RSA NETWITNESS® SUITE

Guide de configuration ESA

pour la version 11.0

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

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 contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

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

EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

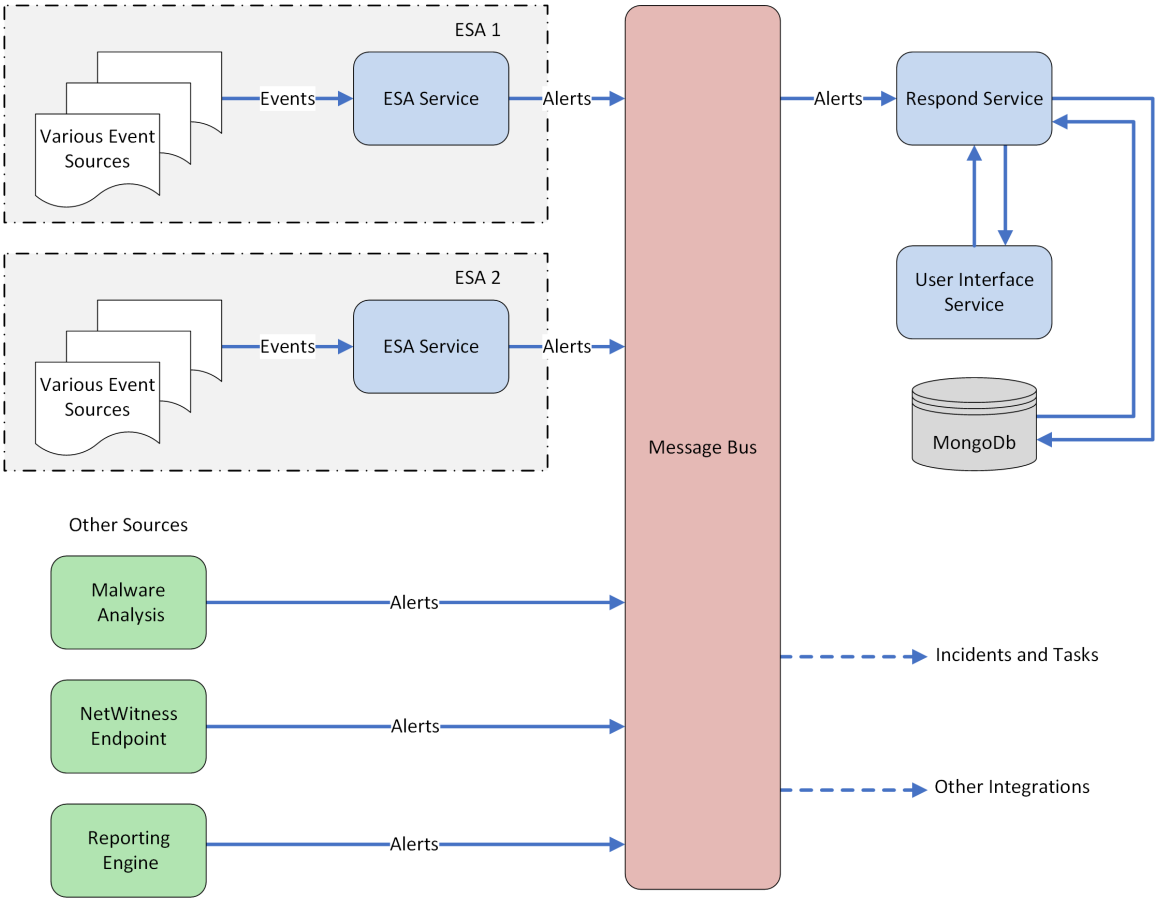
Sommaire

Présentation d'Event Stream Analysis

RSA NetWitness® Suite 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 schéma suivant présente le workflow de données général :



Il existe deux services ESA pouvant s'exécuter sur un hôte ESA :

- Event Stream Analysis (règles de corrélation ESA)
- Event Stream Analytics Server (ESA Analytics)

Le premier service est le service Event Stream Analysis qui crée des alertes à partir de règles ESA, également appelé ESA Correlation Rules, que vous créez manuellement ou téléchargez à partir de Live. Le deuxième service est le service ESA Analytics, qui est utilisé pour la détection automatisée des menaces. Étant donné que le service ESA Analytics utilise des modules ESA Analytics préconfigurés pour la détection automatisée des menaces, vous n'avez pas besoin de créer ou de télécharger des règles pour utiliser la détection automatisée des menaces.

Les services ESA Analytics utilisent l'agrégation basée sur la requête (QBA) pour collecter des événements filtrés pour les modules ESA Analytics à partir des Concentrators. Seules les données requises par un module sont transférées entre le service Concentrator et le système ESA Analytics. Par exemple, en utilisant un module ESA Analytics pour les domaines suspects, par exemple C2 for Packets (http-packet), un service ESA Analytics peut examiner votre trafic HTTP pour déterminer la probabilité que des activités malveillantes se produisent dans votre environnement.

Configurer des règles de corrélation ESA

Cette rubrique décrit les tâches générales permettant de configurer les règles de corrélation RSA NetWitness Suite Event Stream Analysis (ESA) à l'aide du service Event Stream Analysis.

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. Ajoutez un Concentrator comme source de données au service Event Stream Analysis.	Consultez la rubrique Étape 1. Ajouter une source de données à un service ESA
2. Configurez les notifications pour le service Event Stream Analysis.	Reportez-vous à la rubrique « Méthodes de notification » dans le *Guide des alertes basées sur ESA*.
3. Télécharger le contenu d'Event Stream Analysis à l'aide de Live.	Reportez-vous à la rubrique « Vue Live Search » dans le *Guide de gestion des ressources Live*.
4. (Facultatif) Configuration avancée du service Event Stream Analysis.	Reportez-vous à la rubrique Étape 2. Configurer des paramètres avancés pour un service 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 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 NetWitness Suite.

Le service Event Steam Anaysis doit être installé et en cours d'exécution sur NetWitness Suite.

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

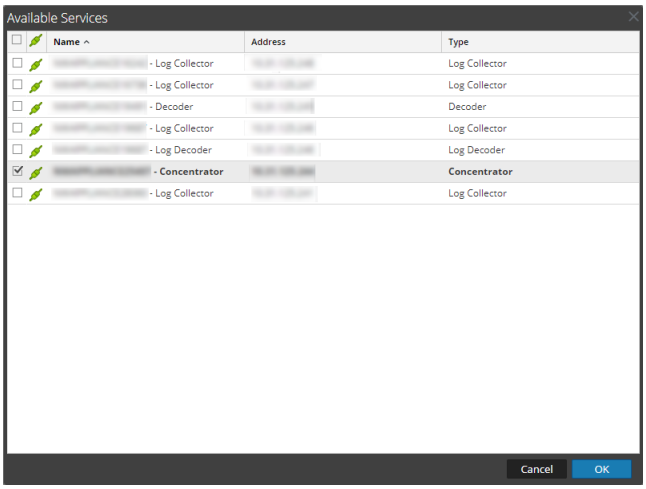
Procédures

Ajouter des services existants comme source de données

1. Accédez à **ADMIN> Services**.
   La vue Services s'affiche.
2. Dans la vue Services, sélectionnez un service ESA et cliquez sur  **> Vue > Config**.

3. Sous l'onglet **Sources de données**, cliquez sur  .

   Les services disponibles s'affichent, comme illustré sur la figure suivante.



4. Sélectionnez un ou plusieurs Concentrators et cliquez sur **OK**.

   Le service est ajouté à la liste des services sous l'onglet **Source de données**.

5. (Facultatif) Cliquez sur **Activer** pour activer la source de données.

6. 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. Accédez à **ADMIN > 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 **Enregistrer**.

Étape 2. Configurer des paramètres avancés pour un service ESA

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

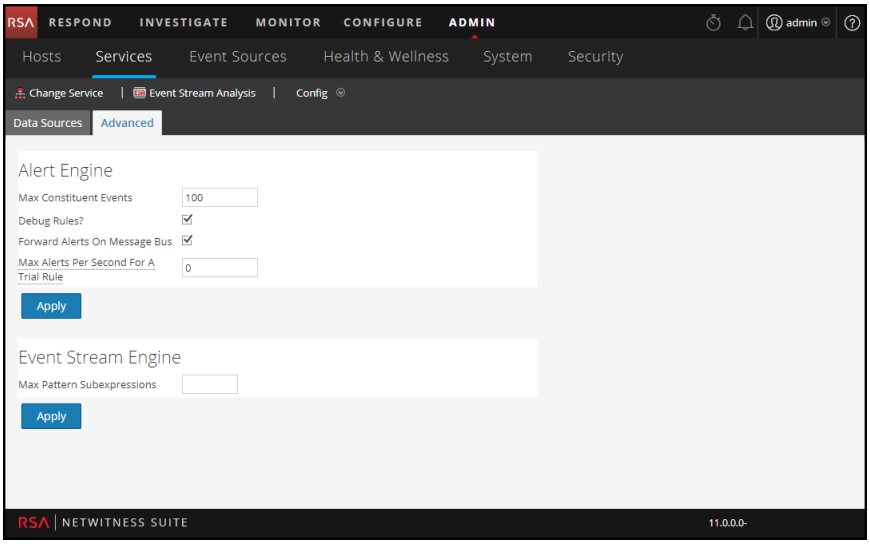
Dans la vue Avancé, vous pouvez configurer les paramètres avancés pour améliorer les performances, pour conserver les événements des règles à plusieurs événements, pour mettre les événements dans le tampon mémoire et pour spécifier le nombre d'événements à stocker dans ESA.

Procédures

Configurer les paramètres avancés

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

1. Accédez à **ADMIN > Services**.
   La vue Services s'affiche.
2. Dans la vue Services, sélectionnez un service ESA et cliquez sur > **Vue > Config**.
3. Sélectionnez l'onglet **Avancé**.
   La vue Avancé s'affiche.



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.

Pour configurer les paramètres du moteur d'alerte :

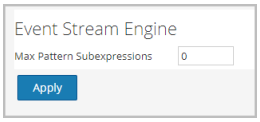
1. Dans la section Moteur d'alerte, saisissez une valeur pour **Nombre maximal d'événements constitutifs**. La valeur par défaut est 100.
2. Sélectionnez**Déboguer les règles ?** pour activer les règles de débogage.
3. Pour que les alertes soient envoyées au bus de messages et à Respond, sélectionnez l'option **Transférer les alertes vers le bus de messages**.
4. Pour spécifier le nombre maximal d'alertes à transférer au bus de messages pour la règle d'évaluation, sélectionnez **Nombre maximal d'alertes par seconde pour une règle d'évaluation**. La valeur par défaut est **10**.
5. 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.

Configurer ESA Analytics

Cette section décrit les tâches générales de configuration des services ESA Analytics pour RSA NetWitness® Suite Automated Threat Detection. La fonctionnalité Automated Threat Detection vous permet d'analyser les données qui résident sur un ou plusieurs services Concentrator en utilisant des modules ESA Analytics préconfigurés, par exemple un module pour les domaines suspects. Par exemple, en utilisant un module pour les domaines suspects, un service ESA Analytics peut examiner votre trafic HTTP pour déterminer la probabilité que des activités malveillantes se produisent dans votre environnement.

Il existe deux services ESA pouvant s'exécuter sur un hôte ESA :

- Event Stream Analysis (règles de corrélation ESA)
- Event Stream Analytics Server (ESA Analytics)

Le premier service est le service Event Stream Analysis qui crée des alertes à partir de règles ESA, également appelé ESA Correlation Rules, que vous créez manuellement ou téléchargez à partir de Live. Le deuxième service est le service ESA Analytics, qui est utilisé pour la détection automatisée des menaces et est configuré dans cette section. Étant donné que le service ESA Analytics utilise des modules ESA Analytics préconfigurés pour la détection automatisée des menaces, vous n'avez pas besoin de créer ou de télécharger des règles pour l'utiliser.

Deux modules ESA Analytics sont actuellement disponibles. Ils concernent toux deux les domaines suspects :

- C2 for Packets (http-packet)
- C2 for Logs (http-log)

Configurer le service de recherche Whois

La fonctionnalité RSA NetWitness Suite Automated Threat Detection vous permet d'analyser automatiquement des sources de données à l'aide des modules ESA Analytics préconfigurés. Un module ESA Analytics est un pipeline composé d'objets d'activité qui enrichissent un événement avec des informations supplémentaires via des calculs mathématiques. Les services ESA Analytics traitent ces modules pour identifier les menaces avancées.

La configuration du service de recherche Whois est requise pour les modules de domaines suspects.

Remarque : (**Important**) RSA vous recommande fortement de configurer le service de recherche Whois pour plus de précision dans les résultats de détection automatisée des menaces.

