RSA NETWITNESS® SUITE

Guide de configuration système

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

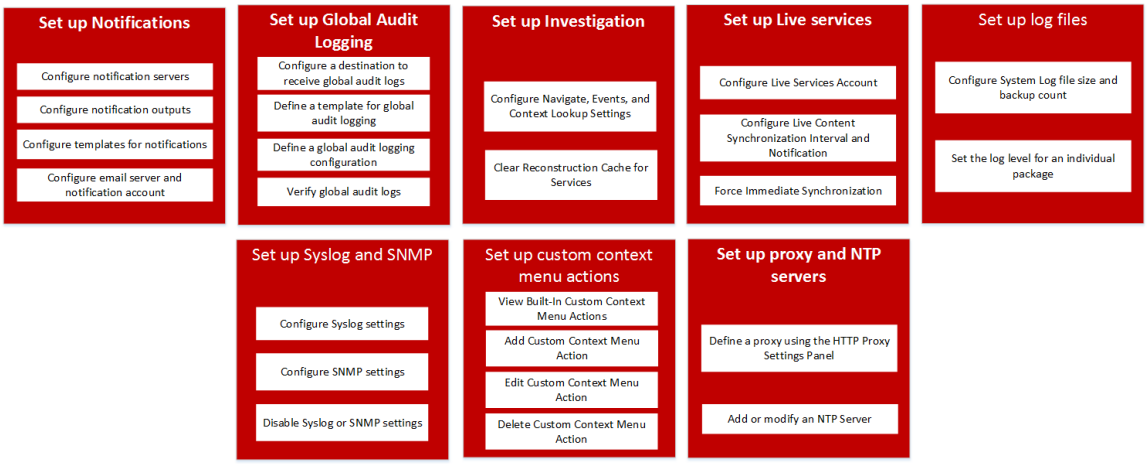
EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

Sommaire

Présentation de la configuration système

Dans la vue Système d'administration, les administrateurs peuvent configurer des paramètres système pour obtenir des performances optimales de NetWitness Suite. Ce schéma montre les options de configuration disponibles.



Dans ce guide, les procédures standard donnent des instructions destinées aux administrateurs qui souhaitent personnaliser des paramètres à appliquer à l'ensemble du système NetWitness Suite. Bien que certains de ces paramètres présentent des valeurs par défaut, l'administrateur a besoin de visualiser et d'évaluer toutes les valeurs par défaut.

Les procédures supplémentaires ne sont pas essentielles pour la configuration de NetWitness Suite. Elles incluent certaines options de personnalisation qui n'entrent pas dans le cadre de la configuration habituelle, par exemple l'ajout de menus contextuels personnalisés ou la configuration d'un proxy.

En outre, les rubriques de référence et les rubriques de dépannage donnent des informations détaillées sur l'interface utilisateur et des suggestions pour résoudre les problèmes éventuels.

Les rubriques suivantes décrivent la configuration du système :

- Les Procédures standard donnent des instructions destinées aux administrateurs qui souhaitent personnaliser des paramètres à appliquer à l'ensemble du système dans NetWitness Suite.
- Les Procédures supplémentaires fournissent des instructions pour la configuration d'options de personnalisation qui n'entrent pas dans la configuration du système habituel.

Procédures standard

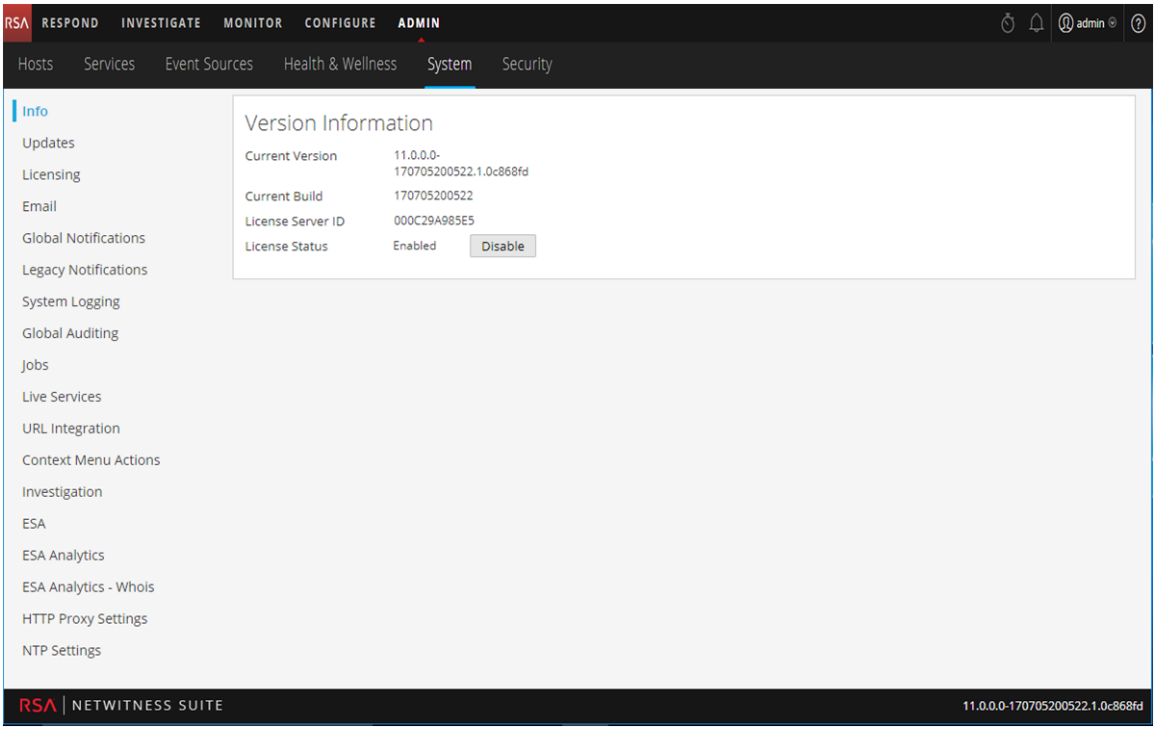
Les rubriques de cette rubrique fournissent des instructions destinées aux administrateurs qui souhaitent personnaliser des paramètres à appliquer à l'ensemble du système de NetWitness Suite. Bien que certains de ces paramètres présentent des valeurs par défaut, l'administrateur a besoin de visualiser et d'évaluer toutes les valeurs par défaut. Les procédures peuvent être exécutées dans n'importe quel ordre et sont répertoriées dans l'ordre alphabétique.

Accéder aux paramètres du système

Cette rubrique présente les possibilités de configuration système de NetWitness Suite dans la vue Système d'administration. Les administrateurs peuvent configurer des notifications, des notifications par e-mail, la consignation globale des audits, les paramètres de consignation, la connexion à Live Services et l'intégration d'URL dans NetWitness Suite.

Pour accéder aux paramètres du système :

Accédez à **ADMIN > Système**.
La vue Système d'administration s'affiche.



Sur le panneau de gauche de la vue Système d'administration se trouve le panneau d'options qui répertorie tous les nœuds système disponibles pour la configuration. Lorsque vous sélectionnez un nœud, le contenu associé s'affiche dans le panneau de droite.

Configurer les serveurs de notification

Cette rubrique fournit des instructions sur la manière de configurer les serveurs de notification. Pour ESA, les serveurs de notification sont obligatoires pour définir une règle ESA. Un serveur de notification est également requis pour configurer la consignation globale des audits.

Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE. Les serveurs de notification définissent les serveurs depuis lesquels vous souhaitez recevoir des notifications issues du système. Pour la consignation globale des audits, définissez des Log Decoders pour les serveurs de notification Syslog.

Vous pouvez définir, supprimer, modifier, importer et exporter un serveur de notification dans NetWitness Suite. Chaque rubrique décrit les procédures applicables. Pour plus d'informations sur la configuration des alertes, reportez-vous à la rubrique « Méthodes de notification » dans le **Guide des alertes basées sur ESA**. Les résultats de notification se suppriment, se modifient, s'importent et s'exportent de la même façon que les modèles. Vous ne pouvez pas désactiver ou supprimer des serveurs de notification associés aux configurations de la consignation globale des audits.

Présentation des serveurs de notification

Cette rubrique fournit une présentation des serveurs de notification. Vous pouvez configurer les serveurs de notification dans la vue Système d'administration (Administration > Système > Notifications > onglet Serveurs).

Les notifications globales sont utilisées par plusieurs composants dans NetWitness Suite, tels que Event Stream Analysis (ESA), RÉPONDRE, Intégrité, Gestion des sources d'événements (ESM) et Consignation globale des audits. Les paramètres de notification sont nommés **Serveurs de notification**.

Event Stream Analysis envoie des notifications aux utilisateurs par e-mail, SNMP ou Syslog concernant les différents événements du système. Dans ESA, ces paramètres de notification d'alerte sont appelés Serveurs de notification. Vous pouvez configurer plusieurs serveurs de notification et les utiliser lors de la définition d'une règle ESA. Par exemple, vous pouvez configurer plusieurs serveurs de messagerie ou des serveurs Syslog et utiliser les paramètres tout en définissant une règle ESA.

Vous pouvez configurer les serveurs de notification suivants :

- E-mail
- SNMP
- Syslog
- Script

Les serveurs de notification par e-mail vous permettent de configurer les paramètres du serveur de messagerie afin d'envoyer des notifications d'alerte. Les serveurs de notification SNMP vous permettent de configurer les paramètres des hôtes de trap SNMP en vue d'envoyer des notifications d'alerte.

Les serveurs de notification Syslog vous permettent de configurer les paramètres Syslog en vue d'envoyer des notifications. En cas d'activation, Syslog propose l'audit via l'utilisation du protocole Syslog RFC 5424. Le format Syslog a fait la preuve de son efficacité pour consolider les logs car il existe de nombreux outils open source et propriétaires pour le reporting et l'analyse. Pour la consignation globale des audits, seuls les serveurs de notification Syslog peuvent être utilisés.

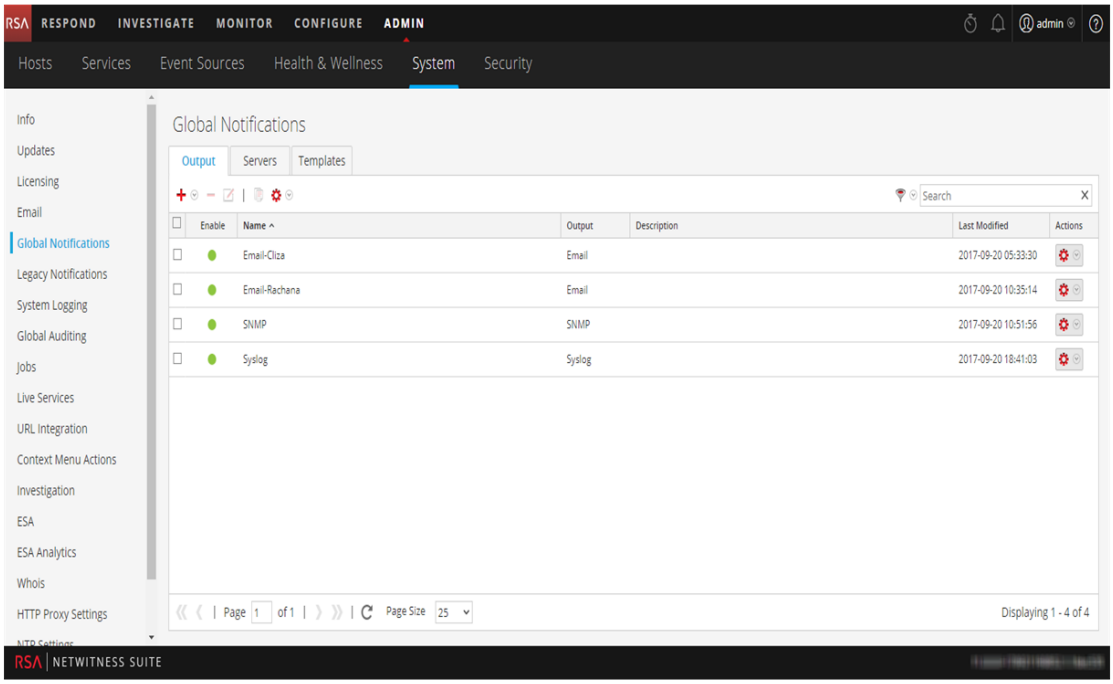
Les serveurs de notification par script vous permettent de configurer un script pour un serveur de notification.

Pour obtenir des informations détaillées sur les différentes configurations de serveur de notification, notamment des paramètres et des descriptions, consultez la rubrique Boîtes de dialogue Définir un serveur de notification.

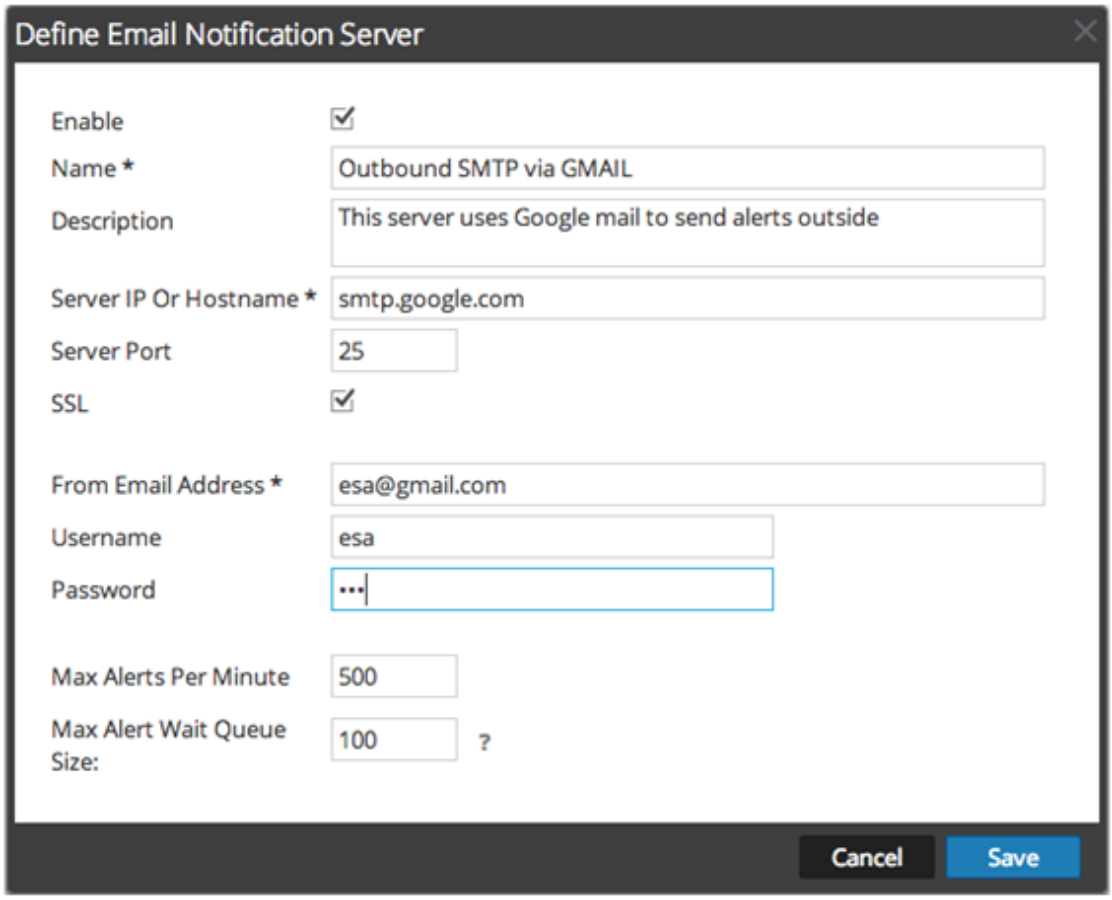
Configurer les paramètres de messagerie d'un serveur de notification

Pour configurer les paramètres du serveur de messagerie comme serveur de notification pour envoyer des notifications d'alerte :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
   Le panneau de configuration **Notifications** s'affiche avec l'onglet **Résultat** ouvert.
3. Cliquez sur l'onglet **Serveurs**.



4. Dans le menu déroulant , sélectionnez **E-mail**.



5. Dans la boîte de dialogue **Définir un serveur de notification par e-mail**, saisissez les informations requises et cliquez sur **Enregistrer**.

Remarque : Pour les notifications ESM/SMS et ESA, vous devez spécifier uniquement le nom d'hôte/nom de domaine complet dans le champ Adresse IP ou nom d'hôte du serveur.

Pour obtenir un complément d'informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

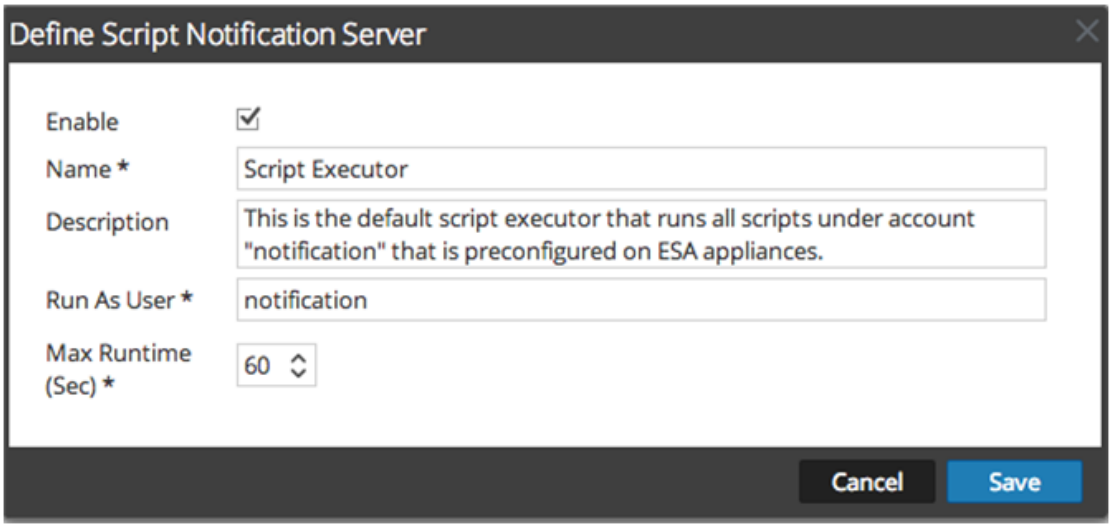
Configurer un script pour un serveur de notification

ESA vous permet d'exécuter des scripts en réponse aux alertes ESA. Cependant, vous devez d'abord configurer l'identité de l'utilisateur ainsi que d'autres informations requises pour pouvoir exécuter les scripts.

Pour configurer un script en tant que serveur de notification :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.

3. Cliquez sur l'onglet **Serveurs**.
4. Dans le menu déroulant , sélectionnez **Script**.



5. Dans la boîte de dialogue **Définir un serveur de notification par script**, saisissez les informations requises et cliquez sur **Enregistrer**.

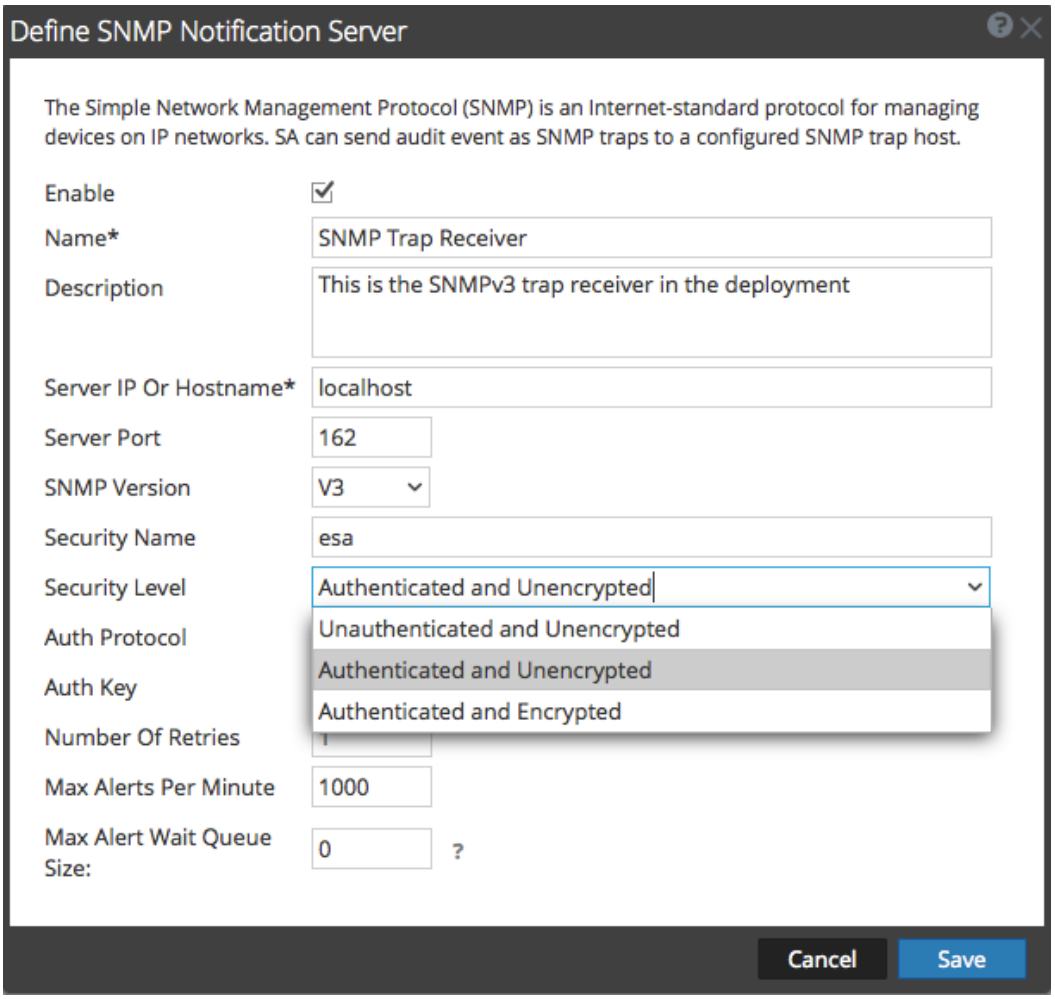
Pour obtenir un complément d'informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer les paramètres SNMP d'un serveur de notification

Pour configurer les paramètres des hôtes de trap SNMP comme serveur de notification pour envoyer des notifications d'alerte :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Serveurs**.

4. Dans le menu déroulant , sélectionnez **SNMP**.



5. Dans la boîte de dialogue **Définir un serveur de notification SNMP**, saisissez les informations requises et cliquez sur **Enregistrer**.

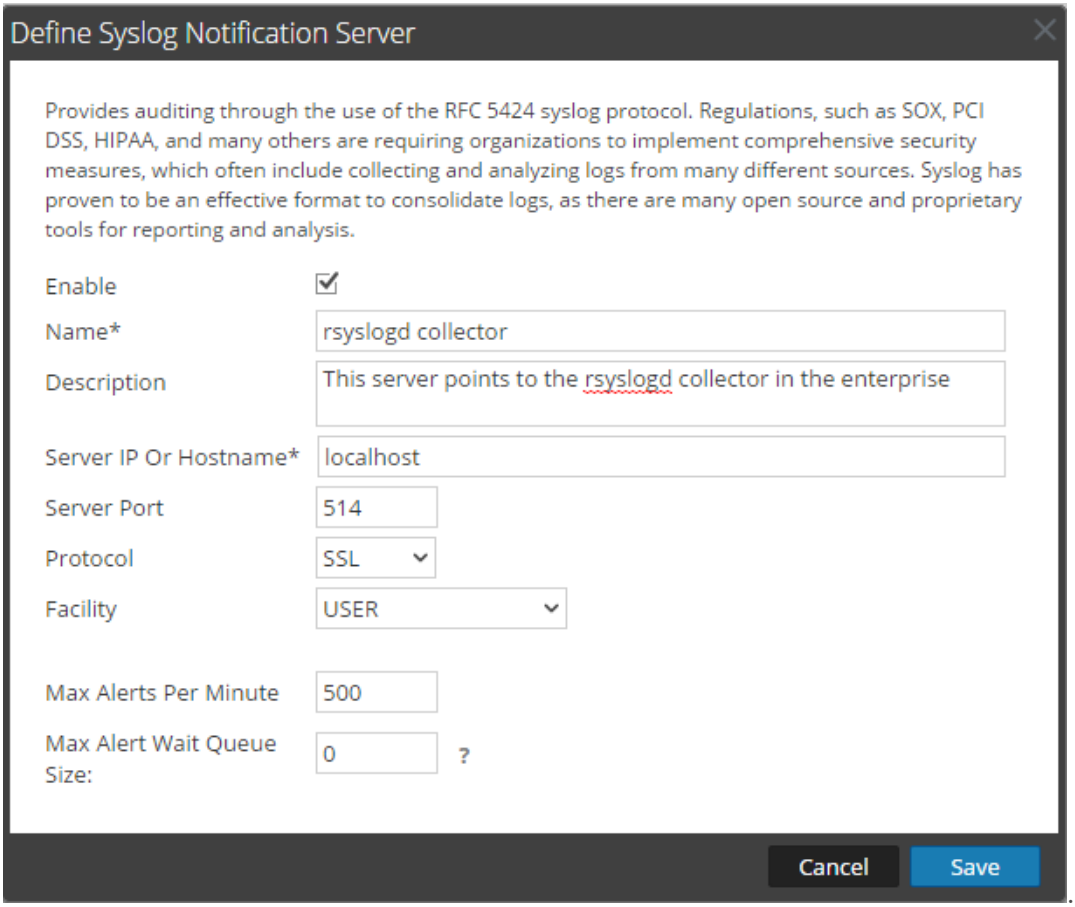
Pour obtenir un complément d'informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer un serveur de notification Syslog

Cette rubrique fournit des instructions sur la manière de configurer un serveur de notification Syslog. En cas d'activation, Syslog propose l'audit via l'utilisation du protocole Syslog RFC 5424. Le format Syslog a fait la preuve de son efficacité pour consolider les logs car il existe de nombreux outils open source et propriétaires pour le reporting et l'analyse.

Pour configurer Syslog comme serveur de notification :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales.**
3. Cliquez sur l'onglet **Serveurs**.
4. Dans le menu déroulant , **sélectionnez** Syslog



5. Dans la boîte de dialogue **Définir un serveur de notification Syslog**, indiquez les informations requises et cliquez sur **Enregistrer**.

Pour obtenir des informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer les résultats de notification

Cette rubrique fournit des instructions sur la manière de configurer les résultats de notification. Ces résultats de notification sont nécessaires pour définir une règle ESA.

Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE.

Vous n'avez pas besoin de configurer l'onglet Résultat pour la consignation globale des audits.

Les configurations des résultats de notification définissent les lignes de l'adresse e-mail et de l'objet, les paramètres OID de trap SNMP, les paramètres de résultat Syslog et le code du script.

Vous pouvez définir, supprimer, modifier, importer et exporter des résultats de notification dans NetWitness Suite. Chaque rubrique décrit les procédures applicables. Pour plus d'informations sur la configuration des alertes ESA, reportez-vous à la rubrique « Méthodes de notification ». Les résultats de notification se suppriment, se modifient, s'importent et s'exportent de la même façon que les modèles. Si vous tentez de supprimer un résultat de notification utilisé par les alertes, vous recevrez un message de confirmation d'avertissement que les alertes qui utilisent la notification ne fonctionneront pas correctement. Le message indique le nombre d'alertes en cours.

Présentation des résultats de notification

Cette rubrique fournit une présentation des résultats de notification. Ces résultats de notification sont nécessaires lors de la définition d'une règle ESA. Vous configurez les résultats de notification dans la vue Système d'administration (Administration > Système > Notifications > onglet Résultats).

Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements (ESM), Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE.

Remarque : Vous n'avez pas besoin de configurer les résultats de notification (onglet résultats) pour la consignation globale des audits.

Les résultats de notification représentent les destinations utilisées pour l'envoi des notifications. Pour ESA, les résultats de notification vous permettent de définir la manière dont vous souhaitez recevoir les alertes ESA. Les résultats de notification suivants sont pris en charge par NetWitness Suite :

- E-mail
- SNMP

- Syslog
- Script

Les paramètres des notifications par e-mail définissent l'adresse e-mail de destination à laquelle vous pouvez envoyer les alertes. Vous pouvez aussi ajouter une description personnalisée dans l'objet de l'e-mail et définir différentes adresses e-mail de destination.

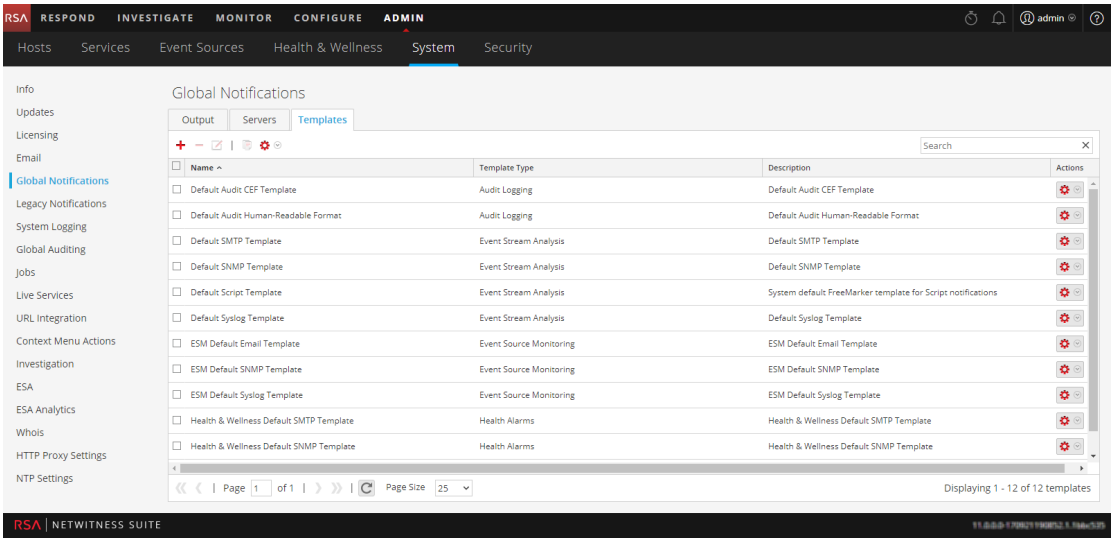
Les paramètres des notifications SNMP vous permettent de définir les paramètres SNMP pour l'envoi des notifications d'alertes. Les notifications Syslog vous permettent de définir les paramètres Syslog utilisés pour envoyer des notifications d'alerte. Les notifications par script vous permettent de définir le script qui s'exécutera en réponse à l'alerte.

