RSA NETWITNESS® SUITE

Guide d'intégration de RSA NetWitness Endpoint

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.

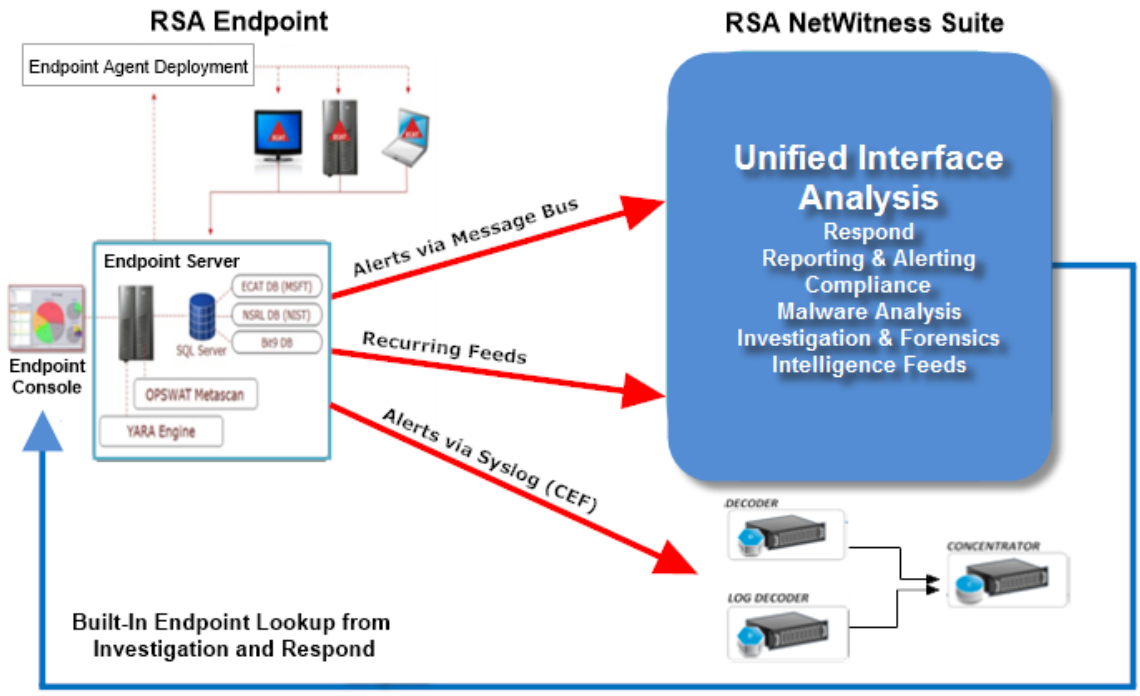
février 2018

Sommaire

Intégration du point de terminaison RSA NetWitness

Les clients RSA qui utilisent RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4 peuvent intégrer NetWitness Endpoint et RSA NetWitness Suite de différentes manières. Ce guide est pour RSA NetWitness Suite version 11.0.

Options d'intégration



Recherche du point de terminaison NetWitness intégrée

Avec l'interface utilisateur RSA NetWitness Endpoint installée sur la même machine que le navigateur utilisé par l'analyste pour accéder à NetWitness Suite, la recherche NetWitness Endpoint intégrée à partir de NetWitness Suite Investigation et NetWitness Suite Répondre fournit un accès par clic droit au serveur de la console NetWitness Endpoint pour les clés méta suivantes : adresse IP (ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip), host (alias-host, domain.dst), client et file-hash. Elles sont décrites dans la rubrique « Lancer la recherche externe d'une clé méta » dans le *Guide Investigation et Malware Analysis* et dans la rubrique « Afficher les alertes » dans le *Guide de l'utilisateur NetWitness Respond.*

La configuration de NetWitness Suite n'est pas requise pour la recherche du point de terminaison lorsque vous utilisez l'un des parsers intégrés, NetWitness Endpoint ou CEF, et que vous n'avez pas personnalisé les clés méta par défaut utilisées lors du chargement des métadonnées dans Investigation. Pour plus d'informations, consultez la rubrique « Gérer et appliquer des clés méta par défaut dans une investigation » dans le *Guide d'utilisation Investigation et Malware Analysis*.

Remarque : Une exception se produit si vous personnalisez NetWitness Suite en modifiant le paramètre d'affichage pour les clés méta par défaut dans Investigation, si vous ajoutez les clés méta au fichier table-map-custom.xml, ou si vous personnalisez les flux NetWitness Endpoint. Un certain degré de configuration est nécessaire pour ajouter les clés méta personnalisées au menu contextuel Recherche NetWitness Endpoint dans la vue **ADMIN** > **Système**, comme décrit dans la rubrique « Actions du menu Ajouter un contexte personnalisé » dans le *Guide de configuration système*.

Méthodes d'intégration

Avec un RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou un serveur de console 4.4 installé sur un hôte Windows et la configuration correcte de NetWitness Endpoint et de NetWitness Suite par un administrateur, trois autres intégrations des données d'analyse NetWitness Endpoint sont possibles.

Voici les méthodes d'intégration RSA NetWitness Endpoint :

- Configurer des alertes de point de terminaison via les bus de messages
- Configurer des données contextuelles à partir du point de terminaison via un flux récurrent
- Configurer des alertes de point de terminaison via Syslog dans un Log Decoder

Alertes de point de terminaison via le bus de messages dans NetWitness Respond. Cette intégration offre la possibilité de transférer les alertes de point de terminaison vers Répondre via le bus de messages.

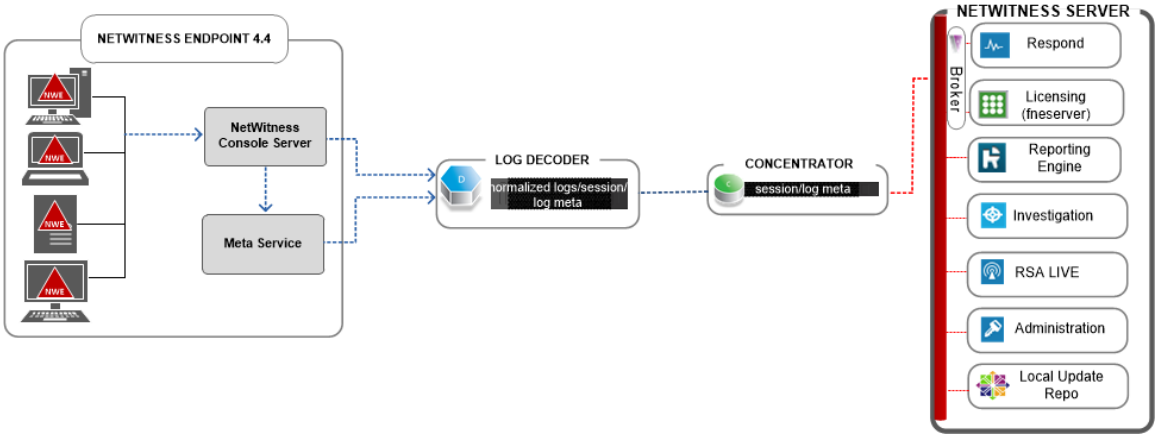
Données contextuelles depuis le point de terminaison via un flux récurrent NetWitness Suite Live. Cette intégration peut enrichir la session affichée dans NetWitness Suite Investigation avec des informations contextuelles ; par exemple, le système d'exploitation hôte, l'adresse MAC, le score IIOC et d'autres données qui peuvent ne pas être présents dans les données du log ou du paquet.

Alertes NetWitness Endpoint via Syslog (CEF) dans les Log Decoders NetWitness Suite. Cette intégration offre la possibilité de transférer les événements de point de terminaison via Syslog et de corréler les événements avec d'autres métadonnées de log ou paquets dans l'écosystème NetWitness Suite.