Conditions préalables

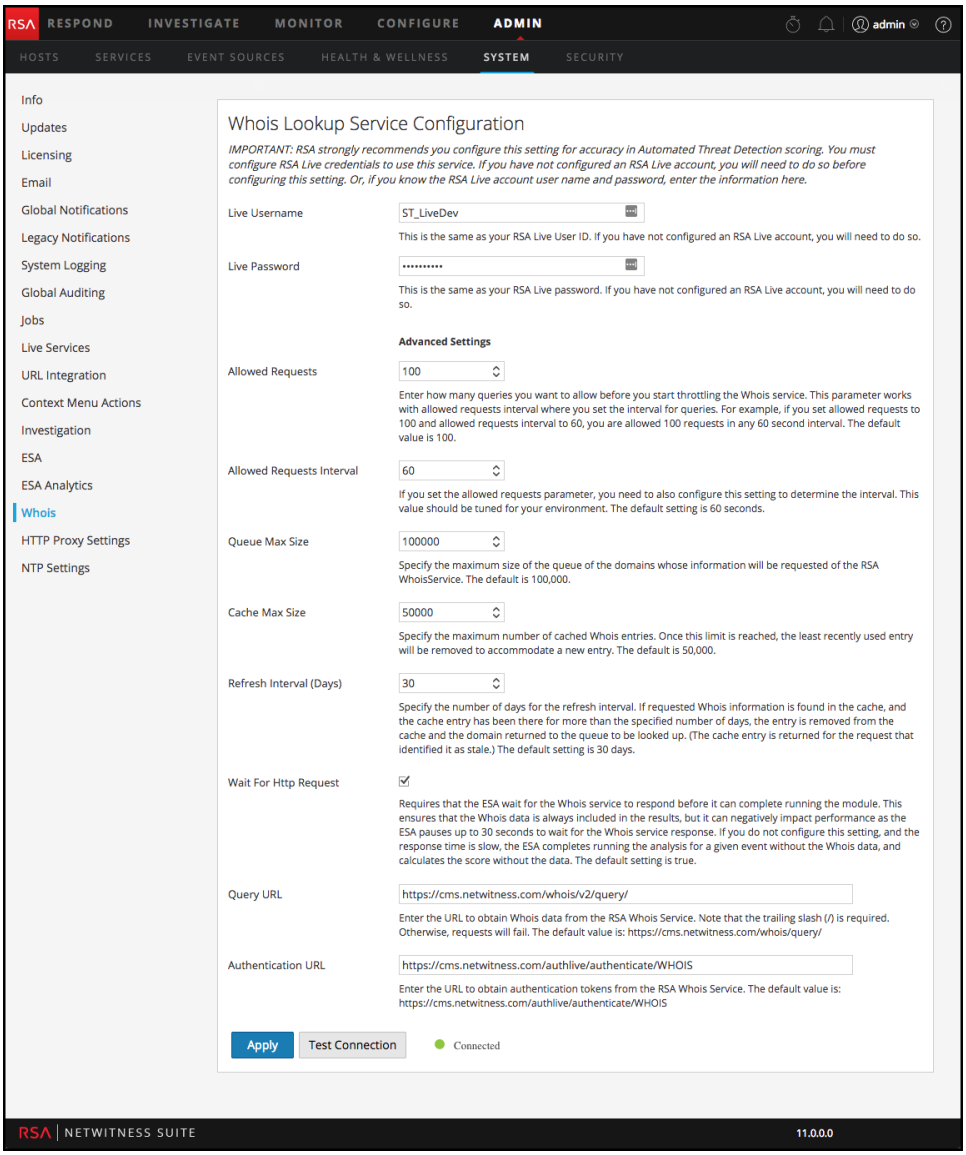
- Vous devez disposer d'un compte RSA Live pour utiliser le service de recherche Whois.
- Le service ESA Analytics Server doit être disponible (afficher un cercle vert) dans la vue ADMIN > Services.

Si vous avez configuré un compte Live dans le panneau Services Live (ADMIN > Système > Live Services), le service de recherche Whois est automatiquement configuré pour vous. Il vous suffit de vérifier la connexion du service de recherche Whois.

Remarque : Si vous ne disposez pas d'un compte RSA Live, vous pouvez en créer un via le portail d'inscription RSA Live :
https://cms.netwitness.com/registration/
Le *Guide de gestion des services Live* fournit des informations supplémentaires.

Configurer le service de recherche Whois

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Whois**.
3. Dans le panneau **Configuration du service de recherche Whois**, vérifiez si le service de recherche Whois est connecté. En bas du panneau, le service connecté est repéré par un cercle vert en regard de **Connecté** :



S’il est connecté, la configuration est terminée et vous pouvez ignorer les étapes restantes.
Pour modifier les paramètres avancés, passez à l’étape 5.
Si le service n’est pas connecté, passez à l'étape 4.

4. Dans les champs **Nom d’utilisateur Live** et **Mot de passe Live**, entrez vos informations d’identification de compte RSA Live pour accéder au serveur RSA Whois.

5. Si nécessaire, vous pouvez modifier les paramètres avancés. Toutefois, RSA recommande d’utiliser les valeurs par défaut. Configuration du service de recherche Whois fournit des informations supplémentaires.

6. Cliquez sur **Tester la connexion** pour vérifier la connexion.
Si la connexion a abouti, un cercle vert s’affiche en regard de **Connecté** : 

7. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Mappage des sources de données ESA aux modules Analytics

Cette rubrique indique aux administrateurs comment mapper des modules spécifiques ESA Analytics aux différentes sources de données et services ESA Analytics pour renforcer l'efficacité du traitement.

Vous pouvez analyser les données qui résident sur un ou plusieurs Concentrators avec la fonctionnalité RSA NetWitness Suite Automated Threat Detection en sélectionnant un module ESA Analytics préconfiguré. Les données analysées par ces modules sont utilisées pour identifier les menaces avancées. Pour mieux utiliser vos ressources réseau et réduire le flux de données inutile, vous pouvez mapper plusieurs sources de données (telles que des Concentrators) à plusieurs services ESA Analytics afin de traiter les données plus efficacement et de tirer parti de capacités supplémentaires.

Un *module ESA Analytics* est un pipeline composé d'objets d'activité qui enrichissent un événement avec des informations supplémentaires via des calculs mathématiques. Les modules ESA Analytics résident dans les services ESA Analytics.

Lorsque vous déployez votre mappage, les services ESA Analytics sélectionnés utilisent l'agrégation basée sur une requête pour collecter les événements filtrés appropriés pour le module sélectionné à partir des Concentrators. L'agrégation basée sur une requête est une requête prédéfinie qui transfère uniquement les données pour le module ESA Analytics sélectionné. Seules les données requises par le module sont transférées entre le service Concentrator et le système ESA Analytics.

Deux modules ESA Analytics sont actuellement disponibles pour les domaines suspects : C2 for Packets (http-packet) et C2 for Logs (http-log).

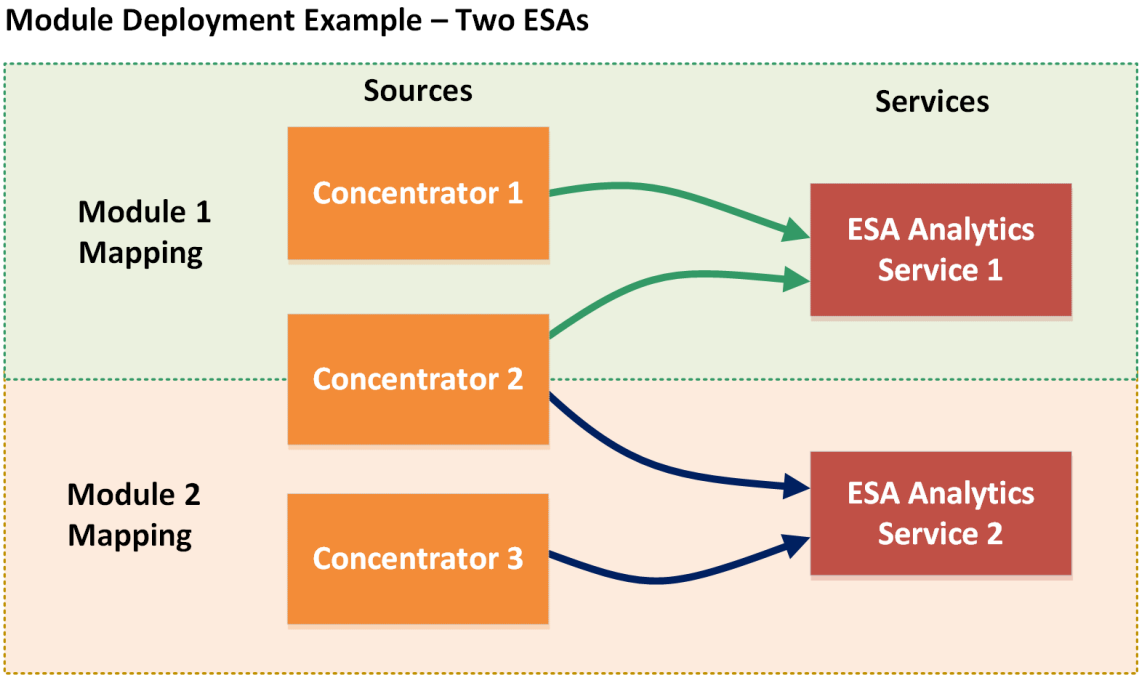
Exemple de déploiement de modules : deux ESA

Pour tirer parti de votre capacité de Concentrator supplémentaire, vous pouvez mapper un module ESA Analytics à un service ESA Analytics et le déployer pour analyser les données à partir de plusieurs sources de données en même temps.

Par exemple, si vous avez trois Concentrators et deux services ESA Analytics, vous pouvez créer et déployer les mappages suivants :

- Mappez le module 1 aux sources 1 et 2 du Concentrator et au service ESA Analytics 1. Le service ESA Analytics 1 analyse les événements filtrés du module 1 issus des Concentrators 1 et 2.
- Mappez le module 2 aux sources 2 et 3 du Concentrator et au service ESA Analytics 2. Le service ESA Analytics 2 traite les événements filtrés du module 2 issus des Concentrators 2 et 3.

Dans cet exemple, le module 1 représente un module ESA Analytics, par exemple C2 for Packets (http-packet) et le module 2 représente un autre module ESA Analytics, par exemple C2 for Logs (http-logs) à un autre emplacement.



Cet exemple montre comment les deux services peuvent traiter les données issues du même Concentrator. Notez que les services ESA Analytics 1 et 2 peuvent tous deux traiter les données issues du Concentrator 2. Le service ESA Analytics 1 interroge les données pour les événements du module 1 et le service ESA Analytics 2 interroge les différentes données pour les événements du module 2.

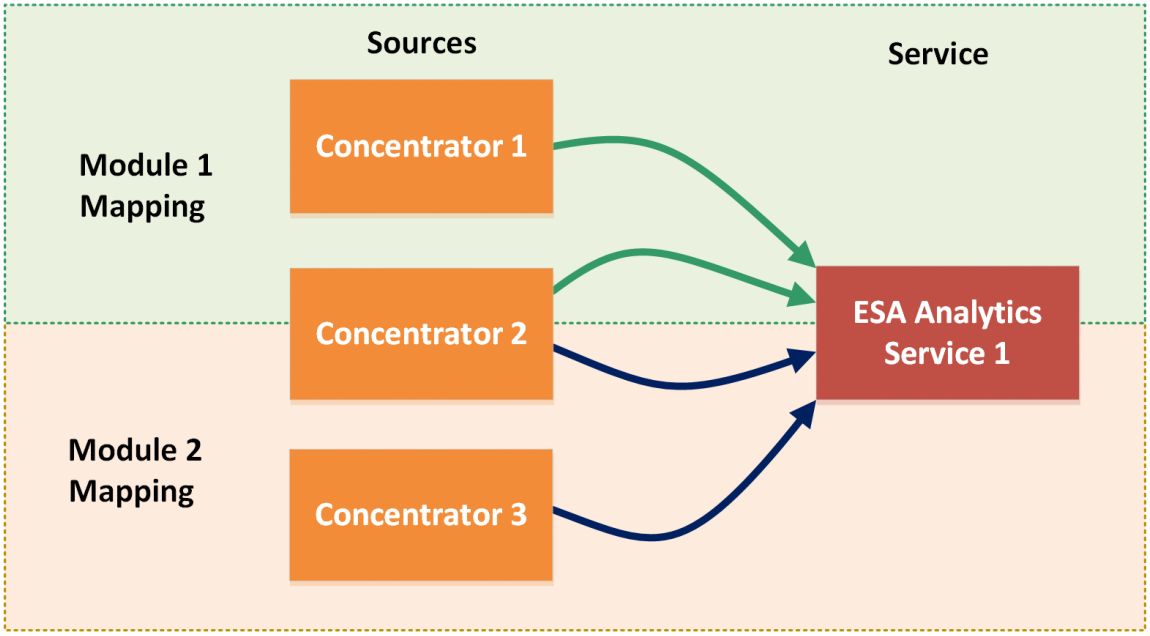
Exemple de déploiement de module : un ESA

En plus de créer des mappages de modules qui sont traités par différents services ESA Analytics, vous pouvez mapper plusieurs modules au même service ESA Analytics.

Par exemple, si vous avez trois Concentrators et un service ESA Analytics, vous pouvez créer et déployer les mappages suivants :

- Mapper le module 1 aux sources 1 et 2 du Concentrator et au service ESA Analytics 1. Le service ESA Analytics 1 analyse les événements filtrés du module 1 issus des Concentrators 1 et 2.
- Mapper le module 2 aux sources 2 et 3 du Concentrator et au service ESA Analytics 1. Le service ESA Analytics 1 traite les événements filtrés du module 2 issus des Concentrators 2 et 3.

Module Deployment Example – One ESA



Cet exemple montre comment un seul service peut traiter les données provenant de plusieurs modules. Notez que le service ESA Analytics 1 peut traiter les données issues des Concentrators 1 et 2 pour le module 1. Il traite également les données issues des Concentrators 2 et 3 pour le module 2. Le service ESA Analytics 1 interroge les données pour les événements du module 1 et interroge les différentes données pour les événements du module 2.

