



RSA | Security Analytics

Guide de configuration d'Event Stream Analysis
pour la version 10.6

Marques commerciales

RSA, le logo RSA et EMC sont des marques commerciales ou des marques déposées d'EMC Corporation aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans le présent document sont la propriété de leurs détenteurs respectifs. Pour obtenir la liste des marques commerciales d'EMC, consultez france.emc.com/legal/emc-corporation-trademarks.htm.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales. Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des accords de licence applicables aux logiciels tiers de ce produit peut être consulté dans le fichier [thirdpartylicences.pdf](#).

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

L'utilisation, la copie et la diffusion de tout logiciel EMC décrit dans cette publication nécessitent une licence logicielle en cours de validité. EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION SONT FOURNIES « EN L'ÉTAT ». EMC CORPORATION NE FOURNIT AUCUNE DÉCLARATION OU GARANTIE D'AUCUNE SORTE CONCERNANT LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION ET REJETTE PLUS SPÉCIALEMENT TOUTE GARANTIE IMPLICITE DE QUALITÉ COMMERCIALE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

Sommaire

Présentation d'Event Stream Analysis (ESA)	6
Configurer Event Stream Analysis (ESA)	7
Conditions préalables	7
Procédure	7
Résultat	8
Étape 1. Ajouter le service Event Stream Analysis	8
Conditions préalables	9
Procédure	9
Étape 2. Ajouter une source de données à un service ESA	10
Conditions préalables	10
Procédures	11
Étape 3. Configurer des paramètres avancés pour un service ESA	12
Procédures	12
Étape 4. Configurer un serveur ESA pour qu'il se connecte à Context Hub sur un autre serveur ESA	14
Conditions préalables	14
Procédure	15
Résultat	15
Procédures supplémentaires	16
Modifier les mots de passe de stockage par défaut	16
Précédent mot de passe de stockage ESA	17
Éléments dépendants	17
Privilèges de base de données	17
Modifier le mot de passe MongoDB pour le compte administrateur	18
Modifier le mot de passe de stockage ESA	19
Changer le mot de passe du compte de la base de données ESA	19
Modifier le mot de passe du service ESA	20
Modifier le mot de passe de stockage Incident Management	21
Changer le mot de passe du compte de la base de données Incident Management ..	21

Modifier le mot de passe du service Incident Management	21
Modifier le mot de passe de stockage Data Science	22
Changer le mot de passe Data Science pour le compte de la base de données	23
Changer le mot de passe Data Science pour Security Analytics	23
Modifier le seuil de mémoire pour les règles d'évaluation	24
Conditions préalables	25
Procédure	25
Configurer le stockage ESA	26
Paramètres de configuration	27
Conditions préalables	28
Procédure	28
Exemple	29
Configurer le service ESA pour utiliser un pool de mémoire	30
Procédure	31
Résultat	34
Configurer ESA pour utiliser l'ordonnancement temporel des captures	34
Workflow d'ordonnancement temporel des captures	35
Conditions préalables	36
Procédures	36
Conseils de résolution des problèmes	38
Désactiver l'ordonnancement temporel des captures	38
Désactiver le suivi de position	39
Démarrer, arrêter ou redémarrer le service ESA	39
Démarrer le service ESA	39
Arrêter le service ESA	39
Redémarrer le service ESA	40
Vérifier la version et l'état des composants ESA	40
Vérifier la version du serveur ESA	40
Vérifier la version de MongoDB	40
Vérifier l'état de MongoDB	40
Références	42
Vue Configuration des services, onglet Avancé	42
Fonctions	42

Vue Configuration des services, onglet Sources de données	44
Fonctions	45

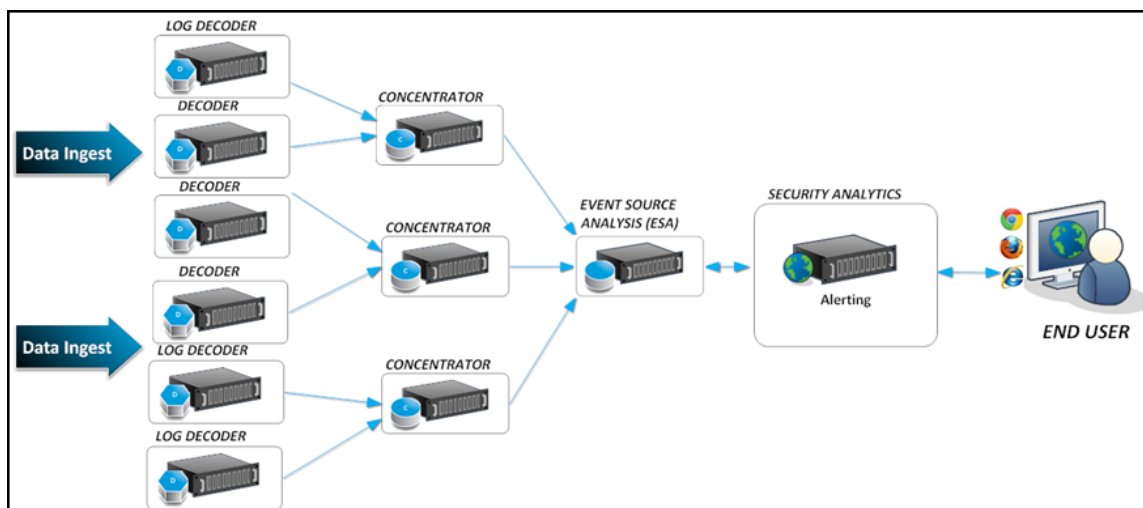
Présentation d'Event Stream Analysis (ESA)

Cette rubrique présente le module Event Stream Analysis.

Le service Security Analytics Event Stream Analysis (ESA) fournit une analytique de flux avancée telle que la corrélation et le traitement complexe d'événements, avec un haut débit et une faible latence. Il est capable de traiter de gros volumes de données d'événements disparates provenant des Concentrators.

Le langage avancé de traitement des événements (Event Processing Language) d'ESA vous permet de réaliser le filtrage, l'agrégation, l'association, la reconnaissance de schémas et la corrélation entre plusieurs flux d'événements disparates. Event Stream Analysis contribue à une puissante fonction de détection et d'alerte des incidents.

Le graphique suivant présente ce workflow :



Configurer Event Stream Analysis (ESA)

Cette rubrique décrit les tâches générales permettant de configurer Event Stream Analysis dans Security Analytics.

Conditions préalables

Veillez à effectuer les opérations suivantes :

- Installez le service Event Stream Analysis dans votre environnement réseau.
- Installez et configurez un ou plusieurs Concentrators dans votre environnement réseau.

Procédure

Remarque : Vous pouvez configurer ESA en utilisant un port SSL (50030) uniquement. Il n'y a pas d'option pour configurer un port non-SSL.

Pour configurer Event Stream Analysis :

Tâches	Référence
1. Vous pouvez découvrir, mettre à jour ou ajouter l'hôte sur lequel le service ESA est installé. (Facultatif) Si ESA n'est pas configuré, vous devez ajouter Event Stream Analysis comme service core et ajouter le service Event Stream Analysis à l'hôte.	Consultez l'« Étape 1 : Ajouter ou mettre à jour des hôtes » dans le « Guide de mise en route de l'hôte et des services. » Reportez-vous aux sections suivantes Étape 1. Ajouter le service Event Stream Analysis.
2. Appliquez la licence au service Event Stream.	Reportez-vous à la rubrique « Afficher les droits actuels » dans le « Guide d'octroi de licence ».
3. Ajoutez le Concentrator comme source de données au service Event Stream Analysis.	Reportez-vous aux sections suivantes Étape 2. Ajouter une source de données à un service ESA

Tâches	Référence
4. Configurez les notifications pour le service Event Stream Analysis.	Reportez-vous à la section « Méthodes de Notification » dans le « Guide des alertes basées sur ESA ».
5. Télécharger le contenu d'Event Stream Analysis à l'aide de Live.	Reportez-vous à la section « Vue Live Search » dans le « Guide de gestion des ressources Live ».
6. (Facultatif) Configuration avancée du service Event Stream Analysis.	Reportez-vous aux sections suivantes Étape 3. Configurer des paramètres avancés pour un service ESA.
7. (Facultatif) Activer Context Hub.	Reportez-vous à l'« Étape 1. Ajouter le service Context Hub » dans « Guide de configuration de Context Hub ».
8. (Facultatif) Configurer la connexion d'un service ESA au service Context Hub sur un autre service ESA.	Reportez-vous aux sections suivantes Étape 4. Configurer un serveur ESA pour qu'il se connecte à Context Hub sur un autre serveur ESA.

Résultat

Le service Event Stream Analysis est configuré et vous pouvez désormais ajouter des règles ESA pour le traitement et les alertes d'événements. Pour plus d'informations sur l'ajout de règles ESA, consultez la rubrique « Ajouter des règles à la Bibliothèque de règles » dans le « Guide des alertes basées sur ESA ».

Étape 1. Ajouter le service Event Stream Analysis

Cette rubrique donne des informations sur la façon d'ajouter le service Event Stream Analysis (ESA) à un hôte.

Conditions préalables

Assurez-vous que vous avez installé un service ESA et ajouté l'hôte dans Security Analytics. Pour plus d'informations, reportez-vous à l'« Étape 1 : Ajouter ou mettre à jour des hôtes » dans le « Guide de mise en route de l'hôte et des services. »

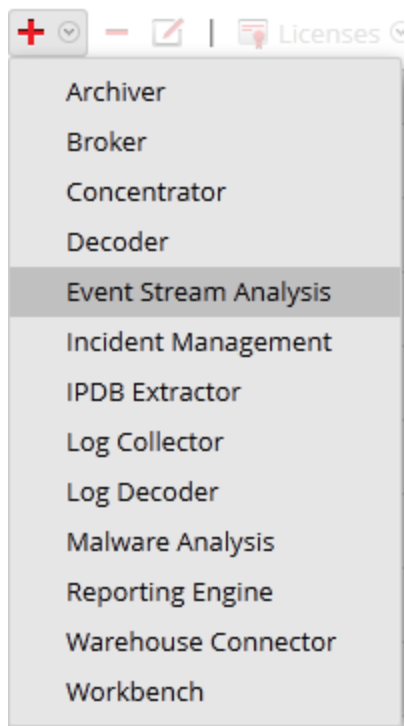
Procédure

Pour ajouter le service Event Stream Analysis :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.

La vue Services s'affiche.

2. Dans le panneau Services, sélectionnez **+** > **Event Stream Analysis**.



La boîte de dialogue **Ajouter un service** s'affiche.

3. Fournissez les informations suivantes :

Champ	Description :
Hôte	Sélectionnez l'hôte sur lequel vous souhaitez installer le service ESA.
Name	Saisissez le nom du service.

Champ	Description :
Port	Le port par défaut est 50030. Remarque : ESA peut être configuré en utilisant le port SSL 50030 uniquement. Vous ne pouvez pas configurer un port non-SSL.
Autoriser le service	Sélectionnez si vous souhaitez appliquer les habilitations configurées actuellement pour ce service.