Intégration des métadonnées du point de terminaison NetWitness

L'intégration des métadonnées NetWitness Endpoint avec RSA NetWitness Suite offre aux clients qui ont les deux produits un moyen de tirer le meilleur parti de leurs produits dans une seule interface utilisateur. Le schéma suivant illustre comment le point de terminaison NetWitness s'intègre avec la NetWitness Suite. Les métadonnées du point de terminaison NetWitness sont collectées et publiées à partir de toutes les machines où les agents de point de terminaison NetWitness sont déployés et ensuite transmises au Log Decoder NetWitness Suite.

Les métadonnées peuvent ensuite être visualisées dans le Concentrator NetWitness Suite associé et également dans NetWitness Suite Investigate.



Indicateurs de compromission et alertes du point de terminaison NetWitness

Un indicateur de compromission instantané NetWitness Endpoint est une requête de base de données qui exécute NetWitness Endpoint sur des données d'analyse NetWitness Endpoint collectées pour déterminer la présence de logiciels malveillants potentiels sur des hôtes analysés. RSA NetWitness Endpoint version 4.1.2 et ultérieure est livré avec des indicateurs de compromission que l'utilisateur peut activer et marquer comme pouvant être alertés.
RSA NetWitness Endpoint exécute les requêtes des indicateurs de compromission régulièrement sur les nouvelles données d'analyse, qui sont collectées et stockées dans la base de données. Si la requête de l'indicateur de compromission est satisfaite, cela indique un indicateur potentiel de compromission, et l'événement peut être signalé à un utilisateur ou envoyé à un système externe comme une alerte.

Voici les types possibles d'alerte :

- Alerte de machine : Cette alerte indique que la machine en question est suspecte.
- Alerte de module : cette alerte indique qu'un module, tel qu'un fichier, une DLL ou un exécutable, est suspect. Elle contient des détails sur le module en question.
- Alerte d'événement : cette alerte représente toute autre activité suspecte détectée par NetWitness Endpoint qui n'entre pas dans les catégories énoncées ci-dessus.

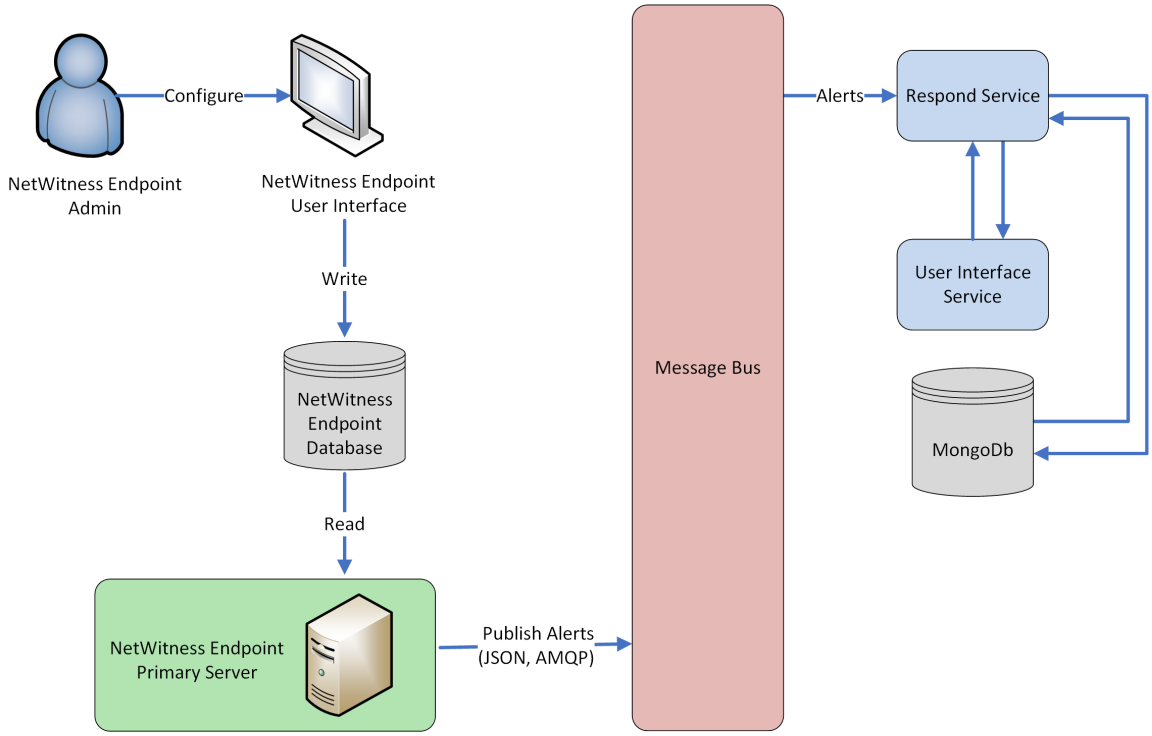
Chacun de ces types d'alerte peut être associé et envoyé à NetWitness Suite.

Configurer des alertes de point de terminaison NetWitness via le bus de messages

Cette procédure est requise pour intégrer NetWitness Endpoint avec NetWitness Suite de façon à ce que les alertes NetWitness Endpoint soient relevées par le composant Répondre de NetWitness Suite et affichées dans la vue **RÉPONDRE > Alertes**.

Remarque : RSA prend en charge NetWitness Endpoint versions 4.3.0.4, 4.3.0.5 ou 4.4 pour l'intégration de NetWitness Respond. Pour plus d'informations, consultez la rubrique « Intégration de RSA NetWitness Suite » dans le *Guide d'utilisation du point de terminaison NetWitness*.

Le diagramme ci-dessous représente le flux d'alertes NetWitness Endpoint de la liste des incidents Répondre de NetWitness Suite et il affiche la vue **RÉPONDRE > Alertes**.



Conditions préalables

Assurez-vous de disposer de ce qui suit :

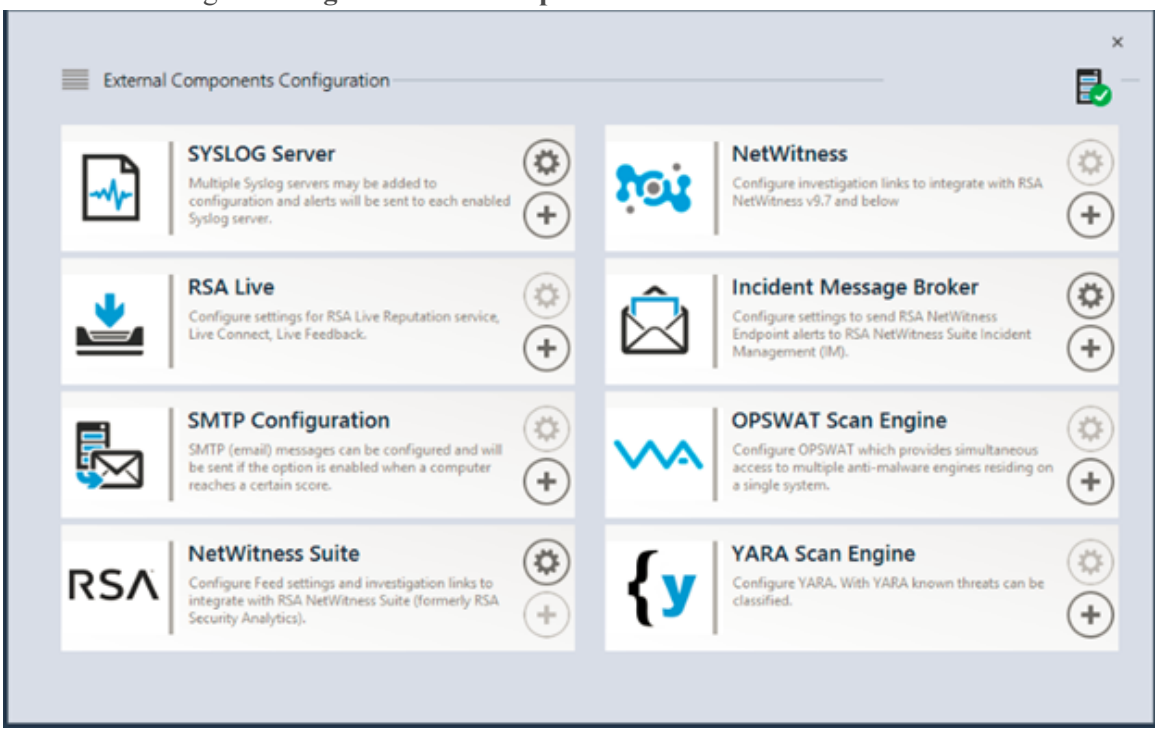
- Le service de réponse est installé et en cours d'exécution sur NetWitness Suite 11.0.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4 est installé et en cours d'exécution.