Attention : Assurez-vous que tous les services d'hôte NetWitness Suite sont synchronisés avec une source de temps cohérente.

Conditions préalables

- Tous les services d'hôte NetWitness Suite doivent être synchronisés avec une source de temps cohérente.
- Les hôtes et services Concentrator doivent être découverts et disponibles dans l'interface utilisateur NetWitness Suite.
- Toutes les exigences spécifiques du module doivent être respectées.
  - Pour les domaines suspects :
    - Configurer les paramètres de log (domaines suspects uniquement pour les logs)
    - Créer une liste blanche à l'aide du service Context Hub.
    - Configurer le service de recherche Whois

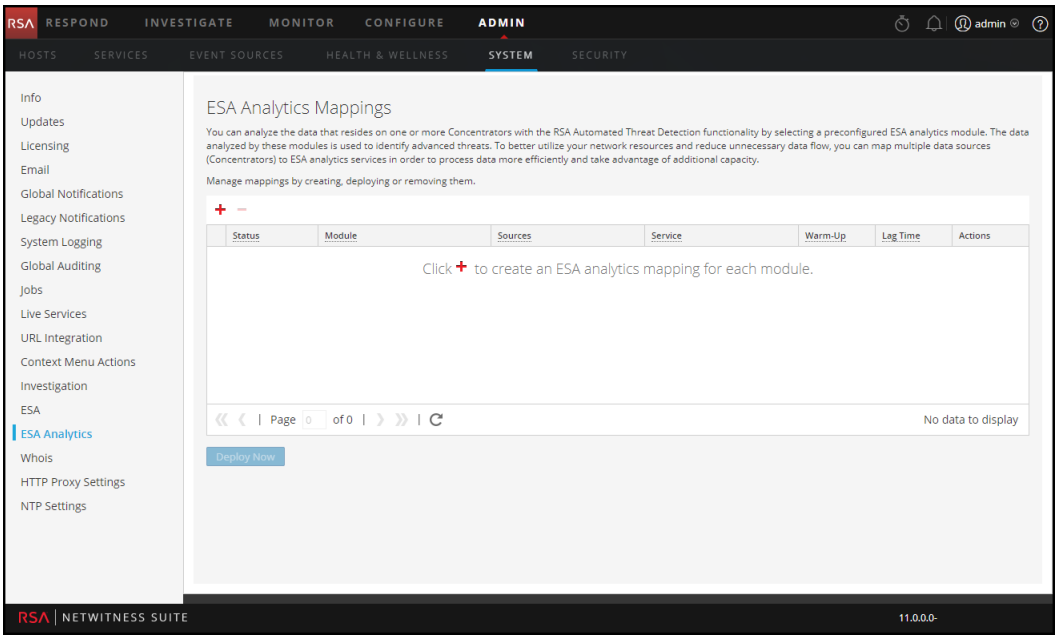
- Vérifier que la règle d'incident C2 est activée et surveiller la pour repérer l'activité.
- Vérifier que les incidents sont regroupés par C&C suspecte.

Pour savoir comment procéder par étape, reportez-vous au *NetWitness Suite Guide de détection automatisée des menaces*.

Créer des mappages ESA Analytics

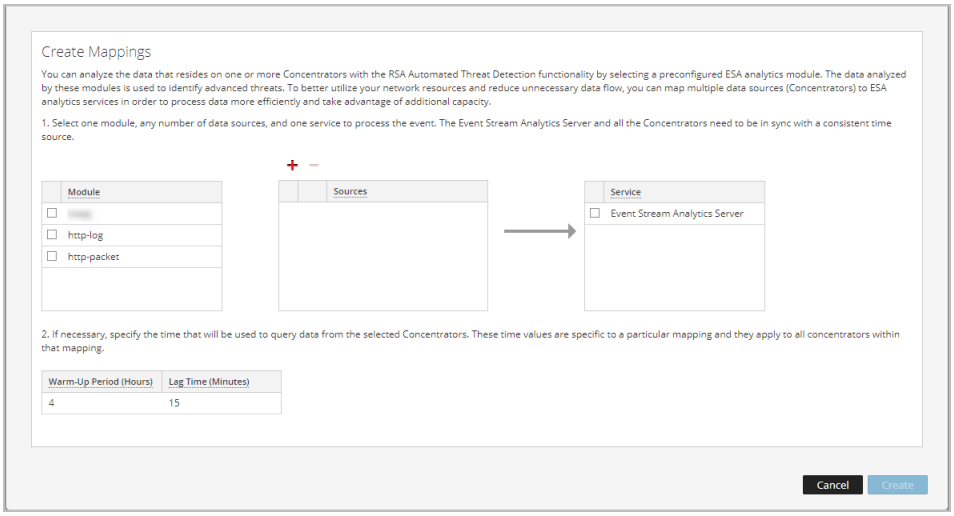
La procédure suivante vous indique comment mapper les modules ESA Analytics aux sources et services. Après avoir créé et revu les mappages, déployez-les pour qu'ils puissent démarrer l'agrégation des données.

1. Accédez à **ADMIN** > **Système**, et dans le panneau d'options, sélectionnez **ESA Analytics**. Le panneau **Mappages ESA Analytics** s'affiche.

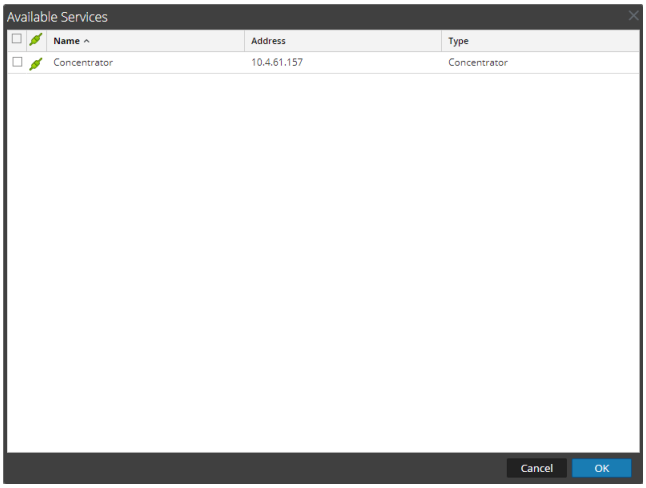


2. Cliquez sur + pour créer un mappage ESA Analytics. Créez un mappage distinct pour chaque module.

La boîte de dialogue **Créer des mappages** s'affiche.

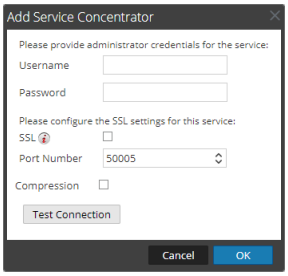


3. Dans la liste **Module**, sélectionnez un module.
4. Configurez une ou plusieurs sources de données (Concentrators) pour vos mappages. Procédez de la façon suivante pour chaque Concentrator :
   a. Cliquez sur + .
      La boîte de dialogue Sources disponibles affiche les sources de données qui sont disponibles dans la vue Admin > Services.



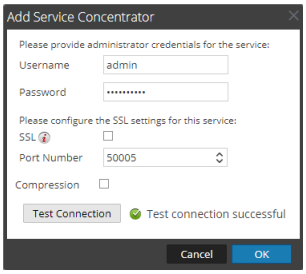
   b. Dans la boîte de dialogue **Sources disponibles**, sélectionnez un Concentrator et cliquez sur **OK**.

La boîte de dialogue Ajouter une source s'affiche.



c. Dans la boîte de dialogue **Ajouter une source**, saisissez le nom d'utilisateur administrateur pour le Concentrator.

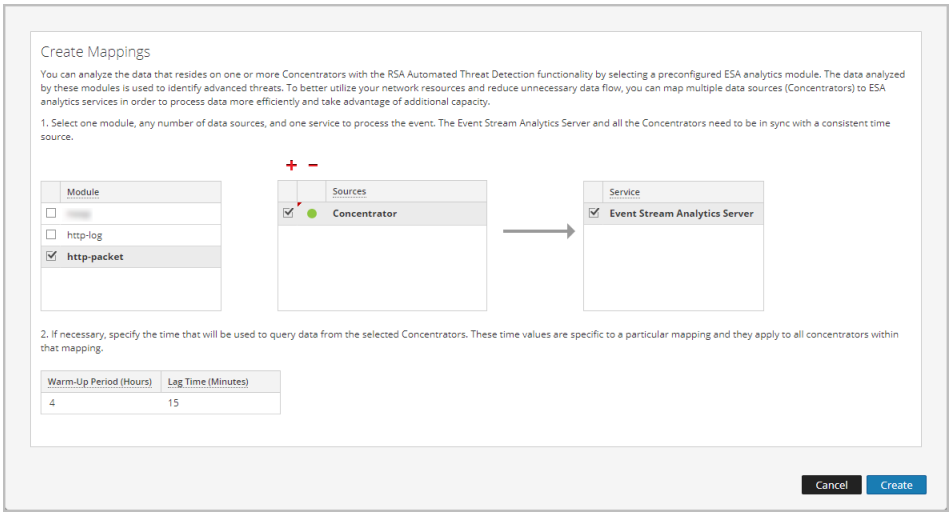
d. Cliquez sur **Tester la connexion** pour vous assurer qu'il peut communiquer avec le service ESA Analytics.



e. Cliquez sur **OK**.

Lorsque vous avez configuré vos sources de données et qu'elles apparaissent dans la liste Sources, vous pouvez les réutiliser pour d'autres mappages.

5. Dans la liste **Sources**, sélectionnez une ou plusieurs sources de données pour agréger les données pour le module.



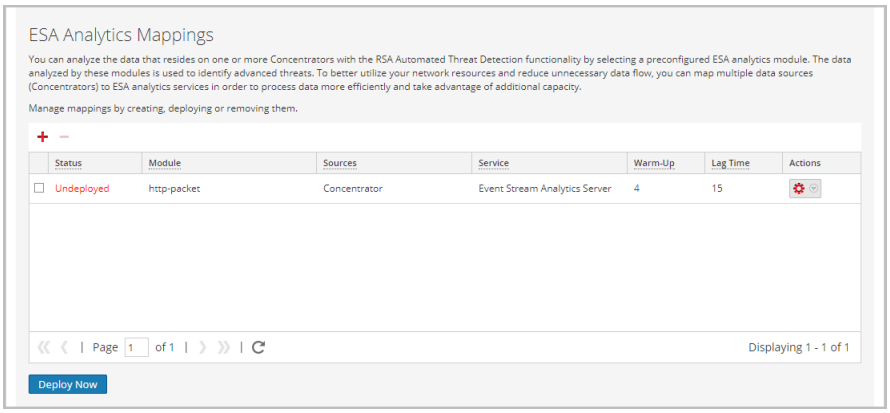
Un cercle vert plein indique un service en cours d'exécution et un cercle blanc indique un service arrêté.

6. Dans la liste **Service**, sélectionnez un service ESA Analytics pour traiter les données pour le module.
7. Si nécessaire, spécifiez l'heure qui sera utilisée pour interroger les données des services Concentrator sélectionnés.

Champ	Description
Période d'initialisation (Heures)	Spécifie une durée d'initialisation (en heures). Une période d'initialisation est nécessaire pour permettre à la détection automatisée des menaces d'en savoir plus sur votre trafic. La période d'initialisation doit s'exécuter lorsqu'un trafic classique est en cours d'exécution. Pendant ce temps, l'alerte relative au mappage de module est supprimée. La période d'initialisation amorce le module avec les données historiques et garantit que le nombre spécifié d'heures de collecte de données est atteint avant l'envoi d'alertes. RSA fournit des modules ESA Analytics préconfigurés. Chaque type de module dispose d'une période d'initialisation définie par défaut, que vous pouvez ajuster à votre environnement, si nécessaire. Après cette période d'initialisation, les alertes peuvent être affichées. Pour plus d'informations sur la période d'initialisation et le temps de latence, reportez-vous à la rubrique Paramètres du module.

Champ	Description
Temps de latence (Minutes)	Spécifie un délai constant, en minutes, qui est ajouté pour éviter de perdre des événements en cours de traitement par les sources de données pendant les périodes d'activité intense. Par exemple, les performances du Concentrator varient en fonction de facteurs tels que la charge entrante, les requêtes en continu et l'indexation. En raison de ces facteurs, un Concentrator peut ne pas agréger les événements en temps réel, ce qui entraîne un retard. Le paramètre de latence donne au service Concentrator une chance de terminer l'agrégation de toutes les données. Une fois la période d'initialisation terminée, l'agrégation des données se poursuit à l'**Heure actuelle (système) - Temps de latence**. Cela est utile lorsqu'un service Concentrator tarde à agréger les données. Le temps de latence garantit que le module ne traite pas les données qui arrivent au Concentrator pendant la période de latence, et un retard suffisant assure que tous les événements générés dans l'entreprise peuvent être traités par le module. Par exemple, si le temps de latence est de 30 minutes et que l'heure actuelle est 14h00, le Concentrator commencera à extraire les enregistrements à 13h30. La période de latence, 30 minutes dans cet exemple, reste constante. Lorsque l'heure actuelle passe à 14h01, le Concentrator extrait la minute de données suivante à 13h31, et ainsi de suite. **Important :** Le temps de latence définit le décalage entre l'heure actuelle et l'heure à laquelle le module réceptionne les données. **Attention :** RSA recommande aux administrateurs d'ajuster le paramètre de latence dynamiquement en fonction des performances de chaque Concentrator pour éviter de manquer des événements lors de l'agrégation. Pour plus d'informations sur la période d'initialisation et le temps de latence, reportez-vous à la rubrique Paramètres du module;

8. Cliquez sur **Créer**.
   Les mappages que vous créez s'affichent dans la liste des mappages existants avec l'état **Non déployé**.