Pour plus d'informations sur les configurations de notification, notamment les paramètres et les descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

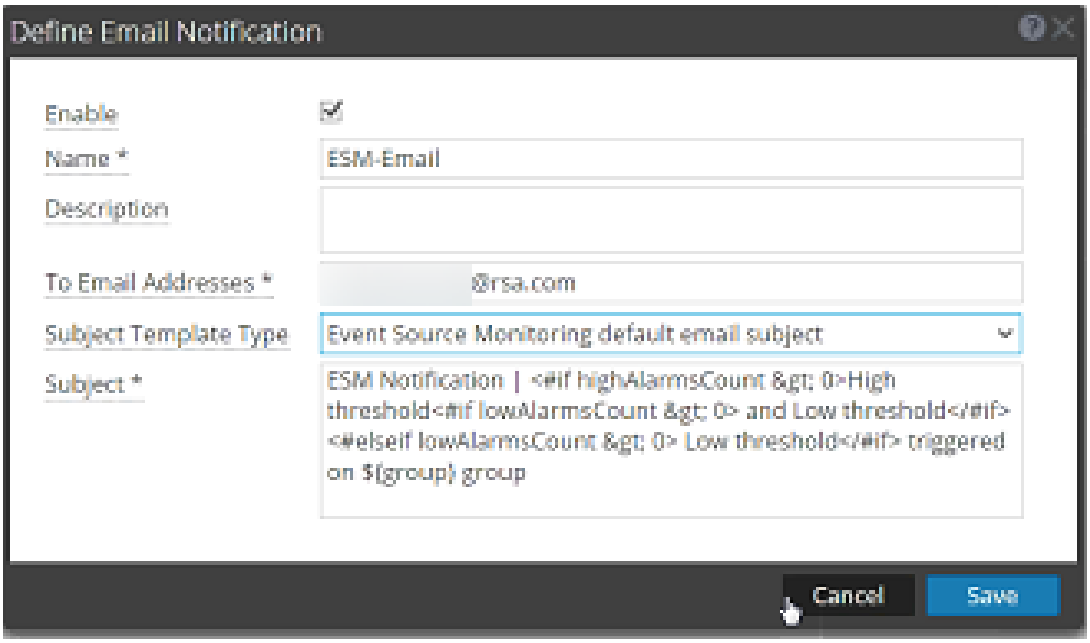
Configurer la messagerie en tant que méthode de notification

Pour configurer la messagerie en tant que méthode de notification :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.



3. Sous l'onglet **Résultat**, dans le menu déroulant , sélectionnez **E-mail**.



4. Dans la boîte de dialogue **Définir une notification par e-mail**, saisissez les informations requises et cliquez sur **Enregistrer**.

Pour obtenir des informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

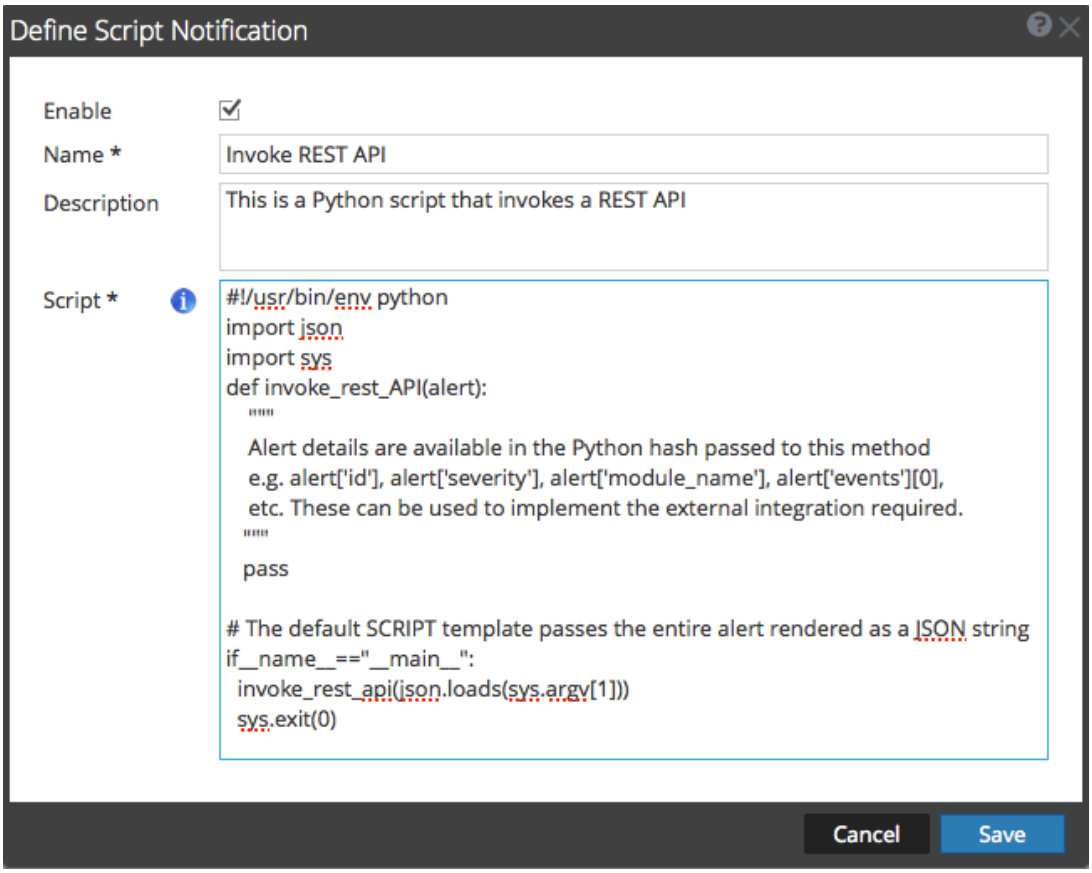
Configurer un script en tant que méthode de notification

Cette rubrique fournit les instructions permettant de définir le script et de le configurer en tant que résultat de notification. ESA vous permet d'exécuter des scripts en réponse aux alertes ESA. Vous devez définir le script à l'aide de l'onglet ADMIN > Système > Notifications > Résultat. Vous pouvez utiliser n'importe quel script pour les notifications ESA.

Pour configurer le script en tant que méthode de notification :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.

3. Sous l'onglet Résultat, dans le menu déroulant , sélectionnez **Script**.



4. Dans la boîte de dialogue **Définir une notification par script**, saisissez les informations requises et cliquez sur **Enregistrer**.

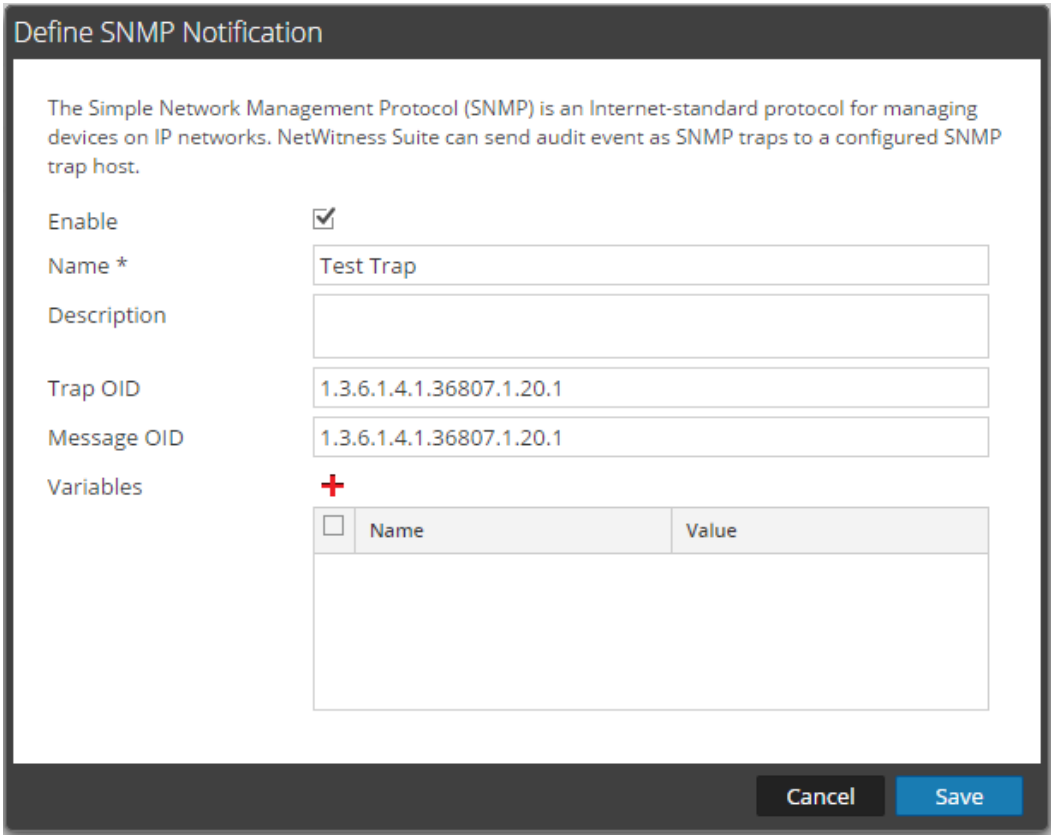
Pour obtenir des informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer le protocole SNMP en tant que méthode de notification

Pour configurer les paramètres SNMP en tant qu'un résultat de notification pour envoyer des notifications d'alerte :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.

3. Sous l'onglet Résultat, dans le menu déroulant , sélectionnez **SNMP**.



4. Dans la boîte de dialogue Notification SNMP, saisissez les informations requises et cliquez sur **Enregistrer**.

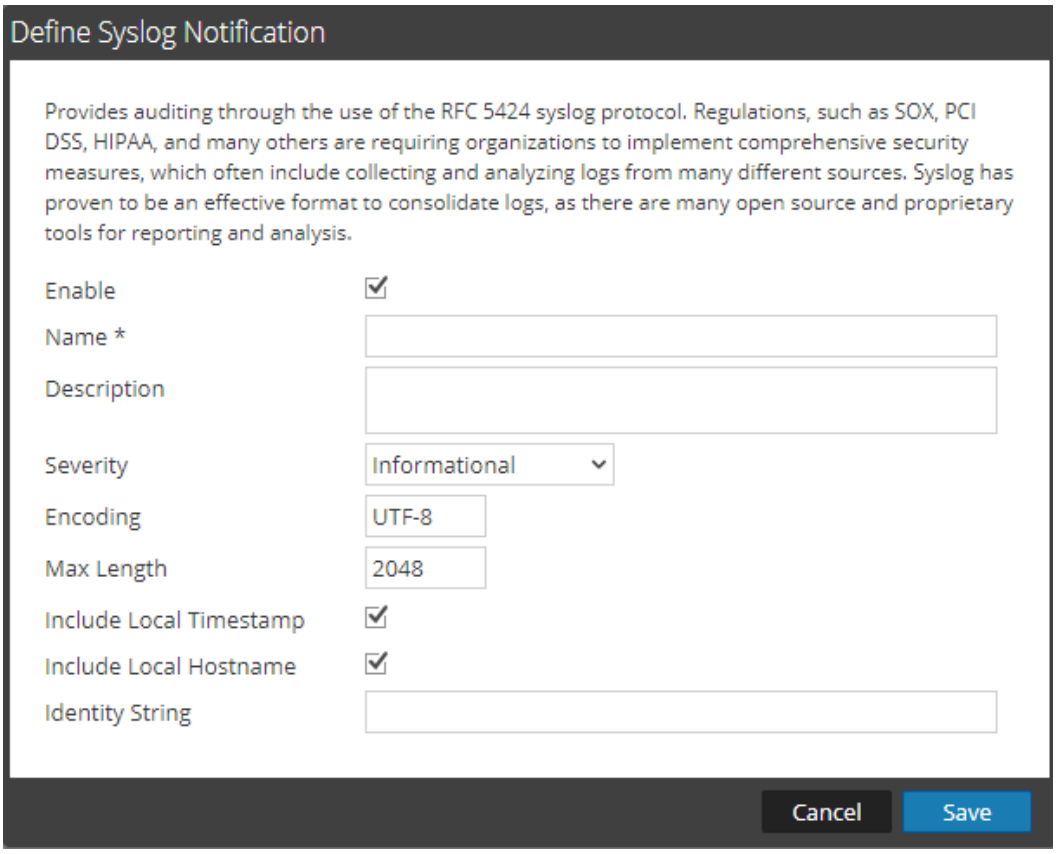
Pour obtenir des informations sur les paramètres et leurs descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer Syslog en tant que méthode de notification

Pour configurer Syslog en tant que résultat de notification quand vous envoyez des notifications d'alerte :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.

3. Sous l'onglet Résultat, dans le menu déroulant , sélectionnez **Syslog**.



4. Dans la boîte de dialogue **Définir une notification Syslog**, saisissez les informations requises et cliquez sur **Enregistrer**.

Pour plus d'informations sur les paramètres et les descriptions, reportez-vous à la rubrique Boîtes de dialogue Définir un serveur de notification.

Configurer des modèles pour les notifications

Configurez les modèles de notification dans la vue Système d'administration (Administration > Système > Notifications > onglet Modèles). Un modèle de notification définit les champs de format et de message des notifications. Il existe plusieurs types de modèles différents pour les notifications que vous pouvez configurer :

- Consignation des audits
- Event Stream Analysis
- Surveillance des sources d'événements
- Alarmes d'intégrité

Vous pouvez utiliser les modèles par défaut disponibles ou vous pouvez configurer vos propres modèles de courrier électronique, SNMP, Syslog et script, selon le type de modèle.

La consignation globale des audits envoie des logs d'audit dans le format spécifié dans le modèle de consignation des audits. Vous pouvez utiliser les modèles de consignation des audits par défaut ou vous pouvez définir vos propres modèles. Pour plus d'informations sur la définition d'un modèle de consignation des audits, consultez la rubrique Définir un modèle pour la consignation globale des audits.

Event Stream Analysis (ESA) envoie des notifications dans le format spécifié dans les modèles Event Stream Analysis. Les modèles Event Stream Analysis par défaut pour les e-mails, SNMP, Syslog et les scripts sont disponibles à l'installation. Vous pouvez personnaliser ces modèles et en créer de nouveaux que vous pouvez utiliser pour les notifications. Pour plus d'informations sur la définition de modèles ESA, consultez la rubrique Définir un modèle pour les notifications d'alerte ESA.

Pour plus d'informations sur la configuration des alertes ESA, consultez la rubrique « Méthodes de notification » dans le **Guide des alertes basées sur ESA**. Vous ne pouvez pas supprimer les modèles associés à des configurations de la consignation globale des audits.

Remarque : Lors de la mise à niveau de NetWitness Suite 10.4, tous les modèles de notification existants migrent vers le type de modèle Event Stream Analysis.

Pour savoir comment définir, supprimer, modifier, dupliquer, importer et exporter un modèle de notification dans NetWitness Suite, consultez :

Configurer des modèles de notification globale

Définir un modèle pour les notifications d'alerte ESA

Importer et exporter un modèle de notifications global

Configurer des modèles de notification globale

Cette rubrique fournit des instructions pour l'ajout, la modification, la duplication et la suppression des modèles de notification globale.

Vous pouvez utiliser les modèles par défaut disponibles ou vous pouvez configurer vos propres modèles de courrier électronique, SNMP, Syslog et script, selon le type de modèle.

La consignation globale des audits envoie des logs d'audit dans le format spécifié dans le modèle de consignation des audits. Vous pouvez utiliser les modèles de consignation des audits par défaut ou vous pouvez définir vos propres modèles. Pour plus d'informations sur la définition d'un modèle de consignation des audits, consultez la rubrique « Définir un modèle pour la consignation globale des audits ».

Event Stream Analysis (ESA) envoie des notifications dans le format spécifié dans les modèles Event Stream Analysis. Les modèles Event Stream Analysis par défaut pour les e-mails, SNMP, Syslog et les scripts sont disponibles à l'installation. Vous pouvez personnaliser ces modèles et en créer de nouveaux que vous pouvez utiliser pour les notifications. Pour plus d'informations sur la définition de modèles ESA, consultez la rubrique Définir un modèle pour les notifications d'alerte ESA.

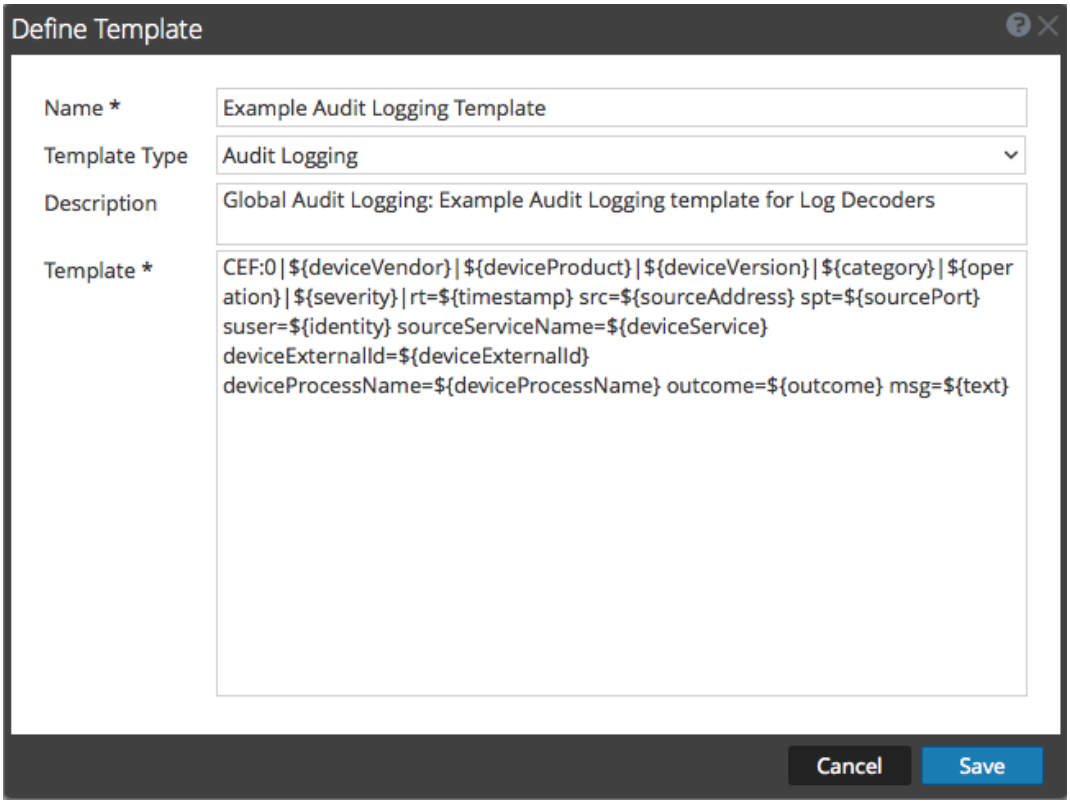
Lors de la mise à niveau de NetWitness Suite 10.4, tous les modèles de notification existants migrent vers le type de modèle Event Stream Analysis.

Ajouter un modèle

Vous pouvez utiliser les modèles par défaut fournis ou configurer vos propres modèles. Suivez cette procédure pour configurer votre propre modèle :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Modèles**.
4. Cliquez sur + pour configurer un modèle.
5. Dans la boîte de dialogue **Définir un modèle**, fournissez les informations suivantes :
   a. Dans le champ **Nom**, saisissez un nom pour le modèle.
   b. Dans le champ **Type de modèle**, sélectionnez le type de modèle à créer. Par exemple, si vous créez un modèle pour la consignation globale des audits, sélectionnez le type de modèle de consignation des audits.
   c. Dans le champ **Description**, saisissez une petite description du modèle.
   d. Dans le champ **Modèle**, indiquez le format du modèle.

e. Cliquez sur **Enregistrer** pour enregistrer le modèle.



Dupliquer un modèle

Vous pouvez réaliser une copie d'un modèle par défaut ou défini par l'utilisateur existant. Pour dupliquer un modèle :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Modèles**.
4. Sélectionnez le modèle que vous souhaitez dupliquer, puis cliquez sur .

   La boîte de dialogue Dupliquer le modèle d'alerte s'affiche.

5. Saisissez le nom du modèle dupliqué.
6. Cliquez sur **OK**.

Vous pouvez modifier un modèle par défaut ou défini par l'utilisateur. Lorsque vous modifiez un modèle, les changements ne sont visibles qu'une fois l'alerte déclenchée.

Modifier un modèle

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Modèles**.
4. Sélectionnez un modèle et cliquez sur  .
5. Dans la boîte de dialogue **Définir un modèle**, modifiez les champs **Nom**, **Type de modèle**, **Description** et **Modèle** si nécessaire.
6. Cliquez sur **Enregistrer** pour enregistrer le modèle.

Supprimer un modèle

Vous pouvez supprimer un modèle défini par l'utilisateur. Lorsque vous supprimez un modèle utilisé dans une règle ESA, le modèle Event Stream Analysis par défaut est utilisé pour les alertes. Vous ne pouvez pas supprimer des modèles associés aux configurations de la consignation d'audit globales.

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Modèles**.
4. Sélectionnez un ou plusieurs modèles, puis cliquez sur .
   Une boîte de dialogue de confirmation s’affiche.
5. Cliquez sur **Yes**.
   Le modèle sélectionné est supprimé.

Définir un modèle pour les notifications d'alerte ESA

Cette rubrique décrit comment définir un modèle pour les notifications d'alerte. Event Stream Analysis (ESA) vous permet de définir des modèles utiles pour les alertes. Vous devez avoir une bonne compréhension de FreeMarker et le modèle de données ESA pour définir un modèle. Pour plus d'informations sur FreeMarker, reportez-vous au FreeMarker Template Author's Guide.

Modèle de données ESA

Une règle d'alerte ESA se présente comme suit :

```
@Name('module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert')
@Description('Brute Force Login To Same Destination')
@RSAAlert(oneInSeconds=0, identifiers={"ip_dst"})
SELECT* FROMEvent (ec_activity = 'Logon',ec_theme = 'Authentication',ec
outcome = 'Failure',ip_dst IS NOT NULL)
.std:groupwin(ip_dst)
.win:time_length_batch(60 seconds, 2)
GROUPBYip_dst HAVING COUNT(*) = 2;
```

Lorsqu'une règle comme celle précitée est déclenchée, l'alerte générée comportera deux événements constitutifs, chacun s'apparentant à une session NextGen avec plusieurs métavaleurs. L'objet associé aux données de l'alerte transmis à l'évaluateur du modèle FreeMarker se présente comme suit :

```
(root)
  |
  +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79"                    // Unique identifier for
each alert
  |
  +- severity = 1                                                    // The severity of the
alert
  +- time = 2013-12-31T11:02Z                                        // The alert time (needs a
?datetime for proper rendering)
  |  +- moduleType = "ootb"                                          // The module type
  |
  +- moduleName = "Brute Force Login To Same Destination"            // A description of the
module
  |
  +- statement = "module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert" // The name of the EPL
statement
  |  +- events                                                       // The constituent events -
as a sequence of event maps
       |   +- [0]                                                   // offset 0 (i.e. the first
constituent event)
       |   |       |   |
       |   +- event_cat_name = "User.Activity.Failed Logins"
       |   +- device_class = "Firewall"                             // event meta (accessible
as ${events[0].device_class}$)
       |   |       |   +- event_source_id = "uttam:50002:1703395"   // Investigation URI to the
individual session (used by SA)
       |   |
       |   +- ...                                                   // Other meta
       |   |
       |   +- sessionid = 1703395                                   // NextGen sessionid
       |   |
       |   +- time = 1388487764                                     // event/session time at
NextGen source (as a long Unix timestamp)
       |   |
       |   +- user_dst = "user5"
       |
       +- [1]                                                       // offset 1 (i.e. the
second consituent event)
           |
           +- device_class = "Firewall"
           |
           +- event_cat_name = "User.Activity.Failed Logins"
           |
```

```
+- event_source_id = "uttam:50002:1703405"
|
+- ...
|
+- sessionid = 1703405
|
+- time = 1388487766
|
+- user_dst = "user5"
```

Il existe deux types de variables de modèle disponibles dans le modèle de données :

- **Les métadonnées d'alerte :** Elles contiennent les détails des niveaux d'alerte, comme le nom de l'instruction, le nom du module, l'ID d'alerte, l'heure de l'alerte, sa gravité, etc. Dans la terminologie FreeMarker, il s'agit des variables de niveau supérieur associées à l'instance d'alerte elle-même et elles peuvent être référencées simplement par leurs noms, comme `${moduleName}`. Le méta `time` est spécial car il est du type `Date` et doit être un suffixe de `?datetime` pour pouvoir s'afficher correctement.

- **Les métadonnées d'événements constitutifs** : Il s'agit des champs de sessions méta provenant de chaque événement qui constitue l'alerte. Une alerte peut avoir plusieurs événements constitutifs, donc il peut y avoir plusieurs mappages de ce type dans la même alerte. Elles s'affichent sous la forme d'une séquence de hachages dans l'évaluateur de modèles FreeMarker et doivent être référencées. Par exemple, l'alerte comporte deux événements constitutifs : l'event_source_id pour le premier est disponible en tant que `${events[0].event_source_id}` et le même pour le deuxième est accessible en tant que ${`events[1].event_source_id`.}. Vous devez également savoir quels champs méta sont à valeurs multiples, car ils doivent être traités en tant que séquences ; par exemple ${`events[0].alias_host`} ne fonctionne pas, car il s'agit d'une séquence.

Remarque : Les métadonnées disponibles dans les événements constitutifs pour une alerte donnée sont déterminés par la clause EPL SELECT. Par exemple, les alertes issues de `SELECT sessionid, time FROM ...` auront seulement deux métavaleurs disponibles (sessionid, time). Les événements constitutifs dans `SELECT * FROM Event ...` porteront tous les champs de métadonnées du type `Event` avec des valeurs qui ne sont pas **nulles**.

Si votre modèle utilise les métaclés qui ne sont pas présentes dans tous les résultats d'alerte, vous devez envisager d'utiliser les provisions de FreeMarker pour les valeurs par défaut.

Par exemple, si un modèle avec le texte Id=${id},ec_outcome=${ec_outcome} est évalué pour une alerte qui n'inclut pas la métaclé `ec_outcome`, alors l'évaluation du modèle échouera. Dans de tels cas, vous pouvez utiliser l'espace réservé à la valeur manquante `${ec_outcome!"default"}`.

Importer et exporter un modèle de notifications global

Cette rubrique fournit les instructions pour importer et exporter un modèle pour les notifications.

- Vous pouvez exporter un modèle par défaut ou défini par l'utilisateur.
- Vous pouvez importer un modèle exporté de l'instance NetWitness Suite. Si vous importez un modèle portant le même nom qu'un modèle existant, ce dernier sera écrasé.

Importer un modèle

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales.**
3. Cliquez sur l'onglet **Modèles**.
4. Dans la barre d'outils, cliquez sur  **> Importer**.
   La boîte de dialogue **Importer** s'affiche.
5. Dans le champ **Saisir un nom de fichier**, saisissez le nom du fichier ou cliquez sur **Parcourir** et sélectionnez le fichier à importer.
6. Cliquez sur **Importer**.

Exporter un modèle

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales.**
3. Cliquez sur l'onglet **Modèles**.
4. Sélectionnez le modèle à exporter.

   Remarque : Vous pouvez exporter tous les modèles à l'aide de l'option  **> Exporter tout**.
5. Dans la colonne **Actions**, sélectionnez  **> Exporter**.
   La boîte de dialogue **Exporter** s'affiche.
6. Dans le champ **Saisir un nom de fichier**, saisissez le nom du fichier.
7. Cliquez sur **Enregistrer**.

Configurer les serveurs de messagerie et les comptes de notification

Cette rubrique fournit des instructions pour la configuration des e-mails afin que les utilisateurs puissent recevoir des notifications dans NetWitness Suite. RSA NetWitness® Suite peut envoyer des notifications aux utilisateurs par e-mail concernant les différents événements système. Pour être en mesure de configurer ces notifications par e-mail, vous devez d'abord configurer le serveur de messagerie SMTP. Le panneau de Configuration de l'e-mail offre un moyen de :

- Configurer le serveur de messagerie.
- Configurer un compte de messagerie pour recevoir les notifications.
- Afficher les statistiques des opérations liées à la messagerie.