Configurer NetWitness Endpoint pour transférer des alertes NetWitness Endpoint

Pour configurer NetWitness Endpoint de manière à envoyer des alertes sur le bus de messages à l'interface utilisateur NetWitness Suite :

1. Dans l'interface utilisateur NetWitness Endpoint, cliquez sur **Configurer > Composants de surveillance et externes**.

   La boîte de dialogue **Configuration des composants** externes s'affiche.



   a. À partir des composants de la liste, sélectionnez **Incident Message Broker**, puis cliquez sur + pour ajouter un nouveau composant IM broker.

2. Saisissez des valeurs pour les champs suivants :

   a. **Nom de l'instance** : Saisissez un nom unique pour identifier le composant IM broker.

   b. **Nom d'hôte/adresse IP du serveur** : Saisissez le DNS de l'hôte ou l'adresse IP du composant IM Broker (Serveur NetWitness).

   c. **Numéro de port** : Le port par défaut est 5671.

3. Cliquez sur **Enregistrer**.

4. Accédez au fichier **ConsoleServer.exe.config** file dans **C:\Program Files\RSA\ECAT\Server**.
5. Modifiez les configurations d'hôte virtuel dans le fichier comme suit :
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Remarque : Dans NetWitness Suite 11.0, l'hôte virtuel est « / rsa/system ». Pour la version 10.6.x et précédente, l'hôte virtuel est « / rsa/sa ».
6. Redémarrez le serveur API et le serveur de console.
7. Pour configurer SSL pour les alertes de réponse, effectuez la procédure suivante sur le serveur de console primaire NetWitness Endpoint pour définir les communications SSL :
   a. Exportez le certificat de l'autorité de certification NetWitness Endpoint au format .CER (chaîne codée X.509 Base 64) du magasin de certificats personnel de l'ordinateur local (sans sélectionner la clé privée).
   b. Générez un certificat client pour NetWitness Endpoint à l'aide du certificat d'autorité de certification NetWitness Endpoint. (Vous devez définir le nom CN sur ecat).

      ```
      makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
      sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir
      LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
      cy end -sy 12 client.cer
      ```

      Remarque : Dans l'exemple de code ci-dessus, si vous avez effectué une mise à niveau vers la version 4.3 du point de terminaison à partir d'une version précédente et que vous n'avez pas généré de nouveaux certificats, vous devez remplacer « EcatCA » par « NweCA ».
   c. Notez l'empreinte du certificat client généré à l'étape b. Saisissez la valeur d'empreinte du certificat client dans la rubrique IMBrokerClientCertificateThumbprint du fichier ConsoleServer.Exe.Config comme indiqué.

      ```
      <add key="IMBrokerClientCertificateThumbprint"
      value="896df0efacf0c976d955d5300ba0073383c83abc"/>
      ```
8. Sur le Serveur NetWitness, copiez le fichier de certificat d'autorité de certification NetWitness Endpoint dans le format .CER dans le dossier d'importation :
   `/etc/pki/nw/trust/import`
9. Exécutez la commande suivante pour démarrer l'exécution de Chef nécessaire :
   `orchestration-cli-client --update-admin-node`
   Elle ajoute tous les certificats dans le magasin d'approbations.
10. Redémarrez le serveur RabbitMQ :
    `systemctl restart rabbitmq-server`
    Le compte NetWitness Endpoint doit être automatiquement disponible sur RabbitMQ.

11. Importez les fichiers `/etc/pki/nw/ca/nwca-cert.pem` et `/etc/pki/nw/ca/ssca-cert.pem` à partir de Serveur NetWitness et ajoutez-les dans les magasins de certificats racines de confiance sur le serveur de point de terminaison.

Résolution des problèmes

Cette rubrique suggère comment résoudre les problèmes que vous pouvez rencontrer lorsque vous configurez des alertes de point de terminaison NetWitness via le bus de messages.

Problèmes connus	Solutions
L'orchestration échoue sur un nœud d'administration.	Vous devez copier et coller le contenu du certificat EcatCA dans `/etc/rabbitmq/ssl/truststore.pem` et redémarrez le service Rabbitmq.

Configurer des données contextuelles à partir de NetWitness Endpoint via un feed récurrent

Vous pouvez configurer des données RSA NetWitness Endpoint dans RSA NetWitness Suite pour fournir des données contextuelles à partir de NetWitness Endpoint aux sessions Decoder et Log Decoder. Cette configuration ajoute des métavaleurs contextuelles en plus des alertes IOC instantanées qui permettent de créer des corrélations à d'autres métadonnées dans l'écosystème NetWitness Suite.

Les administrateurs peuvent configurer NetWitness Suite afin d'utiliser les données contextuelles d'analyse du système NetWitness Endpoint via un feed récurrent NetWitness Suite Live. Cette intégration peut enrichir la session d'un Decoder ou Log Decoder avec des informations contextuelles affichées dans NetWitness Suite Investigation. Certains exemples incluent le système d'exploitation hôte, l'adresse MAC, le score IIOC et d'autres données qui peuvent ne pas être présentes dans les données de logs ou de paquets pour les sessions d'un Decoder ou Log Decoder.

Remarque : Bien que cette fonctionnalité soit ciblée pour les clients avec un paquet Decoder, un flux récurrent peut également être mis en œuvre dans les Log Decoders.

Attention : Dans les environnements avec de nombreux hôtes NetWitness Endpoint, l'utilisation de ce feed récurrent peut entraîner une diminution des performances sur les périphériques d'acquisition NetWitness Suite (Decoder et Log Decoder).

Conditions préalables

- Serveur de console NetWitness Endpoint version 4.3.0.4, 4.3.0.5 ou 4.4 et Serveur NetWitness version 10.4 et supérieure installé.
- RSA Decoder et Concentrator version 11.0 ou supérieure connecté au Serveur NetWitness sur le réseau.

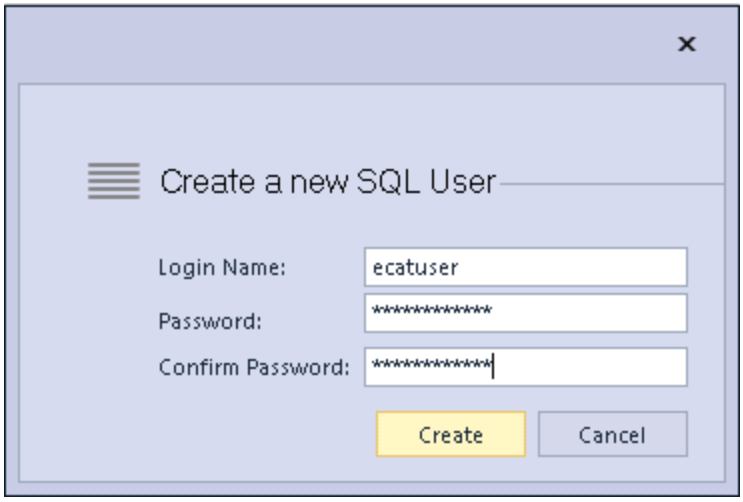
Pour configurer des données contextuelles à partir de NetWitness Endpoint via un feed récurrent, procédez comme suit :

1. Activez le feed NetWitness Endpoint pour NetWitness Suite dans l'interface utilisateur NetWitness Endpoint.
2. Exportez le certificat de l'autorité de certification NetWitness Endpoint du serveur de console NetWitness Endpoint et importez-le vers le magasin d'approbations NetWitness Suite.