4. Cliquez sur **Tester la connexion** pour déterminer si Security Analytics se connecte au service.

Remarque : Tout en ajoutant le service, Security Analytics envoie des paquets ICMP au service afin de vérifier si le nom d'hôte / l'adresse IP saisie est valable pour une connexion d'essai réussie.

5. Si le résultat réussit, cliquez sur **Enregistrer**.

Le service ajouté s'affiche désormais dans le panneau Services.

Remarque : Si le test échoue, modifiez les informations du service et réessayez.

Étape 2. Ajouter une source de données à un service ESA

Cette rubrique décrit comment ajouter une source de données nouvelle ou existante au service Event Stream Analysis.

Un service ESA reçoit les données à partir d'un Concentrator pour détecter les incidents et alerter l'utilisateur. Pour que le service analyse les données, vous devez configurer les sources à partir desquelles ESA lira les données. Utilisez les procédures de cette rubrique pour ajouter des sources de données pour votre ESA.

Conditions préalables

Vous devez avoir un ou plusieurs Concentrators configurés dans Security Analytics.

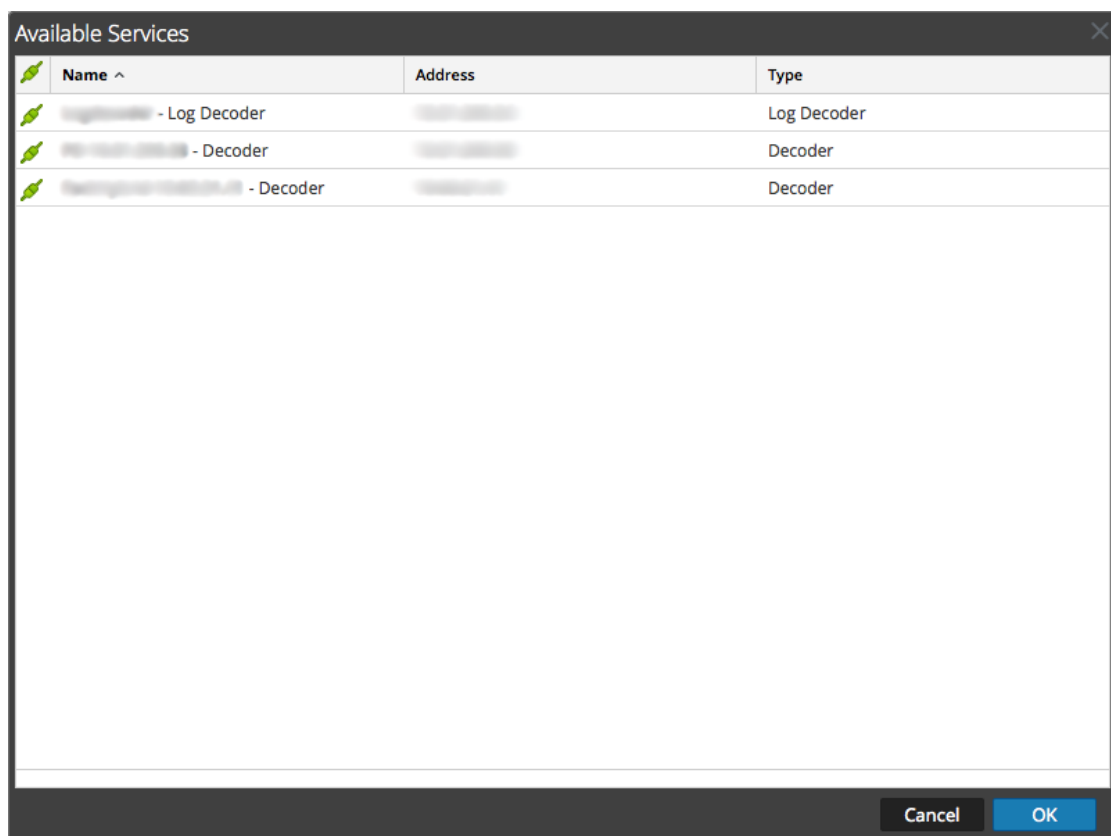
Vous devez effectuer les étapes suivantes pour ajouter une source de données :

- Ajouter une source de données disponible
- Spécifier le nom d'utilisateur et le mot de passe pour la source de données

Procédures

Ajouter des services existants comme source de données

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
La vue Services s'affiche.
2. Dans la vue Services, sélectionnez un service ESA.
3. Dans la colonne **Actions**, sélectionnez **Vue > Configuration**.
4. Sous l'onglet **Sources de données**, cliquez sur **+**.
Les services disponibles s'affichent, comme illustré sur la figure suivante.




5. Sélectionnez un ou plusieurs services, puis cliquez sur **OK**.
Le service est ajouté à la liste des services sous l'onglet **Source de données**.
6. (Facultatif) Cliquez sur **Activer** pour activer la source de données.
7. Cliquez sur **Appliquer** pour enregistrer la configuration.

Spécifier le nom d'utilisateur et le mot de passe de la source de données

Remarque : Vous pouvez ajouter un Log Decoder comme source de données pour ESA mais RSA vous recommande d'ajouter un Concentrator pour tirer profit de l'agrégation non divisée, étant donné que le décodeur peut avoir d'autres processus d'agrégation.

Pour spécifier le nom d'utilisateur et le mot de passe de la source de données :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
La vue Services s'affiche.
2. Dans la vue **Services**, sélectionnez un service Concentrator.
3. Cliquez sur .
4. Indiquez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Save**.

Étape 3. Configurer des paramètres avancés pour un service ESA

Cette rubrique donne des instructions pour configurer les paramètres avancés d'un service Event Stream Analysis.

Dans la vue Avancé, vous pouvez configurer les paramètres avancés pour améliorer les performances, pour préserver les événements des règles à plusieurs événements, pour mettre les événements dans le tampon mémoire et le nombre d'événements à stocker dans ESA.

Procédures

Configurer les paramètres avancés

Pour accéder à la vue Avancé et configurer les paramètres avancés d'un service ESA :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
La vue Services s'affiche.
2. Dans la vue Services, sélectionnez un service ESA.
3. Dans la colonne **Actions**, sélectionnez **Vue > Configuration**.
4. Sélectionnez l'onglet **Avancé**.
La vue Avancé s'affiche.

Alert Engine

Max Constituent Events

Forward Alerts On Message Bus

Debug Rules?

Apply

Event Stream Engine

Max Pattern Subexpressions

Apply

Configurer les paramètres Moteur d'alerte

Dans la section Moteur d'alertes, spécifiez les valeurs pour réserver des événements aux règles qui choisissent plusieurs événements.

Remarque : Une fois la migration vers la version 10.5 terminée, l'option Déboguer les règles est désactivée si elle était activée jusque-là. Vous devrez la réactiver après la mise à niveau.

La figure suivante affiche la section Moteur d'alertes.

Alert Engine

Max Constituent Events

Forward Alerts On Message Bus

Debug Rules?

Apply

Pour configurer les paramètres du moteur d'alerte :

1. Dans la section Moteur d'alerte, saisissez une valeur pour **Nombre maximal d'événements constitutifs**. La valeur par défaut est 100.

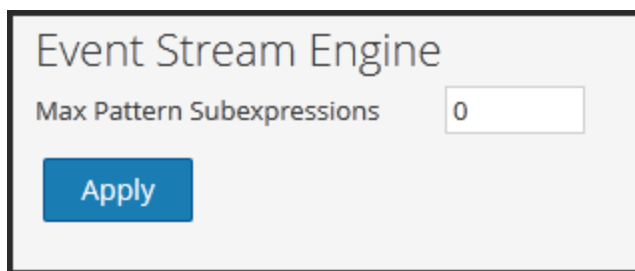
2. Pour que les alertes soient envoyées au bus de messages et à Incident Management, sélectionnez l'option **Transférer les alertes vers le bus de messages**.
3. Sélectionnez **Déboguer les règles ?** pour activer les règles de débogage.
4. Cliquez sur **Appliquer** pour enregistrer les modifications et les appliquer immédiatement.

Remarque : Pour plus d'informations sur les paramètres de la section Moteur d'alerte, reportez-vous aux paramètres du moteur d'alerte dans la vue Avancé ESA.

Configurer les paramètres du moteur de flux d'événements

Dans la section Event Stream Engine, spécifiez les détails pour améliorer les performances.

La figure suivante affiche la section Moteur de flux d'événements.



Pour configurer les paramètres du moteur de flux d'événements :

1. Dans la section Moteur de flux d'événements, saisissez une valeur dans le champ **Nombre maximal de sous-expressions de modèles**.
2. Cliquez sur **Appliquer** pour enregistrer les modifications et les appliquer immédiatement.

Remarque : Pour plus d'informations sur les paramètres de la section Moteur de flux d'événements, reportez-vous aux paramètres du moteur de flux d'événements dans la vue Avancé ESA.

Étape 4. Configurer un serveur ESA pour qu'il se connecte à Context Hub sur un autre serveur ESA



Cette rubrique indique aux administrateurs comment configurer un ESA afin qu'il se connecte au Context Hub d'un autre ESA. Un seul Context Hub peut être installé par installation Security Analytics. Si vous disposez de plus d'un ESA et que vous exécutez le Context Hub, vous devez activer l'ESA ne disposant pas de Context Hub afin qu'il communique avec le Context Hub d'un autre ESA.

Conditions préalables

Vous devez exécuter plusieurs ESA et un Context Hub.

Procédure

Configurez ESA afin qu'il se connecte au Context Hub d'un autre ESA.

1. Notez l'adresse IP de l'ESA qui exécute le service Context Hub.
2. À partir d'Administration > Services, sélectionnez le service ESA qui n'exécute pas le Context Hub, puis   > **Vue** > **Explorer**.
3. Dans le panneau de gauche, naviguez vers **Service** > **ContextHub**, puis sélectionnez **contextHubTransport**.
4. Modifiez le champ **Hôte** afin qu'il pointe vers le nom de domaine ou l'adresse IP de l'ESA qui exécute le service Context Hub.

Résultat

L'ESA se connecte au Context Hub d'un autre service ESA.

Procédures supplémentaires

Cette rubrique regroupe différentes procédures qu'un administrateur peut réaliser à tout moment et qui ne sont pas requises dans la configuration initiale d'ESA. Ces procédures sont classées par ordre alphabétique.

Utilisez cette section si vous recherchez des instructions pour effectuer une tâche spécifique après la configuration initiale d'ESA.

- [Modifier les mots de passe de stockage par défaut](#)
- [Modifier le seuil de mémoire pour les règles d'évaluation](#)
- [Configurer le stockage ESA](#)
- [Configurer le service ESA pour utiliser un pool de mémoire](#)
- [Configurer ESA pour utiliser l'ordonnancement temporel des captures](#)
- [Démarrer, arrêter ou redémarrer le service ESA](#)
- [Vérifier la version et l'état des composants ESA](#)

Modifier les mots de passe de stockage par défaut

Cette rubrique indique aux administrateurs comment modifier les mots de passe de stockage par défaut pour les comptes de base de données qui stockent les alertes dans ESA, Incident Management et Data Science.

