional. Format "/C=EE/O=Company/CN=server.name.tld"
  -x      extension basename, like 'internal' or 'nginx', defaults to basename value
  -a      subjectAltName, optional. Format
"DNS:serverAlt.name.tld,IP:1.1.1.1,IP:2.2.2.2>"
  -p      generate .p12 also, friendly name and password will default to basename value
  -c      configuration directory containing openssl.cnf, defaults to /etc/uxp/ssl
  -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)
  -w      generate Edwards-curve Digital Signature Algorithm (EdDSA) key.
Possible values: '25519' (Ed25519), '448' (Ed448).
May not be accepted by browsers for HTTPS, support is not yet widespread.
```



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

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



- Utilisez l'option `-n elasticsearch` pour spécifier que vous générez le certificat TLS Elasticsearch.
- Utilisez l'option `-p` pour générer le fichier P12 requis.
- L'une des options `-s` ou `-S` est obligatoire. L'option `-S` remplit le sujet avec le nom d'hôte. Utilisez `-s` si vous souhaitez remplir vous-même le champ Objet (voir la description des options pour connaître le format correct).
- `-a` prend en charge un nombre quelconque de noms DNS et/ou d'adresses IP (voir la description des options pour le format correct) ou utilisez `-f` pour remplir automatiquement le nom d'hôte et les adresses IP.

```
sudo /usr/share/uxp/scripts/generate_certificate.sh -S -f -p -n elasticsearch
```

2. Redémarrez PMA :

```
sudo systemctl restart uxp-monitor
```

5.4. Configurer Kibana pour l'analyse

Les données opérationnelles comprennent les enregistrements 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. Vous pouvez éviter les doublons en filtrant les enregistrements pour n'inclure que ceux qui proviennent du serveur de sécurité côté client, c'est-à-dire ceux dont le champ `security_server_type` a la valeur `Client`.

5.4.1. Créer une vue de données pour les 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.

PMA crée son index configuré dans Elasticsearch lorsqu'il envoie les données opérationnelles 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, si des données sont collectées.



Lors de l'importation du tableau de bord ou des visualisations de l'exemple 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`).
 - b. **Index pattern** - saisissez `uxp-request*` (index des données opérationnelles par défaut).
 - c. **Timestamp field** - choisissez `request_in_ts`.
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, naviguez vers **Analytics** → **Discovery**, et sélectionnez la vue de données appropriée dans la liste déroulante **Data view**.

5.4.2. Exemple de tableau de bord

Le paquet `uxp-monitor-analytics` fournit un exemple de tableau de bord `uxp-dashboard.ndjson` ([UXP] Overview) – situé dans le répertoire `/usr/share/doc/uxp-monitor-analytics/examples/kibana-9.x/dashboards`. Ce tableau de bord contient un ensemble de différentes visualisations (carte thermique, graphiques, affichage numérique, tableaux statistiques, etc.)



Toutes les visualisations du tableau de bord de l'exemple reposent uniquement sur les données opérationnelles et leur schéma d'indexation `uxp-request*`.



Toutes les visualisations du tableau de bord de l'exemple incluent les enregistrements 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`).

Pour importer le tableau de bord de l'exemple dans Kibana, procédez comme suit :

1. Copiez le fichier de tableau de bord de l'exemple `uxp-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 du tableau de bord d'exemple, 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.



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**.

5.4.3. 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 dans 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.

6. Maintenance

6.1. Configurer la grappe Zabbix

6.1.1. Ajout d'un nœud Zabbix supplémentaire

Pour ajouter un nœud Zabbix supplémentaire, procédez comme suit :

1. 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](#).
2. 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.
3. Sur PMA (sur chaque serveur de sécurité surveillé par cette grappe Zabbix), connectez le nouveau nœud Zabbix comme indiqué dans la section [Connecter Zabbix à l'agent de surveillance proxy](#).

6.1.2. Supprimer un nœud Zabbix

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

Sur PMA (sur chaque serveur de sécurité surveillé par cette grappe Zabbix)

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. En outre, supprimez la section de nœud restante correspondante. 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 PMA :

```
sudo reload-monitor-agent
```

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
```

6.1.3. 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
```

6.1.4. 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 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 PMA (sur chaque serveur de sécurité surveillé par cette grappe Zabbix)

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 PMA :

```
sudo reload-monitor-agent
```

6.2. Configurer une grappe Elasticsearch

6.2.1. 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 PMA (sur chaque serveur de sécurité connecté à cette grappe Elasticsearch), connectez le nouveau nœud Elasticsearch comme indiqué à la section [Utiliser un cluster Elasticsearch à plusieurs nœuds](#).

6.2.2. 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 PMA (sur chaque serveur de sécurité connecté à cette grappe Elasticsearch)

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]` section. En outre, supprimez la section de nœud restante correspondante. 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 PMA :

```
sudo reload-monitor-agent
```

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` :



S'il reste une grappe à seul 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.

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

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

```
sudo systemctl restart elasticsearch
```

6.2.3. 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 PMA :
 - 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 HTTP API TLS 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 http.p12 fichier de magasin de clés 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 PMA (sur chaque serveur de sécurité connecté à cette grappe Elasticsearch)

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 PMA :

```
sudo reload-monitor-agent
```

7. Dépannage

7.1. Fichier journal

Le fichier journal aide à résoudre les erreurs qui surviennent et à détecter les comportements inattendus potentiels. La lecture du fichier journal nécessite les privilèges root.

- PMA écrit les journaux dans le fichier `/var/log/uxp/proxymonitoragent.log`.

7.2. Recharger l'agent de surveillance Proxy

La plupart des scénarios dans lesquels PMA ne fonctionne pas comme souhaité peuvent être réparés en rechargeant PMA avec la commande :

```
sudo reload-monitor-agent
```

Cette commande permet à PMA de lire sa configuration 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 seront alors reconfigurés s'ils ont la capacité de reconfiguration automatique activée dans le fichier de configuration.

7.3. Modifier la configuration de l'agent de surveillance proxy

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

7.4. 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[cm69dr64e0001tf6miumotwy]" 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 Zabbix server hôte.

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**.