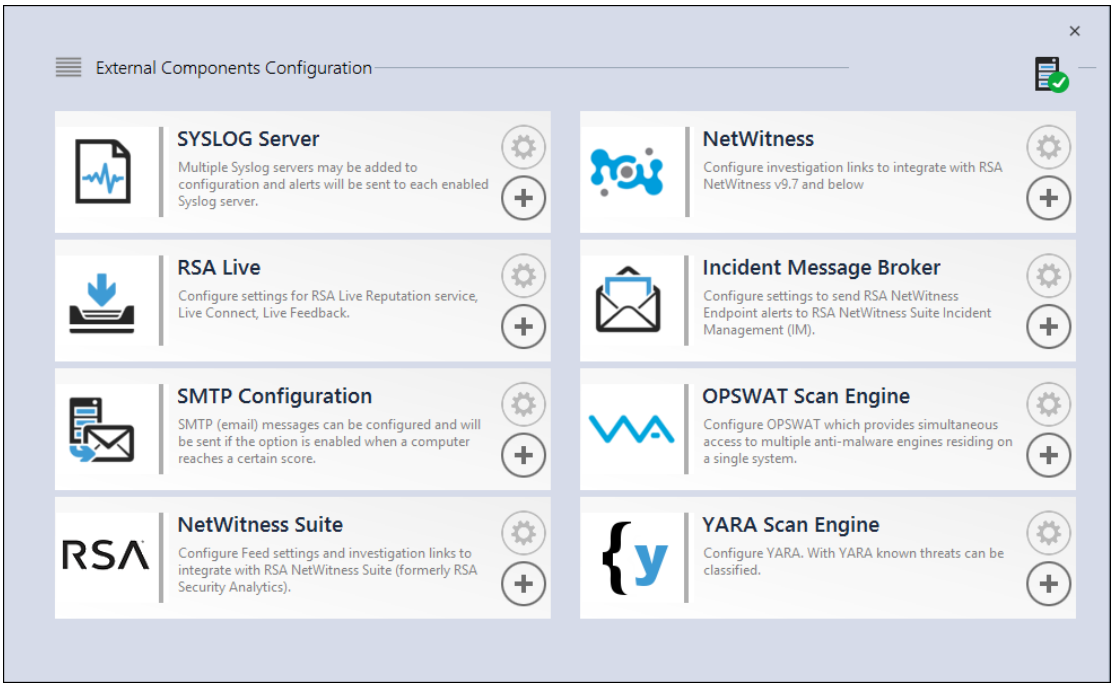
3. Configurez le service NetWitness Suite Concentrator pour définir les clés méta qui sont indexées.
4. Créez un feed récurrent dans NetWitness Suite Live.

Activer le feed NetWitness Endpoint pour NetWitness Suite

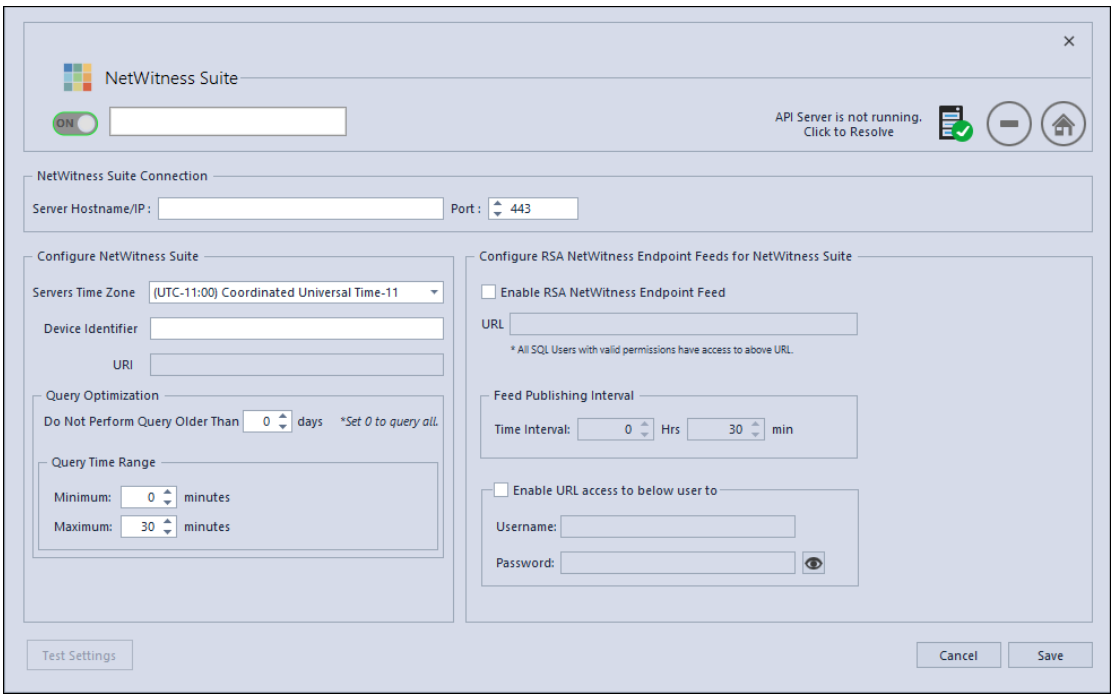
1. Dans l'interface utilisateur NetWitness Endpoint, créez un utilisateur SQL dans NetWitness Endpoint :
   a. Ouvrez l'interface utilisateur NetWitness Endpoint et connectez-vous en utilisant les informations d'identification adéquates.
   b. Dans la barre de menus, sélectionnez **Configure > Gestion des utilisateurs et rôles**, effectuez un clic droit dans le volet, puis sélectionnez **Créer un utilisateur SQL**.
   La boîte de dialogue Créer un nouvel utilisateur SQL s'affiche.



   c. Saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis cliquez sur **Créer**.
2. Dans la barre de menus, sélectionnez **Configurer > Composants de surveillance et externes**.
   .La boîte de dialogue Configuration des composants externes s'affiche.



3. Dans NetWitness Suite, cliquez sur +.
   La boîte de dialogue NetWitness Suite s'affiche.



4. Dans le panneau **NetWitness Suite**, sur **On**, entrez le nom pour identifier le composant NetWitness Suite.

5. Dans le panneau **Connexion à NetWitness Suite**, procédez comme suit.
   a. Dans le champ **Nom d'hôte/IP du serveur**, saisissez le nom d'hôte ou l'adresse IP du Serveur NetWitness.
   b. Dans le champ **Port**, saisissez le numéro de port. Le numéro de port par défaut est 443.
6. Dans le panneau **Configurer NetWitness Suite**, procédez comme suit :
   a. Dans le champ **Fuseau horaire des serveurs**, sélectionnez le fuseau horaire pour le composant dans la liste déroulante.
   b. Dans le champ **Identifiant de périphérique**, saisissez l'ID du périphérique du Concentrator NetWitness Suite.

   Remarque : Vous pouvez trouver l'identifiant du périphérique dans NetWitness Suite si vous chercher un Concentrator ou un Broker dans **Procédure d'enquête > Naviguer >***<Nom du Concentrator ou du Broker>*. L'identifiant du périphérique est le numéro figurant dans l'URL après « investigation ». Par exemple, dans l'URL `https://<IP address>investigation/319/navigate/values`, l'identifiant du périphérique est **319**.