Important : Pour démarrer un module pour qu'il lance l'agrégation des données, vous devez le déployer.

Déployer des mappages ESA Analytics

Une fois que vous avez créé vos mappages, vous devez les déployer afin de lancer l'agrégation des données pour les modules.

1. Dans la liste des mappages, vérifiez que l'état des mappages que vous souhaitez déployer est **Non déployé**.
2. Sélectionnez un ou plusieurs mappages à l'état Non déployé et sélectionnez **Déployer maintenant**.
   Tous les mappages sélectionnés à l'état Non déployé commencent à agréger les données de la façon configurée dans le mappage. L'état du mappage passe à **Déployé**.
   Vous ne pouvez pas déployer un mappage qui a déjà été déployé.

Mettre à jour un mappage

Vous ne pouvez avoir qu'un seul mappage par module. Si vous souhaitez apporter des modifications à un mappage déployé, par exemple en ajoutant ou en supprimant des Concentrators ou en modifiant le service, vous devez annuler le déploiement et supprimer le mappage existant, puis créer et déployer un nouveau mappage pour ce module.

Vous pouvez apporter les mises à jour suivantes à un mappage déployé sans le supprimer :

- Annuler le déploiement d'un mappage
- Modifier la période d'initialisation et le temps de latence

Vous pouvez aussi modifier la période d'initialisation et le temps de latence d'un mappage de module non déployé.

Annuler le déploiement d'un mappage

Si vous souhaitez arrêter l'agrégation des données pour un mappage de module, mais que vous ne souhaitez pas supprimer le mappage, vous pouvez en annuler le déploiement. Vous pouvez alors le déployer ultérieurement. Lorsque vous annulez le déploiement d'un mappage, le service ESA Analytics arrête d'extraire les données de la source de données de ce module.

Attention : L'annulation du déploiement d'un mappage dont l'état est Déployé a une incidence sur l'agrégation des données de ce module.

Pour annuler le déploiement d'un mappage

1. Dans le panneau Mappages ESA Analytics, sélectionnez le mappage déployé dont vous souhaitez annuler le déploiement.
2. Dans la colonne **Actions**, sélectionnez  > **Annuler le déploiement**.
   L'état passe de Déployé à Non déployé et l'agrégation des données s'arrête.

Supprimer un mappage

Vous pouvez supprimer un mappage dont l'état est Non déployé à tout moment. Étant donné qu'un mappage à l'état Non déployé n'est pas en cours d'exécution, il n'affecte pas l'agrégation des données.

Vous devez annuler le déploiement d'un mappage dont l'état est Non déployé avant de le supprimer. L'annulation du déploiement d'un mappage et la suppression de ce mappage efface sa configuration sur le serveur ESA, annule le déploiement de ce mappage et arrête l'extraction des données à partir de la source de données de ce module.

Attention : L'annulation du déploiement d'un mappage et la suppression de ce mappage a une incidence sur l'agrégation des données de ce module.

Pour supprimer un mappage :

1. Dans le panneau Mappages ESA Analytics, sélectionnez le mappage que vous souhaitez supprimer. Vous ne pouvez supprimer qu'un seul mappage à la fois.
2. Cliquez sur .

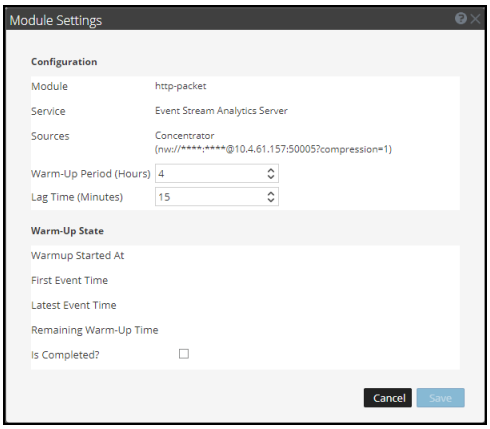
Modifier la période d'initialisation et le temps de latence

Vous voudrez peut-être régler la période d'initialisation d'un mappage de module spécifique. Par exemple, une fois la période d'initialisation dépassée, vous pouvez augmenter le paramètre de la période d'initialisation afin d'autoriser un temps d'initialisation supplémentaire. Vous pouvez même augmenter la période d'initialisation lorsque votre mappage de module s'initialise activement.

Si nécessaire, vous pouvez modifier le temps de latence pour le module. Le temps de latence définit le décalage entre l'heure actuelle (système) et l'heure à laquelle le module réceptionne les données.

1. Dans le panneau Mappages ESA Analytics, sélectionnez le mappage que vous souhaitez modifier puis, dans la colonne **Actions**, sélectionnez > **Modifier le module**.

   La boîte de dialogue Paramètres du module affiche le module sélectionné, le service ESA Analytics et les sources de données pour le mappage. Les sources de données affichent les URL utilisées pour communiquer avec ESA.



2. Consultez la section **État de l'initialisation** pour déterminer l'état actuel de l'initialisation :
   - **Initialisation démarrée à** : heure à laquelle le premier événement a été traité par le module ESA Analytics à partir de la source de données.
   - **Heure du premier événement** : heure à laquelle le premier événement s'est produit. Le temps d'initialisation est basé sur cette heure.
   - **Heure du dernier événement** : heure à laquelle le dernier événement s'est produit.
   - **Temps d'initialisation restant** : nombre d'heures restantes dans la période d'initialisation.
   - **Terminé ?** Indique si la période d'initialisation est terminée. Si c'est le cas, la période d'initialisation est terminée. Si ce n'est pas le cas, le module est toujours en cours d'initialisation et vous pouvez afficher le nombre d'heures restantes dans le champ Temps d'initialisation restant.
3. Dans la section **Configuration**, vous pouvez mettre à jour la **Période d'initialisation (heures)** selon que la période d'initialisation est terminée ou non.
   - **Pendant la période d'initialisation** : Vous pouvez ajouter des heures à la période d'initialisation ou soustraire un temps d'initialisation restant.

- **Après la période d'initialisation** : Vous pouvez ajouter des heures à la période d'initialisation en ajoutant la différence entre l'heure actuelle et l'heure du premier événement aux heures que vous souhaitez ajouter.
  Par exemple, une période d'initialisation de 10 heures est terminée et l'heure du premier événement est 12:00:00. L'heure actuelle est 16:00:00 (4 heures plus tard) et vous souhaitez ajouter 5 heures à la période d'initialisation. Pour ce faire, vous devez ajouter 9 heures (4+5=9) à la période d'initialisation de 10, donc vous devez définir une nouvelle période d'initialisation de 19 heures.
  Vous ne pouvez pas réduire la période d'initialisation si elle est terminée, sauf si vous supprimez le mappage et que vous en créez un nouveau.

4. Si nécessaire, vous pouvez ajuster le **Temps de latence (Minutes)** pour donner aux Concentrators présents dans le mappage plus de temps pour terminer l'agrégation de toutes les données.
5. Cliquez sur **Enregistrer**.
   Les modifications NE prennent PAS effet immédiatement. Pour que les paramètres prennent effet, vous devez annuler le déploiement et redéployer le mappage.
6. Pour annuler le déploiement du mappage, dans le panneau Mappages ESA Analytics, sélectionnez le mappage dont vous voulez annuler le déploiement et  **> Annuler le déploiement**.
   L'agrégation des données s'arrête pour le mappage sélectionné.
7. Pour redéployer le mappage, sélectionnez le mappage que vous souhaitez déployer et  **> Déployer**.
   Le mappage sélectionné se déploie et commence à agréger les données de la façon configurée dans le mappage.

Procédures des règles de corrélation ESA supplémentaires

Cette rubrique regroupe différentes procédures qu'un administrateur peut réaliser à tout moment et qui ne sont pas requises dans la configuration initiale des règles de corrélation ESA.

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

- Modifier le seuil de mémoire pour les règles d'évaluation
- 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 le seuil de mémoire pour les règles d'évaluation

Cette procédure est facultative et s’applique uniquement aux règles de corrélation ESA.

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 influer 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

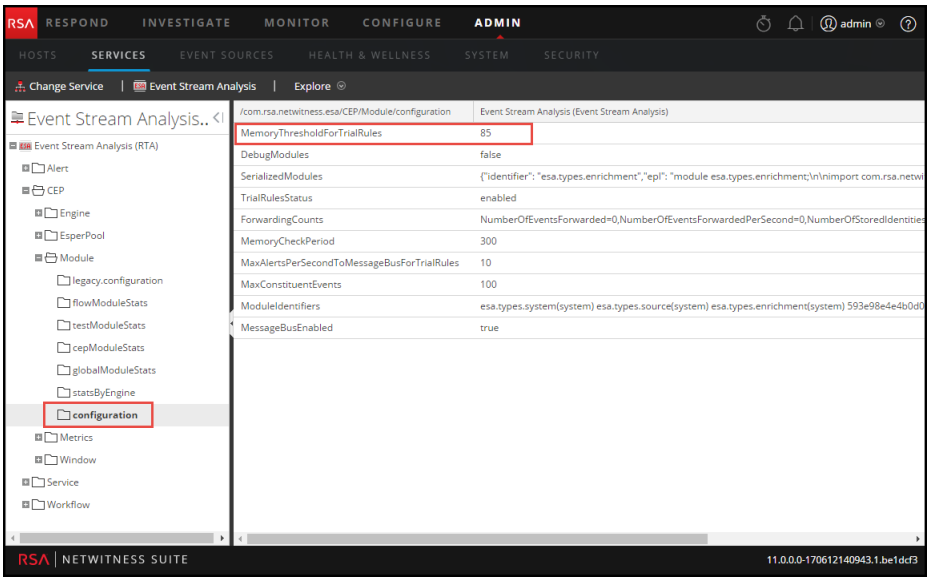
Pour plus de détails, reportez-vous à la rubrique « Utiliser les règles d'évaluation » dans le « Guide des alertes basées sur ESA ».

Conditions préalables

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

Procédure

1. Connectez-vous à NetWitness Suite en tant qu'administrateur.
2. Accédez à **ADMIN** > **Services**.
3. Sélectionnez le service ESA et sélectionnez > **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 service ESA pour utiliser un pool de mémoire

Cette procédure s'applique uniquement aux règles de corrélation ESA.

Les administrateurs peuvent configurer le service ESA pour qu'il utilise 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 influer sur les performances de la mémoire.

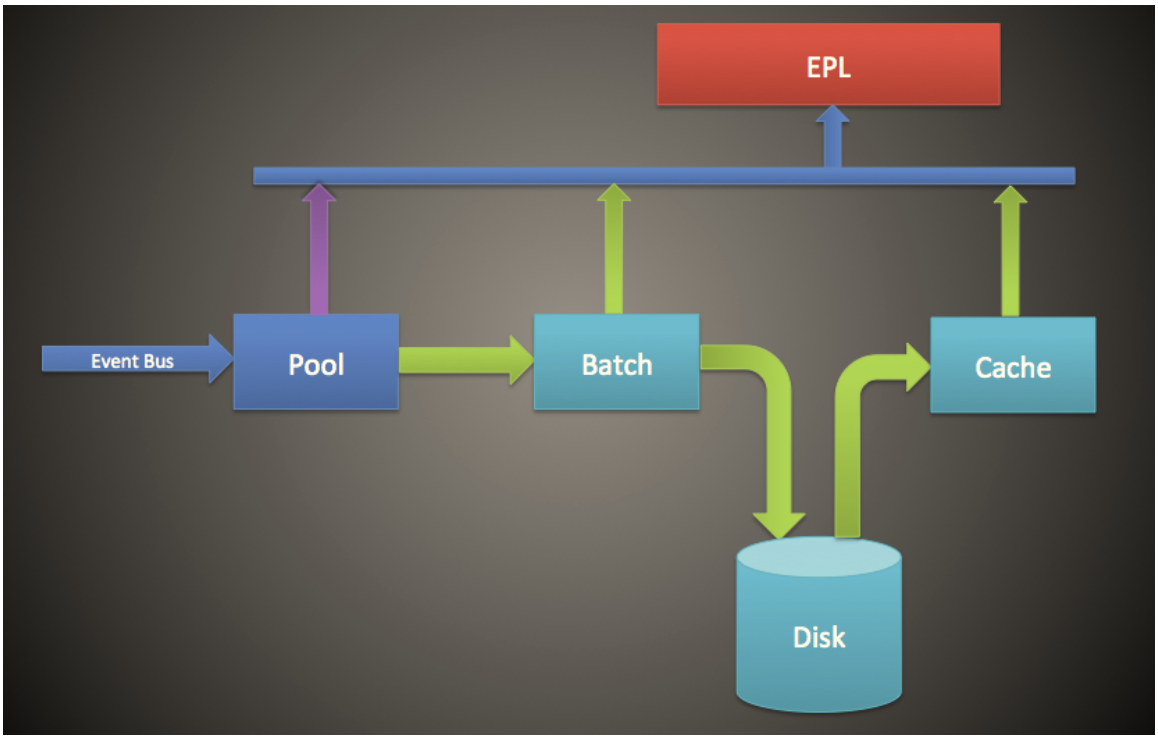
- **Traitement par lots**. En mode Traitement par lots, les événements sont regroupés en lots et ensuite écrits sur le disque. Pour configurer le mode Traitement par lots, définissez l'attribut de taille du lot **MapPoolBatchWriteSize** sur une valeur supérieure à 1. Le mode Traitement par lots donne 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. Accédez à **ADMIN** > **Services**, sélectionnez votre service ESA, puis cliquez sur > **Vue** > **Explorer**.
2. Selectionnez **CEP** > **EsperPool** > **Configuration**.
3. Saisissez des valeurs pour les champs suivants :

Attributs	Description	Configuration

MapPoolPersistenceURI	Emplacement de stockage du fichier pool de mémoire.	La valeur par défaut est **/opt/RSA/ESA/pool/esperPool**. RSA vous recommande de ne pas modifier la valeur par défaut. 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. **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.
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.
MapPoolFlushIntervalSecs	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.	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. **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.