Security Analytics 10.5 utilise MongoDB comme base de données pour stocker des alertes dans les modules suivants :

- ESA
- Gestion des incidents
- Data Science

La base de données de chaque module dispose d'un compte pour contrôler les accès et chaque compte de service Security Analytics possède un mot de passe par défaut.

Pour renforcer la sécurité, RSA vous recommande de modifier les mots de passe par défaut. Certaines organisations n'autorisent pas les mots de passe par défaut. Dans ce cas, vous devez suivre les procédures de cette rubrique.

Cette rubrique explique comment modifier le mot de passe de stockage par défaut du compte de base de données dans chaque module.

Précédent mot de passe de stockage ESA

ESA a été intégré dans Security Analytics 10.3 lorsque la base de données était dans PostgreSQL. Si vous avez utilisé ESA dans la version 10.3 et que vous avez créé un mot de passe personnalisé pour la base de données PostgreSQL, il n'a aucune incidence sur MongoDB. Lorsque vous installez ou migrez vers Security Analytics 10.5, MongoDB est installé avec un mot de passe par défaut.

Incident Management et Data Science ont été intégrés dans Security Analytics 10.4 et n'ont donc utilisé que MongoDB.

Éléments dépendants

MongoDB possède un compte administrateur principal doté de privilèges sur les comptes de base de données pour les services ESA, IM et Data Science.

Remarque : Vous devez d'abord modifier le mot de passe du compte administrateur. Vous pouvez modifier les mots de passe des services dans l'ordre de votre choix.

ESA doit être installé pour Incident Management et Data Science. La configuration de chaque module renvoie à l'hôte qui exécute le service ESA. Les bases de données de ESA, Incident Management et Data Science sont situées sur l'hôte qui exécute le service ESA.

Privilèges de base de données

La figure suivante illustre les privilèges associés à chaque compte pendant l'installation ou la mise à niveau.

Compte	Privilèges	Base de données
admin	readWriteAnyDatabase userAdminAnyDatabase dbAdminAnyDatabase	Tous
Event Stream Analysis	readWrite dbAdmin clusterAdmin	ESA
Gestion des incidents	readWrite dbAdmin clusterAdmin	IM

Compte	Privilèges	Base de données
Data Science	readWrite dbAdmin clusterAdmin	Data Science

Pour plus d'informations sur la modification de chaque mot de passe, consultez :

- [Modifier le mot de passe MongoDB pour le compte administrateur](#)
- [Modifier le mot de passe de stockage ESA](#)
- [Modifier le mot de passe de stockage Incident Management](#)
- [Modifier le mot de passe de stockage Data Science](#)

Modifier le mot de passe MongoDB pour le compte administrateur

Cette rubrique indique aux administrateurs comment modifier le mot de passe de stockage par défaut pour le compte administrateur MongoDB.

Dans Security Analytics, cette procédure est facultative. Cependant, c'est une bonne pratique de sécurité pour les administrateurs que de modifier les mots de passe par défaut. Certaines organisations n'autorisent pas les mots de passe par défaut.

Remarque : Vous devez commencer par modifier le mot de passe du compte administrateur MondoDB. Vous devez le saisir pour changer les mots de passe pour ESA, Incident Management et Data Science.

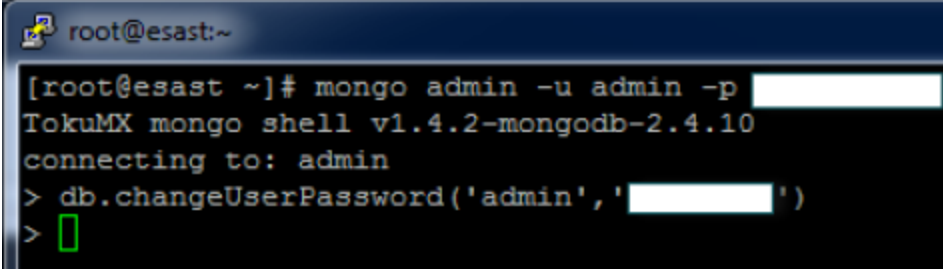
Conditions préalables

Vous devez disposer des privilèges du rôle administrateur.

Procédure

1. Connectez-vous à l'hôte ESA qui exécute le service ESA :
 - a. SSH sur l'hôte ESA.
 - b. Connectez-vous en tant qu'utilisateur root (racine).
2. Connectez-vous à MongoDB en tant qu'administrateur. Le mot de passe par défaut est netwitness.

```
mongo admin -u admin -p <current_password>
```



```

root@esast:~
[root@esast ~]# mongo admin -u admin -p [REDACTED]
TokuMX mongo shell v1.4.2-mongodb-2.4.10
connecting to: admin
> db.changeUserPassword('admin', '[REDACTED]')
>

```

3. Pour modifier le mot de passe du compte administrateur, saisissez

```
db.changeUserPassword('admin', '<new_password>')
```

Vous pouvez maintenant modifier le mot de passe pour les services ESA, Incident Management et Data Science.

Modifier le mot de passe de stockage ESA

Cette rubrique indique aux administrateurs comment modifier le mot de passe de stockage par défaut de la base de données ESA.

Dans Security Analytics, cette procédure est facultative. Cependant, c'est une bonne pratique de sécurité pour les administrateurs que de modifier les mots de passe par défaut. Certaines organisations n'autorisent pas de mots de passe par défaut et rendent cette procédure obligatoire.

Conditions préalables

Vous devez disposer des privilèges du rôle administrateur.

Procédures

Changer le mot de passe du compte de la base de données ESA

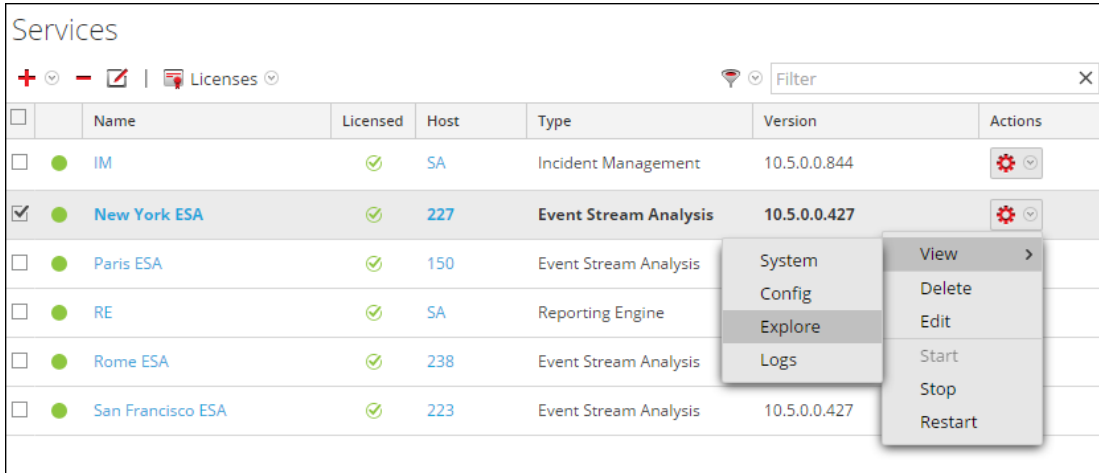
1. Connectez-vous à l'hôte qui exécute le service ESA :
 - a. SSH sur l'hôte ESA.
 - b. Connectez-vous en tant qu'utilisateur **root** (racine).
2. Connectez-vous à MongoDB en tant qu'utilisateur administrateur.


```
mongo esa -u admin -p <current_admin_password> --
authenticationDatabase admin
```
3. Saisissez la commande suivante pour changer le mot de passe du compte ESA. Le mot de passe par défaut est esa.

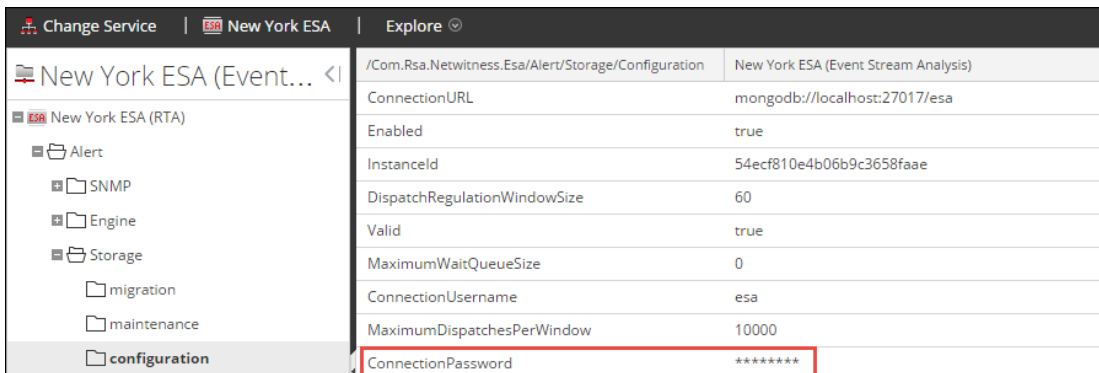

```
db.changeUserPassword('esa', '<new_password>')
```

Modifier le mot de passe du service ESA

1. Connectez-vous à Security Analytics en tant qu'admin.
2. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.



3. Sélectionnez le service ESA, puis [Gear] > **Vue > Explorer**.
4. Dans la vue Explorer située à gauche, sélectionnez **Alerte > Stockage > configuration**.



5. Dans le panneau de droite, saisissez le mot de passe du compte de la base de données dans le champ **ConnectionPassword**.

Remarque : Le mot de passe de la base de données et de la configuration du service Security Analytics doivent être identiques.

6. Pour vérifier que la base de données et les mots de passe Security Analytics correspondent, dans le menu, sélectionnez Analytique de sécurité **Alertes > Résumé**.
 Si le contenu apparaît sous l'onglet Résumé, les mots de passe correspondent et ont été modifiés avec succès.
 Si vous ne voyez pas le contenu sous l'onglet Résumé, réviser le mot de passe du service pour qu'il corresponde avec le mot de passe MongoDB.

Modifier le mot de passe de stockage Incident Management

Cette rubrique indique aux administrateurs comment modifier le mot de passe de stockage par défaut pour la base de données Incident Management.

Dans Security Analytics, cette procédure est facultative. Cependant, c'est une bonne pratique de sécurité que de modifier les mots de passe par défaut. Dans les organisations qui n'autorisent pas les mots de passe par défaut, cette procédure est obligatoire.

Conditions préalables

Vous devez disposer des privilèges du rôle administrateur.

Le mot de passe par défaut pour le compte administrateur MongoDB doit être changé.

Procédures

Changer le mot de passe du compte de la base de données Incident Management

- Connectez-vous à l'hôte qui exécute le service ESA :
 - SSH sur l'hôte ESA.
 - Connectez-vous en tant qu'utilisateur root (racine).
- Connectez-vous à MongoDB en tant qu'administrateur.



```
mongo im -u admin -p {current_admin_password} --
authenticationDatabase admin
```
- Saisissez la commande suivante pour changer le mot de passe du compte Incident Management. Le mot de passe par défaut est **im**.