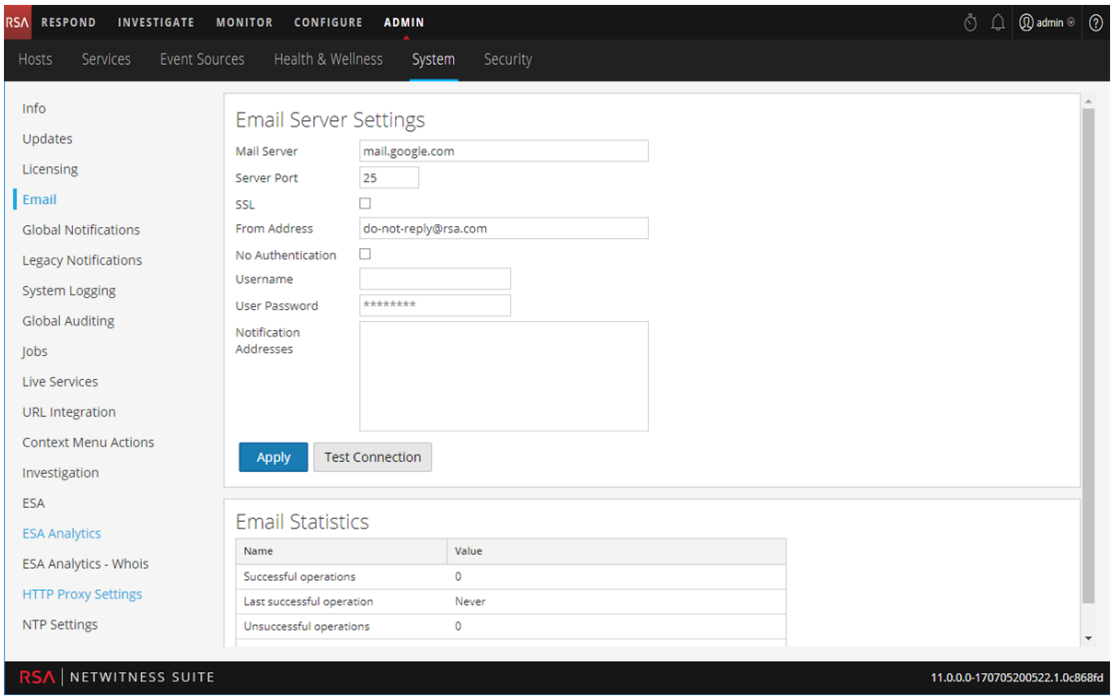
NetWitness Suite nécessite l'accès à un serveur de messagerie SMTP pour envoyer des rapports aux utilisateurs. Chaque compte utilisateur peut être configuré pour recevoir des rapports par e-mail. Ces rapports peuvent être générés manuellement, via l'interface utilisateur, ou automatiquement, par l'intermédiaire du système d'audit. Les règles suivantes s'appliquent :

- Tout hôte de courrier SMTP peut être utilisé pour envoyer des e-mails, et chacun d'entre eux nécessite une configuration différente. Le fournisseur SMTP fournit les paramètres de configuration.
- Certains serveurs SMTP requièrent une authentification de l'utilisateur afin de relayer les e-mails correctement. En règle générale, il s'agit du login et du mot de passe du compte de messagerie.
- Les bonnes pratiques consistent à créer un nouveau compte de messagerie dédié sur le serveur de messagerie SMTP pour les rapports NetWitness Suite.

Pour configurer les notifications par e-mail de NetWitness Suite :

1. Accédez à **ADMIN > Système**.
   La vue Système d'administration s'affiche.

2. Dans le panneau des options, sélectionnez **E-mail**.



3. Si vous souhaitez modifier le serveur de messagerie par défaut, indiquez le nom du **Serveur de messagerie** et le **Port de serveur**.
4. Si le serveur de messagerie communique avec NetWitness Suite à l'aide de SSL, cochez la case en regard de l'option **Utiliser SSL**.
5. Dans le champ **De l'adresse**, saisissez le nom du compte de messagerie d'envoi des notifications par e-mail de NetWitness Suite.
6. Si le serveur SMTP requiert une authentification utilisateur pour relayer les e-mails, saisissez le **Nom d'utilisateur** et le **Mot de passe utilisateur** pour la connexion au compte e-mail.
7. Pour activer les paramètres, cliquez sur **Appliquer**.
   Vous pouvez maintenant configurer les modules NetWitness Suite pour recevoir différentes notifications par e-mail.

Configurer la consignation globale des audits

La consignation globale des audits donne aux auditeurs NetWitness Suite une vue consolidée des activités des utilisateurs au sein de NetWitness Suite, en temps réel et à partir d'un emplacement centralisé. Cette visibilité comprend les logs d'audit collectés à partir du système NetWitness Suite et les différents services au sein de l'infrastructure NetWitness Suite.

Les logs d'audit NetWitness Suite effectuent la collecte dans un système centralisé qui les convertit au format requis et les transfère à un système syslog externe. Le système syslog externe peut être un serveur syslog tiers ou un Log Decoder.

Vous configurez la consignation globale des audits dans le panneau Configuration de la consignation globale des audits. Un modèle de consignation des audits définit les champs de format et de message des entrées de log d'audit. Une configuration de serveur de notification Syslog définit la destination pour envoyer les logs d'audit. Si vous souhaitez transférer des logs d'audit vers un Log Decoder, configurez un type Syslog de serveur de notification pour le Log Decoder.

Les éléments suivants sont quelques-unes des actions utilisateur consignées à partir de NetWitness Suite :

- Connexions utilisateur réussies
- Échec de la connexion utilisateur
- Déconnexions utilisateur
- Nombre d'échecs de la connexion dépassé
- Toutes les pages de l'interface utilisateur consultées
- Modifications de configuration validées (y compris lorsque l'utilisateur modifie son propre mot de passe)
- Requêtes effectuées par l'utilisateur
- Accès utilisateur refusés
- Opérations liées à l'exportation de données

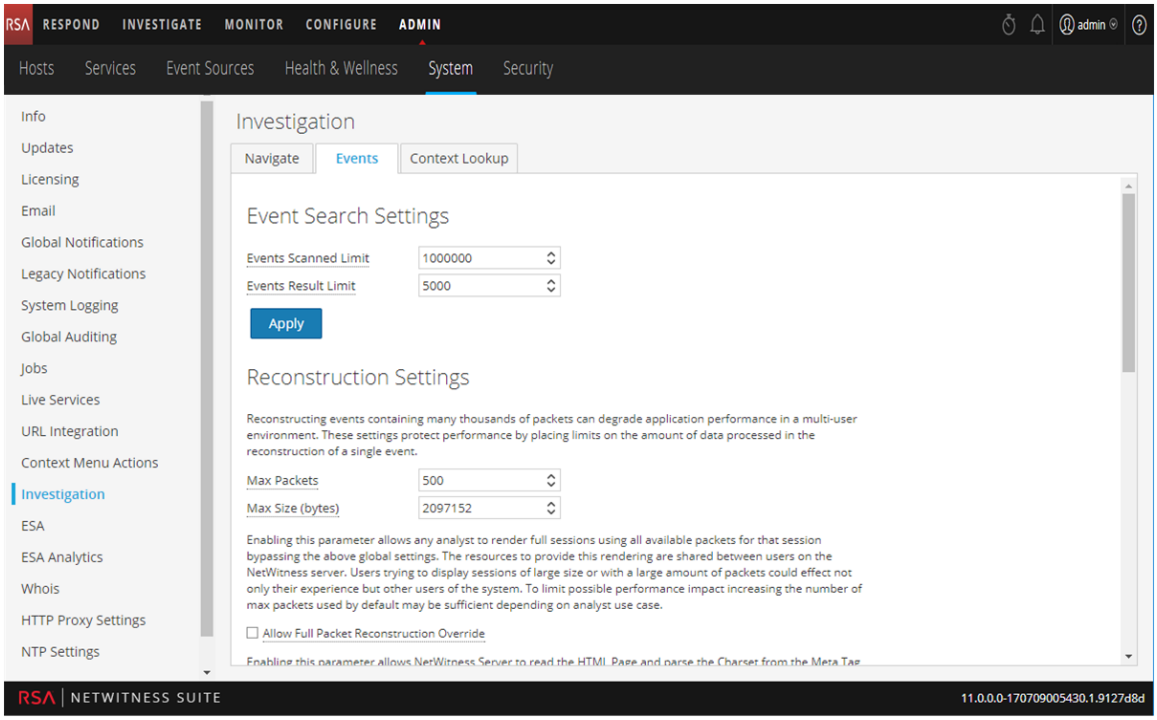
Après la création d'une configuration de consignation globale des audits, les logs d'audit contenant ces actions utilisateur accèdent automatiquement au système syslog externe au format spécifié dans le modèle Consignation des audits sélectionné. Vous pouvez créer plusieurs configurations de la consignation globale des audits pour différentes destinations utilisant différents modèles. Par exemple, vous pouvez créer une configuration de consignation globale des audits pour un serveur Syslog externe avec un modèle qui contient toutes les métaclés disponibles et une autre configuration pour un Log Decoder avec un modèle qui contient les métaclés sélectionnées.

Pour les Log Decoders, utilisez le modèle CEF d'audit par défaut. Vous pouvez ajouter ou supprimer des champs dans le modèle CEF (Common Event Format) si vous avez des exigences spécifiques. Définir un modèle pour la consignation globale des audits fournit des instructions et Métaclés CEF prises en charge décrit les métaclés CEF utilisables dans les modèles de consignation d'audit.

Pour les serveurs syslog tiers, vous pouvez utiliser un modèle de consignation d'audit par défaut ou définir votre propre format (CEF ou non-CEF). Définir un modèle pour la consignation globale des audits fournit des instructions et Variables de métaclés prises en charge pour la consignation globale des audits décrit les variables disponibles.

Les auditeurs peuvent afficher les logs d'audit sur le Log Decoder sélectionné ou un serveur syslog tiers. Si vous utilisez un Log Decoder, les auditeurs peuvent afficher les logs d'audit avec les Investigations ou Rapports NetWitness Suite.

La figure suivante affiche les logs d'audit globaux dans les Investigations (Investigation > Événements).



Pour obtenir des exemples d'actions d'utilisateur consignées, voir Boîte de dialogue Ajouter une nouvelle configuration. Pour obtenir la liste des types de message consignés par les différents composants NetWitness Suite, reportez-vous à la rubrique Référence aux opérations de consignation globale des audits.

Consignation globale des audits - procédure générale

La consignation globale des audits est configuré dans le panneau Configuration de la consignation globale des audits, qui est accessible depuis la vue Administration - Système > Audit global. Avant de pouvoir configurer la consignation globale des audits, vous devez configurer un serveur de notification Syslog et un modèle de consignation des audits. Un serveur de notification Syslog définit la destination pour envoyer les logs d'audit. Un modèle de consignation des audits définit les champs de format et de message de l'entrée de log d'audit.

Le panneau Configurations de consignation d'audit globale fournit un lien aux **paramètres de la vue** qui vous renvoie au panneau Notifications globales (vue Administration système > Notifications globales) où vous pouvez configurer le serveur de notification Syslog et le modèle de consignation des audits.

Effectuez les procédures suivantes dans l'ordre indiqué pour configurer la consignation globale des audits.

Procédures	Référence/Instructions
1. Configurer un serveur de notification Syslog.	Configurez un serveur de notification Syslog à utiliser la consignation globale des audits. Vous pouvez définir un serveur syslog tiers ou un Log Decoder en tant que destination pour recevoir les logs d'audit. Configurer une destination pour recevoir des logs d'audit globaux. Les configurations de la consignation globale des audits utilisent le type de serveur de notification Syslog. Si vous souhaitez transférer des logs d'audit à un Log Decoder, créez un serveur de notification du type Syslog.

Procédures	Référence/Instructions
2. Sélectionnez ou configurez un modèle de consignation des audits à utiliser.	Sélectionnez un modèle de consignation des audits pour le serveur de notification Syslog. Vous pouvez utiliser un modèle de consignation des audits par défaut ou définir votre propre modèle de consignation des audits. Les configurations de la consignation globale des audits utilisent le type de modèle de consignation des audits et un serveur de notification Syslog. Configurer des modèles pour les notifications fournit des informations supplémentaires. Pour les Log Decoders, utilisez le **Modèle CEF d'audit par défaut**. Vous pouvez ajouter ou supprimer des champs dans le modèle CEF (Common Event Format) si vous avez des exigences spécifiques. Définir un modèle pour la consignation globale des audits fournit des instructions. Pour les serveurs syslog tiers, vous pouvez utiliser un modèle de consignation d'audit par défaut ou définir votre propre format (CEF ou non-CEF). Définir un modèle pour la consignation globale des audits fournit des instructions et Variables de métaclés prises en charge pour la consignation globale des audits décrit les variables disponibles.
3. (Facultatif - Uniquement en cas d'utilisation avec un Log Decoder) Déployer l'analyseur Common Event Format (CEF) sur votre Log Decoder à partir de Live.	Vérifiez que vous avez déployé et activé la dernière version de l'analyseur Common Event Format à partir de Live. Les rubriques Rechercher et déployer des ressouces Live et Activer et désactiver les analyseurs de logs fournissent des instructions.

Procédures	Référence/Instructions
4. Définissez une configuration de consignation globale des audits, qui détermine comment les logs d'audit globaux sont transférés vers les systèmes Syslog externes.	La rubrique Définir une configuration de consignation globale des audits fournit des instructions. Après avoir ajouté la configuration de consignation globale des audits, les logs d'audit sont transférés au serveur de notification sélectionné dans la configuration.
5. Vérifiez que les logs d'audit globaux affichent les événements d'audit.	Testez vos logs d'audit pour vérifier qu'ils affichent les événements tels que définis dans votre modèle de consignation des audits. La rubrique Vérifier les logs d'audits globaux fournit des instructions.

Configurer une destination pour recevoir des logs d'audit globaux

Dans la Consignation globale des audits, les serveurs de notification Syslog sont les configurations qui définissent les destinations pour recevoir des logs d'audit globaux. Vous devez configurer un serveur de notification Syslog pour pouvoir utiliser la Consignation globale des audits. Vous pouvez définir un serveur syslog tiers ou un Log Decoder en tant que destination pour recevoir les logs d'audit.

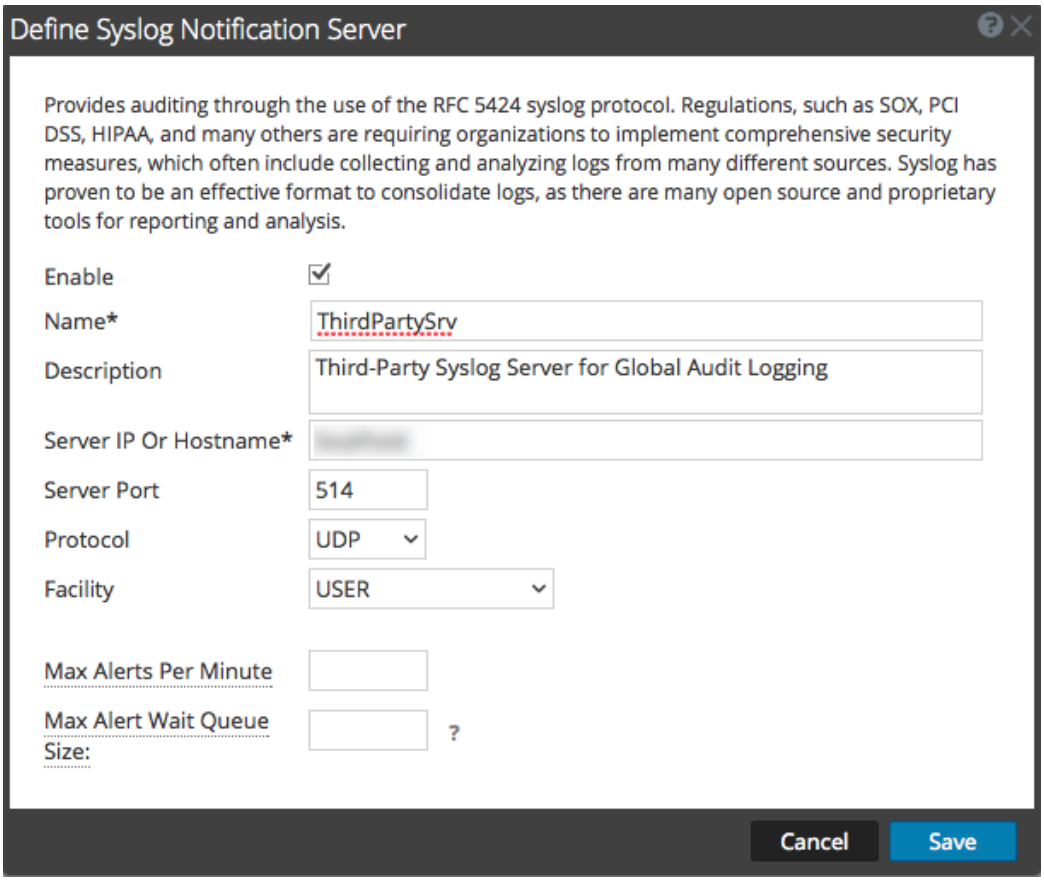
Configurer un Serveur de notification Syslog pour un serveur Syslog tiers

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Serveurs**.

   Remarque : Vous n'avez pas besoin de configurer l'onglet Résultat pour la consignation globale des audits.

4. Dans le menu déroulant  , sélectionnez **Syslog**.

   La boîte de dialogue **Définir un serveur de notification Syslog** s'affiche.



5. Configurez le serveur de notification Syslog comme décrit dans le tableau suivant.

Champ	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller le serveur syslog tiers.
Description	(Facultatif) Brève description du serveur de notification.
Adresse IP ou nom d'hôte du serveur	Adresse IP ou nom d'hôte du serveur syslog tiers.
Port de serveur	Numéro du port où s'effectue l'écoute par le processus Syslog cible.
Protocole	Protocole à utiliser pour transférer des logs d'audit formatés vers le serveur syslog tiers.

Champ	Description
Site	Fonctionnalité syslog à utiliser pour écrire des logs d'audit formatés sur le serveur syslog tiers.

Les champs **Nombre maximal d'alertes par minute** et **Taille max. file d'attente d'alertes** ne sont pas utilisés pour la consignation globale des audits.

6. Cliquez sur **Enregistrer**.

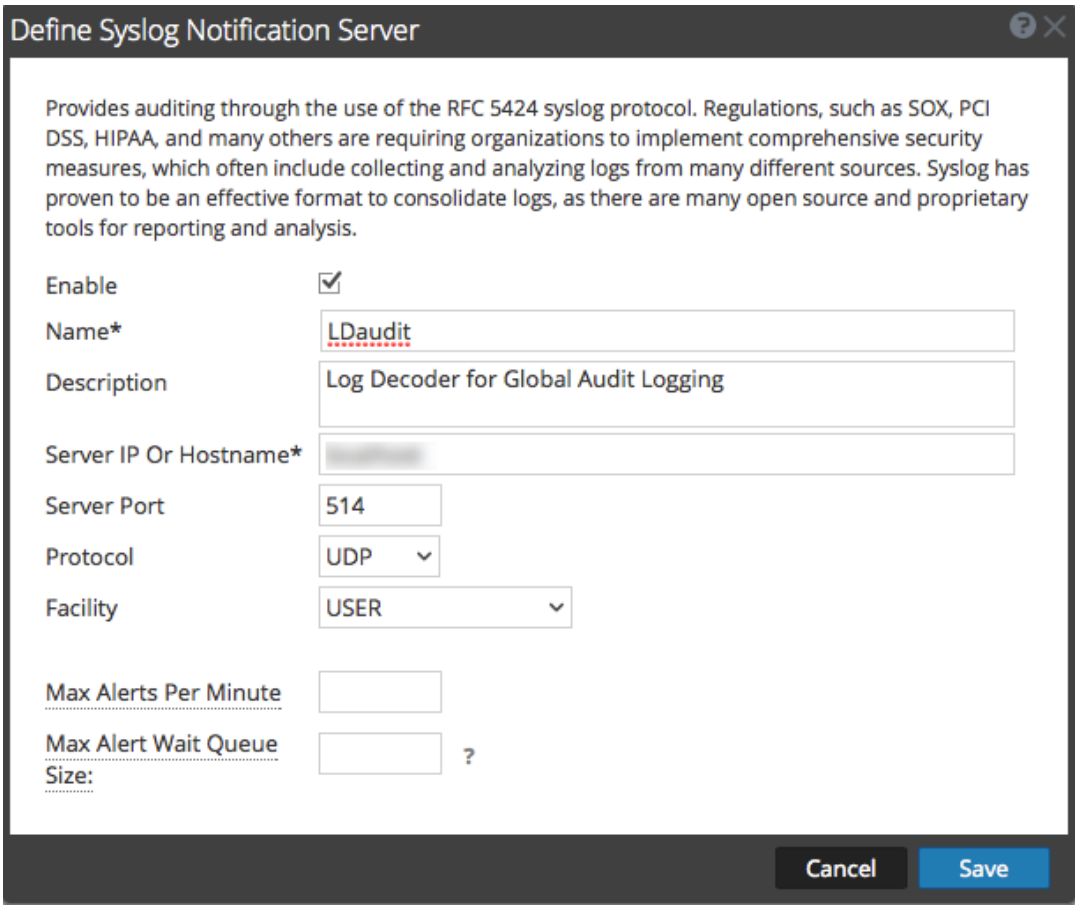
Configurer un serveur de notification Syslog pour un Log Decoder

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Serveurs**.

> **Remarque :** Vous n'avez pas besoin de configurer l'onglet Résultat pour la consignation globale des audits.

4. Dans le menu déroulant  , sélectionnez **Syslog**.

   La boîte de dialogue **Définir un serveur de notification Syslog** s'affiche.



5. Configurez le serveur de notification Syslog comme décrit dans le tableau suivant.

Champ	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller le serveur de notification syslog Log Decoder.
Description	(Facultatif) Brève description du serveur de notification.
Adresse IP ou nom d'hôte du serveur	Nom d'hôte ou adresse IP de Log Decoder.
Port de serveur	Numéro du port où s'effectue l'écoute par le processus Syslog cible.
Protocole	Protocole à utiliser pour transférer des logs d'audit formatés vers le Log Decoder.

Champ	Description
Site	Fonctionnalité Syslog à utiliser pour écrire des logs d'audit formatés sur le Log Decoder.

Les champs **Nombre maximal d'alertes par minute** et **Taille max. file d'attente d'alertes** ne sont pas utilisés pour la consignation globale des audits.

6. Cliquez sur **Enregistrer**.

Étapes suivantes

Sélectionnez un modèle de consignation des audits par défaut pour utiliser la Consignation globale des audits. Si nécessaire, vous pouvez définir votre propre modèle personnalisé. La rubrique Définir un modèle pour la consignation globale des audits fournit des informations supplémentaires.

Définir un modèle pour la consignation globale des audits

Cette rubrique fournit des instructions sur la manière de définir un modèle de consignation d'audits à utiliser dans le cadre de la consignation globale des audits. Avant de configurer la consignation globale des audits, configurez un serveur de notification Syslog et sélectionnez un modèle de consignation d'audit. Vous pouvez choisir d'utiliser un modèle de consignation d'audit par défaut ou vous pouvez définir votre propre modèle.

NetWitness Suite comprend deux modèles de consignation d'audit par défaut :

- **Modèle CEF d'audit par défaut**: Vous pouvez utiliser ce modèle pour les serveurs Syslog tiers et Log Decoders.
- **Format lisible d'audit par défaut**: Vous pouvez utiliser ce modèle uniquement pour les serveurs Syslog tiers. Ne transférez pas les messages de ce modèle vers un Log Decoder.

La première procédure fournit les instructions permettant de définir un modèle de consignation d'audit pour un Log Decoder. Le modèle de consignation d'audit définit les champs format et message des logs d'audit envoyés au serveur Syslog tiers ou Log Decoder.

Les modèles de consignation globale des audits que vous définissez pour un Log Decoder utilisent le format Common Event Format (CEF) et doivent répondre aux exigences standard spécifiques suivantes :

- Contient les en-têtes CEF dans le modèle.
- Utilisez uniquement les extensions (Key=Value) répertoriées dans le tableau Métaclés CEF prises en charge.
- Assurez-vous que les extensions sont au format `key=${string}<space>key=${string}`.

La deuxième procédure fournit des instructions sur la façon de définir un modèle personnalisé de consignation globale des audits au format lisible par l'homme pour un serveur Syslog tiers. Pour les serveurs Syslog tiers, vous pouvez définir votre propre format (CEF ou non-CEF).

Définir un modèle de consignation globale des audits pour un Log Decoder

Vous pouvez utiliser le **modèle CEF d'audit par défaut** pour envoyer des logs d'audit globaux à un Log Decoder. Pour définir votre propre modèle :

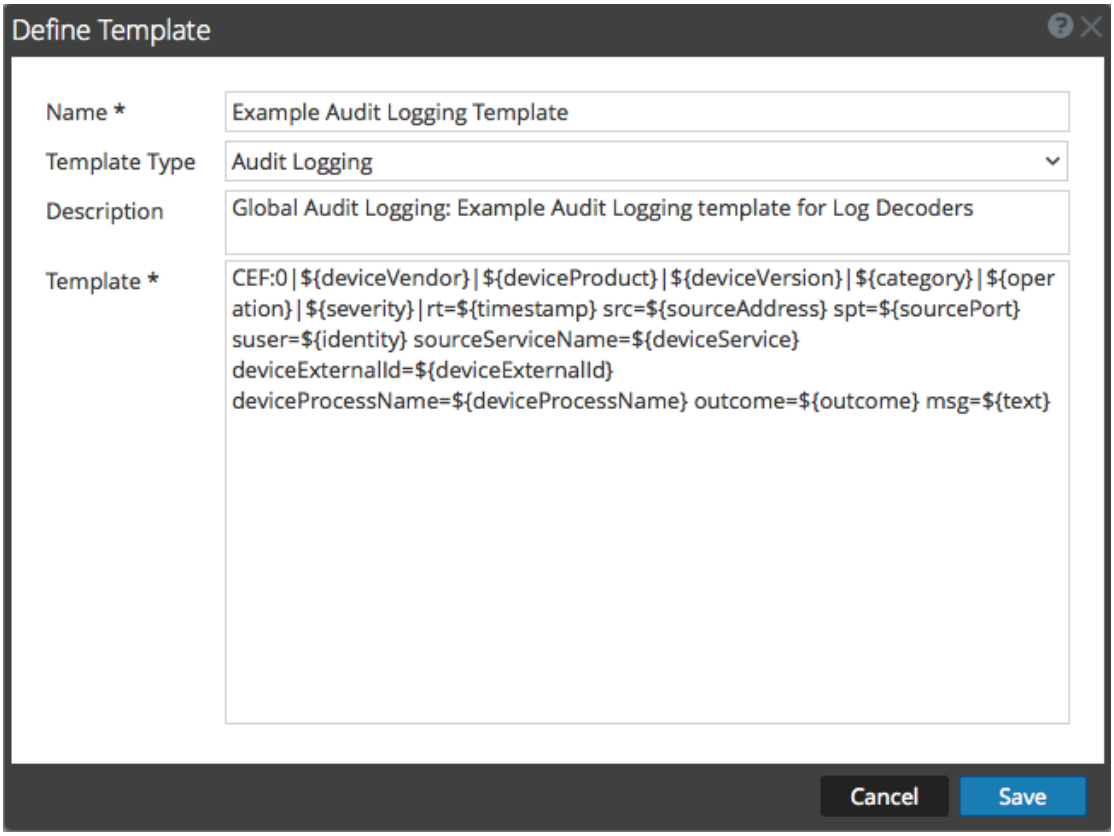
1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Cliquez sur l'onglet **Modèles**.
4. Cliquez sur + pour configurer un modèle.
5. Dans la boîte de dialogue **Définir un modèle**, fournissez les informations suivantes :
   a. Dans le champ **Nom**, saisissez un nom pour le modèle.
   b. Dans le champ **Type de modèle**, sélectionnez le type de modèle **Consignation des audits**.
   c. Dans le champ **Description**, saisissez une petite description du modèle.
   d. Dans le champ **Modèle**, saisissez le format du modèle de consignation globale des audits.
   Le format suivant est un modèle personnalisé fourni à titre d'exemple. Il se distingue du modèle CEF par défaut.

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome}
msg=${text}
```

   L'en-tête Syslog CEF mis en surbrillance doit se conformer à la norme CEF et constitue une exigence pour l'analyseur CEF dans le Log Decoder. Les autres clés sont facultatives, mais vous pouvez les configurer. Reportez-vous aux clés méta prises en charge par l'analyseur CEF du Log Decoder dans la table Métaclés CEF prises en charge.

Remarque : Utilisez toutes les extensions au format suivant : `deviceProcessName=${deviceProcessName} outcome=${outcome}` Ajoutez un `<space>` entre chaque paire key=${string} dans la section des clés d'extension.

6. Cliquez sur **Enregistrer**.



Après avoir défini le modèle de consignation des audits CEF, vérifiez que vous avez déployé et activé la dernière version de l'analyseur CEF (Common Event Format) de Live. Les rubriques « Rechercher et déployer des ressouces Live » et « Activer et désactiver les analyseurs de logs » fournissent des instructions.

Remarque : Si vous avez besoin d'utiliser une clé méta spécifique pour Investigations et Reporting, assurez-vous que les clés méta que vous avez sélectionnées sont indexées dans le fichier **table-map.xml** dans le Log Decoder. Si ce n'est pas le cas, suivez la rubrique Maintenir les fichiers de mappage des tables dans le *Guide de mise en route des hôtes et des services* pour mettre à jour les mappages des tables. Assurez-vous que les clés méta sont également indexées dans **index-concentrator.xml** du Concentrator. La rubrique Modifier un fichier d'index de service du *Guide de configuration de l'hôte et des services* fournit des informations supplémentaires.

Définir un modèle personnalisé de consignation globale des audits

Pour les serveurs syslog tiers, vous pouvez définir votre propre format de modèle (CEF ou non CEF). Vous pouvez utiliser le modèle **Format lisible d'audit par défaut** pour envoyer des logs d'audit globaux à un serveur syslog tiers dans un format qui est plus facile à lire que le format CEF. Si vous souhaitez définir votre propre modèle dans un format lisible, suivez cette procédure.

Pour les Log Decoders, vous devez utiliser un modèle CEF avec certaines exigences spécifiques. La procédure *Définir un modèle de consignation globale des audits pour un Log Decoder* présentée ci-dessus fournit des instructions pour la création d'un modèle au format CEF.

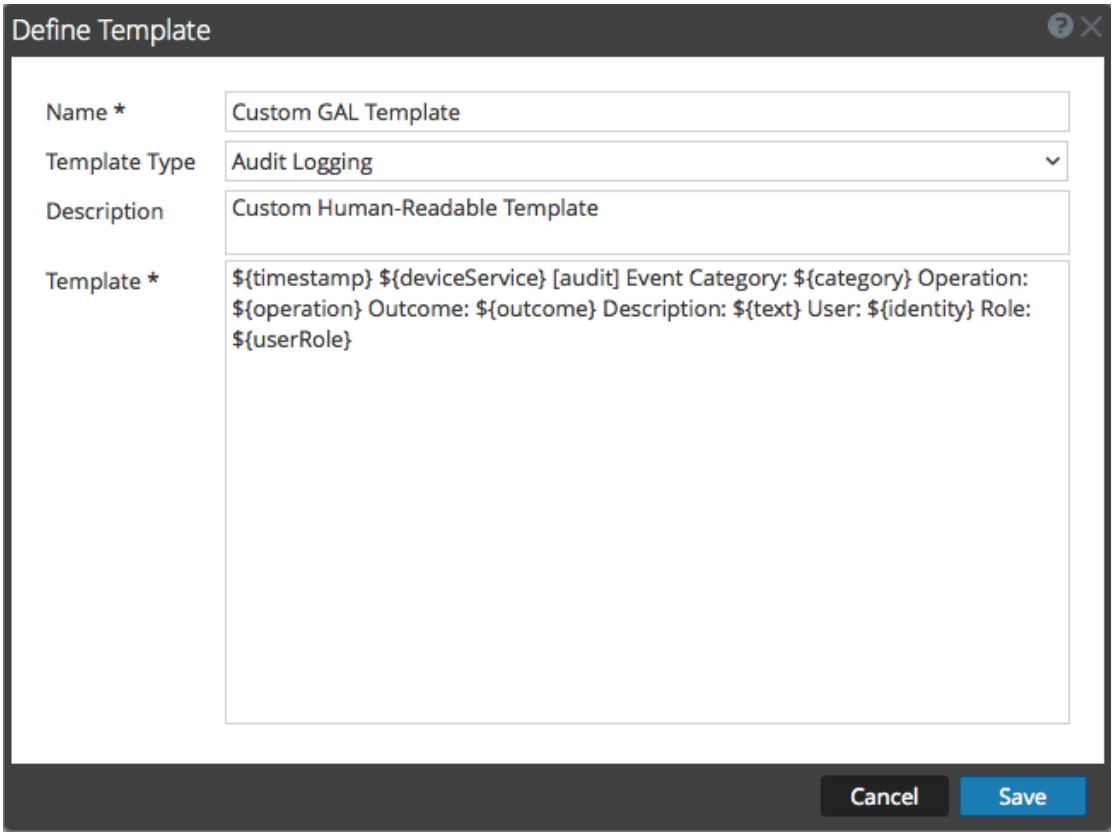
Pour définir un modèle global personnalisé de consignation d'audit dans un format lisible :

1. Accédez à **ADMIN > Système**.
2. Dans le volet de navigation de gauche, sélectionnez **Notifications**.
3. Cliquez sur l'onglet **Modèles**.
4. Cliquez sur  pour configurer un modèle.
5. Dans la boîte de dialogue **Définir un modèle**, fournissez les informations suivantes :
   a. Dans le champ **Nom**, saisissez un nom pour le modèle.
   b. Dans le champ **Type de modèle**, sélectionnez le type de modèle **Consignation des audits**.
   c. Dans le champ **Description**, saisissez une petite description du modèle.
   d. Dans le champ **Modèle**, saisissez le format du modèle de consignation globale des audits. L'exemple suivant est dans un format lisible avec des variables de clés méta sélectionnées.

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
Operation: ${operation} Outcome: ${outcome} Description: ${text}
User: ${identity} Role: ${userRole}
```

Vous pouvez utiliser l'une des variables de clés méta qui sont prises en charge par la consignation globale des audits indiquée dans le tableau Variables de métaclés prises en charge pour la consignation globale des audits.