   Le champ **URI** est renseigné lorsque vous cliquez sur **Enregistrer**.
7. Dans le panneau **Optimisation des requêtes**, dans le champ **Ne pas exécuter de requête pour une période supérieure à**, saisissez le nombre de jours auquel limiter la période de requête. Saisissez **0** pour ignorer cette fonctionnalité.
8. Dans le panneau **Période de requête**, procédez comme suit :
   a. Dans le champ **Minimum**, saisissez le nombre de minutes correspondant à la période de requête minimale. Cette valeur sert à augmenter automatiquement la période soumise à NetWitness Suite. Une requête retourne ainsi une réponse positive si l'heure signalée par l'agent NetWitness Endpoint diffère légèrement de celle de NetWitness Endpoint.
   b. Dans le champ **Maximum**, saisissez le nombre de minutes pour limiter la période. Cette valeur sert à limiter automatiquement la période soumise à NetWitness Suite afin que les requêtes ne surchargent pas le Serveur NetWitness.
9. Dans le panneau **Configurer les feeds RSA NetWitness Endpoint pour NetWitness Suite**, procédez comme suit :
   a. Sélectionnez **Activer le feed RSA NetWitness Endpoint**.
   b. Dans le champ **URL**, saisissez le **Nom d'utilisateur** et le **Mot de passe** SQL (configurés à l'étape 1) pour accéder à l'emplacement du feed.
   Le champ **URL** est renseigné lorsque vous cliquez sur **Enregistrer**.

c. Saisissez l'intervalle de temps correspondant à la fréquence à laquelle les feeds sont publiés.

10. Dans le panneau **Intervalle de publication des feeds**, dans le champ **Intervalle de temps**, sélectionnez l'intervalle de temps dans **h** et **min** pour la fréquence à laquelle les feeds sont publiés.
11. Dans le panneau **Activer l'accès URL pour l'utilisateur ci-dessous pour**, saisissez le **Nom d'utilisateur** et **Mot de passe** de l'utilisateur NetWitness Endpoint.
12. Cliquez sur **Enregistrer**.
    Un feed est créé.

Exporter le certificat SSL de NetWitness Endpoint

Remarque : Cette procédure ne fonctionne que pour NetWitness Suite 10.5 et version ultérieure, puisque la prise en charge de Java 8 a été ajoutée pour la version 10.5. Si vous utilisez une version antérieure de NetWitness Suite, reportez-vous à la version applicable de ce guide.

Pour exporter le certificat de l'autorité de certification NetWitness Endpoint à partir du serveur de console NetWitness Endpoint et le copier sur l'hôte NetWitness Suite :

1. Connectez-vous à la console NetWitness Endpoint.
2. Ouvrez **MMC**.
3. Ajoutez un composant logiciel enfichable de certificat pour le **compte d'ordinateur**.
4. Exportez le certificat nommé **`EcatCA`**.
   a. Effectuez l'exportation sans clé privée.
   b. Exportez au format binaire X.509 encodé DER (`.CER`).
   c. Nommez-le **`EcatCA.cer`**.
5. Copiez le certificat de l'autorité de certification NetWitness Endpoint vers l'hôte NetWitness Suite :
   - Pour une nouvelle installation de NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4 :
     `scp NweCA.cer root@<sa-machine>:.`
   - Pour des mises à niveau NetWitness Endpoint à partir d'une version précédente vers 4.3.0.4 ou 4.3.0.5 :
     `scp EcatCA.cer root@<sa-machine>:.`

6. Pour importer le certificat d'autorité de certification NetWitness Endpoint dans le magasin d'approbations NetWitness Suite, procédez comme suit :

   a. Vérifiez la version Java installée sur votre NetWitness Suite à l'aide de la commande suivante :
   `java -version`
   La version openjdk s'affiche. Par exemple, la version openjdk «`1.8.0_71`»

   b. Pour définir le paramètre JDK, accédez au répertoire java. Saisissez les commandes suivantes :

   - `JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/`
   - Pour une nouvelle installation NetWitness Endpoint:

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   - Pour une mise à niveau de NetWitness Endpoint à partir d'une version précédente :

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   Lorsque vous êtes invité à confirmer la mise à jour du certificat, **Yes** (oui).

7. Sur l'hôte NetWitness Suite, exécutez l'une des opérations suivantes :

   - Pour une nouvelle installation de NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4, modifiez **`/etc/hosts`** pour mapper l'adresse IP du serveur de console NetWitness Endpoint au nom **NweServerCertificate** en ajoutant la ligne suivante au fichier :

     ```
     <ip-address-ecat-cs> NweServerCertificate
     ```

   - Pour une mise à niveau de NetWitness Endpoint 4.3.0.4 ou 4.3.0.5 à partir d'une version précédente, modifiez **`/etc/hosts`** pour mapper l'adresse IP du serveur de console NetWitness Endpoint au nom **`ecatserverexported`** en ajoutant la ligne suivante au fichier :

     ```
     <ip-address-ecat-cs> ecatserverexported
     ```

8. Pour redémarrer NetWitness Suite, saisissez les commandes suivantes :

   ```
   service jetty restart
   ```

Configurer le service NetWitness Suite Concentrator

1. Connectez-vous à NetWitness Suite et accédez à **ADMIN > Services**.
2. Sélectionnez un Concentrateur dans la liste, puis sélectionnez **Vue > Config.**

3. Sélectionnez l'onglet **Fichiers**, et dans le menu déroulant **Fichiers à modifier**, sélectionnez **index-concentrator-custom.xml**.

4. Ajoutez les clés métas NetWitness Endpoint suivantes au fichier, puis cliquez sur **Appliquer**. Vérifiez que ce fichier contient déjà les sections XML et si ce n'est pas le cas, ajoutez-les. Les lignes suivantes sont des exemples ; assurez-vous que les valeurs correspondent à votre configuration et les noms de colonne que vous avez inclus dans la définition du feed, où :
   description est le nom de la clé méta que vous souhaitez afficher dans la procédure d'enquête NetWitness Suite.
   niveau est « IndexValues ».
   nom correspond au nom de colonne du fichier CSV que NetWitness Suite utilise lors de la définition du feed récurrent (reportez-vous au tableau de *Configurer la tâche de feed personnalisée récurrente dans NetWitness Suite* ci-dessous).

   ```
   <key description="Gateway" format="Text" level="IndexValues"
   name="gateway" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Risk Number" format="Float64" level="IndexValues"
   name="risk.num" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Strans Addr" format="Text" level="IndexValues"
   name="stransaddr" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Domain" format="Text" level="IndexValues"
   name="domain" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="User Account" format="Text" level="IndexValues"
   name="username" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Ecat Connectiontime" format="Text"
   level="IndexValues" name="ecat.ctime" valueMax="250000"
   defaultAction="Open"/>
   ```

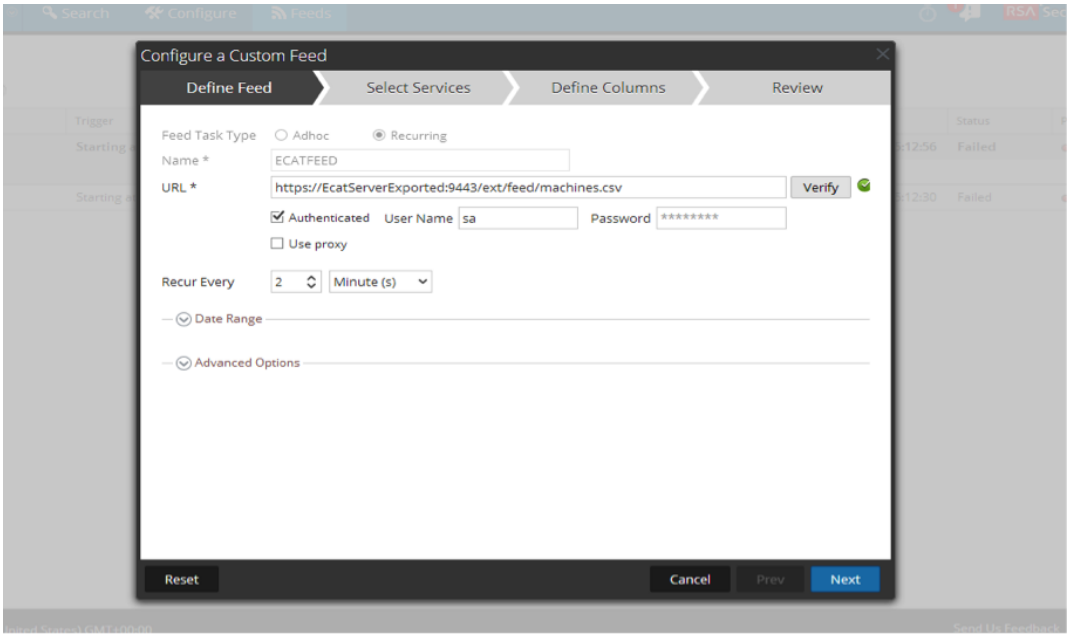
   ```
   <key description="Ecat Scantime" format="Text" level="IndexValues"
   name="ecat.stime" valueMax="250000" defaultAction="Open"/>
   ```