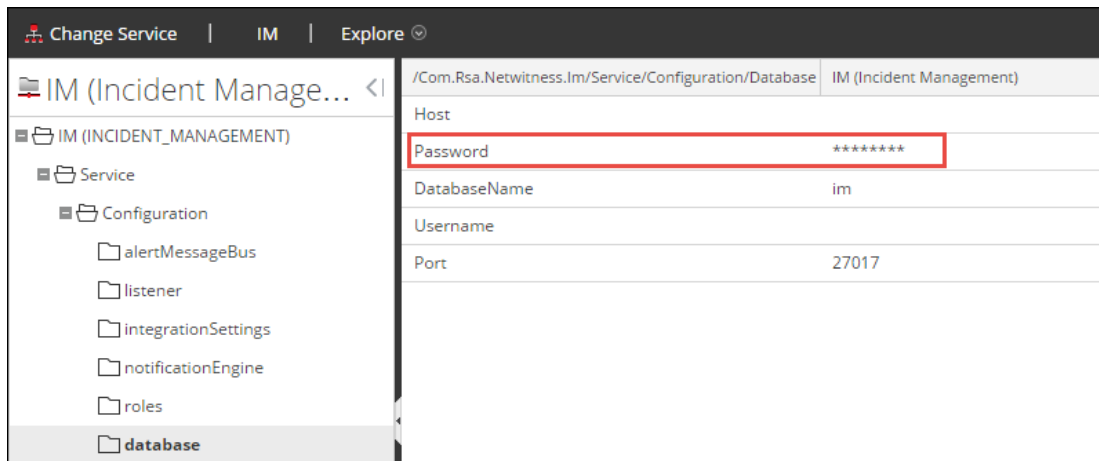

```
db.changeUserPassword('im', '{new_password}')
```

Modifier le mot de passe du service Incident Management

- Connectez-vous à Security Analytics en tant qu'admin.
- Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.


	Name	Licensed	Host	Type	Version	Actions
<input checked="" type="checkbox"/>	IM	✓	SA	Incident Management	10.5.0.0.844	
<input type="checkbox"/>	ipdbextractor	✓	SA	IPDB Extractor		
<input type="checkbox"/>	local-malware	✓	SA	Malware Analysis		
<input type="checkbox"/>	New York ESA	✓	227	Event Stream Analysis	10.5.0.0.427	
<input type="checkbox"/>	Paris ESA	✓	150	Event Stream Analysis	10.5.0.0.427	
<input type="checkbox"/>	RE	✓	SA	Reporting Engine	10.5.0.0.5272-2	

3. Sélectionnez le service Incident Management, puis  > **Vue > Explorer**.
4. Dans la vue Explorer située à gauche, sélectionnez **Configuration > base de données**.



5. Dans le panneau de droite, saisissez le mot de passe du compte de la base de données dans le champ **Mot de passe**.

Remarque : Le mot de passe de la base de données et de la configuration du service Security Analytics doivent être identiques.

6. Redémarrez le service Gestion des incidents pour accepter le changement de mot de passe et forcez la session à démarrer en utilisant le nouveau mot de passe.
 - a. Sélectionnez **Administration > Services**.
 - b. Sélectionnez le service Gestion des incidents, puis cliquez sur  > **Redémarrer**.
7. Pour valider la concordance des nouveaux mots de passe, sélectionnez **Incidents > Alertes**.
 Si vous voyez le contenu sous l'onglet Alertes, vous avez modifié les mots de passe correctement.
 Si vous ne voyez pas le contenu sous l'onglet Alertes, réviser le mot de passe du service pour qu'il corresponde avec le mot de passe MongoDB.

Modifier le mot de passe de stockage Data Science

Cette rubrique indique aux administrateurs comment modifier le mot de passe de stockage par défaut pour la base de données Data Science.

Dans Security Analytics, cette procédure est facultative. Cependant, c'est une bonne pratique de sécurité que de modifier les mots de passe par défaut. Dans les organisations qui n'autorisent pas les mots de passe par défaut, cette procédure est obligatoire.

Conditions préalables

Vous devez disposer des privilèges du rôle administrateur.

Le mot de passe par défaut pour le compte administrateur MongoDB doit être changé.

Procédures

Changer le mot de passe Data Science pour le compte de la base de données

1. Connectez-vous à l'hôte qui exécute le service ESA.
 - a. SSH sur l'hôte ESA.
 - b. Connectez-vous en tant qu'utilisateur root (racine).
2. Connectez-vous à MongoDB en tant qu'administrateur.


```
mongo ds -u admin -p {current_admin_password} --
authenticationDatabase admin
```
3. Pour modifier le mot de passe du compte Data Science, saisissez


```
db.changeUserPassword('ds', '{new_password}')
```

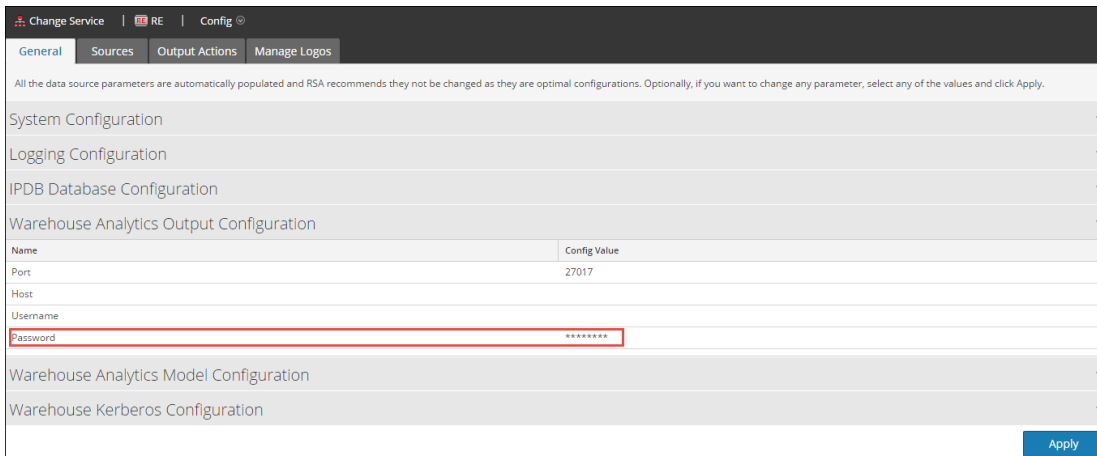
Changer le mot de passe Data Science pour Security Analytics

1. Connectez-vous à Security Analytics en tant qu'admin.
2. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.

<input type="checkbox"/>	Name	Licensed	Host	Type	Version	Actions
<input type="checkbox"/>	IM	✓	SA	Incident Management	10.5.0.0.844	
<input checked="" type="checkbox"/>	RE	✓	SA	Reporting Engine	10.5.0.0.5272-2	
<input type="checkbox"/>	Rome ESA	✓	238	Event Stream Analysis		
<input type="checkbox"/>	San Francisco ESA	✓	223	Event Stream Analysis		

- Sélectionnez le service Reporting Engine, puis   > **Vue > Config.**

La vue Configuration s'ouvre sur l'onglet Général.



Change Service | RE | Config

General Sources Output Actions Manage Logos

All the data source parameters are automatically populated and RSA recommends they not be changed as they are optimal configurations. Optionally, if you want to change any parameter, select any of the values and click Apply.

System Configuration +

Logging Configuration +

IPDB Database Configuration +

Warehouse Analytics Output Configuration -

Name	Config Value
Port	27017
Host	
Username	
Password	*****

Warehouse Analytics Model Configuration +

Warehouse Kerberos Configuration +

Apply

- Sélectionnez **Configuration de sortie Warehouse Analytics.**
- Saisissez le mot de passe du compte de la base de données dans le champ **Mot de passe.**

Remarque : Le mot de passe de la base de données et de la configuration du service Security Analytics doivent être identiques.

- Pour valider la concordance des nouveaux mots de passe, exécutez un rapport sur Reporting Engine qui utilise Warehouse Analytics.

Modifier le seuil de mémoire pour les règles d'évaluation

Cette rubrique indique aux administrateurs comment définir le seuil d'utilisation de la mémoire pour les règles d'évaluation. Lorsque le seuil est dépassé, toutes les règles d'évaluation déployées sont désactivées.

Cette procédure est facultative. Les administrateurs peuvent augmenter ou diminuer le seuil de mémoire pour les règles d'évaluation. Le seuil se réfère à l'utilisation de la mémoire ESA, qui comprend la mémoire de base ESA, les règles d'évaluation et les règles hors évaluation. Lorsque le seuil est dépassé, toutes les règles d'évaluation déployées sur un service ESA sont désactivées.

Vous utilisez des règles d'évaluation pour voir si une règle fonctionne efficacement et qu'elle n'utilise pas de mémoire excessive, ce qui peut influencer sur les performances ou forcer l'arrêt du service.

Par défaut, le seuil de mémoire est de 85, ce qui est le pourcentage de mémoire virtuelle Java (JVM).

- Le seuil de mémoire est par ESA, et non par règle.
- Lorsque le seuil de mémoire est dépassé, toutes les règles d'évaluation en cours d'exécution sur ESA sont automatiquement désactivées.
- La configuration ESA dispose de deux paramètres pour les règles d'évaluation :
 - MemoryThresholdforTrialRules
 - MemoryCheckPeriod, qui a une valeur par défaut de 300 secondes

Pour plus de détails, reportez-vous à la section « Utiliser les règles d'évaluation » dans le « Guide des alertes basées sur ESA ».

Conditions préalables

Un rôle avec des privilèges d'administration doit être attribué.