6. Cliquez sur **Enregistrer**.



L'exemple suivant montre les logs d'audit globaux dans un format lisible correspondant à ce modèle :

```
06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 NW_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

Étape suivante

La rubrique Définir une configuration de consignation globale des audits fournit les instructions permettant de définir la configuration de la consignation d'audit globale pour NetWitness Suite.

Définir une configuration de consignation globale des audits

Cette rubrique indique aux administrateurs comment définir une configuration de consignation globale des audits. Cette procédure n'est obligatoire que si vous configurez la consignation centralisée des audits dans votre environnement. Ces configurations globales définissent la manière dont les logs d'audit globaux sont transmis au système syslog externe ou aux Log Decoders. Les logs d'audit sont transmis aux serveurs de notification sélectionnés.

Conditions préalables

Avant de commencer cette procédure, configurez les éléments suivants que vous utiliserez pour la consignation globale des audits :

- Serveur de notification syslog
- Modèle de consignation des audits

Vous pouvez configurer le serveur et le modèle de notification sur le panneau Notifications globales. Pour accéder au panneau Notifications globales, cliquez sur le lien **Afficher les paramètres** dans le Panneau Configuration de la consignation globale des audits. Vous ne pouvez définir qu'un type Syslog de serveur de notification pour la consignation globale des audits. Pour les Log Decoders, utilisez un type Syslog de serveur de notification et un modèle de consignation des audits au format CEF (Common Event Format). Vous pouvez utiliser un modèle de consignation des audits par défaut ou définir vos propres modèles. Vous pouvez créer plusieurs modèles de consignation des audits et serveurs de notification Syslog et les utiliser avec vos configurations de configuration globale des audits.

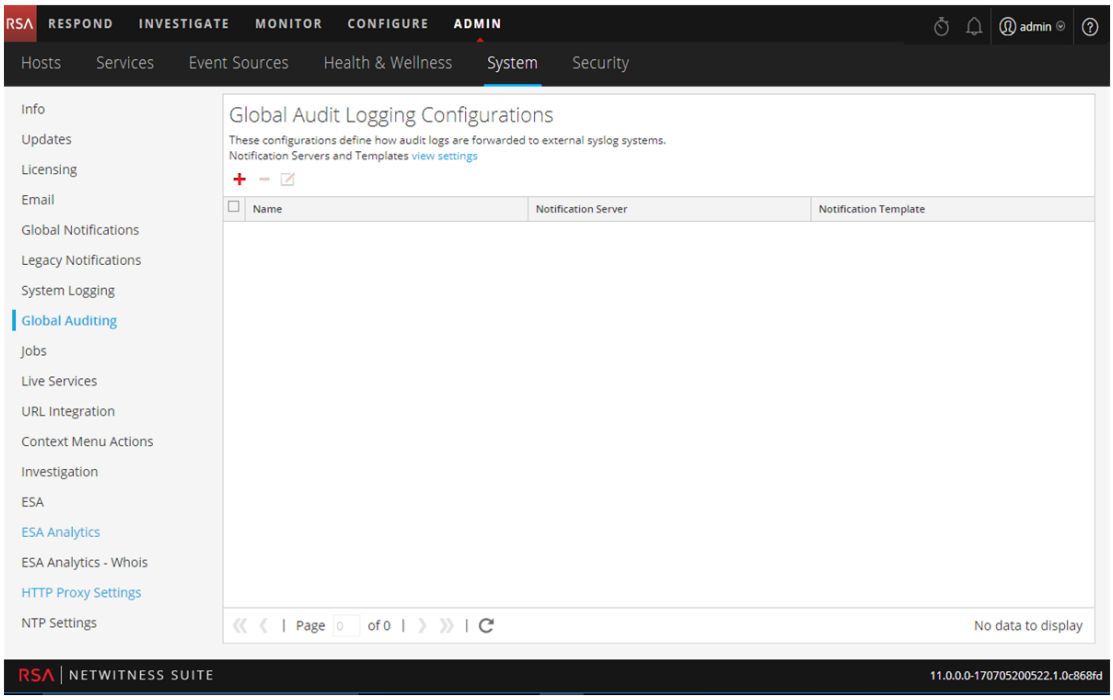
Si vous transmettez des logs d'audit globaux à un Log Decoder, déployez le parser CEF (Common Event Format) sur votre Log Decoder depuis Live.

Ajouter une configuration de consignation d'audit globale

1. Accédez à **ADMIN > Système**.

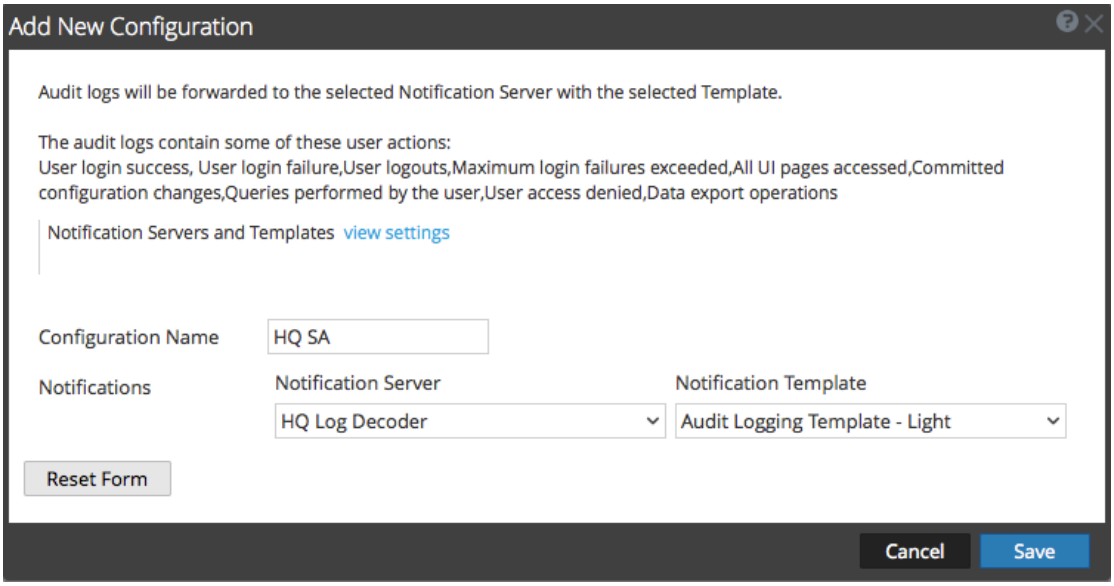
2. Dans le panneau des options, sélectionnez **Audit global**.

   Le panneau **Configuration de la consignation globale des audits** s'affiche.



3. Cliquez sur + pour ajouter une configuration de consignation globale des audits.

   La boîte de dialogue **Ajouter une nouvelle configuration** apparaît.



4. Dans le champ **Nom de configuration**, saisissez un nom unique pour la configuration de consignation d'audit globale. Par exemple, vous pouvez créer une configuration pour un type

de configuration de consignation globale des audits spécifique, par exemple SG SA pour une configuration de siège social NetWitness Suite.

5. Dans la rubrique **Notifications**, sélectionnez le **serveur de notification** syslog à utiliser pour cette configuration. Il s'agit de la destination à laquelle envoyer les logs d'audit globaux.
6. Sélectionnez le **modèle de notification** de consignation d'audit à utiliser pour cette configuration. Le modèle de consignation des audits définit le format et les champs des messages de logs d'audit à envoyer.
7. Cliquez sur **Enregistrer**.

La boîte de dialogue Ajouter une nouvelle configuration fournit des informations complémentaires et des exemples d'actions utilisateur consignées. Pour obtenir la liste des types de message consignés par les différents composants NetWitness Suite, reportez-vous à la rubrique Panneau Configuration de la consignation globale des audits.

Modifier une configuration de consignation globale des audits

Cette rubrique fournit des instructions sur la manière de modifier une configuration de consignation globale des audits. Vous pouvez modifier une configuration de consignation globale des audits pour changer la destination des logs d'audit globaux de vos audits d'utilisateur en sélectionnant un serveur de notification différent. Vous pouvez aussi modifier les champs de format et de message des entrées des logs d'audit en sélectionnant un modèle de notification différent. Pour modifier le serveur de notification ou le modèle de notification, utilisez le panneau Notifications globales. Pour accéder au panneau Notifications globales, cliquez sur le lien **Afficher les paramètres** dans le panneau Configuration de la consignation globale des audits.

Vous ne pouvez pas modifier les types d'actions d'utilisateur NetWitness Suite qui sont consignés et envoyés dans les logs d'audit globaux.

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Audit global**.
3. Dans le panneau **Configuration de la consignation globale des audits**, sélectionnez une configuration à modifier et cliquez sur  .
4. Dans la boîte de dialogue **Ajouter une nouvelle configuration**, modifiez la configuration de consignation globale des audits comme il est nécessaire. Vous pouvez modifier le **nom de configuration** et sélectionner un **serveur de notification** ou un **modèle** différent.
5. Cliquez sur **Enregistrer**.

Supprimer une configuration de consignation globale des audits

La suppression d'une configuration globale des audits ne supprime pas le serveur et le modèle de notification associés. Après la suppression, le transfert des logs d'audits globaux, spécifiés dans cette configuration, est interrompu.

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Audit global**.
3. Dans le panneau **Configuration de la consignation globale des audits**, sélectionnez une configuration à supprimer et cliquez sur .

   Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Yes**.

   La configuration sélectionnée est supprimée.

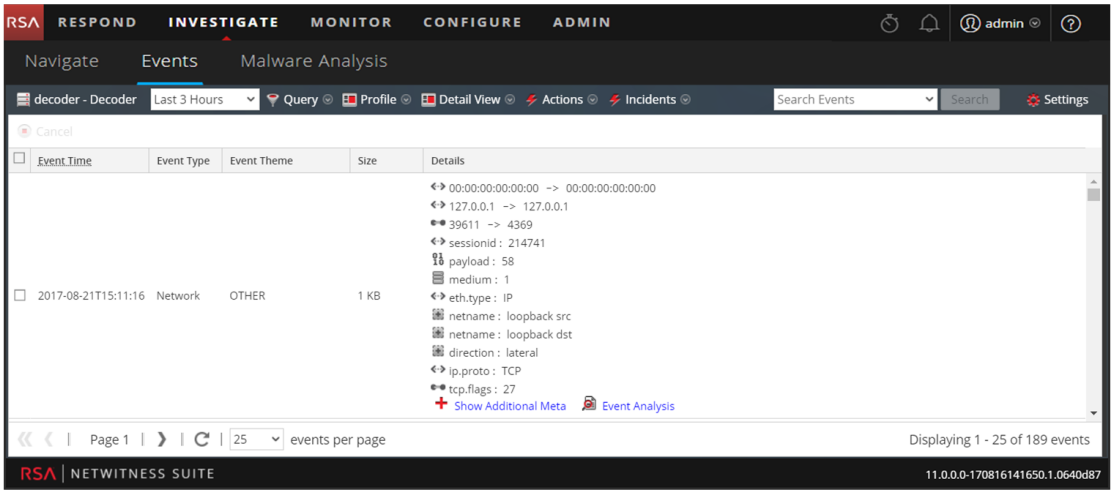
Vérifier les logs d'audits globaux

Cette rubrique fournit des instructions sur le mode de configuration des logs d'audit globaux. Après avoir configuré la consignation globale des audits, il est recommandé de tester vos logs d'audit globaux pour vous assurer qu'ils contiennent les événements d'audit tels que définis dans votre modèle de consignation des audits global.

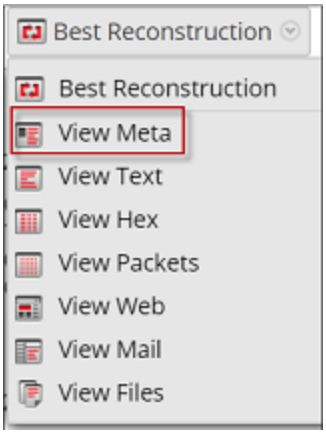
Avant de démarrer cette tâche, suivez les étapes détaillées dans Configurer la consignation globale des audits.

Pour afficher et vérifier les logs d'audit globaux, si vous utilisez un Log Decoder :

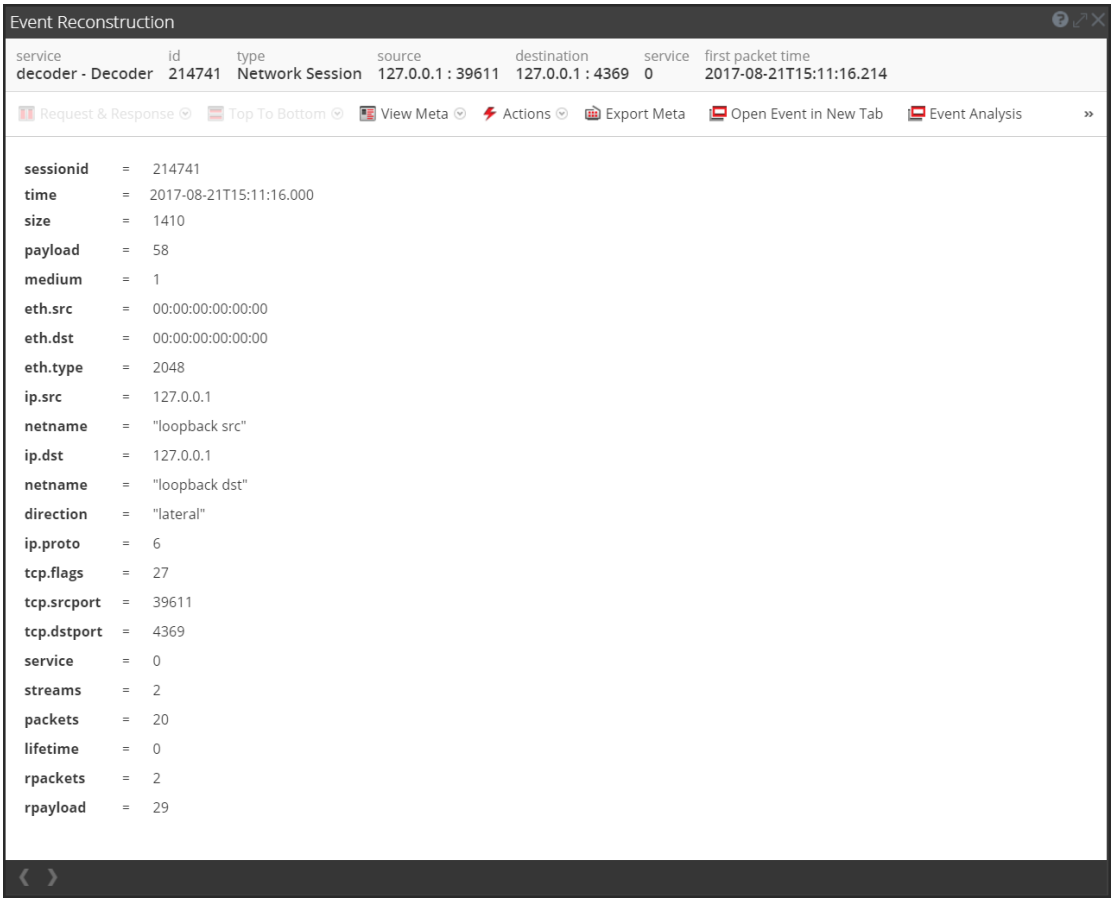
1. Accédez à **Enquêter > Événements**.
2. Dans la vue Parcourir, sélectionnez le Log Decoder et cliquez sur **Parcourir**.



3. Comparez les champs dans les logs d'audit globaux avec les champs définis dans le modèle de consignation des audits global que vous avez utilisé dans votre configuration de consignation d'audit globale.
4. Double-cliquez sur un log, puis, dans la boîte de dialogue Reconstruction d'événement, sélectionnez **Afficher les métadonnées**.



5. Vérifiez que les métadonnées que vous souhaitez auditer sont correctes.



Exemple de sortie CEF

L'exemple suivant affiche les logs d'audit globaux pour un modèle de consignation des audits Common Event Format (CEF).

Modèle :

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome} msg=${text}
```

Exemples de logs :

```
2017-04-09T18:45:46.313096+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|login|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=51366 suser=admin sourceServiceName=LOG_DECODER
deviceExternalId=96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
2017-04-09T18:45:46.322132+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.204.33 spt=47690 suser=admin sourceServiceName=BROKER
deviceExternalId= 314fb8c8-afe4-4249-9468-a36035008a52 outcome=success
2017-04-09T18:45:46.325792+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=59495 suser=admin sourceServiceName=CONCENTRATOR
deviceExternalId= 96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
```

Où `<hostname>` est le nom d'hôte de l'en-tête syslog (alias.host).

Pour les modèles CEF, si un événement d'audit ne possède pas de valeur pour un champ dans le modèle, le champ de l'événement correspondant arrivant sur le serveur syslog tiers ou le Log Decoder sera supprimé.

Exemple de sortie au format lisible

L'exemple suivant présente des logs d'audit globaux pour un modèle de format lisible de consignation d'audit sur un serveur syslog tiers.

Modèle :

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
```

Operation: ${operation} Outcome: ${outcome} Description: ${text}

User: ${identity} Role: ${userRole}

Exemples de logs :

```
06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY
```

```
Apr 06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY
```

```
Apr 06 2017 14:16:04 SA_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

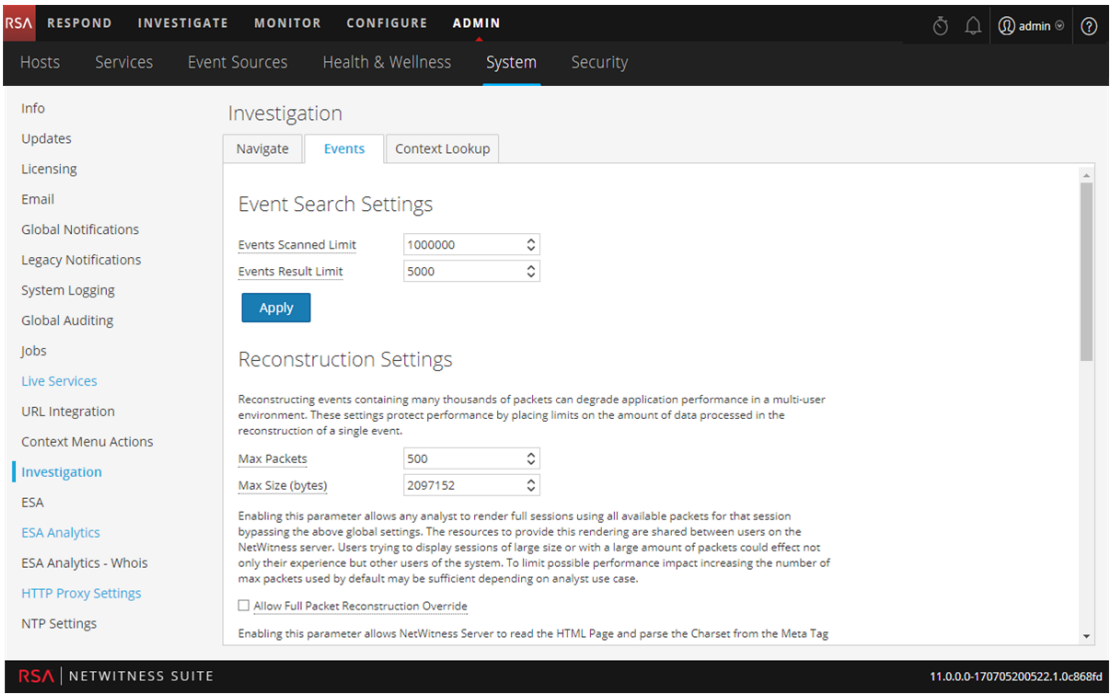
Configurer les paramètres du module Investigation

Cette rubrique fournit des instructions pour les administrateurs qui configurent les paramètres qui s'appliquent à toutes les investigations sur l'instance NetWitness Suite en cours de configuration. Les paramètres permettant de configurer et de régler le comportement d'une investigation NetWitness Suite sont disponibles dans la vue Système > panneau Investigation. Ces paramètres s'appliquent à toutes les investigations et reconstructions sur l'instance active de NetWitness Suite.

Configurer les paramètres Naviguer, Événements et Recherche contextuelle

1. Accédez à **ADMIN > Système.**
2. Dans le panneau des options, sélectionnez **Investigation.**

   Le panneau Configuration des investigations s’affiche.



3. Sous l'onglet **Naviguer**, dans le champ **Générer les paramètres de threads**, sélectionnez le nombre maximal de valeurs de clé méta qui sont chargées par un même utilisateur dans la vue Naviguer. Cliquez sur **Appliquer**.
4. Sous l'onglet **Naviguer**, dans la rubrique **Paramètres de coordonnées parallèles**, définissez les limites maximales des métavaleurs analysées et des résultats des métavaleurs pouvant être incluses dans une visualisation de coordonnées parallèles. Pour obtenir de meilleures performances, voici les paramètres recommandés : Limite d'analyse de valeurs méta -100000 et Limite de résultat de valeurs méta à 1 000-10 000
   Cliquez sur **Appliquer**.
5. Sous l'onglet **Événements**, dans la rubrique **Paramètres de recherche d'événements**, définissez le nombre maximal d'événements analysés et de résultats d'événements affichés lorsqu'un analyste mène une recherche d'événements dans la vue Événements. Cliquez sur **Appliquer**.
6. Sous l'onglet **Événements**, dans la rubrique **Paramètres de reconstruction**, définissez les limites de la quantité de données traitées dans le cadre de la reconstruction d'un seul événement. Les valeurs par défaut sont 100 paquets et 2 097 152 octets au maximum. Si les analystes constatent un ralentissement des performances lors de la reconstruction des sessions en mode Investigation, les paramètres de reconstruction peuvent nécessiter un ajustement. Cliquez sur **Appliquer**.

Attention : La définition d'une valeur plus élevée affecte les performances de Serveur NetWitness en augmentant le temps et la mémoire utilisés pour créer la reconstruction d'un événement. Définir la valeur à zéro désactive toutes les limites et peut conduire à une panne de Serveur NetWitness.

7. (Facultatif) Sous l'onglet **Événements**, dans la rubrique **Paramètres de reconstruction de la vue Web**, activez l'utilisation des fichiers de prise en charge dans une reconstruction de vue Web, puis configurez les paramètres supplémentaires pour calibrer les reconstructions des vues Web. Cela comprend l'intervalle de temps (en secondes) pour analyser les événements connexes, le nombre maximum d'événements liés à l'analyse et les remplacements des paramètres de reconstruction pour une utilisation avec des reconstructions de vue Web. Cliquez sur **Appliquer**.
8. Sous l'onglet **Recherche contextuelle**, gérez le mappage des types méta du service Context Hub avec les clés méta dans Investigation. Vous pouvez ajouter des clés méta à la liste des types méta pris en charge par le service Context Hub sous Investigation, ou les supprimer. Les procédures associées à cet onglet sont fournies dans la rubrique « Gérer le mappage du type de méta et de la clé méta » dans le *Guide Investigation et Malware Analysis*.

Effacer le cache de reconstruction pour les services

Sous Paramètres du cache de reconstruction, les administrateurs peuvent effacer le cache pour un ou plusieurs services. Par exemple, l'administrateur peut effacer le cache pour un Broker seulement, un Broker et Decoder ou tous les services connectés. Voici quelques exemples des causes de cache obsolète utilisé dans une reconstruction.

- Les services en aval peuvent avoir leurs sessions invalidées ou leurs données réinitialisées. À titre d'exemple, si l'Investigation parcourt un Broker et un Concentrator ou si un Decoder fait l'objet d'une réinitialisation de données, les métadonnées et les données de session du service de procédure d'enquête (Broker) ne correspondent pas au contenu si le service en aval a été réinitialisé et renseigné à nouveau. La reconstruction en mode Investigation affiche le contenu du cache, ce qui ne correspond pas au contenu réel. Même si le Decoder est hors ligne, le contenu est toujours affiché dans la reconstruction du Broker. Effacer le cache sur le Broker contraint NetWitness Suite à prendre contact avec le service Decoder et un message d'erreur est renvoyé car le Decoder est hors ligne.
- L'autre cas où le cache peut être obsolète, c'est lorsque l'ID d'un service en aval change. Cela peut se produire lors de l'exportation, l'importation, la suppression et l'ajout de services à NetWitness Suite car NetWitness Suite peut réutiliser les ID de service. Dans ce cas,

l'effacement du cache sur le Broker permet à NetWitness Suite de demander à récupérer les données des services.

Pour effacer le cache de reconstruction, exécutez l'une des opérations suivantes :

1. Pour effacer le cache d'un ou de plusieurs services, sélectionnez les services, puis cliquez sur **Effacer le cache pour les services sélectionnés**.
2. Pour effacer le cache de tous les services répertoriés, cliquez sur **Effacer le cache pour tous les services**
   . Le cache de reconstruction pour les services sélectionnés est effacé. NetWitness Suite envoie une demande de données pour les services.

Configurer les paramètres des services Live

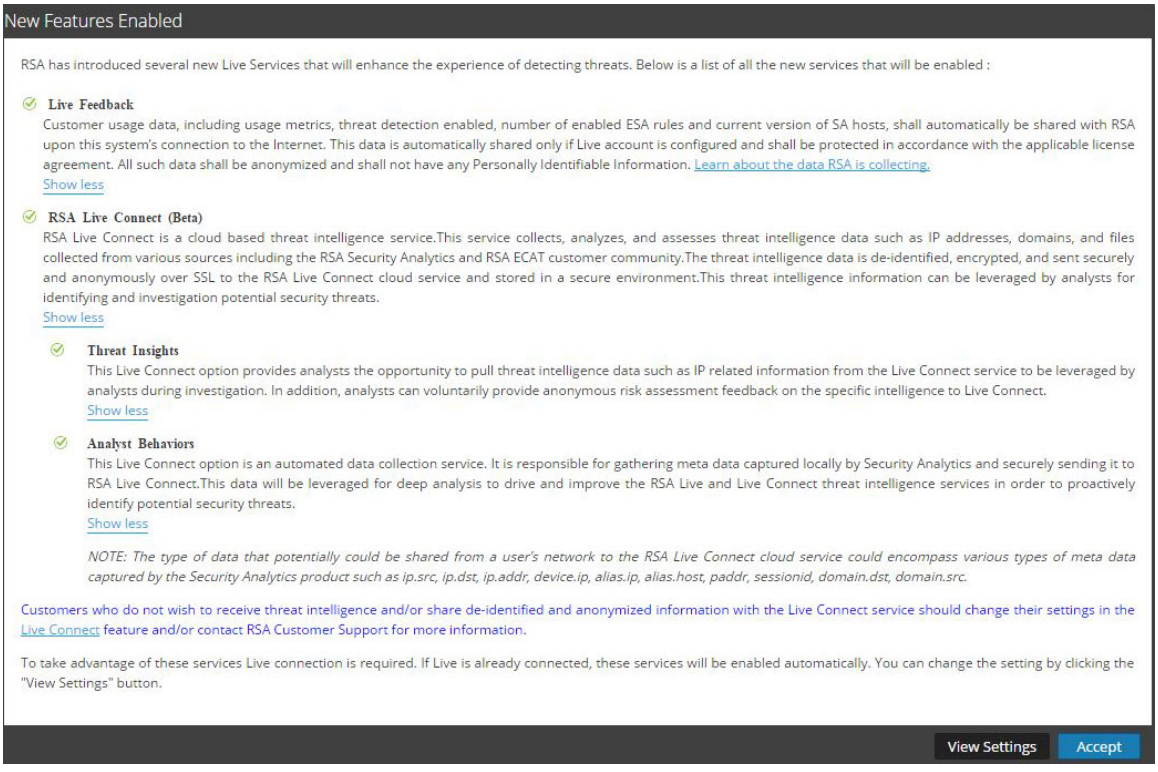
Les options de configuration des services Live se trouvent dans la vue Système > panneau Configuration des services Live. Le panneau Configuration de Live vous permet de configurer :

- Compte Live
- Calendrier des mises à jour du contenu Live et préférences de notification des mises à jour.
- Participation dans Services Live Feedback.
- Partage d'utilisation du contenu Live
- RSA Live Connect (Bêta)

Condition préalable

Pour activer votre compte Live pour NetWitness Suite, veuillez contacter le Support Clients RSA. Lorsque vous aurez obtenu confirmation que votre compte Live a été configuré, vous pourrez configurer et tester la connexion au serveur CMS.