MapPoolBatchWriteSize	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. Pour utiliser le mode Non traitement par lots, appliquez la valeur 1. Pour utiliser le mode Traitement par lots, définissez une valeur supérieure à 1.	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. 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.
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'afficher 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.

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 procédure s’applique uniquement aux règles de corrélation ESA.

Les administrateurs peuvent 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 corréler 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.

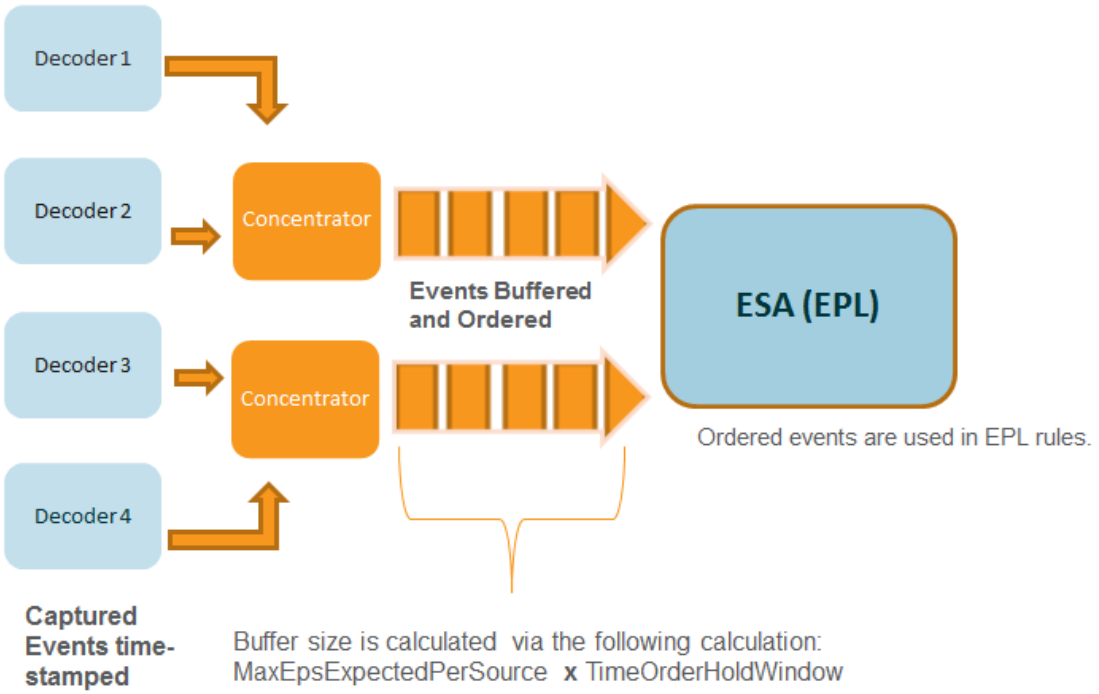
Par exemple, vous avez deux sources avec des événements qui se produisent à 10h00. Grâce à l'ordonnancement temporel des captures, ces événements sont conservés en mémoire tampon jusqu'à ce que ESA détecte que tous les événements qui se produisent à 10:00 ont été ajoutés à la mémoire tampon. Une fois 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 traffic (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. Accédez à **ADMIN** > **Services**, sélectionnez votre service ESA, puis cliquez sur  > **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 évènements 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	Indique en secondes (nombres entiers) la durée autorisée de réception des événements en provenance de toutes les sources. Configurez cette valeur sur la base du temps de latence entre les sources. 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.
IdleSourceAdvanceAfterSeconds	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.

OfflineSourceAdvanceAfterSeconds	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.

Conseils de Dépannage

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. Accédez à **ADMIN** > **Services**, sélectionnez votre service ESA, puis cliquez sur  **> 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. Accédez à **ADMIN** > **Services**, sélectionnez votre service ESA, puis cliquez sur  **> 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. Cette procédure s'applique aux règles de corrélation ESA.

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 :
  `systemctl start mongod`

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 :
   `systemctl start rsa-nw-esa-server`

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 :
   `systemctl stop rsa-nw-esa-server`

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 :
   `systemctl restart rsa-nw-esa-server`

Vérifier la version et l'état des composants ESA

Cette rubrique fournit des informations contient des instructions sur la consignation des audits et des instructions pour vérifier les versions des composants Event Stream Analysis installés. Ces procédures s'appliquent aux règles de corrélation ESA.

Règles de consignation des audits

La consignation des audits vous permet d'afficher d'autres informations sur les règles qui sont créées et modifiées dans NetWitness Suite.

Pour savoir comment accéder à vos logs d'audit, reportez-vous à la rubrique Emplacements des logs d'audit locaux dans le *Guide de Configuration système*.

L'exemple suivant montre comment créer, mettre à jour et supprimer un log pour une règle donnée.

- **Exemple de création de log :** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "CREATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true, Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR"`
- **Exemple de mise à jour de log :** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS" category: SYSTEM operation: "UPDATE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR`
- **Exemple de suppression de log :** `2016-03-10 14:19:37,951 deviceVersion: "10.6.1.0-SNAPSHOT" deviceService: "EVENT_STREAM_ANALYSIS"category: SYSTEM operation: "DELETE RULE" parameters: "Epl Module Identifier: 56e1f2adbee8290008241296, Esper Instance: default, Rule Enabled: true , Trial Rule: false " key: "Epl Rule: @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_ESA_ADMINISTRATOR "`

Chaque log contient les paramètres suivants :

- Horodatage : Heure de modification de la règle. Exemple : 2016-03-10 14:19:37,951
- VersionPériphérique : Version de votre périphérique ESA. Exemple : "10.6.1.0-SNAPSHOT"

- ServicePériphérique : Exemple : EVENT_STREAM_ANALYSIS
- Categorie : Exemple : SYSTEM
- Exemple d'opération : DELETE/CREATE/UPDATE RULE
- Paramètres : Espace réservé pour les clés suivantes :
- Identifiant Module EPL : identifiant unique pour la règle. Exemple : 56e1f2adbee8290008241296
- Instance Esper : Instance Esper sur laquelle la règle est déployée. Exemple : par défaut
- Règle activée : Indique si la règle est activée ou non. Exemple : Règle activée : true
- Règle d'évaluation : Indique si la règle est configurée en tant que règle d'évaluation ou non. Exemple : Règle d'évaluation : false
- Règle EPL : Affiche la syntaxe de la règle. Exemple :

  ```
  @RSAAlert select * from Event;" identity: "admin" userRole: "ROLE_
  ESA_ADMINISTRATOR+ROLE_ESA_ADMINISTRATOR+ROLE_ESA_ADMIN"
  ```

- Identité : Exemple : admin
- userRole: Exemple : "ROLE_ESA_ADMINISTRATOR"

Remarque : Lorsqu'une règle est désactivée, deux logs sont générés pour la même règle. Tout d'abord, un journal d'audit de la règle de suppression « Delete Rule » [Rule enabled attribute = true] est créé, suivi d'un journal d'audit de la règle de création « Create Rule » [Rule enabled attribute =false].

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-nw-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 :
   ```
   systemctl status mongod
   ```
3. Exécutez la commande suivante si MongoDB ne fonctionne pas.
   ```
   systemctl start mongod
   ```

Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur de configuration d'ESA dans NetWitness Suite.

Consultez les rubriques suivantes pour plus d'informations.

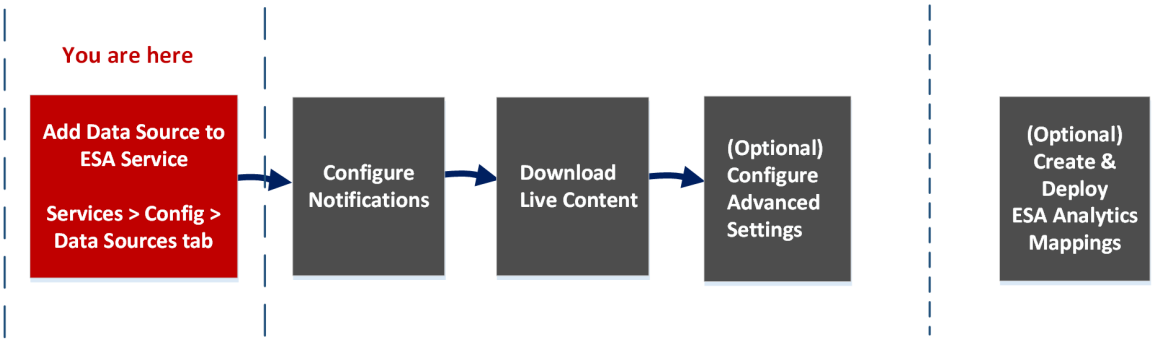
- Vue Configuration des services, onglet Avancé
- Vue Configuration des services, onglet Sources de données
- Mappages ESA Analytics
- Paramètres du module
- Configuration du service de recherche Whois

Vue Configuration des services, onglet Sources de données

L'onglet **vue Configuration des services > Sources de données** du service ESA est utilisé pour configurer les sources de données utilisées par ESA pour analyser les données. Un service ESA réceptionne les données à partir de Concentrators pour détecter les incidents et alerter les analystes d'incidents potentiels.

Workflow

Ce workflow montre l'ensemble du processus de configuration d'ESA. Il indique également l'emplacement dans le processus de la configuration des sources de données.



ESA comprend deux services, le service Event Stream Analysis (règles de corrélation ESA) et le service Event Stream Analytics Server (ESA Analytics). Les quatre premières procédures indiquées se rapportent à la configuration du service Event Stream Analysis :

- Ajouter une source de données à un service ESA
- Configurer les notifications
- Télécharger le contenu
- (Facultatif) Configurer les paramètres avancés

La dernière procédure se distingue des autres et s'applique à la création de mappages pour que les services ESA Analytics détectent automatiquement des menaces avancées :

- (Facultatif) Créer et déployer des mappages ESA Analytics

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Ajouter un Concentrator comme source de données au service Event Stream Analysis *	Voir Configurer des règles de corrélation ESA et Étape 1. Ajouter une source de données à un service ESA
Administrateur	Configurer les notifications	Reportez-vous à la section « Méthodes de notification » dans le *Guide des alertes basées sur ESA*.
Administrateur	Télécharger le contenu	Reportez-vous à la section « Vue Live Search » dans le *Guide de gestion des ressources Live*.
Administrateur	Configurer les paramètres avancés	Étape 2. Configurer des paramètres avancés pour un service ESA

*Vous pouvez effectuer ces tâches ici (c'est-à-dire sous l'onglet Sources de données de la vue Configuration des Services).

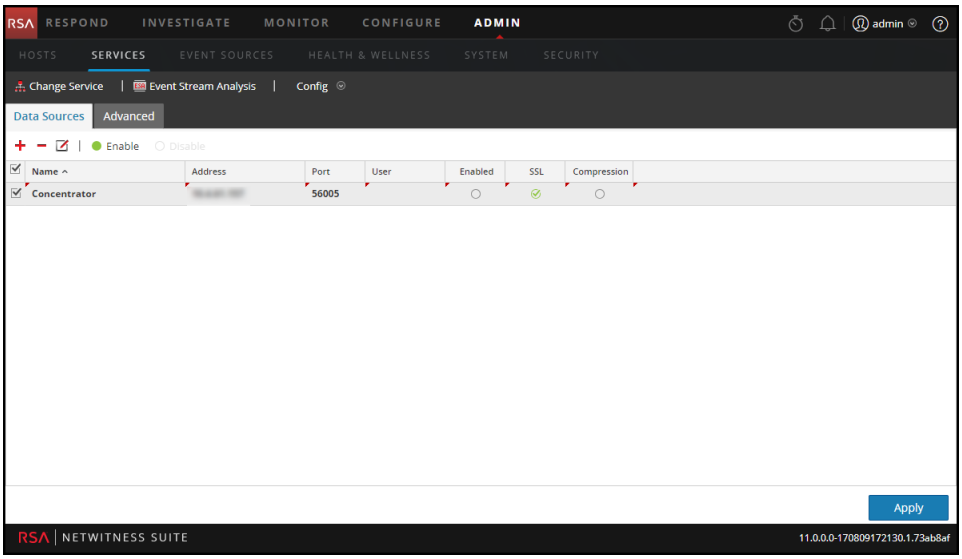
Rubriques connexes

- Consultez la section « Ajouter ou mettre à jour un hôte » dans le *Guide de mise en route de l'hôte et des services*

Aperçu rapide

Pour accéder à l'onglet Source de données, accédez à **ADMIN > Services >** (sélectionnez un service ESA) >  **> Vue > Config**.