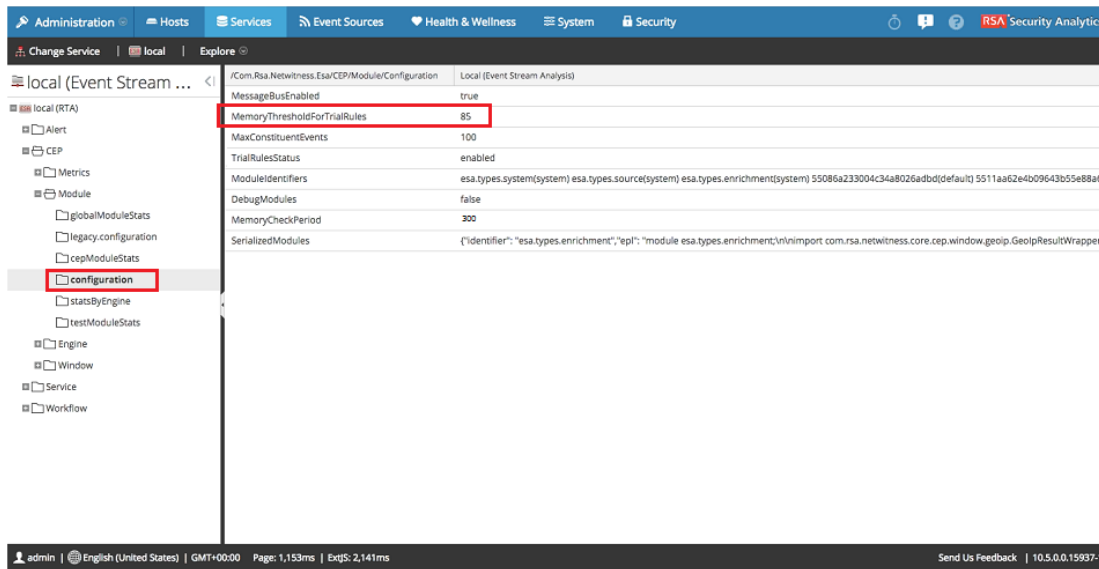
Procédure

1. Connectez-vous à Security Analytics en tant qu'admin.
2. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.

<input type="checkbox"/>	Name	Licensed	Host	Type	Version	Actions
<input type="checkbox"/>	IM	✓	SA	Incident Management	10.5.0.0.844	
<input checked="" type="checkbox"/>	New York ESA	✓	227	Event Stream Analysis	10.5.0.0.427	
<input type="checkbox"/>	Paris ESA	✓	150	Event Stream Analysis		
<input type="checkbox"/>	RE	✓	SA	Reporting Engine		
<input type="checkbox"/>	Rome ESA	✓	238	Event Stream Analysis		
<input type="checkbox"/>	San Francisco ESA	✓	223	Event Stream Analysis	10.5.0.0.427	

3. Sélectionnez le service ESA, puis > **Vue > Explorer**.

4. Sur la gauche, sélectionnez **CEP > Module > Configuration**.



5. Dans le panneau de droite, dans **MemoryThresholdForTrialRules**, saisissez un pourcentage de JVM que les règles d'évaluation sur ESA ne peuvent pas dépasser. Le nouveau seuil de mémoire prend effet immédiatement.

Configurer le stockage ESA

Cette rubrique explique comment configurer la base de données ESA afin de maintenir un niveau d'alerte sain.

Cette procédure est facultative. Les administrateurs peuvent spécifier une période de rétention pour les alertes. La suppression d'anciennes alertes est recommandée comme bonne pratique pour la maintenance de la base de données d'alertes. Autrement, la base de données pourrait continuer à grossir et avoir éventuellement un impact négatif sur les performances.

Par défaut, la fonction de suppression automatique des alertes n'est pas activée car chaque société dispose de ses propres règles de fonctionnement. Cette rubrique vous apprend à effectuer les tâches suivantes :

- Activer la suppression automatique des alertes
- Spécifier des critères pour supprimer les alertes
 - En fonction de la taille de la base de données
 - En fonction de la durée d'existence des alertes
 - En fonction de la taille de la base de données et de la durée d'existence des alertes

Paramètres de configuration

Les paramètres de configuration sont les suivants :

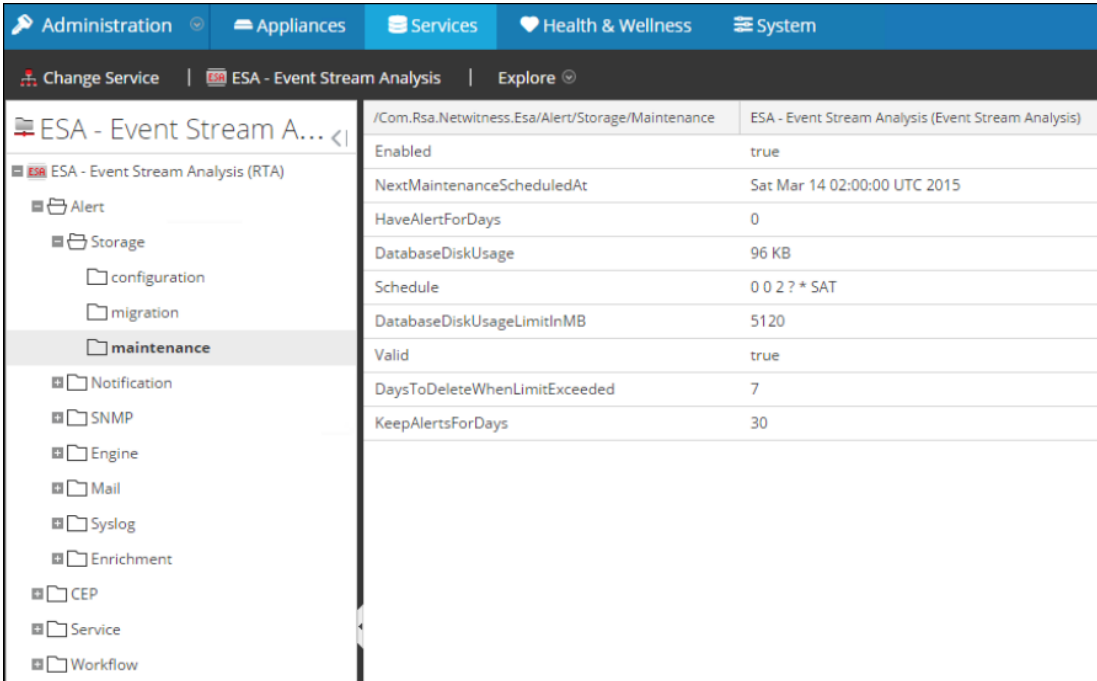
Paramètre	Description
Enabled	Active la fonction de rétention des alertes.
NextMaintenanceScheduledAt	(Lecture seule) À la prochaine exécution planifiée de la maintenance.
HaveAlertForDays	(Lecture seule) Nombre réel de jours durant lesquels les alertes ont été stockées dans la base de données. Par exemple, si le nombre est constaté le 4 juin et que des alertes ont été générées tous les jours depuis le 1er juin, alors la valeur serait égale à 4.
DatabaseDiskUsage	(Lecture seule) Taille de base de données actuelle.
Planning	Planification de l'exécution de la maintenance des alertes. La planification utilise l'onglet Cron UNIX et doit être spécifiée au format approprié de l'onglet Cron. La valeur par défaut s'affiche dans la procédure ci-après. Pour plus d'informations sur la planification Cron, reportez-vous au site http://www.cronmaker.com .
DatabaseDiskUsageLimtInMB	Seuil de la taille de la base de données auquel les alertes sont supprimées lorsqu'il est atteint.
Valid	Paramètre de lecture seule indiquant si la configuration actuelle est valide.
DaysToDeleteWhenLimitExceeded	Nombre de jours à supprimer lorsque le paramètre DatabaseDiskUsageLmitInMB est dépassé.
KeepAlertsForDays	Nombre de jours de conservation des alertes dans la base de données avant leur suppression.

Conditions préalables

Vous devez disposer des autorisations d'administrateur.

Procédure

1. Connectez-vous à Security Analytics en tant qu'admin.
2. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
3. Sélectionnez le service ESA, puis   **Vue > Explorer**.
4. Sur la gauche, sélectionnez **Alerte > Stockage > Maintenance**.



The screenshot shows the 'Administration' menu with 'Services' selected. The left sidebar shows a tree view with 'Alert' > 'Storage' > 'maintenance' selected. The main panel displays the configuration for the service path '/Com.Rsa.Netwitness.Esa/Alert/Storage/Maintenance'.

Property	Value
Enabled	true
NextMaintenanceScheduledAt	Sat Mar 14 02:00:00 UTC 2015
HaveAlertForDays	0
DatabaseDiskUsage	96 KB
Schedule	0 0 2 ? * SAT
DatabaseDiskUsageLimitInMB	5120
Valid	true
DaysToDeleteWhenLimitExceeded	7
KeepAlertsForDays	30

5. Dans le champ **Activé**, sélectionnez la valeur True pour activer la fonction de rétention des alertes.
6. Configurez le mode de suppression des anciennes alertes :
 - En fonction de la taille de la base de données - Saisissez la taille maximale de la base de données dans **DatabaseDiskUsageLimitInMB**. Ensuite saisissez le nombre de jours à supprimer relatifs aux anciennes alertes dans **DaysToDeleteWhenLimitExceeded**. Par exemple, lorsque l'utilisation du disque atteint 5 120 Mo, supprimez les alertes les plus anciennes de 7 jours.
 - En fonction de la durée d'existence des alertes - Toutes les alertes antérieures à **KeepAlertsForDays** sont supprimées.

Remarque : Pour Security Analytics 10.4.1 et version antérieure, vous devez utiliser le paramètre `KeepAlertsForDays`. Vous ne pouvez pas utiliser le paramètre `DatabaseDiskUsageLimitInMB`.

- En fonction de la taille de la base de données et de la durée d'existence des alertes. Si vous configurez ces deux paramètres, la règle qui supprime le plus grand nombre est utilisée.

7. Schedule

Utilisez le paramètre `Schedule` pour indiquer à ESA la fréquence d'exécution de la tâche de maintenance de l'alerte (c'est-à-dire à quelle fréquence vérifier la base de données et appliquer les règles de suppression). Utilisez la syntaxe pour une tâche de planification Cron. Pour plus d'informations sur la planification Cron, reportez-vous à la rubrique <http://www.cronmaker.com>.

8. Réinitialiser le navigateur.

- Les date et heure de la prochaine exécution de maintenance s'affiche dans le champ `NextMaintenanceScheduledAt`.
- Dans le champ `Valid`, la valeur `True` s'affiche pour indiquer la configuration qui est valide.
Si la valeur `False` est affichée, corrigez les paramètres de taille du disque ou de durée d'existence des alertes.

9. (Facultatif) L'état de maintenance peut également être surveillé dans le fichier `/opt/rsa/esa/logs/esa.log` sur l'hôte ESA, qui affiche des messages similaires à l'exemple ci-dessous.

Exemple

L'état de maintenance peut également être surveillé dans le fichier `/opt/rsa/esa/logs/esa.log` sur le service ESA, qui affiche des messages similaires à l'exemple ci-dessous.

```
2015-03-12 09:46:48,197 [Carlos@65dd6c04-56] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
MongoStorageMaintenance changed by admin
2015-03-12 09:46:51,121 [scheduler_Worker-1] INFO
com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Starting the scheduled database maintenance
job with policy {keepAlertForDays=30, maxDiskUsageInMb=5120}
2015-03-12 09:46:51,122 [Carlos@3801f0b3-58] INFO
com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
```

```
Scheduled a database maintenance job with
policy {keepAlertForDays=30, maxDiskUsageInMb=5120} to run at 2/28/15
2:00 AM
2015-03-12 09:46:51,129 [Carlos@3801f0b3-58] INFO
com.rsa.netwitness.carlos.config.ConfigurationMXBean -
MongoStorageMaintenance changed by admin
2015-03-12 09:46:51,133 [scheduler_Worker-1] INFO
com.rsa.netwitness.core.alert.dispatch.SQLStorageMaintenance -
Finished the database maintenance job,
deleted 0 partitions, next run scheduled at 3/14/15 2:00 AM
```

Configurer le service ESA pour utiliser un pool de mémoire

Cette rubrique indique aux administrateurs comment configurer le service ESA en vue d'utiliser un pool de mémoire.