Lorsque vous vous connectez à NetWitness Suite pour la première fois, la boîte de dialogue **Nouvelles fonctions activées** s'affiche.



Lorsque vous cliquez sur **Accepter**, vous acceptez automatiquement ce qui suit :

- Participation à Live Feedback.
- Utiliser les fonctions de Live Connect pour recevoir les données de renseignements sur les menaces.
- Autoriser NetWitness Suite à envoyer anonynyment des données techniques relatives à votre environnement à RSA.

Si vous cliquez sur **Afficher les paramètres**, vous êtes redirigé vers l'interface utilisateur des services Live pour voir les paramètres de Live Feedback and Live Connect Threat Data Sharing. Si vous n'avez pas encore configuré votre compte Live, un écran masqué est affiché.

Pour plus d'informations sur Analyst Behaviors et Data Sharing, reportez-vous à la rubrique **Commentaires et partage de données NetWitness Suite** dans le *Guide de gestion des services Live*.

À propos de la participation à Live Feedback

Lorsque vous participez à Live Feedback, les informations pertinentes sont collectées en vue de procéder à des améliorations. Pour plus d'informations sur Live Feedback, reportez-vous à la rubrique Présentation de Live Feedback.

Lorsque vous installez NetWitness Suite, l'application vous invite à participer à Live Feedback. Pour plus d'informations, consultez Configurer les paramètres des services Live.

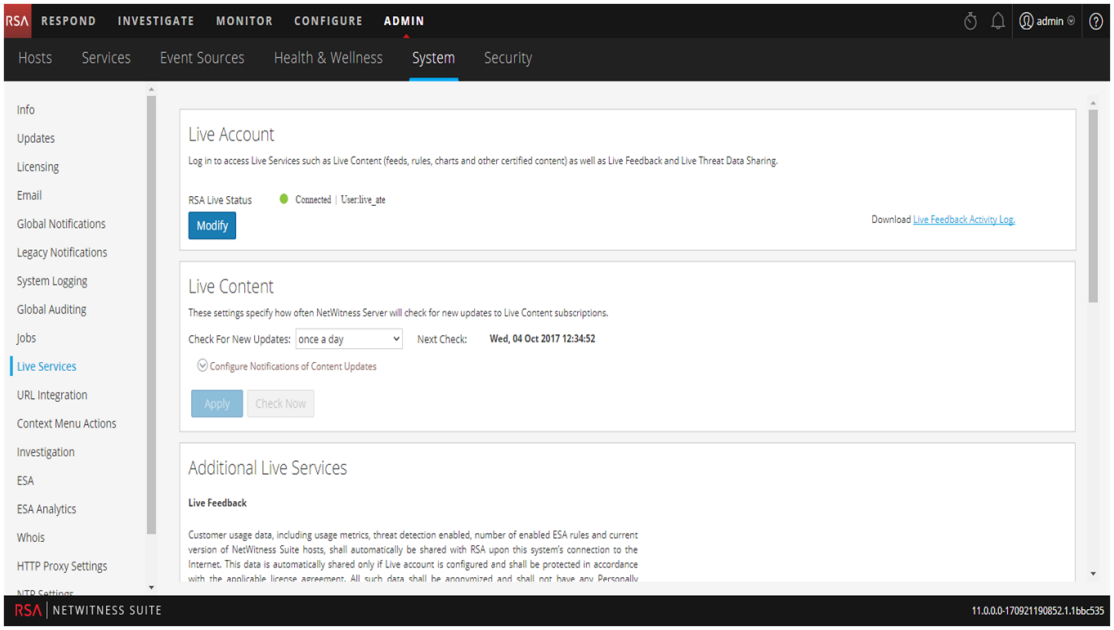
Si nécessaire, vous pouvez télécharger manuellement les données d'utilisation historiques et les partager avec RSA. Pour plus d'informations sur la façon de télécharger les données d'utilisation historiques et les partager avec RSA, reportez-vous à la rubrique Télécharger des données vers RSA pour Live Feedback.

Cette rubrique contient les procédures suivantes :

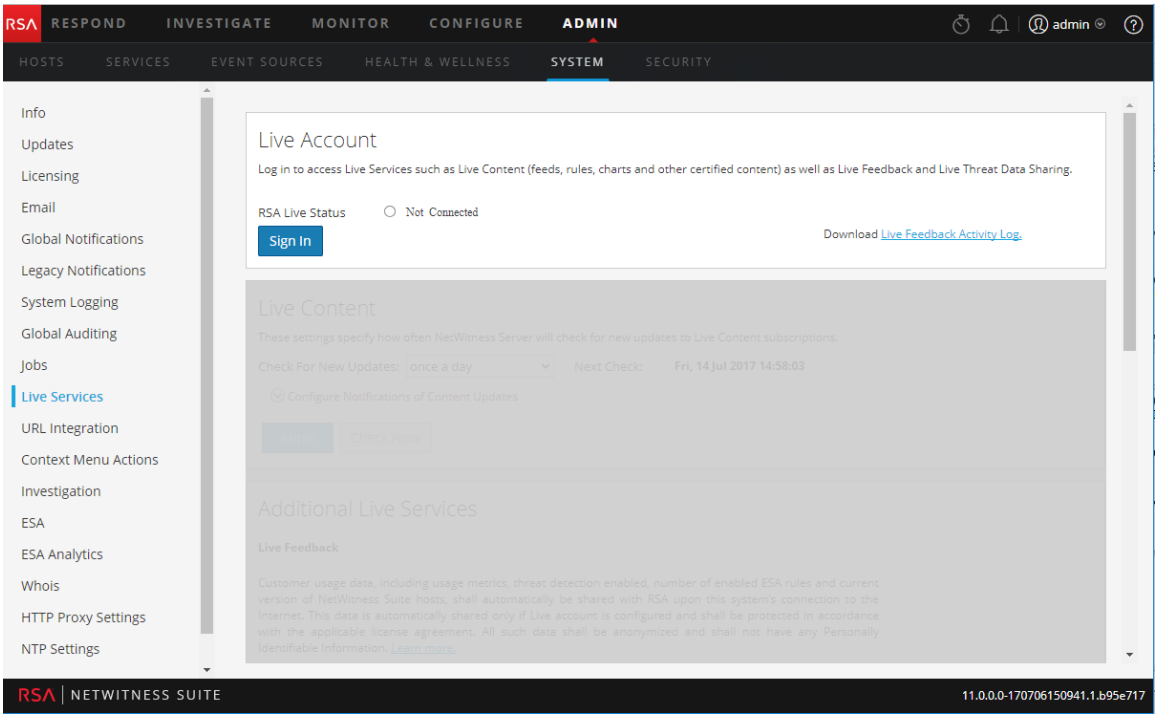
- Accéder au panneau de configuration des Services Live
- Configurer le compte Live
- Configurer l'intervalle de synchronisation et les notifications du contenu Live
- Forcer la synchronisation immédiate
- Utiliser RSA Live Connect (Bêta)

Accéder au panneau de configuration des Services Live

1. Accédez à **ADMIN > SYSTÈME**.
2. Dans le panneau de navigation de gauche, sélectionnez **Services Live**.



Remarque : Si vous ne vous connectez pas avec les informations d'identification de votre compte Live, un écran masqué s'affiche.



Configurer le compte Live

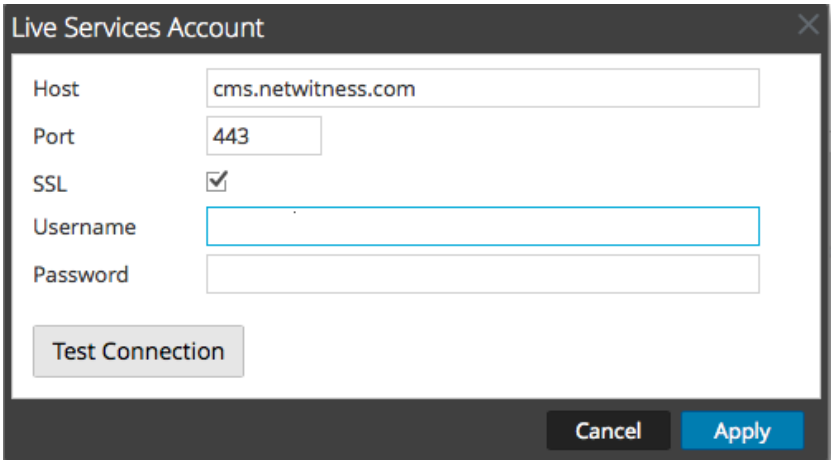
Dans la rubrique **Compte Live**, vous devez configurer le compte Live de l'utilisateur. Les informations requises pour configurer le compte Live de l'utilisateur sont le nom d'utilisateur, le mot de passe et l'URL Live pour le système de gestion de contenu (CMS). Ces informations sont fournies par le Service client.

Pour configurer un compte Live :

1. Dans la rubrique **Compte Live**, cliquez sur **Démarrer la session**.

   Remarque : Le bouton **Modifier** montre que le compte Live est configuré. Cliquez sur **Modifier** pour modifier l'utilisateur qui accède aux services Live.

2. Dans la boîte de dialogue Compte Live Services, saisissez l'hôte (généralement **cms.netwitness.com**) et votre nom d'utilisateur et mot de passe.

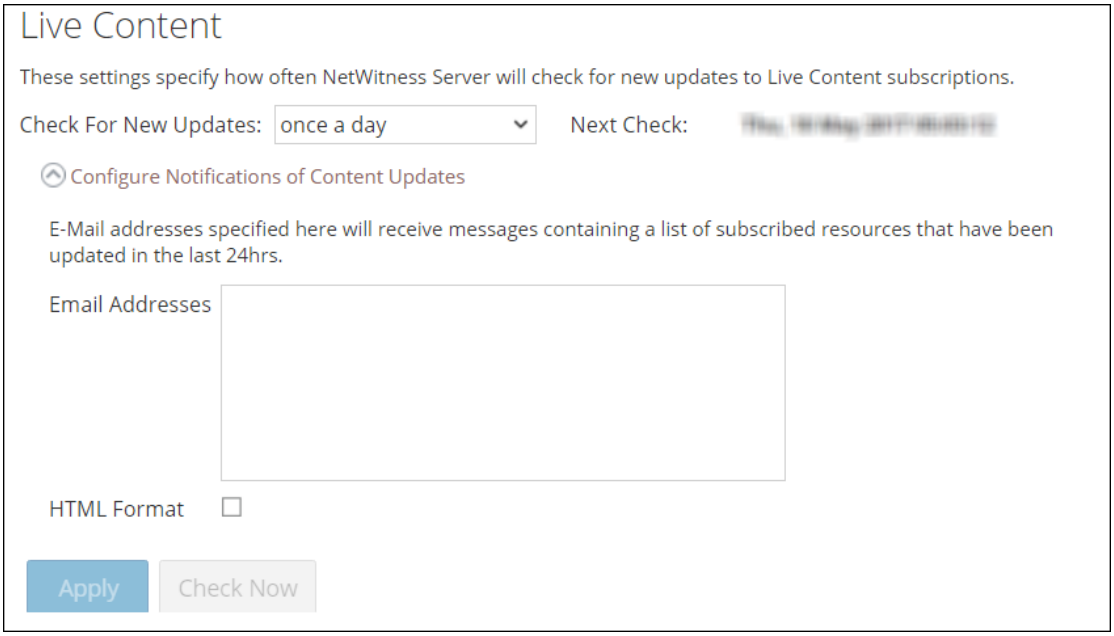


3. (Facultatif) Si vous utilisez un autre CMS, saisissez l'URL hôte du système de gestion de contenu (CMS). La valeur par défaut pointe vers le CMS avec l'URL **cms.netwitness.com**.
4. (Facultatif) Si vous utilisez un autre CMS, saisissez le port de communication permettant à Live d'envoyer des requêtes au système de gestion de contenu (CMS). La valeur par défaut de ce champ est **443**, qui est le port de communication du Content Management System.
5. (Facultatif) Si vous ne souhaitez pas utiliser SSL, décochez l'option **SSL**. (L'option SSL est activée par défaut.)
6. Cliquez sur **Tester la connexion** pour tester la connexion au CMS.
7. Pour enregistrer et appliquer la configuration, cliquez sur **Appliquer**.

Configurer l'intervalle de synchronisation et les notifications du contenu Live

Vous pouvez modifier l'intervalle auquel NetWitness Suite vérifie les nouvelles mises à jour du contenu Live :

1. Utilisez le champ **Rechercher de nouvelles mises à jour** pour modifier l'intervalle. Sélectionnez un intervalle dans la liste déroulante. La valeur par défaut pour ce paramètre est **une fois par jour**.



2. Pour que Services Live envoie des rapports de mises à jour à une ou plusieurs personnes, dans le champ **Adresses e-mail**, saisissez les adresses e-mail sous forme de liste séparée par une virgule, par exemple,
   john@company.com,ted@company.com,brian@company.com
3. (Facultatif) Pour recevoir les messages au format HTML plutôt qu'en texte brut, sélectionnez **Format HTML**.
4. Pour enregistrer et appliquer les paramètres, cliquez sur **Appliquer**.

   L'heure et la date de la prochaine synchronisation Live planifiée, en fonction de l'intervalle configuré pour la vérification, s'affichent.

Forcer la synchronisation immédiate

Au lieu d'attendre le prochain cycle de ressources planifié, cette option contraint Live à démarrer la synchronisation immédiate des ressources souscrites dans cette instance de NetWitness Suite. Vous pouvez utiliser cette option pour voir l'impact immédiat d'une modification de configuration. Par exemple, si un nouveau service a été ajouté ou si de nouvelles ressources ont été basculées vers le déploiement automatique. La synchronisation planifiée pourrait avoir lieu plusieurs heures plus tard si Services Live est configuré pour se synchroniser quelques fois par jour.

Attention : La synchronisation peut entraîner une recharge du parser si un FlexParser est déployé dans le cycle de mise à jour. Cela est acceptable une ou deux fois par jour, mais trop de recharges du parser dos à dos peut provoquer la perte de paquets au niveau du Decoder. S'il s'agit de la configuration initiale et que vous n'avez pas encore configuré les abonnements de ressources Live, n'effectuez pas la synchronisation maintenant. Attendez de configurer les abonnements.

Pour forcer la synchronisation immédiate, cliquez sur **Vérifier maintenant**. NetWitness Suite recherche les mises à jour dans les ressources souscrites.

Utiliser RSA Live Connect (Bêta)

RSA Live Connect est un service de renseignements sur les menaces basé sur le Cloud. Ce service collecte, analyse et évalue des données sur les menaces telles que les adresses IP, les domaines et les fichiers collectés auprès de diverses sources, notamment la communauté de clients RSA NetWitness® Suite et RSA NetWitness® Endpoint. RSA Live Connect comprend les fonctions suivantes :

- Threat Insights
- Comportements d'analyste

Threat Insights

Threat Insights fournit aux analystes la possibilité d'extraire des données de renseignement sur les menaces, telles que des informations liées à la propriété intellectuelle, du service Live Connect, qui seront exploitées par les analystes pendant l'investigation.

Par défaut, **Threat Insights** est activé dans la rubrique **Services Live supplémentaires**. Si le service Context Hub est configuré, Live Connect est automatiquement ajouté comme source de données pour Context Hub. Pour plus d'informations, reportez-vous à la rubrique **Configurer la source de données de Live Connect pour Context Hub** dans le *Guide de Configuration de Context Hub*.

Avec Live Connect comme source de données pour Context Hub, vous pouvez utiliser l'option Recherche contextuelle dans la vue Investigation > Naviguer ou la vue Investigation > Événements pour récupérer des informations contextuelles. Pour plus d'instructions, reportez-vous à la rubrique **Afficher un contexte supplémentaire pour un point de données** dans le *Guide Investigation et Malware Analysis*.

Comportements d'analyste

Comportements d'analyste est une fonction où les analystes participent au partage de données dans la communauté RSA. Il s'agit d'un service de collecte automatisée des données. Son objectif est de partager des données de renseignements sur les menaces potentielles sur le service de Cloud RSA Live Connect à des fins d'analyse. Le type de données pouvant potentiellement être partagé depuis votre réseau vers RSA Live Connect comprend différents types de métadonnées capturées par NetWitness Suite, telles que ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src. Pour plus d'informations sur Analyst Behaviors et Data Sharing, reportez-vous à la rubrique **Commentaires et partage de données NetWitness Suite** dans le *Guide de gestion des services Live*.

Présentation de Live Feedback

Cette section fournit une introduction à Live Feedback. Live Feedback collecte les informations pertinentes telles que les données d'attribution de licence pour les services Packet Decoder, Log Decoder et Malware Analysis, l'état de la détection des menaces activée ou désactivée, le nombre de règles ESA activées, ainsi que le numéro de version de tous les services de NetWitness Suite. Pour plus d'informations sur les données d'attribution de licence pour les services Packet Decoder, Log Decoder et Malware Analysis, consultez la section **Onglet Licences à suivi d'utilisation** dans le *Guide d'octroi de licence*. Les informations sont collectées pour améliorer les futures versions de NetWitness Suite. Vous serez automatiquement connecté à Live Feedback et vous ne pouvez pas désactiver cette option.

De plus, les informations sur l'utilisation du Contenu Live peuvent également être partagées avec RSA. Les metrics d'utilisation du Contenu Live pour les types de ressources accessibles à partir de Live **CONFIGURER > CONTENU LIVE > Critères de recherche**, par exemple le nombre total de règles d'application RSA, de règles de corrélation RSA, etc., peuvent être partagées avec RSA. Les informations collectées servent à améliorer l'utilisation du Contenu Live. Pour plus d'informations sur le partage de la configuration du Contenu Live, reportez-vous à la section Panneau Configuration des services Live.

À propos de la participation à Live Feedback

Lorsque vous participez à Live Feedback, les informations pertinentes sont collectées en vue de procéder à des améliorations. Pour plus d'informations sur Live Feedback, reportez-vous à la rubrique Présentation de Live Feedback.

Lorsque vous installez NetWitness Suite, l'application vous invite à participer à Live Feedback. Pour plus d'informations, consultez Configurer les paramètres des services Live.

Si nécessaire, vous pouvez télécharger manuellement les données d'utilisation historiques et les partager avec RSA. Pour plus d'informations sur la façon de télécharger les données d'utilisation historiques et les partager avec RSA, reportez-vous à la rubrique Télécharger des données vers RSA pour Live Feedback.

Remarque : Live Feedback est activé uniquement si vous avez configuré votre compte Live.

Les données Live Feedback sont au format JSON, comme indiqué ci-dessous. Lorsque vous vous connectez avec vos informations d'identification de compte Live, un fichier JSON chiffré est automatiquement téléchargé sur les serveurs RSA quotidiennement.

Fichier JSON

Le fichier JSON comprend des informations relatives aux données d'utilisation d'un composant ou d'un ensemble de composants. Dans le cas d'un ensemble de composants avec le même ID de licence, les données d'utilisation de tous les composants sont agrégées et représentées sous forme d'un composant appelé Habilitations. Toutefois, même s'il existe un seul composant comme un Log Decoder ou Decoder, un composant Habilitations sera généré et affichera les données d'utilisation pour un seul composant. Cette agrégation concerne les composants, à savoir les Log Decoders, Decoders ou Malware Analysis.

Remarque : La version de Habilitations est toujours la version 0, étant donné qu'il s'agit de l'agrégation des données de licence.

Par exemple, prenons le cas de trois Decoders ayant le même ID de licence « xxx » et les données d'utilisation suivantes :
Decoder1 = 150 Mo
Decoder2 = 250 Mo
Decoder3 = 100 Mo
Les données d'utilisation agrégées s'affichent en indiquant 500 Mo.

Ce fichier JSON est décrit dans les sections suivantes :

- Composants
- Metrics
- Autres informations relatives au produit
- Exemple

Components

Détails de chaque service dans votre déploiement de NetWitness Suite. Ces détails sont indiqués sous la forme d'un composant. Pour chaque composant, les détails ci-dessous sont affichés.

Composant	Description
Version	Numéro de version du composant dans le déploiement de NetWitness Suite. Par exemple, 11.0.0.0.x.x.x.x.
ID	Il s'agit de l'ID de composant unique qui représente l'hôte et sert à créer un lien vers les metrics obtenus.

Composant	Description
Propriétés	• **Nom** : nom de la propriété de ce composant. Par exemple, Malware Analysis, ESA, Log Decoder, etc. • **Valeur** : valeur unique qui identifie le composant.

Metrics

Metrics des composants (hôtes), à savoir Log Decoder, Decoder et Malware Analysis. Les données d'utilisation de licence de chaque hôte sont partagées. Pour les metrics d'utilisation du Contenu Live, les types de ressources accessibles à partir de **Live > Recherche**, par exemple le nombre total de règles d'application RSA, de règles de corrélation RSA, etc., sont partagés.

Composant	Description
StartTimeUTC	Heure à partir de laquelle les metrics sont collectés (au format EPOCH).
Stats	• **Value** : valeur générée pour l'ID de composant spécifique pour chaque composant. • **Name** : nom des statistiques pour lesquelles les metrics sont collectés. Par exemple, le nombre total d'octets de capture.
EndTimeUTC	Heure à laquelle la collecte des metrics est terminée (au format EPOCH).
ID du composant	ID du composant pour lequel la valeur est enregistrée.

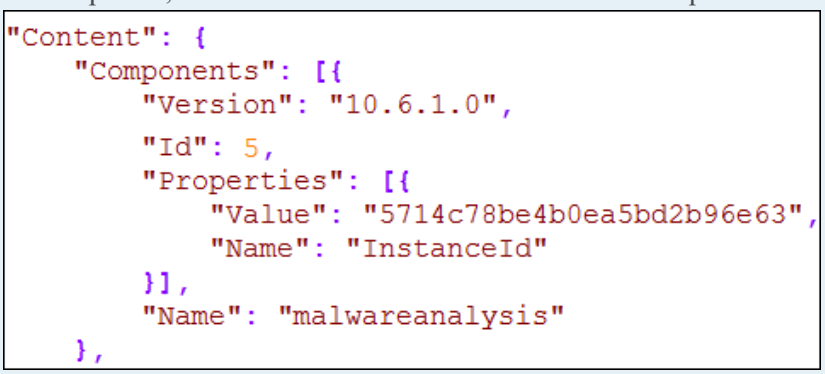
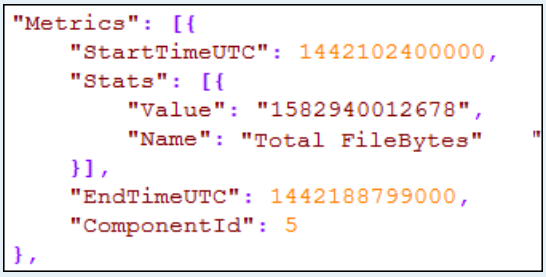
Autres informations relatives au produit

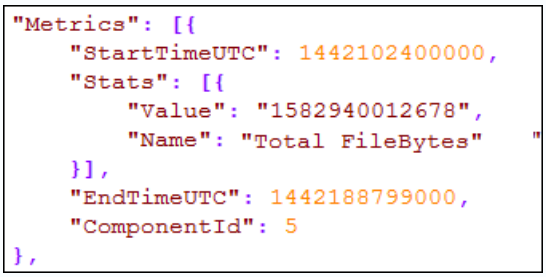
- **ProductType** : nom du produit. Dans cet exemple, le type de produit est NetWitness Suite.
- **Version** : version du fichier JSON qui suit les modifications apportées au format de fichier.
- **ProductInstance** : ID du serveur de licences.
- **Checksum** : informations utilisées pour les contrôles d'intégrité.

Le tableau suivant décrit les détails du fichier JSON avec des exemples.

Metrics	Description
Content	Affiche le contenu qui comprend tous les composants, les metrics, le type de produit et les données d'Instance du produit, excepté le checksum.

Metrics	Description

Components	Les détails de tous les services de NetWitness Suite sont représentés sous forme de composant. Les détails du composant, telles que le numéro de version du composant, le nom et la valeur s'affichent comme indiqué ci-dessous :
	 
	"Content": {
	"Components": [{
	"Version": "10.6.1.0",
	"Id": 5,
	"Properties": [{
	"Value": "5714c78be4b0ea5bd2b96e63",
	"Name": "InstanceId"
	}],
	"Name": "malwareanalysis"
	},
	Version : Affiche la version du service NetWitness Suite. Par exemple, 11.0.0.0.
	ID : Affiche un ID unique qui est généré pour le service NetWitness Suite et sert à créer un lien avec les metrics pour ce composant spécifique. Dans cet exemple, l'ID correspondant à Malware Analysis est 5 et les metrics s'affichent pour ComponentId en octets, comme indiqué ci-dessous :
	 
	"Metrics": [{
	"StartTimeUTC": 1442102400000,
	"Stats": [{
	"Value": "1582940012678",
	"Name": "Total FileBytes"
	}],
	"EndTimeUTC": 1442188799000,
	"ComponentId": 5
	},
	Properties : Affiche les propriétés du composant, telles que le nom et la valeur, comme indiqué dans la figure ci-dessus.
	Value : Affiche la valeur de la propriété, qui est un UUID interne d'un composant, comme illustré dans la figure ci-dessus. Elle est générée par NetWitness Suite. Par exemple, pour Malware Analysis, la valeur affichée est `"55f7a0b30e502231c42d063f"`
	Nom : "InstanceId" : Affiche le nom de la propriété, comme illustré dans la figure ci-dessus.

Metrics	Description
	Name": "malwareanalysis" : Affiche le nom du composant qui est un nom de service comme LogDecoder, Decoder ou MalwareAnalysis.
Metrics	Affiche la liste des metrics avec les données d'utilisation des composants, à savoir Log Decoder, Decoder and Malware Analysis. Dans cet exemple, les metrics s'affichent pour ComponentId 5 en octets, comme indiqué ci-dessous. 
	StartTimeUTC : Affiche l'heure de collecte des metrics, au format EPOCH.
	Stats : Affiche la valeur d'utilisation et les statistiques de type d'utilisation du composant.
	Value : Affiche la valeur des statistiques. Par exemple, "Value": "1582940012678", comme l'illustre la figure ci-dessus.
	Name : Affiche le nom des statistiques. Par exemple, Nombre total d'octets de capture ou Nombre total d'octets de fichier.
	EndTimeUTC: Affiche l'heure à laquelle la collecte des metrics est terminée, au format EPOCH.
	ComponentId : Affiche l'ID du composant pour lequel les valeurs de metric sont collectées. Identique à "ID" dans la section Components.
Content	Affiche le contenu qui comprend tous les composants, les metrics, le type de produit et les données d'Instance du produit, excepté le checksum.

Metrics	Description
Components	Les détails de tous les services de NetWitness Suite sont représentés sous forme de composant. Les détails du composant, telles que le numéro de version du composant, le nom et la valeur s'affichent comme indiqué ci-dessous :


```
"Content": {
    "Components": [{
        "Version": "10.6.2.0",
        "Id": 6,
        "Properties": [{
            "Value": "57444ddde4b0dd618093064d",
            "Name": "InstanceId"
        }],
        "Name": "reportingengine"
    },
```


Version : Affiche la version du service NetWitness Suite. Par exemple, 11.0.0.0

ID : Affiche un ID unique qui est généré pour le service NetWitness Suite et sert à créer un lien avec les metrics pour ce composant spécifique. Dans cet exemple, l'ID correspondant à Reporting Engine est 6 et les metrics s'affichent pour ComponentId 6 dans Nombre total, comme indiqué ci-dessous :


```
"Metrics": [{
    "StartTimeUTC": 1473292800000,
    "Stats": [{
        "Value": "10",
        "Name": "Number of RE Report"
    },
    {
        "Value": "2",
        "Name": "Number of RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of RE Chart"
    },
    {
        "Value": "14",
        "Name": "Number of RE Rule"
    },
    {
        "Value": "2",
        "Name": "Number of Enabled RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of Enabled RE Chart"
    }],
    "EndTimeUTC": 1473379199000,
    "ComponentId": 6
},
```

Metrics	Description
	Propriétés : Affiche les propriétés du composant, telles que le nom et la valeur, comme indiqué dans la figure ci-dessus.
	Value : Affiche la valeur de la propriété, qui est un UUID interne d'un composant, comme illustré dans la figure ci-dessus. Cet événement est généré par NetWitness Suite. Par exemple, pour Reporting Engine, la valeur s'affiche sous la forme suivante : "`57444ddde4b0dd618093064d`"
	Nom : "**InstanceId**" : Affiche le nom de la propriété, comme illustré dans la figure ci-dessus.
	Nom" : "**reportingengine**" : Affiche le nom du composant qui est un nom de service comme LogDecoder, Decoder ou ReportingEngine.

	Nom : Affiche la liste des metrics avec les données d'utilisation des composants, à savoir log decoder, decoder et reportingengine.
	Dans cet exemple, les metrics s'affichent pour ComponentId 6 en octets, comme indiqué ci-dessous.
	"Metrics": [{
	"StartTimeUTC": 1473292800000,
	"Stats": [{
	"Value": "10",
	"Name": "Number of RE Report"
	},
	{
	"Value": "2",
	"Name": "Number of RE Alert"
	},
	{
	"Value": "1",
	"Name": "Number of RE Chart"
	},
	{
	"Value": "14",
	"Name": "Number of RE Rule"
	},
	{
	"Value": "2",
	"Name": "Number of Enabled RE Alert"
	},
	{
	"Value": "1",
	"Name": "Number of Enabled RE Chart"
	}],
	"EndTimeUTC": 1473379199000,
	"ComponentId": 6
	},

	StartTimeUTC : Affiche l'heure de collecte des metrics, au format EPOCH.