La figure suivante illustre l'onglet Source de données de la vue Configuration des services d'un service ESA.



Barre d'outils

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

Option	Description
+	Ajoute une nouvelle source de données au service ESA.
−	Supprime une source de données du service 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.
Disable	Désactive la source de données sélectionnée.

Sources de données

La liste Sources de données affiche toutes les sources de données ajoutées au service ESA. Le tableau suivant décrit les colonnes de la liste Sources de données.

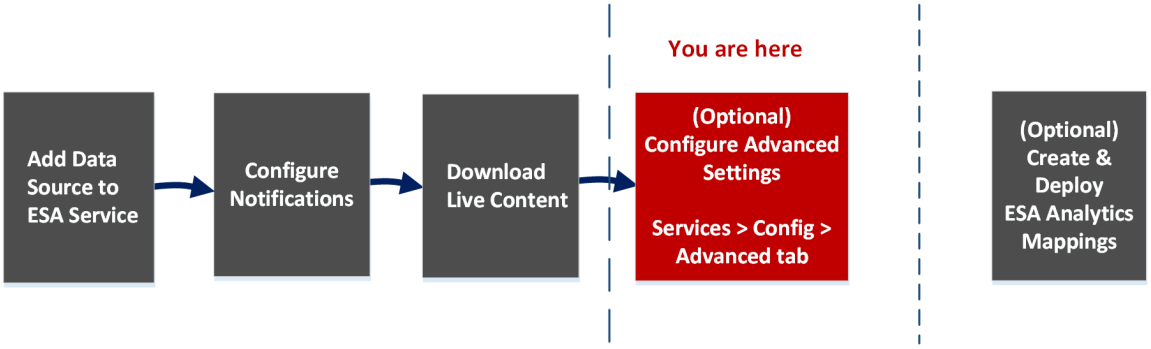
Colonne	Description
Nom	Nom du service de source de données.
Adresse	Adresse du service de source de données.
Port	Port utilisé par la source de données.
Utilisateur	Utilisateur connecté à la source de données.
Activé	Indique si la source de données est activée.
SSL	Indique si la communication SSL est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

Vue Configuration des services, onglet Avancé

L'onglet **vue Configuration des services > Avancé** d'un service ESA vous permet de configurer les paramètres avancés. 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 pour définir le nombre d'événements à stocker dans ESA.

Workflow

Ce workflow montre l'ensemble du processus de configuration d'ESA. Il indique également l'emplacement dans le processus de la configuration des paramètres avancés.



ESA comprend deux services, le service Event Stream Analysis (règles de corrélation ESA) et le service Event Stream Analytics Server (ESA Analytics). Les quatre premières procédures indiquées se rapportent à la configuration du service Event Stream Analysis :

- Ajouter une source de données à un service ESA
- Configurer les notifications
- Télécharger le contenu
- (Facultatif) Configurer les paramètres avancés

La dernière procédure se distingue des autres et s'applique à la création de mappages pour que les services ESA Analytics détectent automatiquement des menaces avancées :

- (Facultatif) Créer et déployer des mappages ESA Analytics

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Ajouter un Concentrator comme source de données au service Event Stream Analysis	Voir Configurer des règles de corrélation ESA et Étape 1. Ajouter une source de données à un service ESA
Administrateur	Configurer les notifications	Reportez-vous à la section « Méthodes de notification » dans le *Guide des alertes basées sur ESA*.
Administrateur	Télécharger le contenu	Reportez-vous à la section « Vue Live Search » dans le *Guide de gestion des ressources Live*.
Administrateur	Configurer les paramètres avancés *	Étape 2. Configurer des paramètres avancés pour un service ESA

*Vous pouvez effectuer ces tâches ici (c'est-à-dire sous l'onglet Avancé de la vue Configuration des Services).

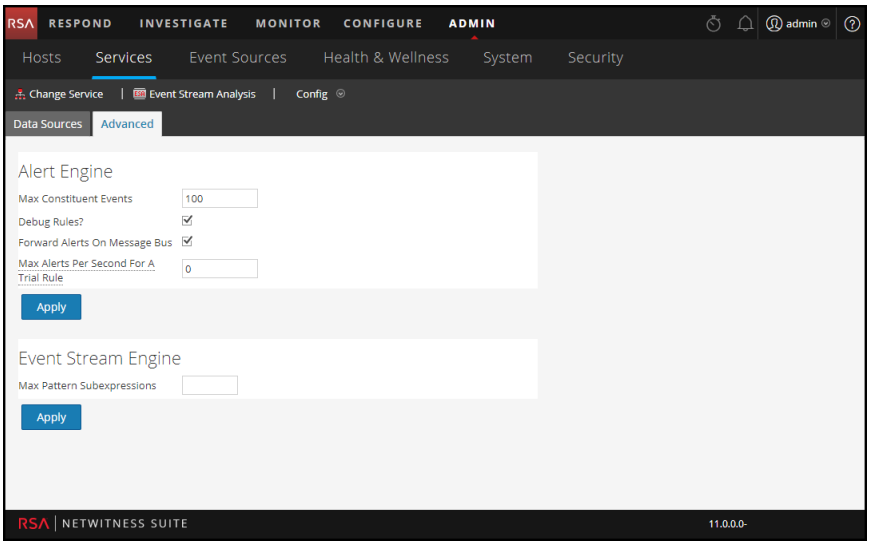
Rubriques connexes

- Consultez la section « Ajouter ou mettre à jour un hôte » dans le *Guide de mise en route de l'hôte et des services*

Aperçu rapide

Pour accéder à l'onglet Avancé, accédez à **ADMIN > Services >** (sélectionnez un service ESA) >  **> Vue > Config**.

La figure suivante illustre l'onglet Avancé de la vue Configuration des services d'un service ESA.



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.

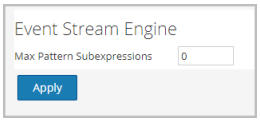
Le tableau suivant reprend les paramètres de la section Moteur d'alerte et leur description.

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**.
La sélection de l'option Déboguer les règles ?	active les règles de débogage.
Transférer les alertes vers le bus de messages	Pour transférer les alertes ESA à NetWitness Respond, vous devez sélectionner cette option. Les alertes ESA générées sont envoyées au bus de message, puis à Répondre. Cette option est sélectionnée par défaut. Vous pouvez vérifier si le service Serveur Respond est en cours d'exécution.

Paramètre	Description
Nombre maximal d'alertes par seconde pour une règle d'évaluation	Vous pouvez spécifier le nombre maximal d'alertes à transférer au bus de messages pour la règle d'évaluation. Par exemple, si la valeur est définie sur **50**, seules 50 alertes seront transmises au bus de messages pour la règle d'évaluation. Si la valeur est définie sur **0**, les alertes générées par la règle d'évaluation ne seront pas transférées vers le bus de messages. La valeur par défaut est **10**.

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.

Configuration du service de recherche Whois

Dans le panneau Configuration du service de recherche Whois (ADMIN > Système > Whois), vous pouvez configurer une connexion au service de recherche Whois pour vos modules ESA Analytics préconfigurés utilisés avec la fonctionnalité RSA de détection automatisée des menaces. Le service Whois vous permet d'obtenir des données précises sur les domaines auxquels vous vous connectez. Afin de garantir une évaluation efficace, il importe de configurer les paramètres du service Whois.

Vous devez disposer d'un compte RSA Live pour utiliser ce service.

Si vous avez configuré un compte Live dans le panneau Live Services (ADMIN > Système > Live Services), le service de recherche Whois est automatiquement configuré pour vous. Il vous suffit de vérifier la connexion du service de recherche Whois.

Remarque : Si vous ne disposez pas d'un compte RSA Live, vous pouvez en créer un via le portail d'inscription RSA Live :
https://cms.netwitness.com/registration/
Le *Guide de gestion des services Live* fournit des informations supplémentaires.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer le service de recherche Whois.	Configurer le service de recherche Whois
Administrateur	Vérifiez la connexion du service de recherche Whois.	Configurer le service de recherche Whois

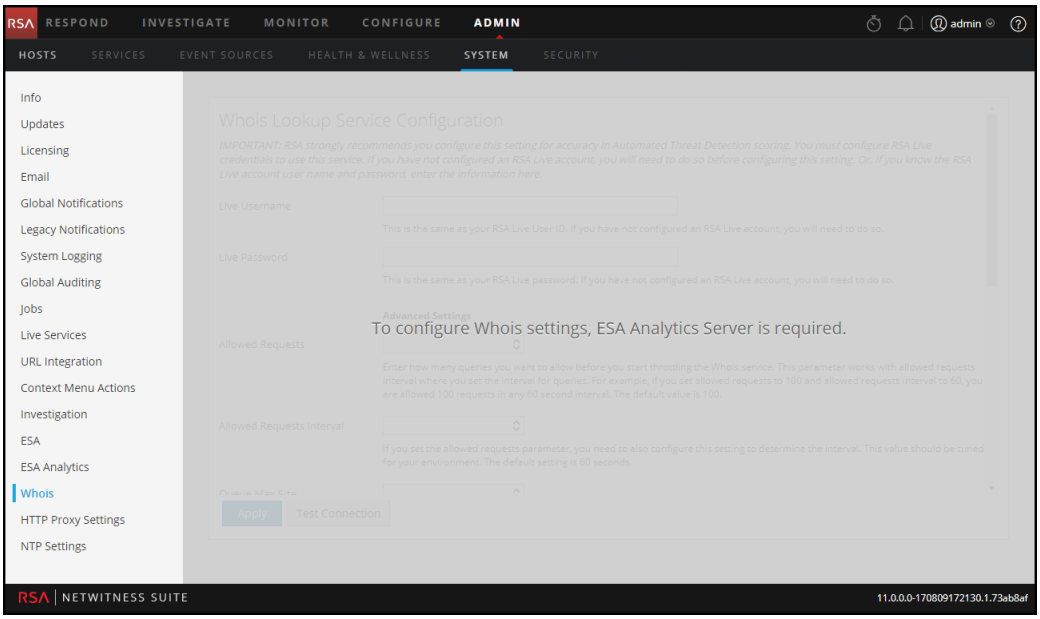
Rubriques connexes

- Mappages ESA Analytics

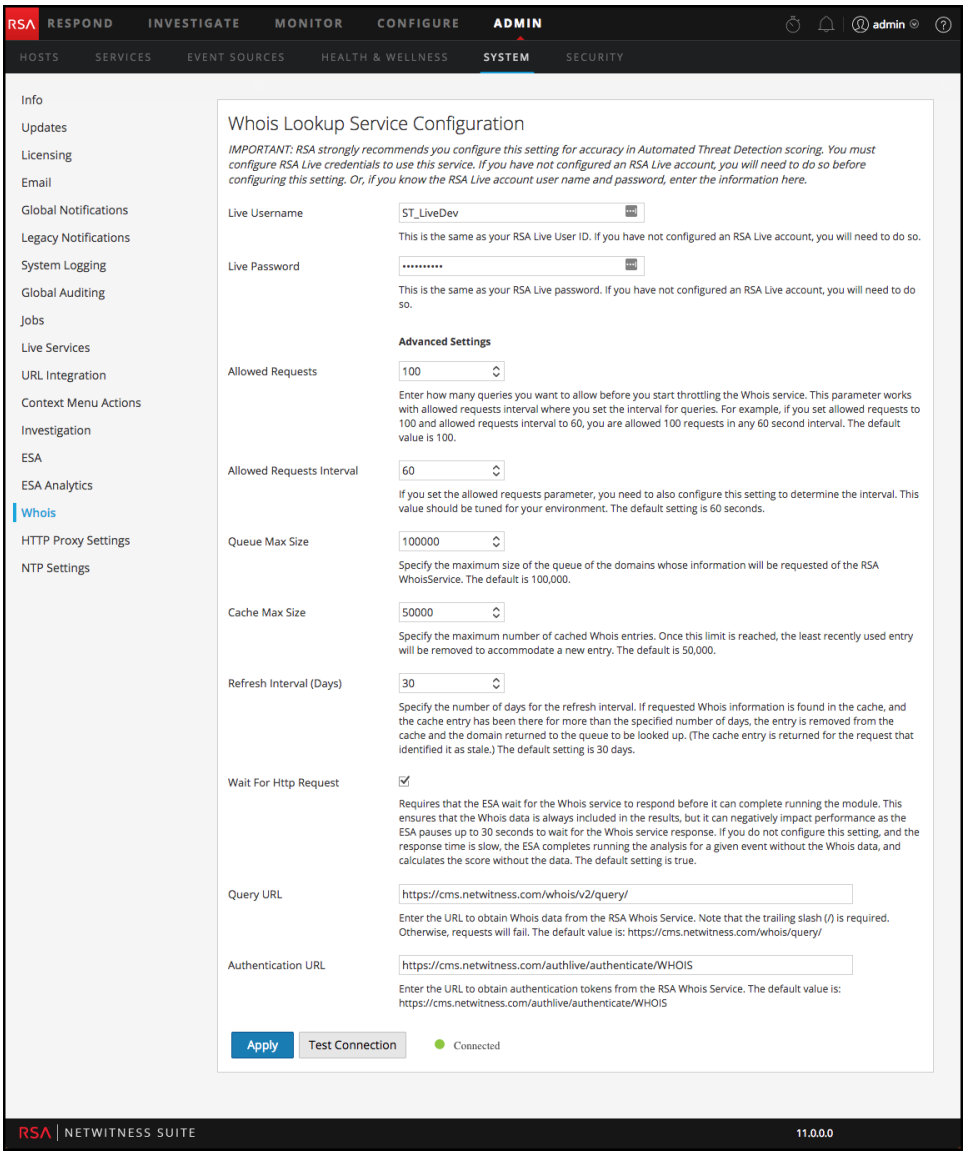
Configuration du service de recherche Whois

Pour accéder à la Configuration du service de recherche Whois, accédez à ADMIN > Système et, dans le panneau des options, sélectionnez Whois.