5. Redémarrez le Concentrator pour activer les mises à jour personnalisées.

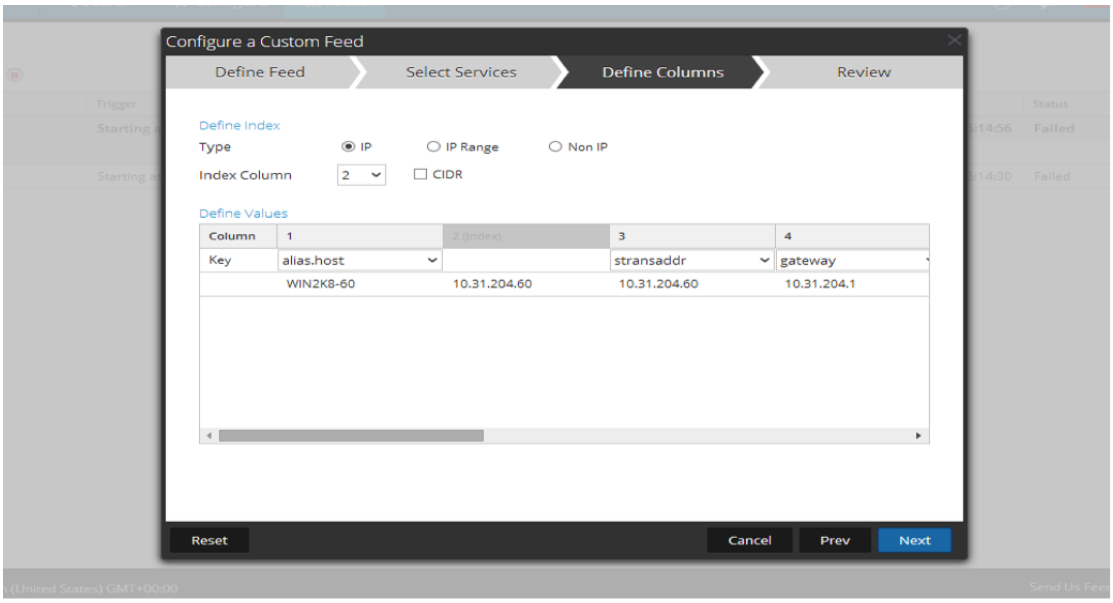
Configurer la tâche de feed personnalisée récurrente dans NetWitness Suite

1. Connectez-vous à NetWitness Suite et accédez à **CONFIGURER > Feeds personnalisés**.
   La vue Feeds s'affiche.
2. Dans la barre d'outils, cliquez sur  .
   La boîte de dialogue Configurer le feed s'affiche.
3. Dans la boîte de dialogue Configurer le feed, sélectionnez **Personnaliser le feed**, puis cliquez sur **Suivant**.
   Le panneau Configurer un feed personnalisé s'affiche avec le formulaire Définir le feed ouvert.
4. Dans le champ **Définir le feed**, procédez comme suit :
   a. Dans le champ **Type de tâche de feed**, sélectionnez **Récurrent**.
   b. Dans le champ **Nom**, saisissez le nom du feed. Par exemple, EndpointFeed.
   c. Dans le champ **URL**, saisissez l'URL avec le nom d'hôte du serveur Windows sur lequel est installé NetWitness Endpoint :
      - Pour une nouvelle installation de NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4, utilisez l'URL `https://NweServerCertificate:9443/api/v2/feed/machines.csv`.
      - Pour des mises à niveau NetWitness Endpoint à partir d'une version précédente vers 4.3.0.4 ou 4.3.0.5, utilisez l'URL `https://ecatserverexported:9443/api/v2/feed/machines.csv`.
   d. Activez la case à cocher **Authentifié** et saisissez le nom d'utilisateur et le mot de passe tels que notés dans *Activer le feed ECAT* ci-dessus.
   e. Cliquez sur **Vérifier** pour vérifier si NetWitness Suite peut atteindre la ressource web.

f. Définissez un calendrier, puis cliquez sur **Suivant**.



5. Sous l'onglet **Sélectionner des services**, sélectionnez le Decoder ou les groupes pour utiliser le feed. Cliquez sur **Suivant**.
6. Sous l'onglet **Définir des colonnes**, saisissez les noms de colonnes comme indiqué dans le tableau ci-dessous et enregistrez le feed.

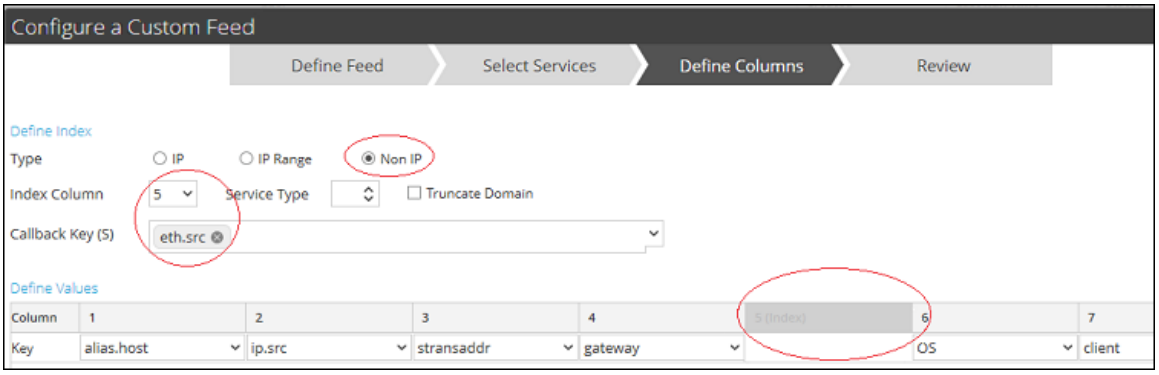


Le tableau suivant présente les colonnes dans le fichier CSV pour le feed NetWitness Endpoint.

Colonne	Nom	Description	Nom de la colonne dans NetWitness Suite (Nom de la clé méta)
1	MachineName	Nom d'hôte de l'agent Windows	alias.host
2	LocalIp	Adresse IPv4	Type d'adresse IP (colonne indexée)
3	RemoteIp	Adresse IP distante telle qu'elle est vue par le routeur	stransaddr
4	GatewayIp	Adresse IP de la passerelle	gateway
5	MacAddress	Adresse MAC	eth.src
6	OperatingSystem	Système d'exploitation utilisé par l'agent Windows	Système d'exploitation
7	AgentID	ID d'agent de l'hôte (ID unique attribué à l'agent)	client
8	ConnectionUTCTime	Dernière heure à laquelle l'agent s'est connecté au serveur NetWitness Endpoint	ecat.ctime
9	Domaine source	Domaine	domain.src
10	ScanUTC time	La dernière fois que l'agent a été analysé	ecat.stime
11	UserName	Nom d'utilisateur de la machine cliente	username

Colonne	Nom	Description	Nom de la colonne dans NetWitness Suite (Nom de la clé méta)
12	Note de l'ordinateur	Score de l'agent indiquant le niveau suspect	risk.num

Remarque : Dans le tableau, le paramètre d'index recommandé est LocalIp. Toutefois, si le LocalIp pour PC de l'Agent NetWitness Endpoint est alloué par un serveur DHCP et le bail DHCP a expiré, et si l'adresse IP est ensuite réattribuée à un autre PC, les métadonnées créées par le feed seront incorrectes. Pour éviter ce risque, utilisez le nom de machine ou l'adresse Mac au lieu de l'adresse localIP comme index du feed. Par exemple, pour utiliser une adresse Mac, vous pouvez saisir les valeurs comme indiqué dans la figure suivante.