Metrics	Description
	Stats : Affiche la valeur d'utilisation et les statistiques de type d'utilisation du composant.
	Value : Affiche la valeur des statistiques. Par exemple, le nombre de rapports RE est de 10, le nombre d'alertes RE est de 2, le nombre de graphiques RE est de 1 ..., comme illustré dans la figure ci-dessus.
	Nom : Affiche le nom des statistiques. Par exemple, Nombre de rapports RE, Nombre d'alertes RE, Nombre de graphiques RE, Nombre de règles RE, Nombre d'alertes RE activées, Nombre de graphiques RE activés.
	EndTimeUTC : Affiche l'heure à laquelle la collecte des metrics est terminée, au format EPOCH.
	ComponentId : Affiche l'ID du composant pour lequel les valeurs de metric sont collectées. Identique à "ID" dans la section Components.
ProductType	Affiche le type de produit qui génère le fichier. Par exemple, `"ProductType": "NetWitness Suite"`
ProductInstance	Affiche l'ID du serveur de licences et est propre à NetWitness Suite. Par exemple, `"ProductInstance": "00-0C-29-6C-66-E3"`
Checksum	Affiche le checksum de la section "Content" du fichier. Utilisé par RSA pour le contrôle d'intégrité. Par exemple : `"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"`

Exemple

Exemple de fichier JSON.


```
{
    "Content": {
        "Components": [{
            "Version": "10.6.1.0",
            "Id": 7,
            "Properties": [{
                "Value": "57470c96e4b0cf62c7bfbd53",
                "Name": "InstanceId"
            }],
            "Name": "esa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 4,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e69",
                "Name": "InstanceId"
            }],
            "Name": "incidentmanagement"
        },
        {
            "Version": "10.6.1.0",
            "Id": 2,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e65",
                "Name": "InstanceId"
            }],
            "Name": "sa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 1,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e63",
                "Name": "InstanceId"
            }],
            "Name": "malwareanalysis"
        },
        {
            "Version": "10.6.1.0",
            "Id": 3,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e67",
                "Name": "InstanceId"
            }],
            "Name": "reportingengine"
        }],
        "Metrics": [{
            "StartTimeUTC": 1464480000000,
            "Stats": [{
                "Value": "Disabled",
                "Name": "Threat Detection"
            },
            {
                "Value": "3.0",
                "Name": "Number Of Enabled ESA Rules"
            }],
            "EndTimeUTC": 1464566399000,
            "ComponentId": 7
        }],
        "EndTime": 1464566399000,
        "Version": "1.0",
        "StartTime": 1464479999000,
        "ProductType": "Security Analytics",
        "ProductInstance": "00-0C-29-A2-57-B4"
    },
    "Checksum": "6445C704D3F9E67D24DBA8F11EB6C003CBCC0E199576342E6E6D2545524F583F"
}
```

Télécharger des données vers RSA pour Live Feedback

Cette rubrique fournit les instructions permettant à un administrateur NetWitness Suite d'exporter les metrics dans NetWitness Suite pour Live Feedback.

Si le compte Live n'est pas configuré, vous pouvez manuellement télécharger les données d'utilisation de RSA. Pour plus d'informations, consultez le Panneau Configuration des services Live.

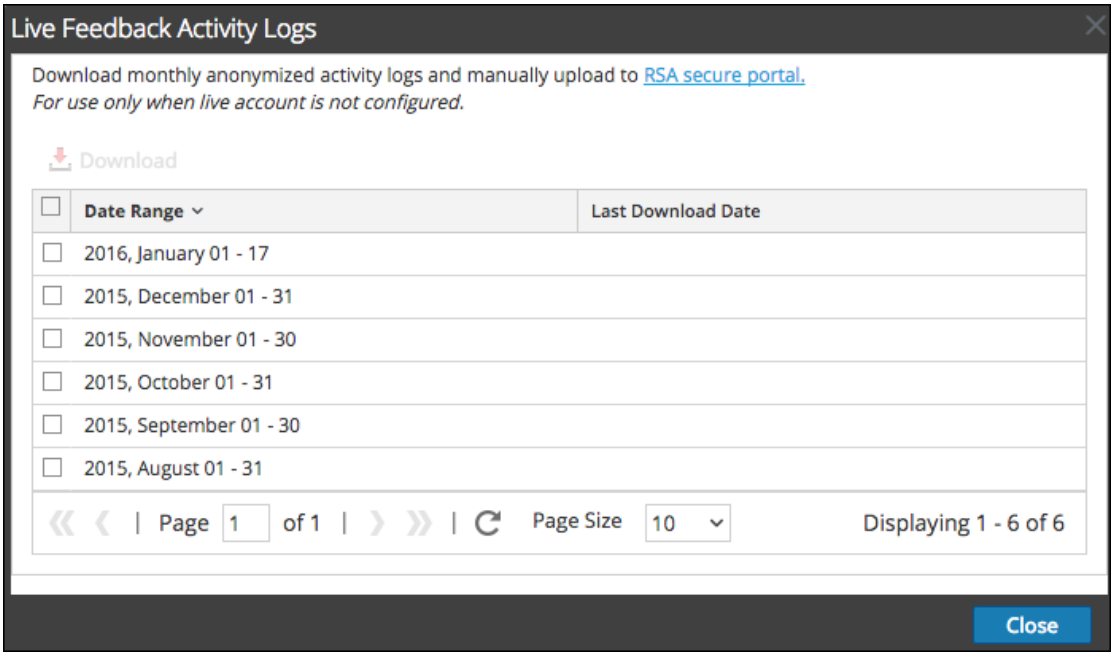
La rubrique Compte Live contient un log d'activité Live Feedback qui vous permet de télécharger les données d'utilisation requises pour Live Feedback. Il reste toujours actif quelle que soit la configuration du compte Live.

Vous pouvez télécharger en aval au préalable l'historique des données Live Feedback, puis le télécharger en amont pour effectuer un partage avec RSA.

Télécharger l'historique des données Live Feedback

Pour télécharger l'historique des données Live Feedback :

1. Accédez à **ADMIN** > **système**.
2. Dans le panneau des options, sélectionnez **Services Live**.
   L'écran **Compte Live** composé des affichages **État Live RSA** et **Télécharger le log d'activité Live Feedback** apparaît.
3. Cliquez sur **Télécharger le log d'activité Live Feedback**.
   La fenêtre **Télécharger les logs d'activité Live Feedback** s'ouvre pour permettre à l'utilisateur NetWitness Suite de télécharger l'historique des données Live Feedback requis.



4. Sélectionnez une ou plusieurs entrées en sélectionnant les cases à cocher, puis cliquez

sur **Télécharger**.

Remarque : Si vous sélectionnez plusieurs entrées dans l'historique, le fichier zip téléchargé se compose d'un fichier JSON individuel par mois.

Les données Live Feedback téléchargées sont au formatJSON et sont compressées en fichier .zip. Pour plus d'informations, reportez-vous à la rubrique Présentation de Live Feedback.

Partager des données avec RSA

Après avoir téléchargé en aval les données Live Feedback, vous pouvez ensuite les télécharger en amont à l'aide de la procédure suivante.

Pour partager les données dans RSA :

1. Cliquez sur le **Portail sécurisé RSA** disponible dans la fenêtre **Logs d'activité Live Feedback**.
   L'écran de connexion RSA NetWitness® Suite Live Feedback s'affiche.
2. Connectez-vous au portail Télécharger en amont les logs d'activité Live Feedback à l'aide de vos informations d'identification Live.
3. Cliquez sur **Choisir un fichier**, puis sélectionnez le fichier téléchargé en aval.
4. Cliquez sur **Télécharger**.

Configurer les paramètres du fichier de consignation

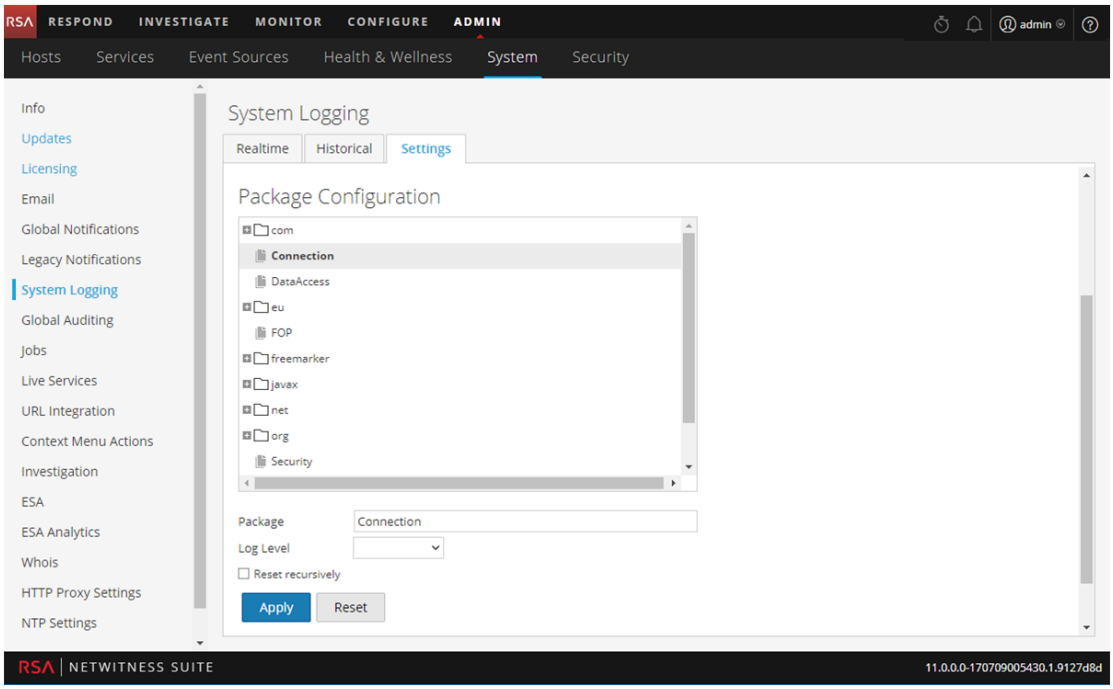
Dans RSA NetWitness® Suite , vous pouvez configurer la taille des fichiers logs, le nombre de fichiers logs de sauvegarde gérés, ainsi que le niveau de consignation par défaut des packages dans NetWitness Suite.

Configurer la taille et le nombre de sauvegardes des fichiers logs système

La taille et le nombre de sauvegardes des fichiers logs sont configurés par défaut. Pour modifier ces valeurs par défaut :

1. Accédez à **ADMIN > Système.**
2. Dans le panneau des options, cliquez sur **Système Consignation**.
   Le panneau Configuration de la consignation système qui s'ouvre affiche par défaut l'onglet En temps réel.

3. Cliquez sur l'onglet **Paramètres**.

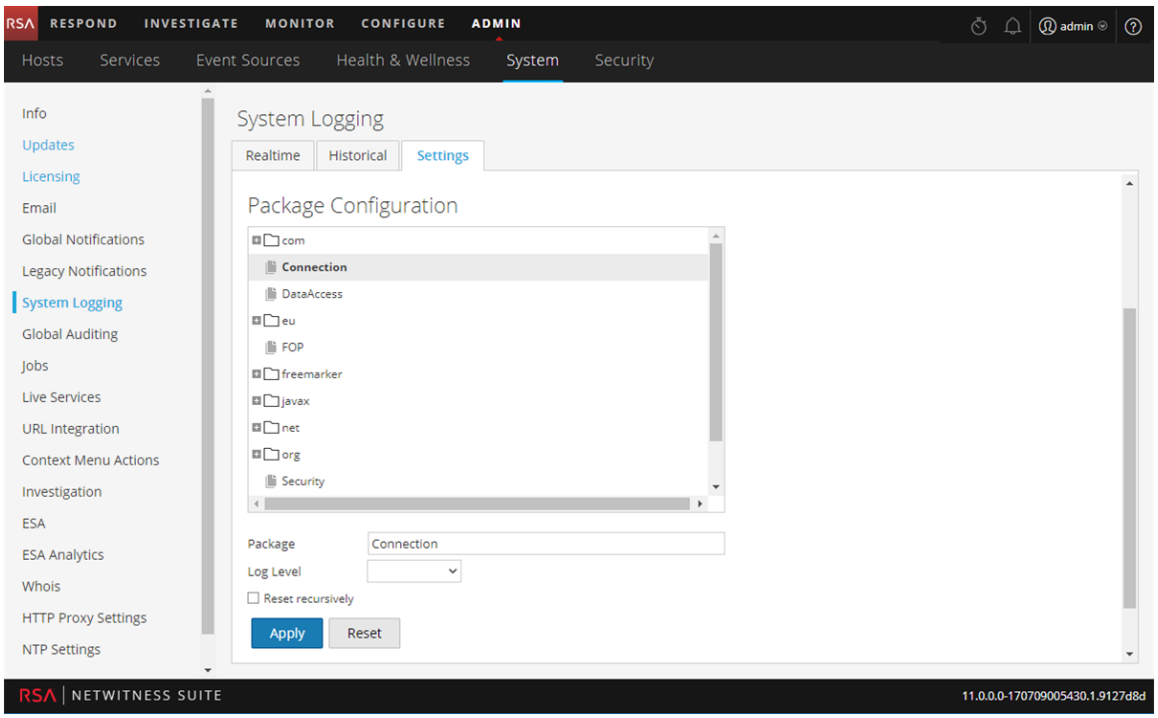


4. Dans le champ **Taille de log max.**, saisissez la taille maximale en octets. La valeur minimale de ce paramètre est **4096**.
5. Dans le champ **Nbre max. de fichiers de sauvegarde**, saisissez le nombre maximal de fichiers logs de sauvegarde à gérer. La valeur minimale de ce paramètre est **0**. Lorsque le nombre maximum de fichiers log est atteint et que le nouveau fichier de sauvegarde est élaboré, la sauvegarde la plus ancienne est ignorée.
6. Cliquez sur **Appliquer**.
   Les modifications prennent effet immédiatement.

Définir le niveau de consignation d'un package

La rubrique Configuration des packages affiche les NetWitness Packets sous forme d'arborescence. L'arborescence contient tous les packages utilisés dans NetWitness Suite. Vous pouvez descendre dans l'arborescence pour afficher les niveaux de consignation de chaque package. Le niveau de consignation de tous les packages qui ne sont pas définis explicitement est le niveau **root**. Pour définir le niveau de consignation d'un package :

1. Sélectionnez le package dans l'arborescence **Package**.
   Le nom du package est affiché dans le champ **Package**. Si un niveau de consignation est déjà défini pour le package, ce niveau est indiqué.



2. Sélectionnez le **Niveau du log** dans la liste déroulante.
3. Cliquez sur **Appliquer**.

   Le nouveau niveau de consignation prend effet immédiatement.
4. (Facultatif) Pour rétablir le niveau de consignation par défaut indiqué pour **root**, cliquez sur **Réinitialiser**.

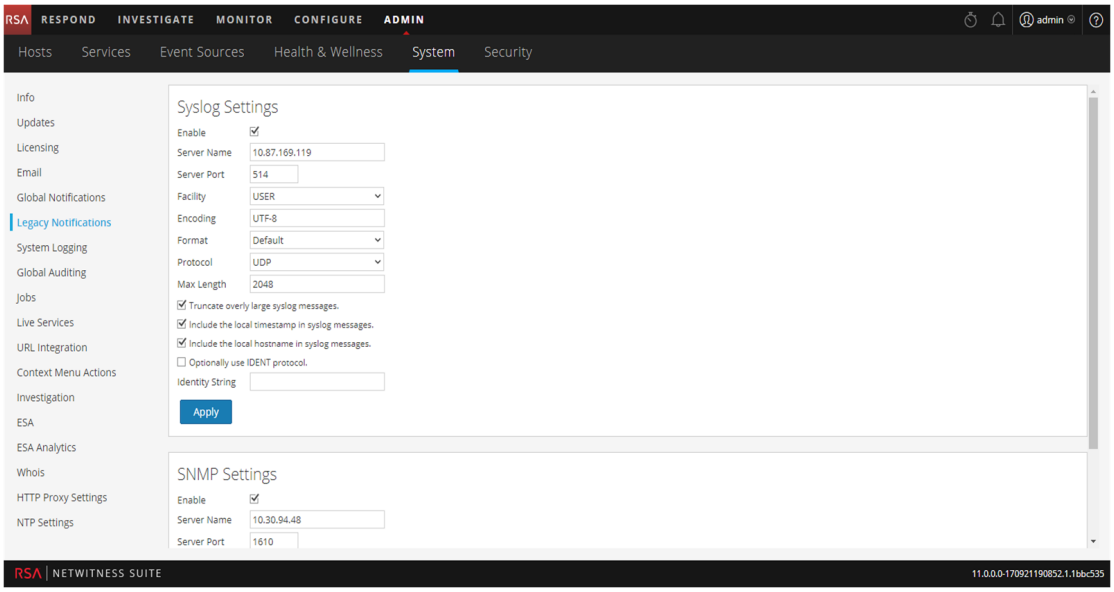
Configurer les paramètres Syslog et SNMP

Dans le panneau Notification existantes, vous pouvez configurer les paramètres de notification syslog et SNMP. Ces configurations permettent de contrôler les habilitations, Event Source Management (ESM), Warehouse Connector et Archiver d'ancienne génération.

Configurer et activer les paramètres syslog

1. Accédez à **ADMIN > Système**.

2. Dans le panneau des options, cliquez sur **Notifications existantes**.
   Le panneau Configuration des notifications existantes s'affiche.

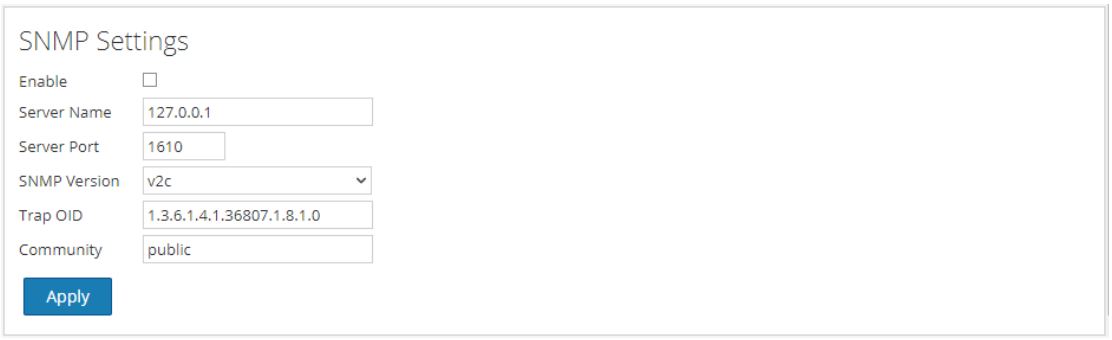


3. Dans les champs **Nom du serveur** et **Port de serveur** de **Paramètres Syslog**, saisissez le nom de l'hôte sur lequel le processus syslog cible est exécuté et le port sur lequel écoute ce processus.
4. Dans les champs **Site**, **Codage**, **Format** et **Longueur maximale**, indiquez le site syslog, le codage texte des messages, le format des messages et la longueur maximale des messages.
5. Dans le champ **Protocole**, sélectionnez UDP ou TCP.
6. (Facultatif) Sélectionnez les options des éléments dans lesquels inclure les messages : **Tronquer les messages Syslog trop longs**, **Inclure l'horodatage local dans les messages Syslog** et **Inclure le nom d'hôte local dans les messages Syslog**.
7. (Facultatif) Configurer syslog pour ajouter une chaîne d'identité devant chaque alerte syslog.
8. Cochez la case **Activer**.
9. Cliquez sur **Appliquer**.
   Les notifications syslog sont activées immédiatement.

Le Panneau Configuration des notifications existantes fournit des informations détaillées sur ces paramètres.

Configurer et activer les paramètres SNMP

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications existantes**.
   Le panneau Configuration des notifications existantes s'affiche avec les paramètres SNMP au bas du panneau.



3. Dans les champs **Nom de serveur** et **Port de serveur** sous **Paramètres SNMP**, saisissez le nom d'hôte et le port d'écoute de l'hôte de trap SNMP.
4. Sélectionnez la **version SNMP** dans le menu déroulant, à savoir **v1** ou **v2c**.
5. Dans le champ **ID d'objet de trap**, indiquez l'ID d'objet pour le trap SNMP sur l'hôte trap qui reçoit l'événement d'audit. La valeur par défaut est **0.0.0.0.0.1**.
6. Dans le champ **Communauté**, indiquez la chaîne de communauté utilisée pour l'authentification sur l'hôte de trap SNMP ; la valeur par défaut est **public**.
7. Cochez la case **Activer**.
8. Cliquez sur **Appliquer**.
   Les notifications SNMP sont activées immédiatement.

Le Panneau Configuration des notifications existantes fournit des informations détaillées sur ces paramètres.

Désactiver les paramètres syslog ou SNMP

Pour désactiver les paramètres syslog ou SNMP sur cette instance NetWitness Suite :

1. Désélectionnez la case **Activer** appropriée.
2. Cliquez sur **Appliquer**.
   Les paramètres sélectionnés sont désactivés immédiatement.

Procédures supplémentaires

Les procédures supplémentaires ne sont pas essentielles pour la configuration de NetWitness Suite. Elles incluent certaines options de personnalisation qui n'entrent pas dans le cadre de la configuration habituelle, par exemple l'ajout de menus contextuels personnalisés ou la configuration d'un proxy.

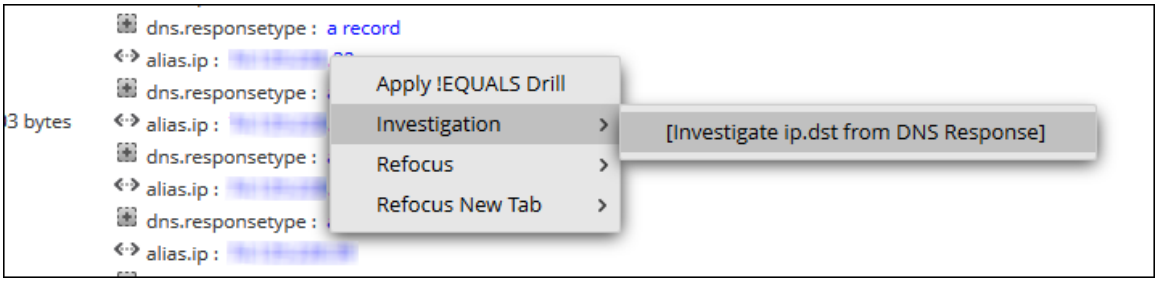
Actions du menu Ajouter un contexte personnalisé

Dans le panneau Actions de menu contextuel, les administrateurs peuvent afficher, ajouter et modifier les actions d'un menu contextuel pour l'instance active de NetWitness Suite. Chaque action du menu contextuel s'applique à un contexte spécifique dans l'interface utilisateur NetWitness Suite, et apparaît en tant qu'option lorsque vous cliquez avec le bouton droit de la souris sur un emplacement spécifique dans l'interface utilisateur.

Certaines actions du menu contextuel sont intégrées à NetWitness Suite ; vous ne pouvez pas modifier ni supprimer les actions de menu contextuel par défaut. En revanche, vous pouvez créer des actions de menu contextuel personnalisées et les modifier. Si vous souhaitez créer une variante personnalisée d'une action de menu contextuel intégrée, vous pouvez copier la configuration dans une nouvelle action de menu contextuel, puis modifier l'action de menu contextuel personnalisée. Une action de menu contextuel est définie par le code de feuilles de style en cascade (CSS) qui spécifie :

- Le titre de l'option dans le menu contextuel.
- Le module NetWitness Suite dans lequel le menu contextuel est disponible.
- Le contenu auquel l'action s'applique.

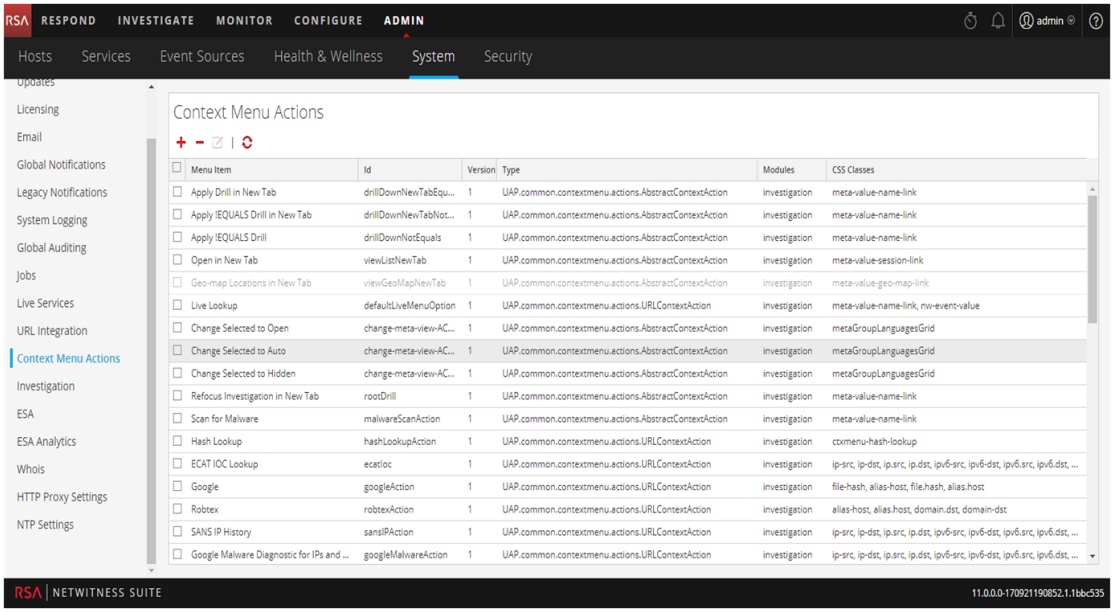
Voici un exemple d'action de menu contextuel personnalisée ; les étapes et le code CSS pour créer cet exemple sont fournis dans la procédure ci-dessous.



Afficher les actions d'un menu contextuel dans NetWitness Suite

Pour afficher les actions de contexte par défaut et personnalisées de NetWitness Suite :

1. Accédez à **ADMIN > Système.**
2. Dans le panneau des options, sélectionnez **Actions de menu contextuel**.



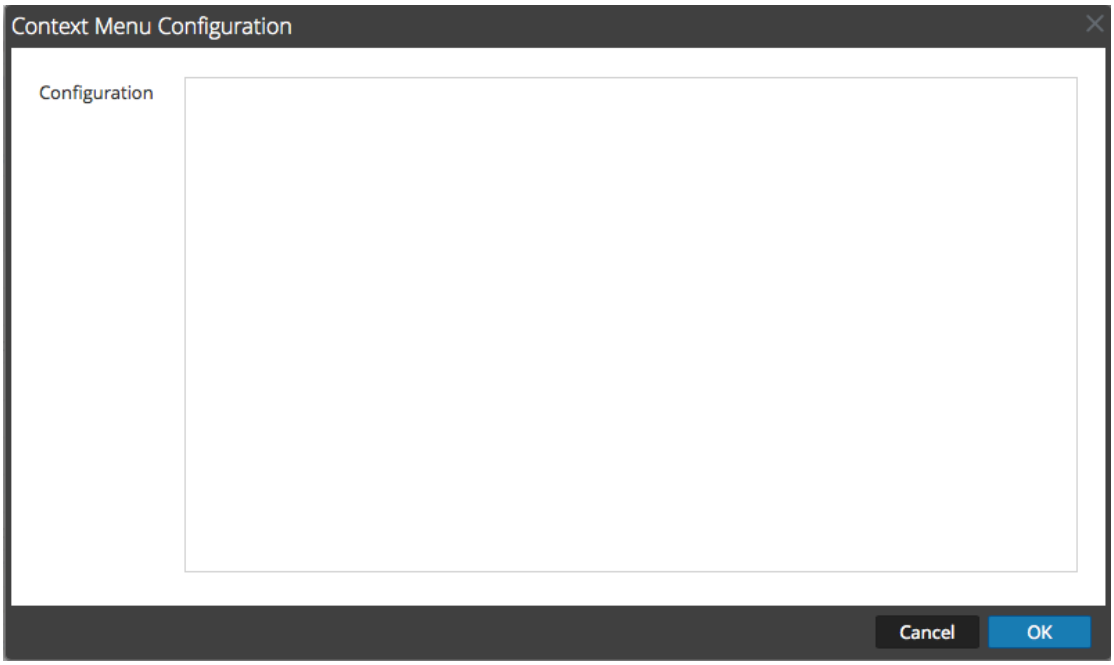
Les détails des informations du panneau Actions de menu contextuel sont fournis dans le Panneau Actions des menus contextuels.

Ajouter une action à un menu contextuel

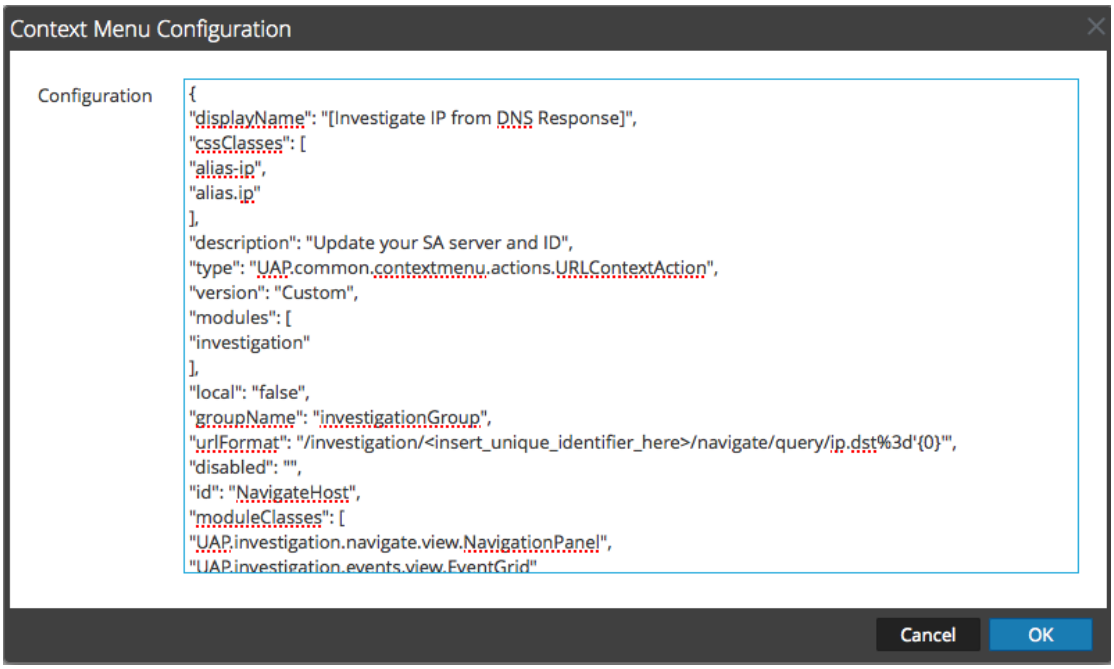
Pour ajouter une action à un menu contextuel dans NetWitness Suite :

1. Dans la barre d'outils, cliquez sur +.

   La boîte de dialogue Configuration du menu contextuel s'affiche.