Le service ESA Analytics Server doit être disponible (affichant un cercle vert) dans la vue ADMIN > Services. Si vous ne disposez pas d'un service ESA Analytics Server disponible, le panneau suivant s'affiche.



Si vous disposez d'un service ESA Analytics Server disponible, le panneau suivant s'affiche.



Le tableau suivant décrit les paramètres de Configuration du service de recherche Whois.

Paramètre	Description
Nom d'utilisateur Live	**Obligatoire uniquement si vous n'avez pas déjà configuré le service de recherche Whois.** Indiquez les informations d'authentification du serveur RSA Whois. Elles correspondent à votre ID d'utilisateur Live RSA. Si vous n'avez pas configuré de compte Live RSA, vous devez le faire. La valeur par défaut est « whois ».

Paramètre	Description
Mot de passe Live	**Obligatoire uniquement si vous avez déjà configuré le service de recherche Whois.** Indiquez les informations d'authentification du serveur RSA Whois. Elles correspondent à votre mot de passe Live RSA. Si vous n'avez pas configuré de compte Live RSA, vous devez le faire. La valeur par défaut est null.
Demandes autorisées	(Facultatif) Indiquez le nombre de requêtes à autoriser avant de commencer à réguler le service Whois. Ce paramètre s'utilise avec l'**Intervalle de demandes autorisé** (en secondes), pour lequel vous définissez l'intervalle entre les requêtes. Par exemple, si vous définissez **Demandes autorisées** sur 100 et **Intervalle de demandes autorisé** sur 60, vous êtes autorisé à effectuer 100 demandes dans un intervalle de 60 secondes. La valeur par défaut est 100.
Intervalle de demandes autorisé	(Facultatif) Si vous définissez le paramètre **Demandes autorisées**, vous devez aussi configurer ce paramètre pour déterminer l'intervalle. Cette valeur doit être optimisée pour votre environnement. La valeur par défaut est égale à 60 secondes.
Taille max. file d'attente	(Facultatif) Spécifiez la taille maximale de la file d'attente des domaines. Cette information sera demandée au service RSA Whois. La valeur par défaut est 100 000.
Taille max. cache	(Facultatif) Spécifiez le nombre maximal d'entrées Whois mises en cache. Une fois cette limite atteinte, la dernière entrée utilisée sera supprimée afin d'accepter une nouvelle entrée. La valeur par défaut est 50 000.
Intervalle d'actualisation (jours)	(Facultatif) Spécifiez le nombre de secondes correspondant à l'intervalle d'actualisation. Si les informations Whois demandées sont détectées et que l'entrée en cache est présente depuis un plus grand nombre de jours que le nombre de jours spécifié, celle-ci est supprimée du cache et le domaine retourne dans la file d'attente afin d'être recherché. (L'entrée en cache est renvoyée pour la demande qui l'a identifiée comme périmée.) Paramètre par défaut : 30 jours.

Paramètre	Description
Attendre la demande HTTP	(Facultatif) Indiquez au service ESA d'attendre que le service Whois réponde avant d'exécuter le module. Cela garantit que les données Whois sont toujours incluses dans les résultats, mais peut avoir un effet négatif sur les performances étant donné que le serveur ESA s'interrompt jusqu'à 30 secondes en attendant la réponse du service Whois. Si vous ne configurez pas ce paramètre et que le temps de réponse est trop lent, le serveur ESA termine l'exécution de l'analyse pour un événement donné sans les données Whois et calcule l'indice sans les données. Le paramètre par défaut est **true**.
URL de requête	(Facultatif) Indiquez l'URL nécessaire pour obtenir les données Whois du service RSA Whois. Notez que la barre oblique ('/') de fin est obligatoire. Sinon, les demandes échouent. La valeur par défaut est : **https://cms.netwitness.com/whois/v2/query/**
URL d'authentification	(Facultatif) Indiquez l'URL nécessaire pour obtenir les tokens d'authentification du service RSA Whois. La valeur par défaut est : **https://cms.netwitness.com/authlive/authenticate/WHOIS**

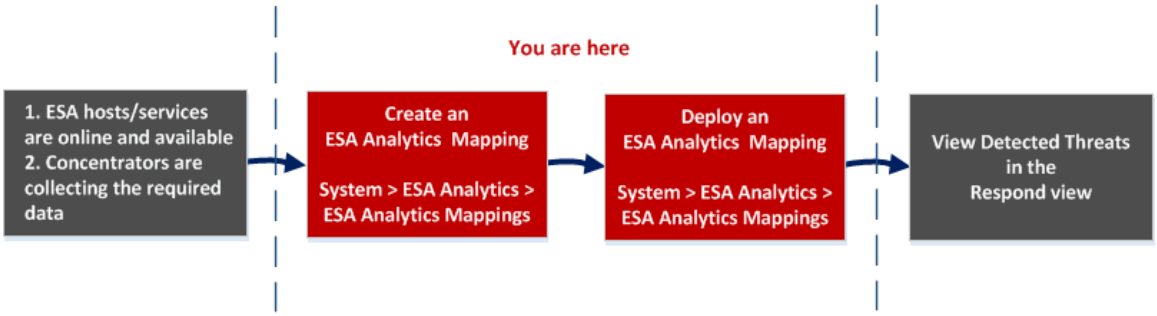
Mappages ESA Analytics

Dans le panneau Mappages ESA Analytics (ADMIN > Système > ESA Analytics), vous définissez la façon dont la fonctionnalité RSA de détection automatisée des menaces doit détecter automatiquement les menaces avancées. Vous pouvez analyser les données qui résident sur un ou plusieurs Concentrators en sélectionnant un module ESA Analytics préconfiguré.

Pour mieux utiliser vos ressources réseau et réduire le flux de données inutile, vous pouvez mapper plusieurs sources de données (telles que des Concentrators) aux services ESA Analytics disponibles afin de traiter les données plus efficacement et de tirer parti de capacités supplémentaires.

Workflow

Ce workflow montre le processus de création et d'activation d'un mappage ESA Analytics pour une détection automatique des menaces avancées.



Avant de créer un mappage ESA Analytics, assurez-vous que les hôtes et services ESA que vous souhaitez utiliser pour vos mappages sont en ligne et disponibles. Tous les services doivent être synchronisés avec une source de temps cohérente. Assurez-vous également que les Concentrators collectent les données nécessaires. Lorsque vous créez un mappage ESA Analytics, sélectionnez le module ESA Analytics à mapper, par exemple, Domaines suspects. Ensuite, sélectionnez les sources de données, telles que les Concentrators, à utiliser pour ce module, ainsi qu'un service ESA Analytics pour traiter les données. Lorsque vous êtes prêt à démarrer l'agrégation des données, déployez le mappage. Les analystes peuvent afficher les menaces détectées pour ce module dans la vue Répondre.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Vérifiez que les hôtes et services ESA sont en ligne et disponibles.	ADMIN > HÔTES et ADMIN > SERVICES Consultez le *Guide de mise en route des hôtes et des services*.
Administrateur	Assurez-vous que les Concentrators collectent les données nécessaires.	Consultez le *Guide de configuration de Broker et Concentrator*
Administrateur	Créer des mappages ESA Analytics*	Mappage des sources de données ESA aux modules Analytics
Administrateur	Déployer des mappages ESA Analytics*	Mappage des sources de données ESA aux modules Analytics
Administrateur, analyste	Afficher les menaces détectées	Consultez le *Guide d'utilisation de NetWitness Respond*.

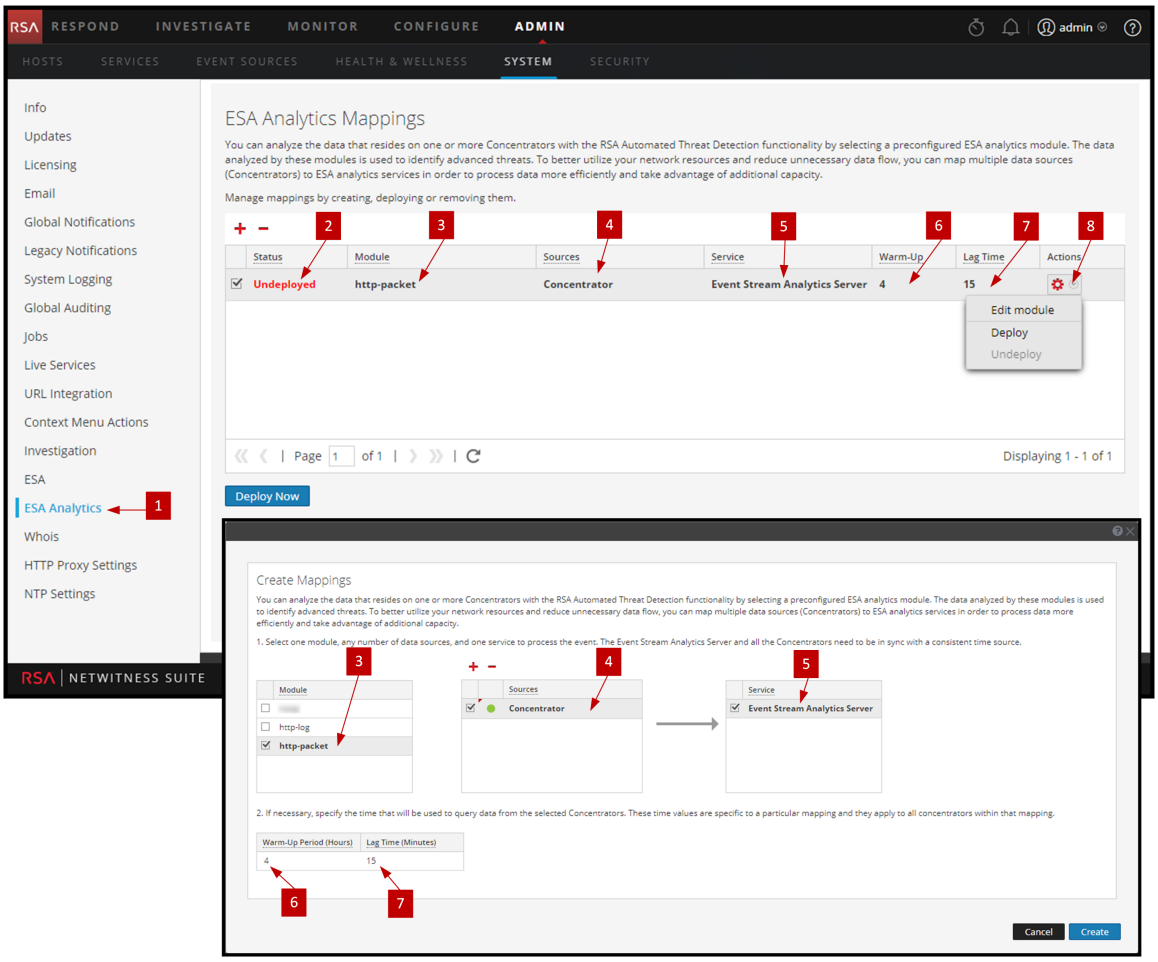
*Vous pouvez effectuer ces tâches ici (c'est-à-dire dans le panneau mappages ESA Analytics).

Rubriques connexes

- Configurer ESA Analytics
- Mettre à jour un mappage
- Annuler le déploiement d'un mappage
- Supprimer un mappage
- Modifier la période d'initialisation et le temps de latence
- Paramètres du module

Aperçu rapide

L'exemple suivant illustre un mappage ESA Analytics. La configuration définit les sources de données du module sélectionné et le service ESA Analytics qui traitera les événements à partir de ces sources de données.



1	Affiche le panneau Mappages ESA Analytics.
2	Affiche l'état du mappages ESA Analytics.
3	Nom du module mappé.
4	Sources de données, telles que les Concentrators, attribuées au mappage.
5	Service ESA Analytics qui traite les données pour le mappage.
6	Configuration de la période d'initialisation (en heures) sur les sources de données pour le mappage.
7	Configuration du temps de latence (en minutes) sur les sources de données pour le mappage.
8	Actions permettant de modifier les paramètres et les mappages de module et d'annuler le déploiement des mappages de module.

Barre d'outils

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

Icône/bouton	Description
	Ouvre la boîte de dialogue Créer des mappages dans laquelle vous pouvez créer un mappage ESA Analytics. Créez un mappage distinct pour chaque module. Après avoir créé et consulté les mappages, vous pouvez les déployer.
	Supprime un mappage ESA Analytics. • Vous pouvez supprimer un mappage dont l'état est Non déployé à tout moment. Étant donné qu'un mappage à l'état Non déployé n'est ni déployé, ni en cours d'exécution, il n'affecte pas l'agrégation des données. • La suppression d'un mappage déployé efface sa configuration sur le serveur ESA, annule le déploiement de ce mappage et arrête l'extraction des données à partir de la source de données pour ce module. Vous devez annuler le déploiement d'un mappage dont l'état est Non déployé avant de le supprimer.
Déployer maintenant	Une fois que vous avez créé vos mappages, vous devez les déployer afin de lancer l'agrégation des données pour les modules. Vous pouvez sélectionner un ou plusieurs mappages dont l'état est Non déployé pour les déployer.