Résultat

Lors de la visualisation des données de feed dans NetWitness Suite, en cas de correspondance de la valeur indexée (ip.src), les métadonnées sont renseignées dans les interfaces Investigation, Reporting, et Alerting.

Configurer des alertes de point de terminaison via Syslog dans un Log Decoder

Vous pouvez configurer l'utilisation de données RSA NetWitness Endpoint dans RSA NetWitness Suite pour fournir des alertes NetWitness Endpoint via Syslog dans des sessions de Log Decoder. Cette configuration génère des métadonnées utilisées par les services Investigation, Alertes et Reporting Engine de NetWitness Suite.

Pour les réseaux NetWitness Suite qui consomment des logs, l'intégration de NetWitness Endpoint avec NetWitness Suite transmet les événements NetWitness Endpoint vers le Log Decoder via des messages syslog au format CEF (Common Event Format) et génère des métadonnées utilisées par les services Investigation, Alertes et Reporting Engine de NetWitness Suite. Le cas d'utilisation pour cette intégration est l'intégration SIEM qui permet la gestion centralisée des événements, la corrélation entre des événements NetWitness Endpoint et d'autres données Log Decoder, le reporting NetWitness Suite sur les événements NetWitness Endpoint, et les alertes NetWitness Suite sur les événements NetWitness Endpoint.

Conditions préalables

Cette intégration requiert ce qui suit :

- Version d'interface utilisateur NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou 4.4.
- Serveur NetWitness version 11.0 installée.
- RSA Log Decoder et Concentrator version 10.4 ou supérieure connectés au serveur Serveur NetWitness sur le réseau.
- Port UDP- 514 ou TCP - 1514 ouvert entre le serveur NetWitness Endpoint et Log Decoder derrière le pare-feu.

Procédure

1. Déployez le parser requis (CEF ou rsaecat) vers le Log Decoder, comme décrit dans la rubrique « Gérer les ressources Live » dans *Gestion des services Live*. Une fois que vous déployez le parser, assurez-vous que le parser est activé. Pour plus d'informations, reportez-vous à la Vue Configuration des Services - Onglet Général.

Remarque : N'utilisez qu'un seul de ces parsers. Lorsque le parser CEF est déployé, il prévaut sur le parser NetWitness Endpoint, et tous les messages CEF dans NetWitness Suite sont traités par le parser CEF. L'activation des deux parsers est un fardeau inutile sur les performances.

2. Configurez NetWitness Endpoint afin qu'il envoie le résultat syslog vers NetWitness Suite et qu'il génère des alertes NetWitness Endpoint dans le Log Decoder.
3. (Facultatif) Modifiez le mappage de table dans `table-map-custom.xml` et dans `index-concentrator-custom.xml` pour ajouter des champs en fonction des préférences utilisateur pour les métadonnées devant être mappées dans NetWitness Suite.

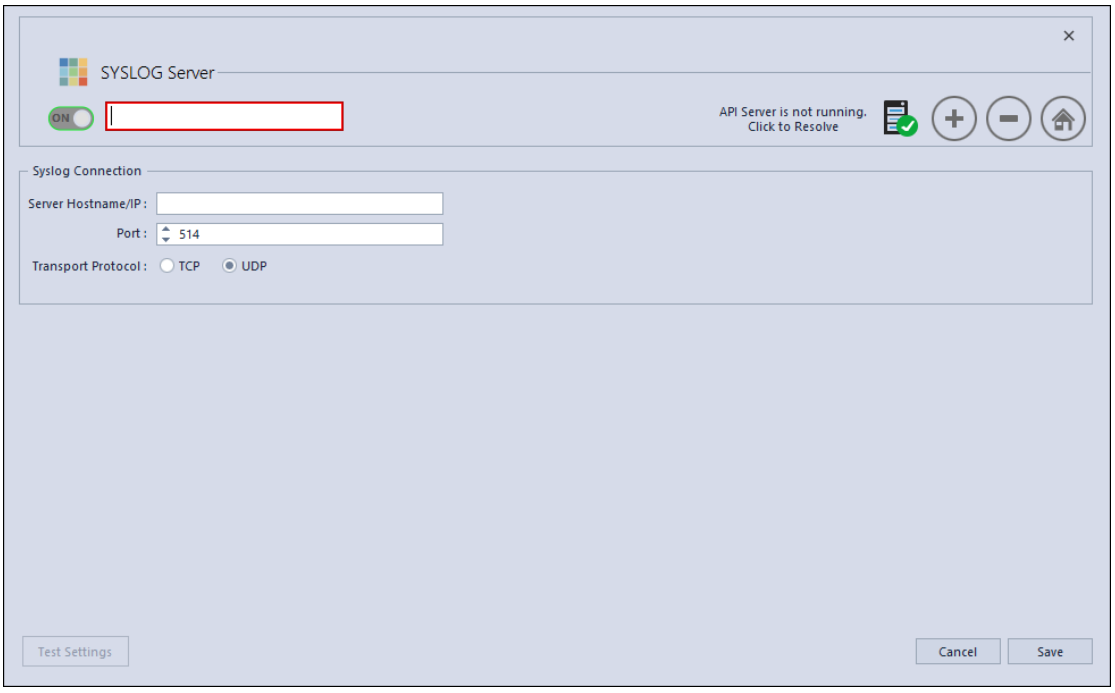
Configurer le point de terminaison NetWitness pour l'envoi du résultat Syslog vers NetWitness Suite

Pour ajouter le Log Decoder en tant que composant externe Syslog et générer des alertes NetWitness Endpoint vers Log Decoder :

1. Ouvrez l'interface utilisateur NetWitness Endpoint et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre du menu, sélectionnez **Configurer > Composants de surveillance et externes**.

   La boîte de dialogue Configuration des composants externes s'affiche.
3. Dans **Serveur SYSLOG**, cliquez sur +.

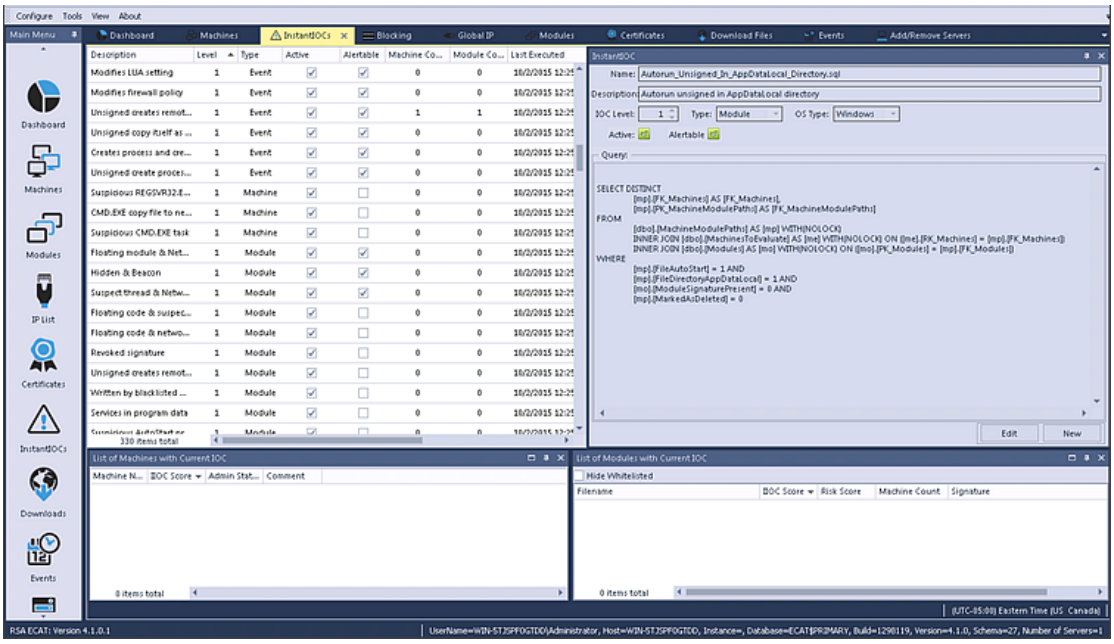
   La boîte de dialogue SYSLOG Server s'affiche.