Un pool de mémoire est une implémentation personnalisée de la mémoire virtuelle pour les événements gérés par les règles dans ESA. Ainsi, les fonctionnalités des règles évoluent par ordre de grandeur. Lorsque vous souhaitez créer des règles qui couvrent une longue période ou qui sont très complexes, vous pouvez choisir d'utiliser un pool de mémoire pour gérer plus efficacement la mémoire. Lorsque vous utilisez un pool de mémoire, au lieu de conserver tous les événements en mémoire, ils peuvent être écrits sur le disque. Cela est pratique lorsqu'une règle existante est complexe ou étendue à une longue période, dans ce cas, un grand nombre d'événements doit être conservé en mémoire.

Vous pouvez configurer le pool de mémoire pour qu'il s'exécute en mode Non traitement par lots ou Traitement par lots :

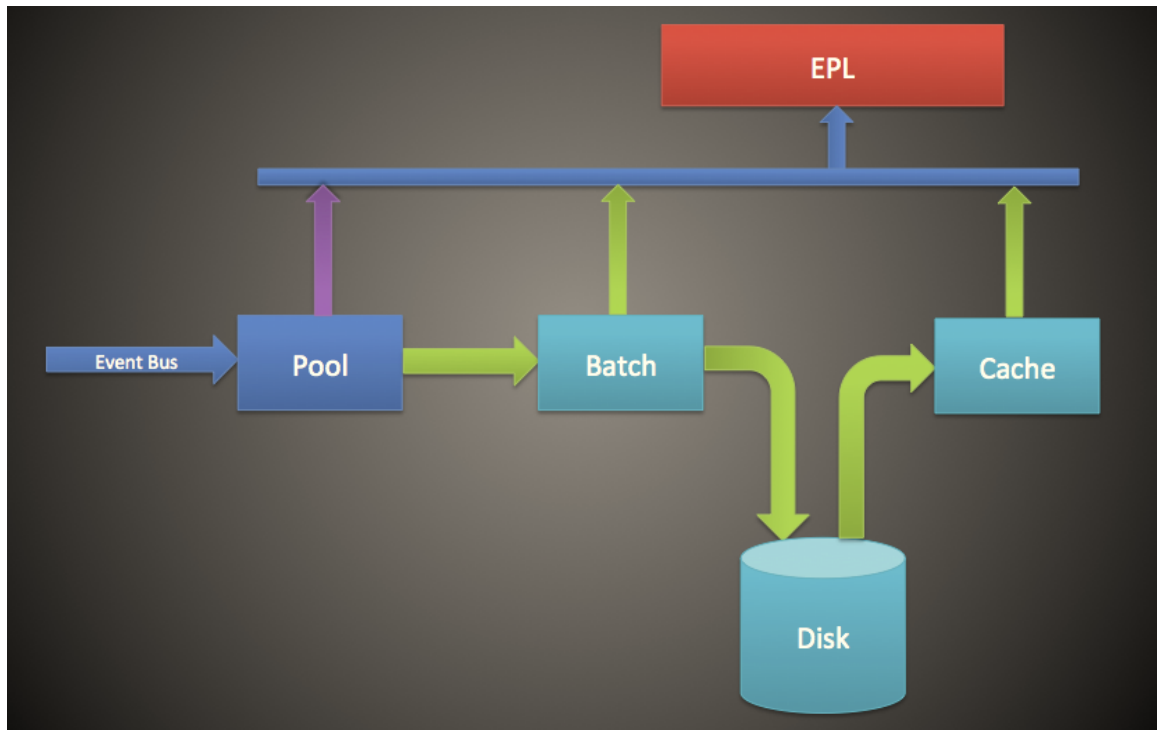
- **Non traitement par lots.** En mode Non traitement par lots, les événements sont écrits sur le disque au fur et à mesure qu'ils sont insérés dans le pool de mémoire. Pour configurer le mode Non traitement par lots, définissez l'attribut **MapPoolBatchWriteSize** sur 1. Le mode Non traitement par lots fournit une solution plus stable parce que chaque événement est traité séparément sans influencer sur les performances de la mémoire.
- **Traitement par lots.** En mode Traitement par lots, les événements sont regroupés en lots et ensuite écrits sur le disque. Pour configurer le mode Traitement par lots, définissez l'attribut de taille du lot **MapPoolBatchWriteSize** sur une valeur supérieure à 1. Le mode Traitement par lots donne de meilleures performances puisque l'activité du disque contenant les événements est optimisée.

Remarque : En cas de modification de ces paramètres, il faudra redémarrer le service ESA. Lorsque ESA redémarre, si des événements sont conservés par le pool de mémoire, ils seront ignorés au redémarrage.

Attention : Bien que cette fonctionnalité puisse être très utile pour la gestion de la mémoire, elle peut avoir un impact sur le taux de traitement des événements du service ESA. Les performances peuvent être affectées de 10 à 30 % en fonction de vos règles et paramètres de configuration.

Workflow


Le schéma suivant illustre le flux de données en utilisant le pool de mémoire pour le mode Traitement par lots :



1. Les événements sont ajoutés au pool de mémoire et les références aux événements sont stockées dans le pool de mémoire.
2. Les événements sont ensuite regroupés pour être envoyés vers le disque (en mode Non traitement par lots, cette étape est ignorée).
3. Une fois que le lot a atteint le seuil, les événements sont écrits sur le disque (en mode Non traitement par lots, aucun seuil n'est nécessaire).
4. Lorsque la règle EPL nécessite un événement qui a été écrit sur le disque, l'événement est envoyé à la mémoire cache et utilisé dans la règle EPL.

Procédure

Pour configurer un pool de mémoire ESA, suivez les étapes ci-après :

1. Sous **Administration** > **Services**, sélectionnez votre service ESA, puis  > **Vue** > **Explorer**.
2. Sélectionnez **CEP** > **EsperPool** > **Configuration**.
3. Saisissez des valeurs pour les champs suivants :

Attributs	Description :	Configuration
MapPoolPersistenceURI	Emplacement de stockage du fichier pool de mémoire.	<p>La valeur par défaut est /opt/RSA/ESA/pool/esperPool. RSA vous recommande de ne pas modifier la valeur par défaut.</p> <p>Si vous modifiez ce paramètre pour utiliser une partition différente, assurez-vous que la partition contient au moins 10 fois plus d'espace que la mémoire allouée pour le service ESA.</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p>Attention : Si le pool de mémoire est en cours d'utilisation alors que ce chemin est modifié, vous devrez redémarrer ESA. Dans ce cas précis, ESA tient compte des événements stockés mais vous laisse les supprimer manuellement.</p> </div>
MapPoolEnable	Activez ou désactivez le pool de mémoire.	La valeur par défaut est False . Définissez la valeur sur True pour activer le pool de mémoire. Lorsque vous activez ou désactivez le pool de mémoire, un redémarrage est nécessaire.

<p>MapPoolFlushIntervalSecs</p>	<p>Intervalle de temps pour vider les événements sur le disque. Par exemple, tout événement présent sur le moteur Esper plus de 15 minutes est systématiquement vidé sur le disque.</p>	<p>La valeur par défaut est 15 minutes. Une valeur inférieure garantit la stabilité du service ESA lorsque des EPL contiennent un grand nombre d'événements en mémoire. Une plus grande valeur (supérieure à 30 minutes) est la garantie que seuls les événements pertinents sur une longue période sont écrits sur le disque.</p> <div data-bbox="885 520 1419 804" style="border: 1px solid green; padding: 5px;"> <p>Remarque : En raison de la conception de la gestion de mémoire Java, quelquefois des événements non conservés par EPL peuvent être envoyés directement sur le disque. Pour éviter que cela se produise, vous pouvez définir une valeur plus élevée pour MapPoolFlushIntervalSecs.</p> </div>
<p>MapPoolBatchWriteSize</p>	<p>Indiquez la taille du lot (et si vous souhaitez utiliser le mode Traitement par lots). Les événements sont traités par lots au sein de groupes, puis transférés vers le disque.</p> <p>Pour utiliser le mode Non traitement par lots, appliquez la valeur 1.</p> <p>Pour utiliser le mode Traitement par lots, définissez une valeur supérieure à 1.</p>	<p>La taille du lot par défaut est 100 000 événements. À la fin de l'intervalle de vidage, si la capacité de charge n'est pas atteinte, le lot expire en 30 secondes et tout le contenu du lot est écrit sur le disque sous forme de fichiers de pool de mémoire.</p> <p>Une valeur plus petite pour la taille du lot (par exemple, 10 000 événements) garantit que lorsque les événements sont récupérés du disque, ils ne risquent pas d'affecter la mémoire, ce qui crée une plus grande stabilité. En revanche, une taille de lot plus importante (100 000 événements) réduit l'activité d'entrée et de sortie lors de l'écriture des événements sur le disque, ce qui peut créer de meilleures performances.</p>

MapPoolMinSize	Taille minimale du pool de stockage. Généralement, cette valeur est utilisée pour l'initialisation, donc aucune modification n'est nécessaire.	La valeur par défaut est de 10 000 événements. Une valeur plus élevée permet d'augmenter les performances. Une valeur plus faible garantit la stabilité du système.
MapPool Persist Type	Ce paramètre est en lecture seule, il permet d'activer le type d'optimisation utilisé.	La valeur par défaut est RMSerialize .

Remarque : L'efficacité de cette fonction dépend de votre environnement. Si vous écrivez des règles qui nécessitent un accès fréquent aux événements sur une période, cette fonction peut dégrader les performances avec ou sans amélioration minimale en termes d'évolutivité.

Remarque : Les fichiers de pool de mémoire sont supprimés lorsque tous les événements contenus dans le fichier du pool ne sont plus référencés par une règle EPL.

Résultat

Pour une règle EPL simple, le service ESA améliore généralement la mémoire 8 à 9 fois plus.

Configurer ESA pour utiliser l'ordonnancement temporel des captures

Cette rubrique indique aux administrateurs comment configurer ESA afin d'utiliser l'ordonnancement temporel des captures lors de l'utilisation de deux ou plusieurs services Concentrator en tant que sources.

Par défaut, ESA utilise l'horodatage ESA (heure à laquelle les événements sont reçus par ESA) pour corrélérer les événements. Cependant, ESA prend également en charge l'ordonnancement des sessions en fonction de l'heure de capture (heure à laquelle le paquet ou l'événement de log a atteint les services Decoder). Cette fonctionnalité est utile si vous mettez en corrélation des événements issus d'au moins deux Concentrators. Lorsque vous avez deux ou plusieurs services Concentrator comme sources, l'ordonnancement temporel vérifie que leurs sessions sont corrélées entre elles par heure de capture. Ainsi, vous avez l'assurance que les sessions capturées simultanément sont corrélées et que les alertes sont conformes aux attentes des utilisateurs, même avec des retards de transmission. Si l'une des sources se déconnectent ou est lente à envoyer des sessions, ESA fait une pause pour vérifier que les sessions avec les mêmes horodatages de capture sont corrélées conjointement.