2. Saisissez le code CSS définissant l'action de menu contextuel. L'exemple de procédure à la fin de cette rubrique fournit des instructions détaillées vous permettant de créer une action de menu contextuel utile.



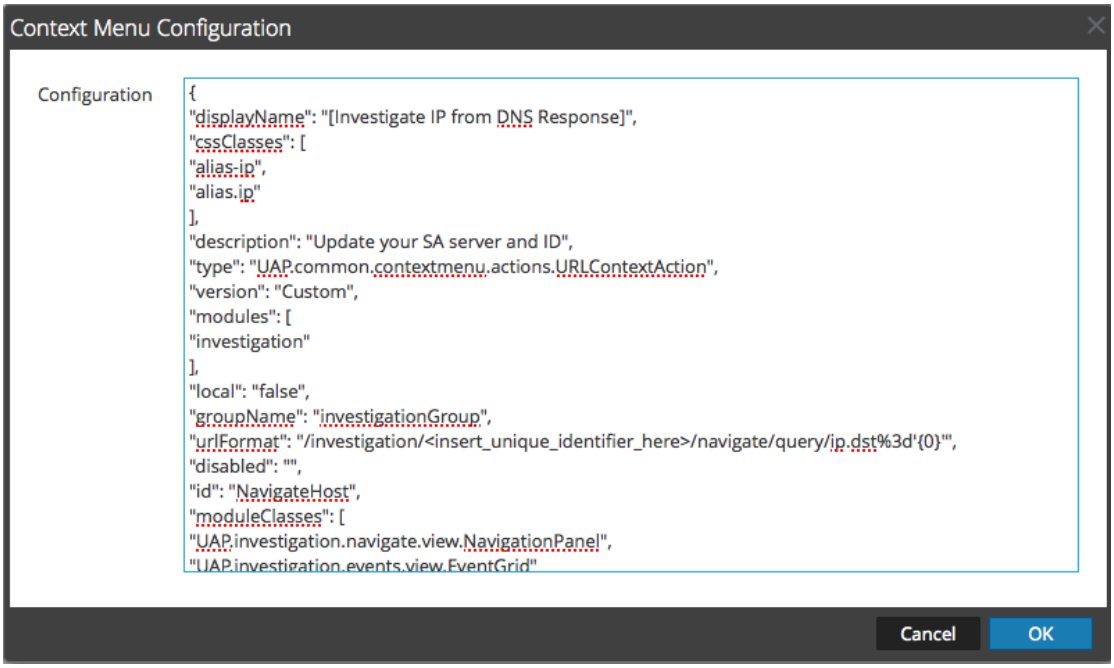
3. Cliquez sur **OK**.
   La nouvelle action de menu contextuel est créée et ajoutée à la fin de la liste des actions de menu contextuel.

4. Pour activer la nouvelle action de menu contextuel, redémarrez le navigateur.
   L'action de menu contextuel devient disponible à l'emplacement configuré.

Modifier une action de contexte

Pour modifier une action de contexte :

1. Sélectionnez la ligne dans la grille, puis **double-cliquez** sur la ligne ou cliquez sur .
   La **boîte de dialogue Configuration du menu contextuel** s'affiche.



2. Modifiez la **configuration**.
3. Pour enregistrer les modifications, cliquez sur **OK**.
4. Pour utiliser l'action mise à jour, redémarrez le navigateur.

Supprimer une action de contexte

Pour supprimer entièrement une action de menu contextuel de NetWitness Suite :

1. Sélectionnez l'action.
2. Cliquez sur .
   Une boîte de dialogue vous invite à confirmer la suppression de l'action de menu contextuel.
3. Cliquez sur **Yes**.
   L'option est supprimée du panneau Actions de menu contextuel.

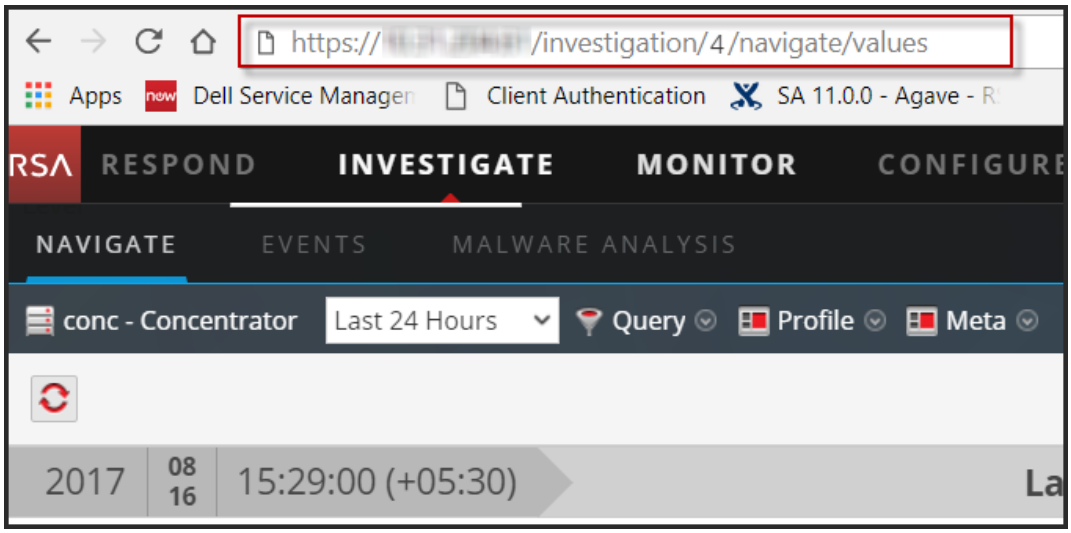
4. Redémarrez le navigateur pour supprimer l'action des menus contextuels dans lesquels elle apparaît.

Exemple de procédure : action de menu contextuel pour analyser la clé méta ip.dst dans les valeurs alias.ip

Cet exemple ajoute une action de menu contextuel qui permet aux analystes de pivoter entre les valeurs `alias.ip` (adresses IP renvoyées par une requête DNS) et la clé méta `ip.dst`. Il permet aux analystes de localiser tout le trafic détecté sur l'adresse IP qui a été renvoyée dans le cadre d'une requête DNS.

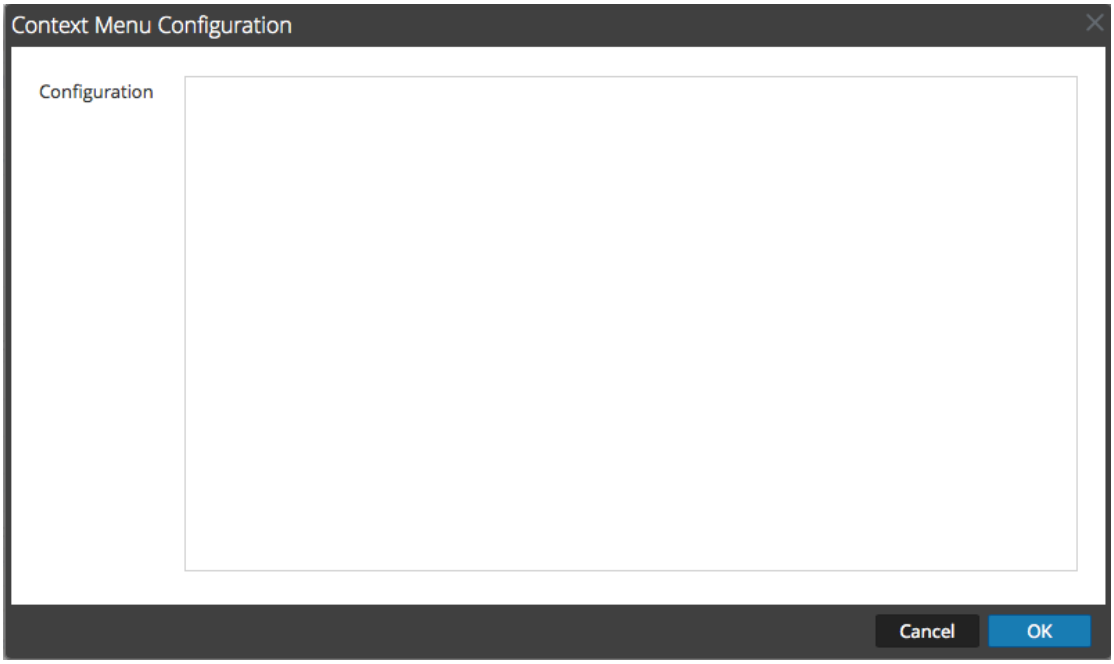
Pour implémenter l'action de menu contextuel :

1. Déterminez l'identificateur unique de votre Serveur NetWitness comme suit :
   a. Connectez-vous à NetWitness Suite, dans le Menu principal, sélectionnez **Investigation** > **Naviguer**, sélectionnez un service (par exemple, un Concentrator) à analyser, puis attendez que les valeurs se chargent.
   b. Recherchez l'URL et localisez le numéro après `investigation`. Dans cet exemple, l'identificateur unique de l'action est 4. Cet identificateur unique doit être ajouté à l'action de menu contextuel.



2. Dans la barre d'outils, cliquez sur +.

   La boîte de dialogue Configuration de menu contextuel s'affiche.

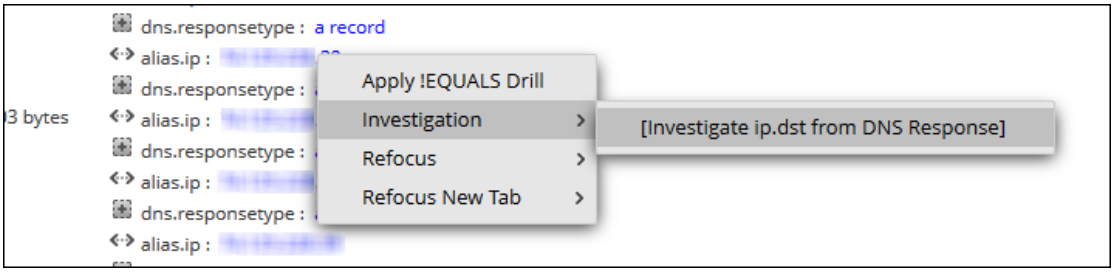


3. Copiez le bloc d'exemple de code entier ci-dessous et collez-le dans la fenêtre.

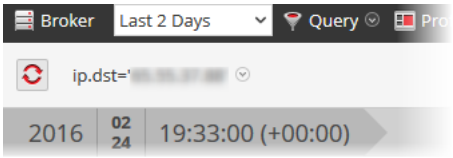
```
{
    "displayName": "[Investigate IP from DNS Response]",
    "cssClasses": [
        "alias-ip",
        "alias.ip"
    ],
    "description": "Update your NW server and ID",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "Custom",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "investigationGroup",
    "urlFormat": "/investigation/<insert_unique_identifier_
here>/navigate/query/ip.dst%3d'{0}'",
    "disabled": "",
    "id": "NavigateHost",
    "moduleClasses": [
```

```
            "UAP.investigation.navigate.view.NavigationPanel",
            "UAP.investigation.events.view.EventGrid"
        ],
        "openInNewTab": "true"
    }
```

4. Sur la ligne **urlFormat**, remplacez **<insérer-identificateur_unique_ici>** par votre identificateur unique.
   L'URL ressemble à ceci :
   `"/investigation/4/navigate/query/ip.dst%3d'{0}'"`
5. Cliquez sur **OK**, puis redémarrez votre navigateur.
6. Pour tester l'action, ouvrez une investigation dans la vue Naviguer, puis cliquez avec le bouton droit sur la clé méta `alias.ip`.
   Le menu contextuel avec l'option Investigation devrait ressembler à la figure suivante.



7. Il doit produire un pivot comme celui-ci.



8. Si vous utilisez cet exemple pour l'examen du trafic DNS, vous voudrez peut-être envisager la création d'un groupe méta spécifique au trafic DNS comme décrit dans le *Guide Investigation et Malware Analysis*.

Configurer les serveurs NTP

Cette rubrique fournit des instructions sur la configuration des serveurs NTP (Network Time Protocol). Le protocole NTP est conçu pour synchroniser les horloges des machines hôtes sur un réseau. Pour plus d'informations sur le protocole NTP, accédez à la page d'accueil correspondante (http://www.ntp.org/).

Remarque : Les hôtesNW Core doivent pouvoir communiquer avec l'hôte NW associé au port UDP 123 pour la synchronisation horaire NTP.

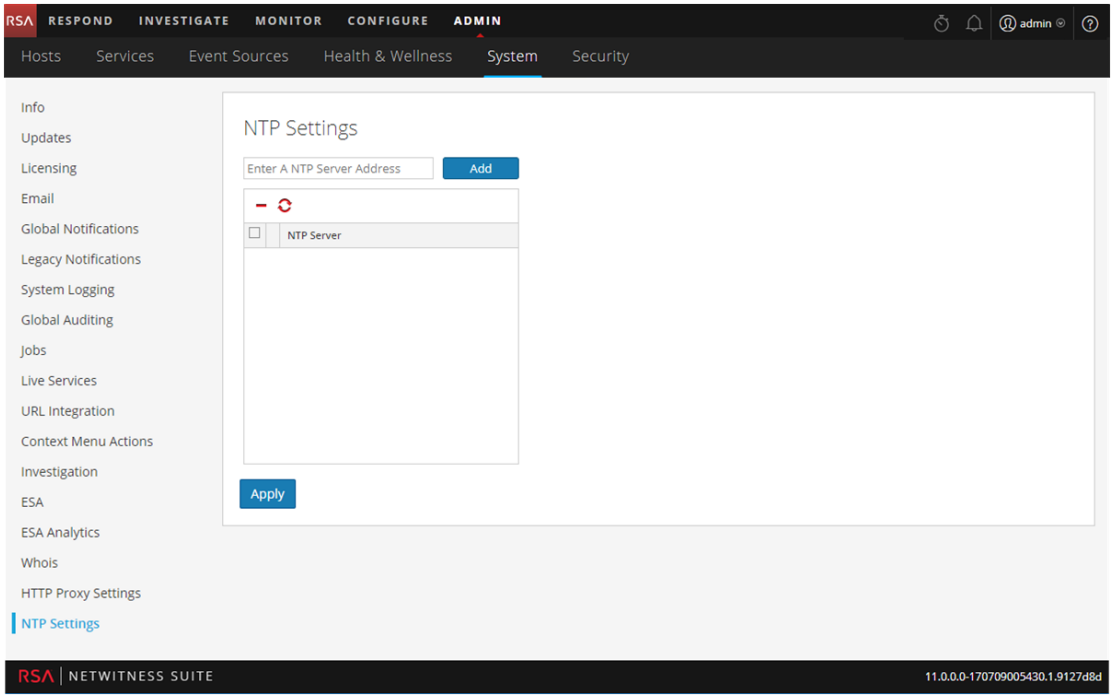
Utilisez la vue **Administration** > **Système** > **Paramètres NTP** pour configurer un ou plusieurs serveurs NTP. Après avoir configuré un serveur NTP, NetWitness Suite utilise le protocole NTP pour synchroniser les horloges des machines hôtes. Configurez plusieurs serveurs NTP à des fins de basculement sur incident. Cette rubrique contient les procédures suivantes :

- Ajouter un serveur NTP
- Modifier un serveur NTP

Ajouter un serveur NTP

Pour ajouter un serveur NTP :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Paramètres NTP**.
   Le panneau Paramètres NTP s'affiche en vous invitant à saisir le nom d'hôte (en d'autres termes, l'adresse IP ou le nom de domaine complet) d'un serveur NTP.



3. Saisissez l'adresse IP ou le nom de domaine complet d'un serveur NTP.
   Si la syntaxe du nom d'hôte n'est pas valide, NetWitness Suite désactive les boutons **Ajouter**et **Appliquer** puis affiche le **Nom d'hôte saisi non valide**.
4. Cliquez sur **Ajouter**.
   - Si la syntaxe du nom d'hôte est valide et si NetWitness Suite peut joindre le serveur, il affiche **Validation**.

- Si la syntaxe du nom d'hôte est valide et si NetWitness Suite ne peut pas joindre un serveur, le message suivant s'affiche (***hostname*** correspond au nom d'hôte que vous avez tenté d'ajouter) : **Le serveur NTP *hostname* est inaccessible. Vérifiez l'adresse ou les paramètres de votre pare-feu.**

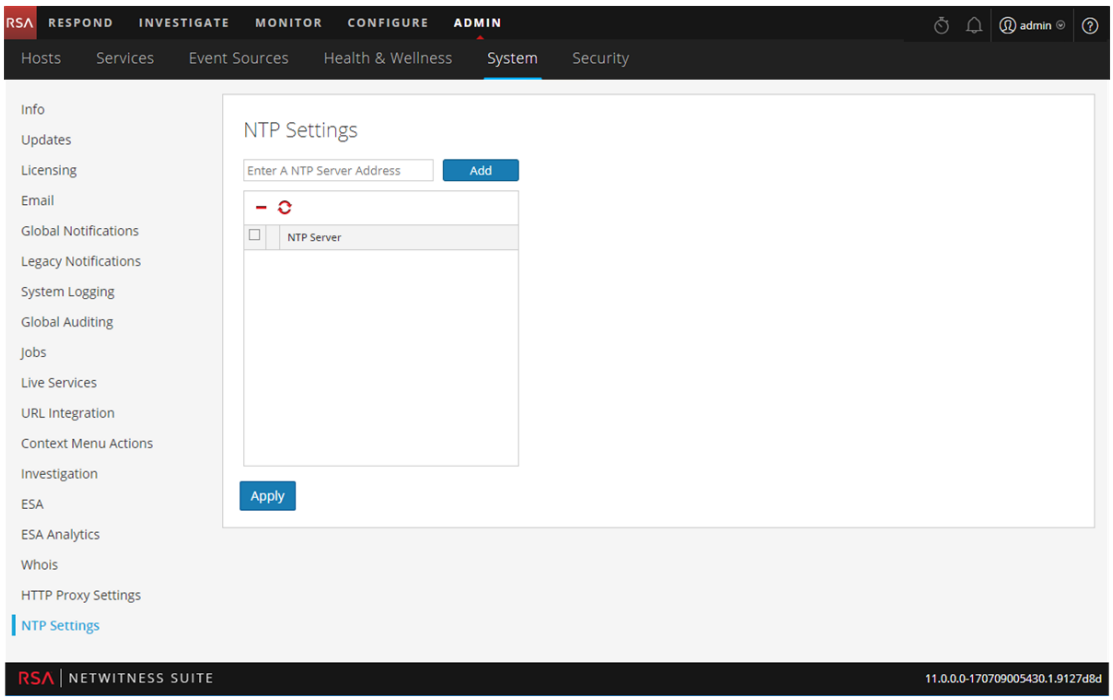
5. Cliquez sur **Appliquer**.
   Une boîte de dialogue affiche la notification indiquant que les paramètres ont été enregistrés et vous demande de confirmer que vous souhaitez appliquer les paramètres maintenant.
6. Cliquez sur **Yes**.
   Le serveur NTP spécifié s'assure désormais que les horloges de vos machines hôtes sont synchronisées. Si vous décidez de configurer plusieurs serveurs NTP et si un serveur tombe en panne, NetWitness Suite effectue un basculement sur incident vers le serveur suivant configuré.

Pour plus d'informations sur les paramètres et les descriptions, reportez-vous à Panneau Paramètres NTP.

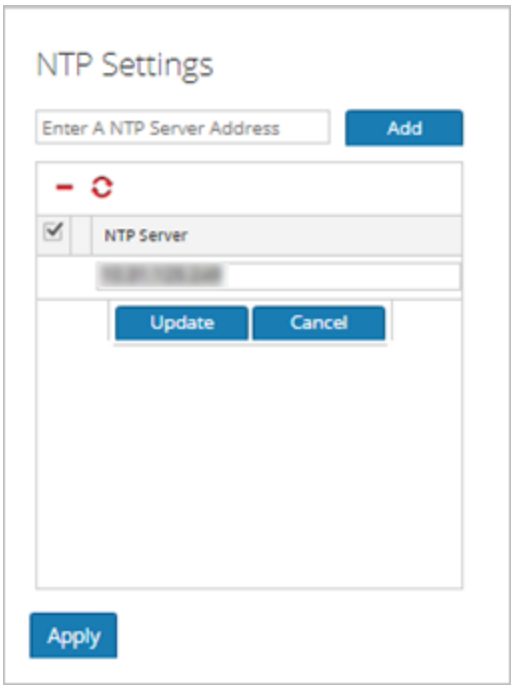
Modifier un serveur NTP

Pour modifier un serveur NTP existant :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Paramètres NTP**.
   Le panneau Paramètres NTP s'affiche
   .



3. Double-cliquez sur le nom d'hôte du **serveur NTP** à modifier.
   La zone de texte Serveur NTP devient modifiable. De plus, les boutons Mettre à jour et Annuler s'affichent.



4. Modifiez le nom d'hôte, cliquez sur **Mettre à jour**, puis cliquez sur **Appliquer.** (Cliquez sur **Annuler** avant de cliquer sur **Appliquer** pour annuler la modification).
   NetWitness Suite modifie le nom d'hôte en fonction de vos modifications.

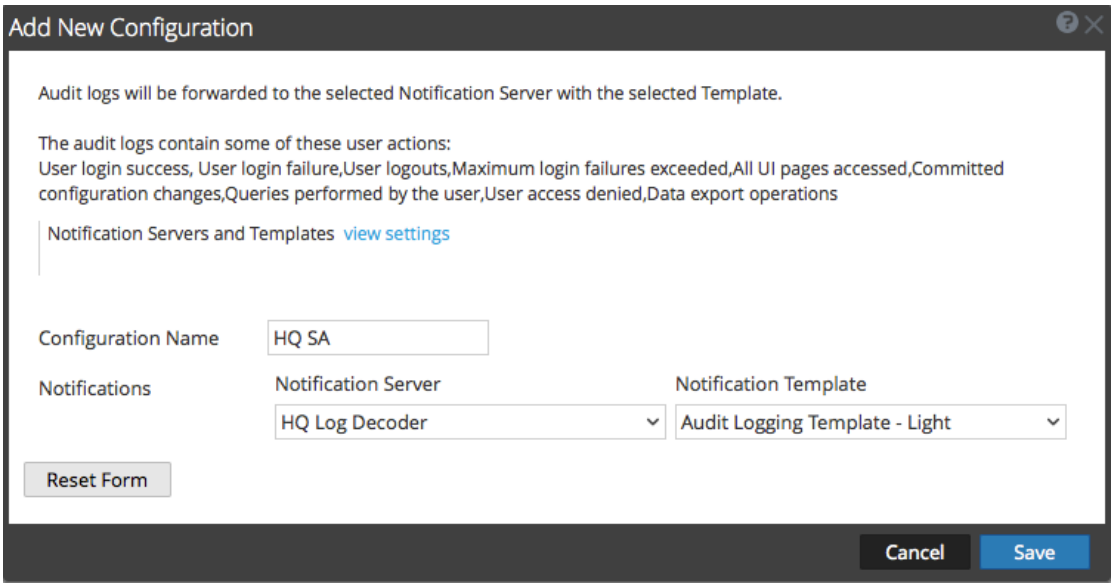
Boîte de dialogue Ajouter une nouvelle configuration

Dans la vue Administration - Système de RSA NetWitness® Suite , sous le panneau Configurations de consignation d'audit globale, vous pouvez créer plusieurs configurations de consignation globale des audits. Ces configurations permettent de transférer les logs d'audit globaux vers un emplacement central pour effectuer les audits utilisateur.

Les procédures liées à la consignation globale des audits sont décrites dans la section Configurer la consignation globale des audits.

Pour accéder à la boîte de dialogue **Ajouter une nouvelle configuration** :

1. Dans le Menu principal, sélectionnez **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Audit global**.
3. Dans le panneau **Configurations de consignation d'audit globale**, cliquez sur +.
   La boîte de dialogue **Ajouter une nouvelle configuration** s'affiche.



La section Notifications vous permet de sélectionner un serveur de notification Syslog pour la configuration de la consignation globale des audits et un modèle à utiliser pour les logs d'audits globaux. Le modèle définit les détails des entrées de logs d'audit globaux.

Fonctions

Le tableau suivant décrit les fonctions des boîtes de dialogue Ajouter une nouvelle configuration et Modifier la configuration.

Fonctionnalité	Description
Lien vers les **paramètres de la vue** Serveurs et modèles de notification	Vous renvoie au panneau Notifications globales où vous pouvez afficher ou configurer le serveur et le modèle de notification. Un serveur de notification Syslog et un modèle de consignation d'audit sont nécessaires pour pouvoir créer une configuration de consignation globale des audits.
Nom de configuration	Indique le nom unique utilisé pour identifier la configuration de consignation globale des audits.
Serveur de notification	Indique le serveur de notification Syslog chargé d'envoyer les informations de consignation globale des audits. La section Configurer une destination pour recevoir des logs d'audit globaux fournit des instructions sur le mode de création d'un serveur de notification Syslog pour une consignation globale des audits.
Modèle de notification	Indique le modèle à utiliser pour la configuration de la consignation globale des audits. Le modèle doit correspondre à un modèle de consignation d'audit. Pour les services Log Decoder, utilisez le **modèle CEF d'audit par défaut**. Vous pouvez ajouter ou supprimer des champs dans le modèle CEF (Common Event Format) si vous avez des exigences spécifiques. La section Définir un modèle pour la consignation globale des audits fournit des instructions. Pour les serveurs Syslog tiers, vous pouvez utiliser un modèle de consignation d'audit par défaut ou définir votre propre format (CEF ou non-CEF). La section Définir un modèle pour la consignation globale des audits fournit des instructions et la section Variables de métaclés prises en charge pour la consignation globale des audits décrit les variables disponibles.
Bouton **Réinitialiser l'écran**	Efface les paramètres de configuration au sein de la boîte de dialogue.

Actions d'utilisateur consignées

Le tableau suivant fournit des exemples d'actions d'utilisateur consignées à partir de NetWitness Suite. Ces actions désignent les actions utilisateur consignées par défaut, le cas échéant.

Action de l'utilisateur	Exemple
Connexions utilisateur réussies	Un utilisateur se connecte avec les informations d'identification valides.
Échec de la connexion utilisateur	Un utilisateur tente de se connecter avec des informations d'identification non valides.
Déconnexions utilisateur	Un utilisateur se déconnecte de NetWitness Suite (Administration> Déconnexion) ou un utilisateur se déconnecte pour cause d'expiration du délai de session.
Maximum d'échecs de connexion dépassé	Un utilisateur tente de se connecter avec des informations d'identification non valides à cinq reprises. Cinq (5) est le nombre maximal d'échecs de connexion définis dans la vue Administration - Sécurité > onglet Paramètres (Administration> Sécurité> onglet Paramètres).
Toutes les pages de l'interface utilisateur consultées	Lorsqu'un utilisateur accède au module Reporting (Administration > Rapports), il se connecte en tant que `[REP] Reports`. Lorsqu'un utilisateur accède à la vue Administration - Système (Administration > Système), il se connecte en tant que `[ADM] System`.
Changements de configuration validés	Un utilisateur change son mot de passe ou ses paramètres de sécurité (Administration > Sécurité > onglet Paramètres).

Action de l'utilisateur	Exemple
Requêtes effectuées par l'utilisateur	Un utilisateur effectue une requête de procédure d'enquête.
Accès utilisateur refusés	Un utilisateur tente d'accéder à un module et ne dispose pas des autorisations pour y accéder.
Opérations liées à l'exportation de données	Un utilisateur exporte des données de la vue Événements (Procédure d'enquête > Événements > Actions > Exporter).

Pour obtenir la liste des types de messages en cours de consignation par les différents composants NetWitness Suite, reportez-vous à la section Référence aux opérations de consignation globale des audits.

Métaclés CEF prises en charge

Cette section décrit les métaclés Common Event Format (CEF) prises en charge par la fonctionnalité de consignation globale des audits de NetWitness Suite.

Les modèles de consignation globale des audits que vous définissez pour un Log Decoder utilisent le format Common Event Format (CEF) et doivent répondre aux exigences standard spécifiques suivantes :

- Contient les en-têtes CEF dans le modèle.
- Utilisez uniquement les extensions et les extensions personnalisées présentant un format (Clé=Valeur) issues du tableau des métaclés ci-dessous.
- Assurez-vous que les extensions et extensions personnalisées sont au format `key=${string}<space>key=${string}`.

Pour les serveurs Syslog tiers, vous pouvez définir votre propre format (CEF ou non-CEF).

Les procédures relatives à ce tableau sont décrites dans les sections Définir un modèle pour la consignation globale des audits et Configurer la consignation globale des audits.

Métaclés Common Event Format (CEF) prises en charge

Le tableau suivant décrit les métaclés CEF Syslog prises en charge par la consignation globale des audits NetWitness Suite. Les champs Date/heure et Nom d'hôte du préfixe Syslog ne sont pas configurables ni inclus dans le modèle, mais ils sont ajoutés au début de chaque message de log par défaut. L'en-tête CEF est requis pour se conformer à la norme CEF ou pour tout parser CEF. Les extensions et extensions personnalisées sont facultatives. Le modèle CEF d'audit par défaut contient bon nombre des champs de ce tableau. Vous pouvez ajouter les extensions et les extensions personnalisées répertoriées de votre choix au modèle de consignation globale des audits que vous définissez.