4. Dans le panneau **NetWitness Suite**, dans **Sur**, saisissez le nom descriptif pour le Log Decoder.
5. Dans le panneau **Connexion Syslog**, procédez comme suit pour activer les messages Syslog :

   Nom d'hôte/IP du serveur = le nom d'hôte DNS ou l'adresse IP du Log Decoder RSA
   Port = 514
   Protocole de transport = sélectionnez **UDP** ou **TCP** comme protocole de transport de votre serveur Syslog.

6. Cliquez sur **Enregistrer.**
7. Ouvrez la fenêtre**InstantIOCs** dans l'interface utilisateur du point de terminaison NetWitness et, dans la colonne **Alertable**, cliquez pour activer chaque IIOC pour lequel vous souhaitez que les alertes soient envoyées vers le Log Decoder.



Lorsque les IOC instantanés sont déclenchés, les alertes Syslog du serveur NetWitness Endpoint sont envoyées au Log Decoder. Les alertes Log Decoder sont alors ajoutées au Concentrator. Ces événements sont alors injectés au Concentrator comme métadonnées.

Modifiez le mappage de table dans table-map-custom.xml

Dans le fichier table-map.xml fourni par RSA par défaut, les clés méta du fichier `table-map.xml` sont définies sur `Transient`. Dans le but d'afficher les clés méta dans Investigation, les clés doivent être définies sur `None`. Pour modifier le mappage, vous devez ajouter des entrées à `table-map-custom.xml` dans le Log Decoder.

Voici la liste des clés méta dans `table-map.xml`.

Champs NetWitness Endpoint	Mappage NetWitness Suite	Transitoire dans NetWitness Suite
agentid	client	Non
CEF Header Hostname Field	alias.host	Non
CEF Header Product Version	version	Oui
CEF Header Product Name	Produit	Oui
CEF Header Severity	severity	Oui
CEF Header Signature ID	event.type	Non
CEF Header Signature Name	event.desc	Non
destinationDnsDomain	ddomain	Oui
deviceDnsDomain	domain	Oui
dhost	host.dst	Non
dst	ip.dst	Non
Fin	endtime	Oui
fileHash	checksum	Oui
fname	filename	Non
fsize	filename.size	Oui
gatewayip	gateway	Oui
instantIOCLevel	threat.desc	Non
instantIOCName	threat.category	Non
machineOU	dn	Oui

Champs NetWitness Endpoint	Mappage NetWitness Suite	Transitoire dans NetWitness Suite
machineScore	risk.num	Non
md5sum	checksum	Oui
os	Système d'exploitation	Oui
port	ip.dstport	Non
protocol	protocol	Oui
Raw Message	msg	Oui
remoteip	stransaddr	Oui
rt	alias.host	Non
sha256sum	checksum	Oui
shost	host.src	Non
smac	eth.src	Oui
src	ip.src	Non
start	starttime	Oui
suser	user.dst	Non
timezone	timezone	Oui
totalreceived	rbytes	Oui
totalsent	bytes.src	Non
useragent	user.agent	Non
userOU	org	Oui

Ces sept clés ne sont pas dans `table-map.xml`. Pour utiliser ces clés dans NetWitness Suite, vous devez les ajouter à `table-map-custom.xml` et définir les balises sur `None`.

Champs NetWitness Endpoint	Mappage NetWitness Suite	Transitoire dans NetWitness Suite
moduleScore	cs.modulescore	Oui
moduleSignature	cs.modulesign	Oui
Target module	cs.targetmodule	Oui
YARA result	cs.yararesult	Oui
Source module	cs.sourcemodule	Oui
OPSWATResult	cs.opswatresult	Oui
ReputationResult	cs.represult	Oui

Voici les entrées à ajouter à `table-map-custom.xml` si nécessaire.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
 <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
 <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
 <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
 <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
 <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
 <mapping envisionName="cs_yararesult" nwName="cs.yararesult" flags="None"
envisionDisplayName="YaraResult"/>
```

Remarque : Redémarrez le Log Decoder ou rechargez les parsers de logs afin que les changements prennent effet.

Configurer le Service de Concentrator NetWitness Suite

1. Connectez-vous à NetWitness Suite et accédez à **ADMIN** > **Services**.
    1. Sélectionnez un Concentrator dans la liste, puis sélectionnez **Vue > Config.**
2. Sélectionnez l'onglet **Fichiers**, et dans le menu déroulant **Fichiers à modifier**, sélectionnez **index-concentrator-custom.xml**.

3. Ajoutez les clés méta NetWitness Endpoint au fichier et cliquez sur **Appliquer**. Vérifiez que ce fichier contient déjà les rubriques XML et si ce n'est pas le cas, ajoutez-les.
4. Redémarrez le Concentrator.
5. Pour ajouter le Concentrator comme source de données dans Reporting Engine, dans la vue **ADMIN** > **Services**, sélectionnez le Reporting Engine, puis sélectionnez **Vue> Config > Sources.** Les métadonnées
   NetWitness Endpoint sont renseignées dans le Reporting Engine, et vous pouvez exécuter des rapports en sélectionnant les clés méta appropriées.

Exemple

Remarque : Les lignes suivantes sont des exemples ; assurez-vous que les valeurs correspondent à votre configuration et aux noms de colonne que vous avez inclus dans la définition du flux, où :
description est le nom de la clé méta que vous souhaitez afficher dans l'investigation NetWitness Suite.
niveau est « IndexValues »
. **nom** est le nom de clé méta NetWitness Endpoint dans le tableau ci-dessous.

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
 <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
 <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
 <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
 <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
 <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
 <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
 <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
 <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
 <key description="Module Sign" format="Text" level="IndexValues"
```

```
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
 <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
 <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
 <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
 <key description="yara result" format="Text" level="IndexValues"
name="cs.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
 <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
 <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
 <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
 <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
 <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
 <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
 <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
 <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
 </language>
```

Résultat

Les analystes peuvent :

- Créer des alertes NetWitness Suite en fonction des événements NetWitness Endpoint en configurant des événements NetWitness Endpoint comme source d'enrichissement.
- Créer des règles ESA en utilisant des méta NetWitness Endpoint comme décrit dans la rubrique « Ajouter des règles à la bibliothèque de règles » dans le *Guide des alertes basées sur ESA*.
- Générer des rapports sur des événements NetWitness Endpoint à l'aide de métadonnées NetWitness Endpoint, comme décrit dans la rubrique « Configurer une règle » dans le *Guide de Reporting*.
- Afficher les alertes NetWitness Endpoint dans NetWitness Respond, comme décrit dans la rubrique « Afficher les alertes » dans le *Guide d'utilisation de NetWitness Respond*.

- Afficher les clés méta NetWitness Endpoint dans Investigation avec les clés méta standard NetWitness Suite Core comme décrit dans la rubrique « Mener une investigation » dans le *Guide d'utilisation Investigation et Malware Analysis*.