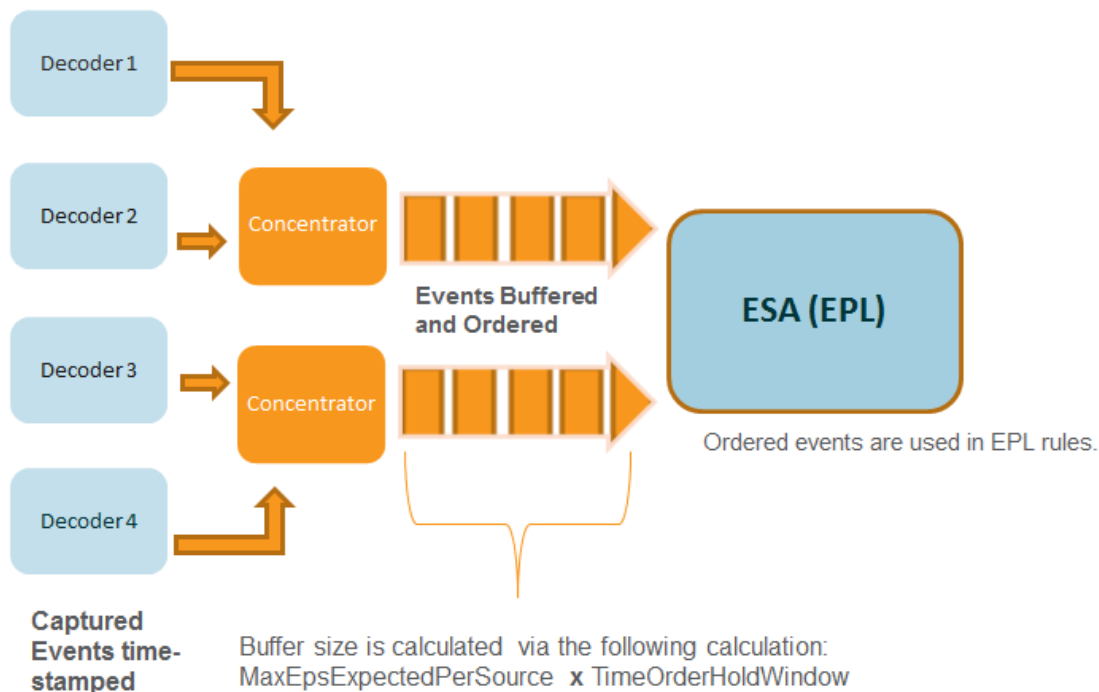
Par exemple, vous avez deux sources avec des événements qui se produisent à 10h00. Grâce à l'ordonnancement temporel des captures, ces événements sont conservés en mémoire tampon jusqu'à ce que ESA détecte que tous les événements qui se produisent à 10:00 ont été ajoutés à la mémoire tampon. Une fois que tous les événements sont arrivés, les événements sont ensuite traités en utilisant des règles EPL. Cela garantit que la règle dispose de tous les événements avec le même horodatage à partir de différentes sources afin d'obtenir des résultats corrects. Si, par exemple, un service Concentrator a du retard par rapport à un autre, ESA fait une pause jusqu'à ce que tous les événements soient horodatés à 10h00 sur les deux sources avant d'exécuter les règles EPL sur les événements.

Attention : Bien que cette fonctionnalité accroît la précision, elle a un impact sur les performances. La configuration par défaut de ESA s'assure que les données sont constamment en streaming, mais parce que l'ordonnancement temporel des captures utilise une mémoire tampon, il faut plus de temps pour traiter les événements. Cela est particulièrement vrai si ESA doit faire une pause pendant une certaine durée en attendant le remplissage de la mémoire tampon. Vous pouvez configurer plusieurs paramètres (voir ci-dessous) pour gérer cette situation ; cependant, il peut encore y avoir un impact sur les performances.

Cette fonction est désactivée par défaut.

Workflow d'ordonnancement temporel des captures

Le schéma suivant illustre le workflow lorsque l'ordonnancement temporel des captures est activé.



1. Les événements sont horodatés au fur et à mesure qu'ils sont capturés par le service Decoder.
2. Après le traitement Concentrator, les événements sont mis en mémoire tampon et ordonnancés. La taille de la mémoire tampon est calculée via deux paramètres MaxEPSExpectedPerSource (volume maximal du trafic (EPS) envisagé **par source** pour que ESA reçoivent les heures) et TimeOrderHoldWindow (période autorisée pour recevoir les événements issus de toutes les sources).
3. Les événements ordonnancés sont alors corrélés correctement dans les règles EPL.

Conditions préalables

Deux ou plusieurs services Concentrator doivent être configurés en tant que sources de données dans ESA.


Lorsque le paramètre **StreamEnabled** est défini sur true, il est important que toutes les machines exécutant les services de base soient en mode synchronisation NTP.

Procédures

Les procédures suivantes vous indiquent comment activer et configurer l'ordonnancement temporel des captures.

Activer la mise en mémoire cache et l'ordonnancement temporel des captures

Remarque : Après une mise à niveau ou dans un environnement EPS de haut niveau, vous devez rajouter les sources de données pour commencer à percevoir les avantages. Ou, vous devez attendre que les sessions rattrapent leur retard avant d'activer l'ordonnancement temporel des captures.

1. Dans le menu Security Analytics, sélectionnez **Administration** > **Services**. Sélectionnez le service ESA, puis  > **Vue** > **Explorer**.
2. Accédez à **Workflow** > **Source** > **nextgenAggregationSource**.
3. Définissez l'attribut **StreamEnabled** sur **true**. StreamEnabled permet à ESA de mettre en mémoire tampon les événements reçus des services Concentrator.
4. Définissez l'attribut **TimeOrdered** sur **true**. Cela permet aux événements horodatés d'être ordonnancés en fonction de l'horodatage du service Concentrator.

Configurer l'ordonnancement temporel des captures

Lorsque vous utilisez l'ordonnancement temporel des captures, vous devez configurer plusieurs autres paramètres pour garantir les performances. Le tableau ci-dessous présente les paramètres et leur description. La configuration de ces paramètres nécessite la connaissance de votre volume et de votre taux de trafic.

Remarque : Si vous ne connaissez pas votre volume de trafic ou sa latence, consultez votre représentant des Services professionnels avant de configurer cette fonctionnalité.

MaxEPSExpectedPerSource

Spécifie le volume maximal de trafic (EPS ou événements par seconde) correspondant à la capacité souhaitée de réception du service ESA basée sur votre source la plus occupée (par exemple, si une source reçoit 20 K EPS, et une autre reçoit 25 K EPS, définissez la valeur sur 25K EPS).

Si vous définissez ce taux trop bas, il y aura un impact à court terme sur les performances. Cependant, ESA augmente automatiquement la valeur de MaxEPSExpectedPerSource en fonction des besoins afin de progresser en mode Ordonnancement temporel.


La valeur par défaut est 20K

TimeOrderHoldWindow	<p>Indique en secondes (nombres entiers) la durée autorisée de réception des événements en provenance de toutes les sources.</p> <p>Configurez cette valeur sur la base du temps de latence entre les sources.</p> <p>La valeur par défaut est 2 secondes. La diminution de cette valeur peut augmenter le risque de suppression d'événements. L'augmentation de cette valeur peut réduire les performances système car la mémoire est plus sollicitée.</p>
IdleSourceAdvanceAfterSeconds	<p>Spécifie l'intervalle (en secondes), après lequel ESA traite une source en veille (aucun événement issu de la source, mais la source n'est pas hors ligne) en dehors de l'équation pour permettre la progression d'un flux avec ordonnancement temporel des captures. La valeur par défaut est 0, ce qui signifie que ESA attend indéfiniment l'arrivée d'événements.</p>
OfflineSourceAdvanceAfterSeconds	<p>Spécifie l'intervalle (en secondes), après lequel ESA traite une source hors ligne en dehors de l'équation pour permettre la progression d'un flux avec ordonnancement temporel des captures. La valeur par défaut est 0, ce qui signifie que ESA patiente indéfiniment. Ce paramètre n'a pas d'incidence sur les tentatives de reconnexion ; elles s'effectuent dans tous les cas.</p>

Conseils de résolution des problèmes

Grâce à cette fonctionnalité, il est possible de faire face à une situation où les événements sont retardés. Pour résoudre ce problème, vous pouvez effectuer l'une des opérations suivantes :



Désactiver l'ordonnancement temporel des captures

1. Dans le menu Security Analytics, sélectionnez **Administration** > **Services**. Sélectionnez le service ESA, puis  > Vue > Explorer.
2. Accédez à **Workflow** > **Source** > **nextgenAggregationSource**.
3. Définissez l'attribut StreamEnabled sur false.
4. Définissez l'attribut TimeOrdered sur false.

Si vous désactivez l'ordonnancement temporel des captures, vous perdrez les données en attente d'émission et les événements ne seront plus ordonnancés en fonction de l'heure de capture.

Désactiver le suivi de position

Le suivi de position permet à ESA de localiser le point d'arrêt du traitement des événements en cas d'arrêt ou de panne. Le suivi de position est activé par défaut avec l'ordonnancement temporel des captures. Si vous désactivez le suivi de position, ESA peut alors ignorer les événements retardés. Par exemple, si ESA connaît une défaillance à 07h00, et que vous le redémarrez à 11h00 avec le suivi de position désactivé, ESA commencera le traitement des événements ayant eu lieu à 10h55. Avec le suivi de position activé, ESA reprendra le traitement des événements au point où il s'est arrêté.

1. Dans le menu Security Analytics, sélectionnez **Administration** > **Services**. Sélectionnez le service ESA, puis   > **Vue** > **Explorer**.
2. Accédez à **Workflow** > **Source** > **nextgenAggregationSource**.
3. Définissez l'attribut **PositionTrackingEnabled** sur false.

Si vous désactivez le suivi de position, vous perdrez les données consignées, mais par la suite, les événements seront ordonnancés en fonction de l'heure des captures.

Démarrer, arrêter ou redémarrer le service ESA

Cette rubrique contient les instructions de démarrage, d'arrêt ou de redémarrage du service Event Stream Analysis.

Démarrer le service ESA.

Avant de commencer :

- Vérifiez que MongoDB fonctionne.
- Si le service MongoDB ne fonctionne pas, utilisez la commande suivante pour le démarrer :
`service tokumx start`

Pour démarrer le service ESA :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :
`service rsa-esa start`

Arrêter le service ESA

Pour arrêter le service ESA :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :

```
service rsa-esa stop
```

Redémarrer le service ESA

Pour redémarrer le service ESA :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :

```
service rsa-esa restart
```

Vérifier la version et l'état des composants ESA

Cette rubrique contient des instructions pour vérifier les versions des composants Event Stream Analysis installés.

Vérifier la version du serveur ESA

Pour vérifier la version du serveur ESA :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :

```
rpm -qa | grep rsa-esa-server
```

La version du serveur ESA s'affiche.

Vérifier la version de MongoDB

Pour vérifier la version de MongoDB :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :

```
mongo --version
```

La version MongoDB s'affiche.