Remarque : Si vous souhaitez apporter des modifications à un mappage déployé, par exemple en ajoutant ou en supprimant des Concentrators ou en modifiant le service, vous devez annuler le déploiement et supprimer le mappage existant, puis créer et déployer un nouveau mappage pour ce module.

Mappages ESA Analytics

Le tableau suivant décrit les mappages ESA Analytics répertoriés.

Titre	Description
	Pour sélectionner un mappage individuel, cochez la case située en regard du mappage.

Titre	Description
État	Affiche l'état du mappage. Il existe deux états : **Non déployé** - Un mappage non déployé mappe un module ESA Analytics aux sources et à un service ESA Analytics. Il ne démarre pas l'agrégation des données pour le module tant que le mappage n'est pas déployé. **Déployé** - Un mappage déployé est déployé et en cours d'exécution. Dans un mappage déployé, le service ESA Analytics sélectionné utilise l'agrégation basée sur une requête pour collecter les événements filtrés appropriés pour le module sélectionné à partir des Concentrators.
Module	Indique le module ESA Analytics sélectionné. Un module ESA Analytics est un pipeline composé d'objets d'activité qui enrichissent un événement avec des informations supplémentaires via des calculs mathématiques. Le module réside dans les services ESA Analytics.
Sources	Les sources sont des sources de données (par exemple, des Concentrators) à partir desquelles ESA va agréger les données du module spécifié.
Service	Indique le service ESA Analytics qui traite les données du module spécifié. Le service sélectionné doit être synchronisé avec une source de temps cohérente.
Période d'initialisation (Heures)	Spécifie une durée d'initialisation (en heures). Une période d'initialisation est nécessaire pour permettre à la détection automatisée des menaces d'en savoir plus sur votre trafic. La période d'initialisation doit s'exécuter lorsqu'un trafic classique est en cours d'exécution. Pendant ce temps, l'alerte relative au mappage de module est supprimée. La période d'initialisation amorce le module avec les données historiques et garantit que le nombre spécifié d'heures de collecte de données est atteint avant l'envoi d'alertes. RSA fournit des modules ESA Analytics préconfigurés. Chaque type de module dispose d'une période d'initialisation définie par défaut, que vous pouvez ajuster à votre environnement, si nécessaire. Au terme de cette période d'initialisation, les alertes peuvent être affichées. Pour plus d'informations relatives à la période d'initialisation et au temps de latence, reportez-vous à la section Paramètres du module.

Titre	Description
Temps de latence (Minutes)	Spécifie un délai constant, en minutes, qui est ajouté pour éviter de perdre des événements en cours de traitement par les sources de données pendant les périodes d'activité intense. Par exemple, les performances du Concentrator varient en fonction de facteurs tels que la charge entrante, les requêtes en continu et l'indexation. En raison de ces facteurs, un Concentrator peut ne pas agréger les événements en temps réel, ce qui entraîne un retard. Le paramètre de latence donne au service Concentrator une chance de terminer l'agrégation de toutes les données. Une fois la période d'initialisation terminée, l'agrégation des données se poursuit à l'**Heure actuelle (système) - Temps de latence**. Cela est utile lorsqu'un Concentrator tarde à agréger les données. Le temps de latence garantit que le module ne traite pas les données qui parviennent au Concentrator pendant la période de latence, et un retard suffisant assure que tous les événements générés dans l'entreprise peuvent être traités par le module. Par exemple, si le temps de latence est de 30 minutes et que l'heure actuelle est 14h00, le Concentrator commencera à extraire les enregistrements à 13h30. La période de latence, 30 minutes dans cet exemple, reste constante. Lorsque l'heure actuelle passe à 14h01, le Concentrator extrait la minute de données suivante à 13h31, et ainsi de suite. **Important :** Le temps de latence définit le décalage entre l'heure actuelle et l'heure à laquelle le module réceptionne les données. **Attention :** RSA recommande aux administrateurs d'ajuster le paramètre de latence dynamiquement en fonction des performances de chaque Concentrator pour éviter de manquer des événements lors de l'agrégation. Pour plus d'informations relatives à la période d'initialisation et au temps de latence, reportez-vous à la section Paramètres du module.

Titre	Description
	Vous permet de sélectionner des actions supplémentaires pour le mappage de module sélectionné : • **Modifier le module** - Permet de configurer la période d'initialisation et le temps de latence pour le mappage de module sélectionné. • **Déployer** - Déploie le mappage de module sélectionné. Le service ESA Analytics spécifié commence à extraire les données issues des sources de données de ce module. • **Annuler le déploiement** - Annule le déploiement du mappage de module sélectionné. Le service ESA Analytics spécifié arrête d'extraire les données issues des sources de données de ce module. **Attention :** L'annulation du déploiement d'un mappage dont l'état est Déployé a une incidence sur l'agrégation des données de ce module.

Paramètres du module

Une fois que vous avez créé ou déployé un mappage de module dans le panneau Mappages ESA Analytics (ADMIN > Système > ESA Analytics), vous avez la possibilité de modifier certaines configurations de module pour ce mappage.

Que voulez-vous faire ?

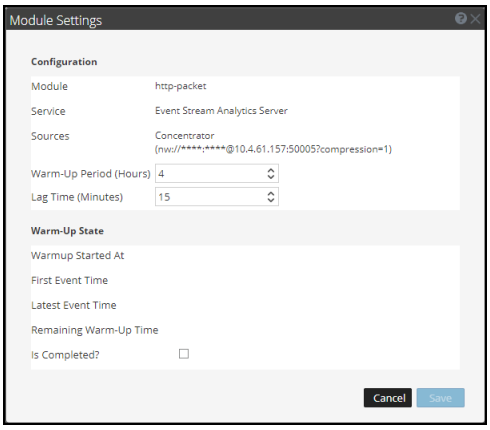
Rôle	Je souhaite...	Me montrer comment
Administrateur	Modifier la période d'initialisation d'un mappage de module non déployé.	Modifier la période d'initialisation et le temps de latence
Administrateur	Modifier la période d'initialisation pour un mappage de module au cours de la période d'initialisation.	Modifier la période d'initialisation et le temps de latence
Administrateur	Modifier la période d'initialisation pour un mappage de module après la période d'initialisation.	Modifier la période d'initialisation et le temps de latence

Rubriques connexes

- Mappage des sources de données ESA aux modules Analytics
- Mappages ESA Analytics

Paramètres du module

Pour accéder aux paramètres du module, dans le panneau Mappages ESA Analytics, sélectionnez le mappage que vous souhaitez modifier puis, dans la colonne **Actions**, sélectionnez  > **Modifier le module**. La boîte de dialogue Paramètres du module comporte la section Configurations et la section État de l'initialisation.



Configurations

La section Configurations vous permet de modifier les configurations de la période d'initialisation et du temps de latence.

Le tableau suivant décrit les paramètres disponibles pour un mappage de module d'analytique d'ESA.

Champ	Description
Module	Nom du module mappé.
Service	Affiche le service ESA Analytics qui traite les données pour le mappage.
Sources	Affiche les sources de données mappées et les URL permettant de communiquer avec ESA.

Champ	Description
Période d'initialisation (Heures)	Spécifie une durée d'initialisation (en heures). Une période d'initialisation est nécessaire pour permettre à la détection automatisée des menaces d'en savoir plus sur votre trafic. La période d'initialisation doit s'exécuter lorsqu'un trafic classique est en cours d'exécution. Pendant ce temps, l'alerte relative au mappage de module est supprimée. La période d'initialisation amorce le module avec les données historiques et garantit que le nombre spécifié d'heures de collecte de données est atteint avant l'envoi d'alertes. RSA fournit des modules ESA Analytics préconfigurés. Chaque type de module dispose d'une période d'initialisation définie par défaut, que vous pouvez ajuster à votre environnement, si nécessaire. Après cette période d'initialisation, les alertes peuvent être affichées. Vous pouvez mettre à jour la période d'initialisation d'un mappage de module déployé selon que la période d'initialisation est terminée ou non : • **Pendant la période d'initialisation** - Vous pouvez ajouter des heures à la période d'initialisation ou soustraire un temps d'initialisation. • **Après la période d'initialisation** - Vous pouvez ajouter des heures à la période d'initialisation en ajoutant la différence entre l'heure actuelle et l'heure du premier événement aux heures que vous souhaitez ajouter. Par exemple, une période d'initialisation de 10 heures est terminée et l'heure du premier événement est 12:00:00. L'heure actuelle (système) est 16:00:00 (4 heures plus tard) et vous souhaitez ajouter 5 heures à la période d'initialisation. Pour ce faire, vous devez ajouter 9 heures (4+5=9) à la période d'initialisation de 10, donc vous devez définir une nouvelle période d'initialisation de 19 heures. Vous ne pouvez pas réduire la période d'initialisation si elle est terminée, sauf si vous supprimez le mappage et que vous en créez un nouveau. La valeur de la période d'initialisation est spécifique à un mappage en particulier, et elle s'applique à tous les Concentrators au sein de ce mappage une fois qu'il est déployé. Si un Concentrator est partagé entre deux modules associés à des périodes d'initialisation différentes, le Concentrator utilise des valeurs de période d'initialisation distinctes pour chaque mappage de module.

Champ	Description
Temps de latence (Minutes)	Spécifie un délai constant, en minutes, qui est ajouté pour éviter de perdre des événements en cours de traitement par les sources de données pendant les périodes d'activité intense. Par exemple, les performances du Concentrator varient en fonction de facteurs tels que la charge entrante, les requêtes en continu et l'indexation. En raison de ces facteurs, un Concentrator peut ne pas agréger les événements en temps réel, ce qui entraîne un retard. Le paramètre de latence donne au service Concentrator une chance de terminer l'agrégation de toutes les données. Lorsque vous spécifiez un temps de latence, la première fois que le module est déployé, l'agrégation des données débute à l'**Heure actuelle (système) - Temps de latence**. Par exemple, si l'heure actuelle indique 14h00, le temps de latence 30 minutes et la période d'initialisation 4 heures, lorsque le module est déployé pour la première fois, la collecte des données commence à 9h30 (14h00 - 0,5 heure - 4 heures). Une fois la période d'initialisation terminée, l'agrégation des données se poursuit à l'**Heure actuelle (système) - Temps de latence**. Cela est utile lorsqu'un Concentrator tarde à agréger les données. Le temps de latence garantit que le module ne traite pas les données qui arrivent au Concentrator pendant la période de latence, et un retard suffisant assure que tous les événements générés dans l'entreprise peuvent être traités par le module. Par exemple, si le temps de latence est de 30 minutes et que l'heure actuelle est 14h00, le Concentrator commencera à extraire les enregistrements à 13h30. La période de latence, 30 minutes dans cet exemple, reste constante. Lorsque l'heure actuelle passe à 14h01, le Concentrator extrait la minute de données suivante à 13h31, et ainsi de suite. **Important** : Le temps de latence définit le décalage entre l'heure actuelle et l'heure à laquelle le module réceptionne les données. La valeur du temps de latence est spécifique à un mappage en particulier, et elle s'applique à tous les Concentrators au sein de ce mappage une fois qu'il est déployé. Si un Concentrator est partagé entre deux modules associés à des temps de latence différents, le Concentrator utilise des valeurs de latence distinctes pour chaque mappage de module. **Attention :** RSA recommande aux administrateurs d'ajuster le paramètre de latence dynamiquement en fonction des performances de chaque Concentrator pour éviter de manquer des événements lors de l'agrégation. Pour déterminer le temps de latence correct, additionnez les données suivantes pour obtenir un temps de latence environnemental : 1. **Latence de log ou de paquet** - Temps nécessaire au Log Decoder pour recevoir les logs ou au Decoder (Paquet) pour recevoir des paquets. Par

Champ	Description
	exemple, le Log Decoder peut recevoir les logs toutes les 20 minutes. Dans ce cas, vous pouvez définir des temps de latence d'au moins 20 minutes, de préférence 25 minutes, afin de ne manquer aucun événement. 2. **Latence d'agrégation** - Temps nécessaire pour récupérer les données à partir du Log Decoder pour le Concentrator. 3. **Autre tampon** - Ajoutez tout autre délai supplémentaire spécifique à votre environnement.

État de l'initialisation

Cette section fournit des informations sur l'état de l'initialisation qui vous permettent de déterminer les ajustements nécessaires à la période d'initialisation.

Champ	Description
Initialisation démarrée à	Heure à laquelle le premier événement a été traité par le module ESA Analytics à partir de la source de données.
Heure du premier événement	Heure à laquelle le premier événement s'est produit. La période d'initialisation est basée sur cette heure.
Heure du dernier événement	Heure à laquelle le dernier événement s'est produit.
Temps d'initialisation restant	Nombre d'heures restantes dans la période d'initialisation.
Terminé ?	Indique si la période d'initialisation est terminée. Si c'est le cas, la période d'initialisation est terminée. Si ce n'est pas le cas, le module est toujours en cours d'initialisation et vous pouvez afficher le nombre d'heures restantes dans le champ Temps d'initialisation restant.