Vérifier l'état de MongoDB

Pour vérifier l'état de MongoDB :

1. Utilisez SSH pour vous connecter au service ESA et connectez-vous en tant qu'utilisateur root.
2. Saisissez la commande suivante et appuyez sur ENTRÉE :
`service tokumx status`
3. Exécutez la commande suivante si MongoDB ne fonctionne pas.
`service tokumx start`

Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur d'ESA dans Security Analytics. Ces rubriques sont présentées par ordre alphabétique.

Utilisez cette section si vous recherchez la description des attributions de droits et définitions des fonctions de l'interface utilisateur.

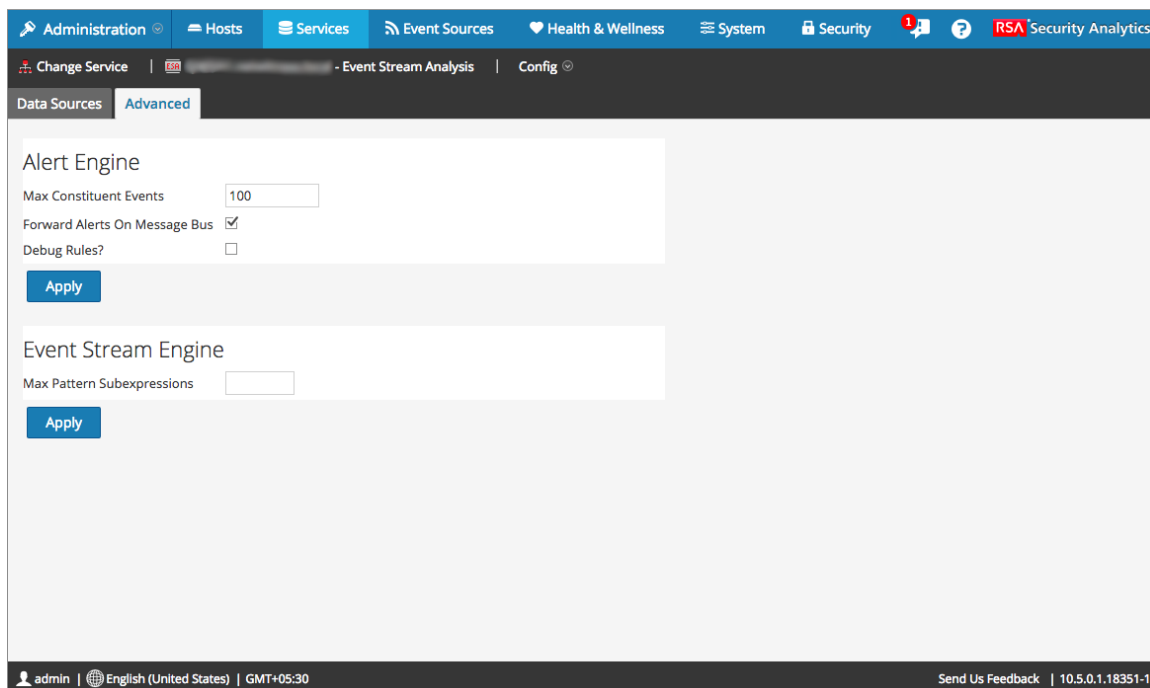
Pour obtenir des détails supplémentaires, consultez l'une des sections suivantes :

- [Vue Configuration des services, onglet Avancé](#)
- [Vue Configuration des services, onglet Sources de données](#)

Vue Configuration des services, onglet Avancé

Cette rubrique décrit les composants de la vue Configuration des services, onglet Avancé d'ESA.

Pour configurer les paramètres avancés d'un service ESA, accédez à la **vue Configuration des services d'ESA > onglet Avancés d'ESA**.



Fonctions

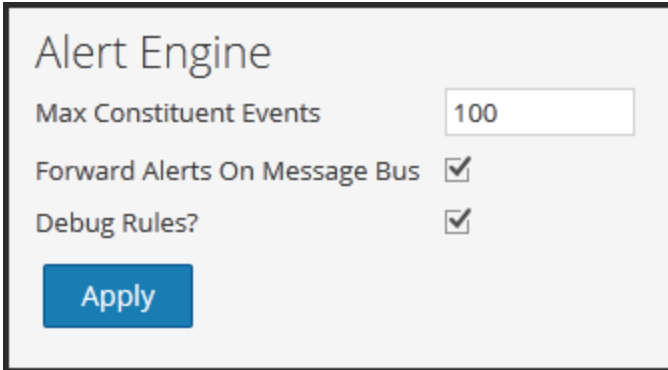
La vue Avancé se compose des sections suivantes :

- Moteur d'alerte
- Moteur de flux d'événements

Paramètres du moteur d'alerte

Dans la section Moteur d'alertes, spécifiez les valeurs pour réserver des événements aux règles qui choisissent plusieurs événements.

La figure suivante affiche la section Moteur d'alertes.



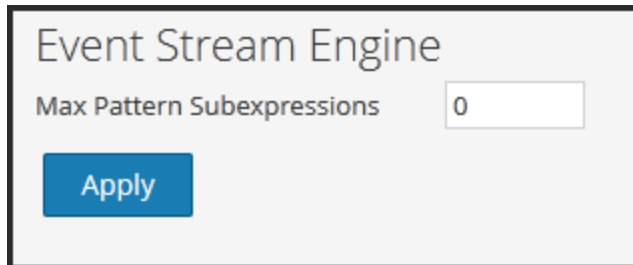
Le tableau suivant reprend les paramètres de la section Moteur d'alerte et leur description :

Paramètre	Description :
Nombre maximal d'événements constitutifs	Pour les règles qui choisissent plusieurs événements, cette valeur de configuration détermine le nombre d'événements associés qui sont conservés. Par exemple, si une règle déclenche une alerte avec 200 événements associés et que ce paramètre est défini sur 100, seuls les 100 premiers sont conservés par ESA, les autres sont supprimés. La valeur par défaut est 100 .
Transférer les alertes vers le bus de messages	Pour transférer les alertes ESA pour Incident Management, vous devez sélectionner cette option. Les alertes ESA générées sont envoyées au bus de message, puis à Incident Management. Cette option est sélectionnée par défaut. Vous pouvez vérifier si le service Gestion des incidents est en cours d'exécution.
La sélection de l'option Déboguer les règles ?	active les règles de débogage.

Paramètres du moteur de flux d'événements

Dans la section Event Stream Engine, spécifiez les détails pour améliorer les performances.

La figure suivante affiche la section Moteur de flux d'événements.



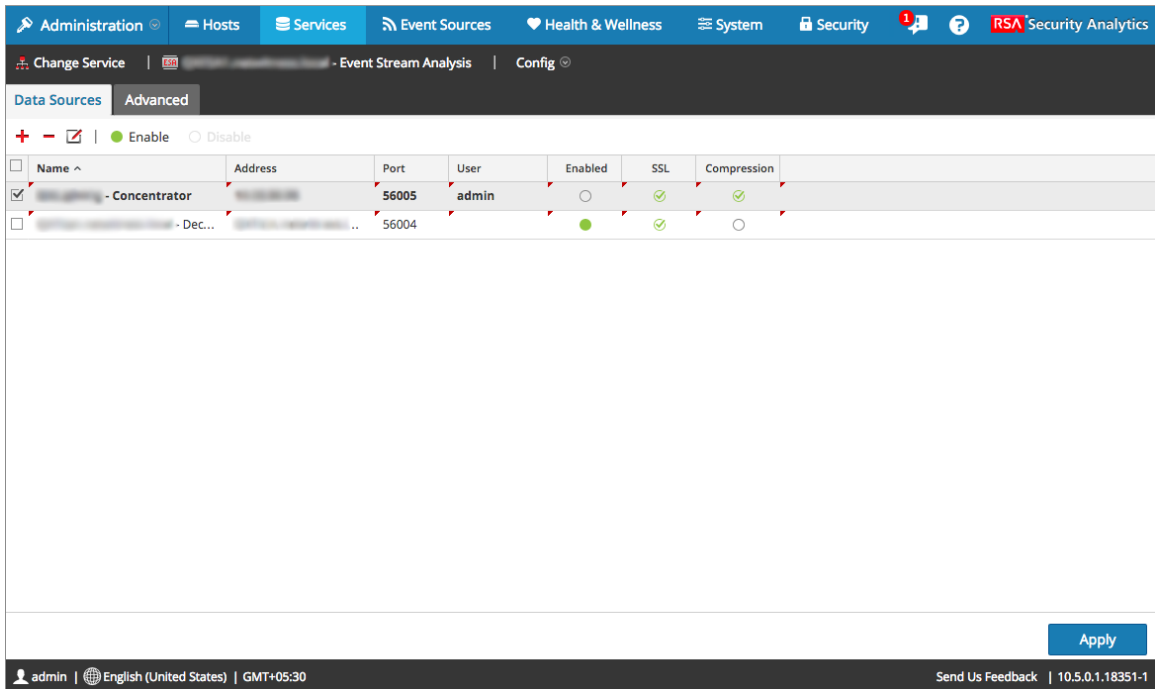
Le tableau suivant reprend les paramètres de la section Moteur de flux d'événements et leur description :

Paramètre	Description :
Nombre maximal de sous-expressions de modèles	Certaines règles requièrent ESPER pour maintenir les sous-expressions en mémoire avant de décider de leur déclenchement ou non. Ces sous-expressions consomment de la mémoire et risquent d'entraîner l'arrêt du service par saturation de la mémoire si elles restent sans contrôle. Ce paramètre constitue une mesure de sécurité qui maintient sous contrôle les règles de monopolisation de la mémoire. Si une règle dépasse le nombre de sous-expressions spécifié, son traitement est retardé. La valeur par défaut est 0 ; ce paramètre est donc désactivé. Vous devez définir une valeur en cas de problème de stabilité du service.

Vue Configuration des services, onglet Sources de données

Cette rubrique décrit les composants de la vue Configuration des services, onglet Sources de données d'ESA.

La vue **Configuration des services > onglet Sources de données** du service ESA est utilisé pour configurer les sources de données d'ESA.







Fonctions

Les éléments suivants sont les sections de l'onglet Source de données :

- Barre d'outils
- Grille Source de données

Barre d'outils

Le tableau suivant décrit les options de la barre d'outils.

Paramètre	Description
	Ajoute une nouvelle source de données à ESA.
	Supprime une source de données d'ESA.
	Modifie une source de données. Vous devez posséder les informations d'identification (nom d'utilisateur et mot de passe) pour le service pour pouvoir effectuer des modifications.
 Enable	Active la source de données sélectionnée.

Paramètre	Description
<input type="radio"/> Disable	Désactive la source de données sélectionnée.

Grille Source de données

Dans la grille Source de données, toutes les sources de données qui ont été ajoutées au service ESA sont affichées. Le tableau suivant décrit les paramètres de la grille Source de données.

Paramètre	Description
Name	Nom du service de source de données.
Adresse	Adresse du service de source de données.
Port	Port utilisé par la source de données.
Utilisateur	Utilisateur connecté à la source de données.
Enabled	Indique si la source de données est activée.
SSL	Indique si la communication SSL est activée.
Compression	Indique si la compression est activée.