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
Préfixe Syslog				
Datetime	Non configurable	Date/heure d'en-tête Syslog	event.time.str	Transient
Nom de l'hôte	Non configurable	Nom d'hôte d'en-tête Syslog	alias.host	Aucun

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
En-tête CEF		Les champs d'en-tête CEF sont requis pour se conformer à la norme CEF ou pour tout parser CEF.		
CEF:Version	CEF:0	En-tête CEF	--STATIQUE--	s.o.
DeviceVendor	${deviceVendor}	Fournisseur du produit, RSA	-	s.o.
DeviceProduct	${deviceProduct}	Gamme de produits Il s'agit toujours de NetWitness Suite Audit.	product	Transient
DeviceVersion	${deviceVersion}	Version de l'hôte/du service	version	Transient
Signature ID	${category}	Identifiant de l'événement d'audit. Il indique la catégorie de l'événement d'audit.	event.type	Aucune
Name	${operation}	Description de l'événement	event.desc	Aucune

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
Gravité	${severity}	Gravité de l'événement d'audit	severity	Transient
Extensions				
deviceExternalId	${deviceExternalId}	ID unique de l'hôte ou du service générant l'événement d'audit	hardware.id	Transient
deviceFacility	${deviceFacility}	Fonction Syslog utilisée lors de l'écriture de l'événement dans le processus Syslog. Par exemple, authpriv.	cs.devfacility	Custom
deviceProcessName	${deviceProcessName}	Nom du fichier exécutable correspondant à dvcpid	process	Aucune
dpt	${destinationPort}	Port de destination	ip.dstport	Aucune
dst	${destinationAddress}	Adresse IP de destination	ip.dst	Aucune

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
dvcpid	${deviceProcessId}	ID du processus générant l'événement, qui est l'ID de processus du service NetWitness Suite	process.id	Transient
msg	${text}	Texte libre, informations supplémentaires ou description réelle de l'événement	msg	Transient
outcome	${outcome}	Résultat de l'opération effectuée correspondant à l'événement d'audit	result	Transient
proto	${transportProtocol}	protocole réseau utilisé.	protocol	Transient
requestClientApplication	${userAgent}	Détails du navigateur de l'utilisateur accédant à la page	user.agent	Transient
rt	${timestamp}	Heure à laquelle l'événement est signalé	event.time	Aucune

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
sourceServiceName	${sourceService}	Service chargé de la génération de cet événement	service.name	Transient
spt	${sourcePort}	Port source	ip.srcport	Transient
spriv	${userRole}	Attribution des autorisations du rôle d'utilisateur. Par exemple : admin.owner, appliance.manage, connections.manage, everyone, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	privilege	Transient
src	${sourceAddress}	Adresse IP d'origine	ip.src	None

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
suser	${identity}	Identité de l'utilisateur connecté chargé de la génération de l'événement d'audit	user.dst	Aucun
Extensions personnalisées				
deviceService	${deviceService}	Service chargé de la génération de l'événement	cs.devservice	Custom
paramètres	${parameters}	Paramètres API et Operation qui permettent de capturer les paramètres spécifiques d'une requête	index	Transient
paramKey	${key}	Clé d'élément de configuration. Il s'agit d'un paramètre de configuration pour lequel l'événement d'audit est capturé. Par exemple : /sys/config/stat.interval	cs.key	Custom

Champ CEF	String	Description	Métaclés NW	Index dans Log Decoder
paramValue	${value}	Valeur de configuration. Il s'agit de la valeur capturée lors de la mise à jour.	cs.value	Custom
userGroup	${userGroup}	Attribution de rôle. Par exemple : Administrateurs, Analystes, Analystesdumalware, Analystes_du_malware, Opérateurs, PRIVILEGED_CONNECTION_AUTHORITY, Responsables_du_SOC	group	None
referrerURL	${referrerUrl}	URL parente faisant référence à l'URL actuelle	url	Transient
sessionId	${sessionId}	Identifiant de session ou de connexion	log.session.id	Transient

Remarque : Utilisez toutes les extensions au format suivant :
`deviceProcessName=${deviceProcessName} outcome=${outcome}`
Insérez un `<space>` entre une valeur et un nom de balise.

Par défaut, les métaclés ne sont pas toutes indexées. Dans le tableau ci-dessus, la colonne **Index dans Log Decoder** affiche l'état du mot clé `flags` (Transient, None et Custom). Si une clé est définie sur `Transient`, elle est analysée, mais elle n'est pas stockée dans la base de données. Si elle est définie sur `None`, elle est indexée et stockée dans la base de données. Une clé répertoriée avec le type « Personnalisé » n'existe pas dans le fichier table-map.xml et n'est donc pas stockée ni analysée du tout.

La rubrique « Maintenir les fichiers de mappage des tables » fournit des instructions pour vérifier et mettre à jour les mappages des tables. La section « Modifier un fichier d'index de service » fournit des informations sur la mise à jour du fichier d'index personnalisé sur le Concentrator.

Variables de métaclés prises en charge pour la consignation globale des audits

Cette section décrit les variables de métaclés prises en charge par la consignation globale des audits de NetWitness Suite.

NetWitness Suite inclut des modèles prédéfinis de consignation globale des audits que vous pouvez utiliser pour les configurations correspondantes. Pour les serveurs Syslog tiers, vous pouvez définir votre propre format (CEF ou non-CEF) en utilisant les variables de métaclés prises en charge.

Les procédures relatives à ce tableau sont décrites dans les sections Définir un modèle pour la consignation globale des audits et Configurer la consignation globale des audits.

Variables de métaclés prises en charge pour la consignation globale des audits

Le tableau suivant décrit les variables de métaclés prises en charge par la consignation globale des audits NetWitness Suite. Utilisez ces valeurs pour créer un modèle de consignation personnalisée des audits pour un serveur syslog tiers.

Variable	Description
${category}	Identifiant de l'événement d'audit. Il indique la catégorie de l'événement d'audit.
${destinationAddress}	Adresse IP de destination
${destinationPort}	Port de destination
${deviceExternalId}	ID unique du service générant l'événement d'audit
${deviceFacility}	Fonction Syslog utilisée lors de l'écriture de l'événement dans le processus Syslog. Par exemple, authpriv.
${deviceProcessId}	ID du processus générant l'événement, qui est l'ID de processus du service NetWitness Suite
${deviceProcessName}	Nom du fichier exécutable correspondant à dvcpid
${deviceProduct}	Gamme de produits Il s'agit toujours de NetWitness Suite Audit.

Variable	Description
${deviceService}	Service chargé de la génération de l'événement
${deviceVendor}	Fournisseur du produit, RSA
${deviceVersion}	Host/Service version
${identity}	Identité de l'utilisateur connecté chargé de la génération de l'événement d'audit
${key}	Clé d'élément de configuration. Il s'agit d'un paramètre de configuration pour lequel l'événement d'audit est capturé.
${operation}	Description de l'événement
${outcome}	Résultat de l'opération effectuée correspondant à l'événement d'audit
${parameters}	Paramètres API et Operation qui permettent de capturer les paramètres spécifiques d'une requête
${referrerUrl}	URL parente faisant référence à l'URL actuelle
${sessionId}	Identifiant de session ou de connexion
${severity}	Gravité de l'événement d'audit
${sourceAddress}	Adresse IP d'origine
${sourcePort}	Port source
${sourceService}	Service chargé de la génération de cet événement
${text}	Texte libre, informations supplémentaires ou description réelle de l'événement
${timestamp}	Heure à laquelle l'événement est signalé
${transportProtocol}	protocole réseau utilisé.
${userAgent}	Détails du navigateur de l'utilisateur accédant à la page

Variable	Description
${userGroup}	Attribution de rôle
${userRole}	Attribution des autorisations du rôle d'utilisateur
${value}	Valeur de configuration. Il s'agit de la valeur capturée lors de la mise à jour

Référence aux opérations de consignation globale des audits

Cette section répertorie les types de messages consignés par les différents composants NetWitness Suite. La plupart des messages indique clairement l'opération consignée. En cas de besoin, la signification du message est expliquée.

Une fois que vous avez créé une configuration de consignation globale des audits, les logs d'audit vont automatiquement dans le système syslog externe au format spécifié dans le modèle de consignation des audits sélectionné. Les types de messages consignés par les différents composants NetWitness Suite sont indiqués dans les tableaux suivants.

CARLOS

Le tableau suivant répertorie les opérations consignées par CARLOS.

Serial #	Nom de l'opération	Signification
1	SetProviderConfiguration	Un nouveau serveur de notification (par exemple, un serveur SMTP) a été ajouté ou mis à jour
2	SetInstanceConfiguration	Un nouveau type de notifications (par exemple, une destination d'e-mail) a été ajouté ou mis à jour
3	SetTemplateDefinition	Un nouveau modèle a été ajouté ou mis à jour
4	RemoveProviderConfiguration	Un serveur de notification a été supprimé
5	RemoveInstanceConfiguration	Un type de notifications a été supprimé
6	RemoveTemplateDefinition	Une définition de modèle a été supprimée
7	Commit	Une modification de bean de configuration a été validée

Serial #	Nom de l'opération	Signification
8	Set	Une valeur de propriété JMX a été définie via la vue Explorer de NetWitness Suite

ESA

Le tableau suivant répertorie les opérations consignées par Event Stream Analysis (ESA).

Serial #	Nom de l'opération	Signification
9	SetSourceRequest	Un Concentrator a été ajouté ou mis à jour dans ESA en tant que source
10	RemoveSourceRequest	Un Concentrator a été supprimé d'ESA en tant que source
11	SetEplModule	Un module EPL a été déployé ou mis à jour dans ESA
12	RemoveEplModule	Un module EPL a été supprimé d'ESA
13	SetEnrichmentSourceRequest	Une source d'enrichissement ESA a été ajoutée/mise à jour
14	RemoveEnrichmentSourceRequest	Une source d'enrichissement ESA a été supprimée
15	SetDatabaseReference	Une référence de base de données d'enrichissement a été définie dans ESA
16	UpdateEnrichmentData	Lignes de données ajoutées à une source d'enrichissement ESA

Serial #	Nom de l'opération	Signification
17	SetEnrichmentConnection	Une connexion a été établie entre un module EPL et une source d'enrichissement
18	RemoveEnrichmentConnection	Une connexion entre un module EPL et une source d'enrichissement a été supprimée
19	DisableTrialModule	Les règles d'évaluation ESA ont été désactivées

Investigation

Le tableau suivant répertorie les opérations consignées par Investigations.

Serial #	Nom de l'opération	Signification
1	VisualizePreferences	Opérations liées à la demande de visualisation Informateur.
2	ParallelCoordinates	Opérations liées au chargement de la navigation dans la vue Coordonnées.
3	TimeLine	Opérations liées au chargement de la navigation dans la vue Chronologie.
4	ExternalQuery	Opération lors du déclenchement d'une requête directe via une URL.
5	PrintView	Opérations pour ouvrir la procédure d'enquête en mode Impression.
6	submitExtractFiles	Opération de soumission d'une demande d'extraction de fichiers depuis les sessions.

Serial #	Nom de l'opération	Signification
7	submitExtractLogs	Opération de soumission d'une demande d'extraction de logs depuis les sessions.
8	submitExtractPcap	Opération de soumission d'une demande d'extraction de logs depuis les sessions.
9	DataScienceDrill	Opération de recherche dans le rapport Data Science.
10	breadCrumbs	Opération d'accès à la requête Breadcrumbs.
11	Create	Opération lorsqu'une nouvelle requête de procédure d'enquête est enregistrée en tant que prédicat à utiliser pour l'intégration d'URL.
12	userPredicates	Opération d'accès aux requêtes récentes d'un utilisateur.
13	chartDefaultMetas	Opération d'accès aux dernières métadonnées utilisées afin de générer le graphique des coordonnées.
14	defaultDevice	Opération d'accès au périphérique de procédure d'enquête par défaut.
15	deleteDefaultDevice	Opération de suppression du périphérique de procédure d'enquête par défaut.

Serial #	Nom de l'opération	Signification
16	chartPreferences	Opération de modification d'un paramètre de graphique de navigation, par exemple Hauteur.
17	devicePreferences	Opération d'enregistrement des préférences relatives au périphérique de la procédure d'enquête, par exemple Période, Profil, Groupes méta, etc.
18	topValues	Opération d'obtention des valeurs principales des métas. Normalement, appelée à partir du dashlet Valeurs principales.
19	MetaLanguages	Opération de lecture des méta-langues méta à partir d'un périphérique.
20	MetaGroups	Opérations liées aux groupes méta de procédure d'enquête.
21	DefaultMetaKeys	Opérations liées aux clés méta par défaut de procédure d'enquête.
22	UpdateDefaultMetaKeys	Opérations de mise à jour des clés méta par défaut de procédure d'enquête.
23	UpdateMetaGroup	Opérations de mise à jour des groupes méta de procédure d'enquête.
24	ApplyMetaGroup	Opérations d'utilisation des groupes méta de procédure d'enquête.

Serial #	Nom de l'opération	Signification
25	DeactivateMetaGroup	Opérations de réinitialisation des groupes méta de procédure d'enquête dans l'interface utilisateur.
26	DeleteMetaGroup	Opérations de suppression d'un groupe méta de procédure d'enquête.
27	DeleteMetaGroups	Opérations de suppression de plusieurs groupes méta de procédure d'enquête.
28	ImportMetaGroups	Opérations d'importation de groupes méta de procédure d'enquête.
29	ExportMetaGroup	Opérations d'exportation de plusieurs groupes méta de procédure d'enquête.
30	GeoMap	Opération d'accès à la vue de la carte géospatiale de procédure d'enquête.
31	deleteEndpointCache	Opération d'effacement du cache de reconstruction d'un périphérique.
32	delete	Opération de suppression de modèles d'alerte.
33	CustomColumnGroup	Opération d'application ou de lecture d'un groupe de colonnes personnalisé.
34	Import	Opérations liées à l'importation d'un groupe de colonnes ou de profils.

Serial #	Nom de l'opération	Signification
35	Export	Opérations liées à l'exportation d'un groupe de colonnes, ou de profils.
36	SaveProfile	Opération d'enregistrement d'un profil de procédure d'enquête.
37	ApplyProfile	Opération d'application d'un profil de procédure d'enquête.
38	DeactivateProfile	Opération de désactivation d'un profil de procédure d'enquête.
39	DeleteProfile	Opération de suppression d'un profil de procédure d'enquête.
40	DeleteProfiles	Opération de suppression de plusieurs profils de procédure d'enquête.

Reporting Engine

Le tableau suivant répertorie les opérations consignées par Reporting Engine.

Serial #	Nom de l'opération	Signification
1	TEMPLATE	Pour toutes les opérations relatives à un modèle
2	CHART	Pour toutes les opérations relatives à un graphique
3	REPORT	Pour toutes les opérations relatives à un rapport
4	RULE	Pour toutes les opérations relatives à une règle

Serial #	Nom de l'opération	Signification
5	IMAGE	Pour toutes les opérations relatives aux images de logo utilisées dans les rapports.
6	LIST	Pour toutes les opérations relatives à une liste
7	ALERT	Pour toutes les opérations relatives à une alerte
8	CONFIG	Pour toutes les opérations relatives à une modification de configuration
9	SCHEDULE	Pour toutes les opérations relatives à une planification
10	ROLE	Pour toutes les opérations relatives à un rôle/une autorisation
11	BATCH_JOB	Pour toutes les opérations relatives à des tâches par lots
12	SCHEDULER	Pour toutes les opérations relatives au planificateur
13	QUERYPROCESSOR	Pour toutes les opérations relatives au processeur de requête
14	FORMATTER	Pour toutes les opérations relatives au programme de mise en forme
15	OUTPUTACTION	Pour toutes les opérations relatives à une action de sortie
16	STATUSMANAGER	Pour toutes les opérations relatives au gestionnaire d'état

Serial #	Nom de l'opération	Signification
17	BATCH_RUNDEF	Pour toutes les opérations relatives à une définition d'exécution d'un lot
18	CHARTGROUP	Pour toutes les opérations relatives à un groupe de graphiques
19	REPORTGROUP	Pour toutes les opérations relatives à un groupe de rapports
20	RULEGROUP	Pour toutes les opérations relatives à un groupe de règles
21	LISTGROUP	Pour toutes les opérations relatives à un groupe de listes
22	DISKSPACE	Pour toutes les opérations relatives à l'espace disque

Warehouse Connector

Le tableau suivant répertorie les opérations consignées par Warehouse Connector.

Serial #	Nom de l'opération	Signification
1	Création du mot de passe LockBox	Opération de création du mot de passe LockBox.
2	Mise à jour du mot de passe LockBox	Opération de mise à jour du mot de passe LockBox.
3	Actualisation du mot de passe LockBox	Opération d'actualisation du mot de passe LockBox.
4	Ajout d'un flux	Opération d'ajout d'un flux.
5	Ajout d'une source	Opération d'ajout d'une source.
6	Ajout d'une destination	Opération d'ajout d'une destination.

Serial #	Nom de l'opération	Signification
7	Suppression	Opération de suppression d'une source, d'un flux ou d'une destination.
8	Modification du mot de passe	Opération de modification du mot de passe.
9	Mise à jour de la source	Opération de mise à jour d'une source.
10	Ajout d'une source à un flux	Opération d'ajout d'une source à un flux.
11	Suppression d'une source d'un flux	Opération de suppression d'une source dans un flux.
12	Définition de la destination d'un flux	Opération de définition d'une destination dans un flux.
13	Finalisation d'un flux	Opération de finalisation d'un flux et de lancement de l'agrégation.
14	Arrêt d'un flux	Opération d'arrêt d'un flux.
15	Démarrage d'un flux	Opération de démarrage d'un flux.
16	Rechargement d'un flux	Opération de rechargement d'un flux.

Intégrité

Le tableau suivant répertorie les opérations consignées par le module d'intégrité Health & Wellness.

Serial #	Nom de l'opération	Signification
1	SavePolicyRequest	Opération pendant l'ajout ou la modification d'une règle.
2	RemovePolicyRequest	Opération pendant la suppression d'une stratégie.

Services de base NetWitness Suite

Le tableau suivant répertorie les opérations consignées par les services NetWitness Suite Core.

Serial #	Nom de l'opération	Signification
1	FILE_Command	Opération visant à répertorier, récupérer et supprimer des fichiers sur ce périphérique dans les répertoires approuvés.
2	SERVICE_Start	Service démarré
3	SERVICE_Stop	Service arrêté
4	REDIRECT_Syslog	Opération de transfert du syslog.
5	ADD_Monitor	Déclenchement d'une opération de surveillance du système de fichiers
6	DELETE_Monitor	Déclenchement d'une opération de suppression de la surveillance du système de fichiers
7	SHUTDOWN_Service/shutdown.service	Arrêt du service Appliance
8	REBOOT_Service	Redémarrage du service Appliance
9	CONFIGURE_Network	Déclenchement de la modification de configuration réseau
10	SET_NTP	Déclenchement de l'opération de définition NTP
11	STOP_NTP	Déclenchement de l'opération d'arrêt NTP
12	NTP_Timesync	Déclenchement de l'opération de synchronisation horaire NTP

Serial #	Nom de l'opération	Signification
13	SET-SNMP	Déclenchement de l'opération de définition SNMP
14	UPGRADE/upgrade	Déclenchement de l'opération de mise à niveau
15	create.collection	Opération de création d'une collecte vide.
16	restore	Déclenchement de la restauration
17	session.aggregation	Déclenchement du démarrage/de l'arrêt de l'agrégation
18	add.device	Ajout d'un périphérique pour l'agrégation
19	edit.device	Modification d'un périphérique utilisé pour l'agrégation
20	delete.device	Suppression d'un périphérique utilisé pour l'agrégation
21	capture.start	Démarrage de l'opération de capture
22	capture.stop	Arrêt de l'opération de capture
23	select.interface	Sélection d'une interface de capture
24	export	Opération d'exportation des paquets ou des sessions.
25	reload	Déclenchement du rechargement d'un parser
26	schema	Déclenchement d'une demande de schéma pour des parsers chargés

Serial #	Nom de l'opération	Signification
27	upload/file.upload	Déclenchement d'un téléchargement de fichier
28	notify	Déclenchement d'une notification de flux
29	delete	Déclenchement d'une suppression de fichier
30	edit.config	Opération de modification de configuration
31	parsers.transforms	Transformation d'une clé de langage
32	data.reset	Opération de réinitialisation des données
33	timeout	Expiration du délai de demande REST
34	cancel	Annulation d'une requête en cours d'exécution
35	timeroll	Opération de suppression des fichiers de base de données qui dépassent une limite donnée.
36	dump	Opération de vidage des informations de la base de données sous forme de fichiers nwd.
37	session.wipe	Déclenchement d'une opération d'effacement de session
38	REPLACERule	Déclenchement d'une opération de remplacement de règle

Serial #	Nom de l'opération	Signification
39	MERGERule	Déclenchement d'une opération de fusion de règles
40	ERASERule	Déclenchement de la suppression d'un groupe comprenant toutes les règles
41	ADDRule	Déclenchement d'une opération d'ajout de règle
42	DELETERule	Déclenchement de la suppression d'un groupe de règles
43	sdk.info	Déclenchement des informations de récapitulatif SDK.
44	sdk.session	Déclenchement des informations de session SDK.
45	sdk.language	Déclenchement du langage SDK
46	sdk.aliases	Déclenchement d'une demande d'alias SDK
47	sdk.transform	Déclenchement d'une demande de transformation SDK
48	sdk.search	Déclenchement d'une demande de recherche de contenu de session
49	sdk.cache	Opération relative au cache du contenu de session
50	sdk.content	Déclenchement d'une demande de contenu de session

Serial #	Nom de l'opération	Signification
51	check.authorization	Opération de vérification des rôles d'utilisateur pour les autorisations d'exécution d'une opération.
52	close.connection	Déclenchement d'une opération de fermeture de connexion
53	handshake	Déclenchement de l'établissement d'une liaison SSL
54	logon/login	Opération de connexion depuis SA vers les autres services, principalement pour les utilisateurs privilégiés.
55	STOREDPROCOP	Déclenchement de l'annulation/du démarrage du téléchargement de fichiers
56	ADDTask	Tâche planifiée ajoutée
57	DELETETask	Tâche planifiée supprimée
58	logoff	Déclenchement de l'opération de déconnexion
59	list.cacerts	Déclenchement de l'opération visant à répertorier les certificats d'autorités de certification de confiance
60	delete.cacerts	Déclenchement de l'opération de suppression de certificats d'autorités de certification de confiance

Serial #	Nom de l'opération	Signification
61	add.cacerts	Déclenchement de l'opération d'ajout de certificats d'autorités de certification de confiance
62	restart.command	Déclenchement du redémarrage de l'option de ligne de commande
63	delete.file/file.delete	Opération de suppression de fichiers de configuration système.
64	update.file/file.update	Opération de mise à jour du fichier de configuration système.
65	create.file	Déclenchement de l'opération de création de fichier
66	query	Déclencher une requête de base de données
67	unlock	Déclenchement d'une opération de déverrouillage de compte utilisateur
68	user.add	Opération de création de comptes utilisateur sur différents périphériques.
69	user.delete	Opération de suppression d'un utilisateur sur différents périphériques.
70	group.create	Opération d'ajout d'un nouveau groupe au système.
71	user.remove	Supprimer un compte utilisateur d'un groupe
72	group.delete	Supprimer un groupe de l'arborescence des utilisateurs/des groupes

Serial #	Nom de l'opération	Signification
73	add.user	Déclenchement de la commande d'ajout d'un utilisateur à une collecte
74	delete.user	Déclenchement de la commande de suppression d'un utilisateur d'une collecte
75	remove.user	Suppression d'un utilisateur d'une collecte
76	collection.open	Déclenchement d'une commande d'ouverture d'une collecte
77	collection.close	Déclenchement d'une commande de fermeture d'une collecte
78	collection.delete	Déclenchement d'une commande de suppression de collecte
79	reingest.start	Opération pour commencer la réingestion des données de paquet dans la collecte.
80	feed.notify	Déclenchement d'une commande de notification de flux
81	collect	Déclenchement d'une commande de collecte
82	collect.start	Déclenchement du démarrage d'une collecte de données
83	collection.global	Déclenchement d'une commande d'importation de parser

Serial #	Nom de l'opération	Signification
84	parser.reload	Émet une commande de recharge du parser
85	reingest	Opération de réingestion de données de paquet dans une collecte.
86	collection.create	Déclenchement d'une commande de création de collecte
87	collection.restore	Déclenchement d'une commande de restauration de collecte
88	collection.clone	Déclenchement d'une commande de clonage de collecte
89	parser.reload	Émet une commande de recharge du parser
90	sdk.query	Effectue une requête sur la base de données méta
91	sdk.msearch	Recherche des correspondances de modèles dans de nombreuses sessions ou de nombreux paquets
92	sdk.values	Effectue une requête sur un nombre de valeurs et renvoie les valeurs correspondantes pour un rapport
93	sdk.timeline	Renvoie le nombre de sessions/tailles/paquets dans les intervalles de temps discrets

Malware Analysis

Le tableau suivant répertorie les opérations consignées par le composant Malware Analysis (MA).

Serial #	Nom de l'opération	Signification
1	GetDashBoardSummaryRequest	Obtenir les statistiques d'analyse du tableau de bord
2	GetFileScoreSummaryRequest	Obtenir les scores de fichiers agrégés par type de scores et par niveau de risque
3	CountEventsAndFilesRequest	Obtenir le nombre d'événements et de fichiers sur un laps de temps
4	GetAvVendorDetectionRequest	Obtenir les résultats d'analyse des fournisseurs antivirus
5	GetAVVendorsRequest	Obtenir la liste des fournisseurs antivirus pris en charge
6	SetInstalledAVVendors	Demander la liste des mises à jour des fournisseurs antivirus installés dans la configuration
7	CountEventByCriteriaRequest	Dénombrer les événements par critères
8	FindEventByIdRequest	Obtenir un événement par ID
9	FindEventByCriteriaRequest	Obtenir un événement par critères
10	DeleteEventRequest	Supprimer un événement
11	CommentOnEventRequest	Ajouter un commentaire à un événement
12	ReSubmitEventRequest	Resoumettre un événement pour analyse

Serial #	Nom de l'opération	Signification
13	FindEventScoreByIdRequest	Obtenir le score d'un événement par ID d'événement
14	FindEventScoreByCriteriaRequest	Obtenir le score d'un événement par critères
15	FindMetaByIdRequest	Obtenir des métadonnées par ID
16	FindMetaByCriteriaRequest	Obtenir des métadonnées par critères
17	FindMetaValueByCriteriaRequest	Obtenir des métavaleurs par critères
18	CountByDistinctMetaValueRequest	Dénombrer les métavaleurs distinctes
19	CountByMetaNameAndValueWithDate RangeIntervalRequest	Dénombrer les métadonnées et les valeurs avec un intervalle pour les graphiques
20	CountByValueAndAverageOverallScore Request	Dénombrer les métadonnées et les mapper aux scores globaux des événements
21	CountByValueAndAverageGroupScore Request	Dénombrer les métadonnées et les mapper aux scores de groupe des événements
22	CountFileEntryByCriteriaRequest	Dénombrer les fichiers par critères
23	FindFileEntryByIdRequest	Obtenir un fichier par ID
24	FindFileEntryByCriteriaRequest	Obtenir un fichier par critères
25	ReSubmitFileEntryRequest	Resoumettre un fichier pour analyse
26	FileDownloadRequest	Télécharger un fichier à partir du référentiel

Serial #	Nom de l'opération	Signification
27	FileUploadRequest	Télécharger un fichier pour analyse
28	FindFileScoreByIdRequest	Obtenir un score de fichier par ID
29	FindFileScoreByCriteriaRequest	Obtenir un score de fichier par critères
30	FindHashValueByIdRequest	Obtenir une valeur de hachage pour liste blanche/liste noire par id
31	FindHashValueByCriteriaRequest	Obtenir une valeur de hachage pour liste blanche/liste noire par critères
32	AddHashValueRequest	Ajouter une valeur de hachage pour liste blanche/liste noire
33	UpdateHashValueRequest	Mettre à jour une valeur de hachage pour liste blanche/liste noire
34	DeleteHashValueRequest	Supprimer une valeur de hachage pour liste blanche/liste noire
35	FindHashValueByMd5Request	Rechercher une valeur de hachage pour liste blanche/liste noire par md5
36	AddHashValueInFileRequest	Ajouter un fichier au référentiel, ainsi qu'une valeur de hachage
37	GetDefaultRulesRequest	Obtenir la configuration des règles d'IOC par défaut

Serial #	Nom de l'opération	Signification
38	ResetToDefaultRulesRequest	Réinitialiser la configuration des règles d'IOC par défaut
39	GetAllOverrideRulesRequest	Obtenir la configuration des règles d'IOC de remplacement créées par l'utilisateur
40	FindOverrideRuleByIdRequest	Rechercher une règle d'IOC de remplacement par ID
41	AddOverrideRuleRequest	Ajouter une règle d'IOC de remplacement
42	UpdateOverrideRuleRequest	Mettre à jour une règle d'IOC de remplacement
43	DeleteOverrideRuleRequest	Supprimer une règle d'IOC de remplacement
44	SubmitOnDemandNextGenRequest	Soumettre une nouvelle analyse nextgen à la demande
45	FindOnDemandJobEntryByIdRequest	Obtenir une entité de tâche à la demande par ID
46	FindOnDemandJobEntryByCriteria Request	Obtenir une entité de tâche à la demande par critères
47	GetOnDemandJobInfoRequest	Obtenir une entité de référence pour une tâche à la demande par ID
48	GetOnDemandDefaultConfiguration	Demander/obtenir une configuration par défaut à la demande
49	CancelOnDemandJobRequest	Annuler une tâche à la demande en cours d'exécution
50	DeleteOnDemandJobRequest	Supprimer une tâche à la demande

Serial #	Nom de l'opération	Signification
51	ReSubmitOnDemandJobRequest	Resoumettre une tâche à la demande
52	SubscriptionRequest	S'abonner à la communication Cloud MA
53	UnSubscribeRequest	Se désabonner de la communication Cloud MA
54	GetTopEventInfluencesRequest	Obtenir les N premières influences d'événement
55	GetServerInfoRequest	Obtenir les informations d'un serveur, par exemple l'heure
56	DataResetRequest	Réinitialiser la base de données
57	OnDemandJobStatusNotification	Signaler la progression d'une tâche à la demande aux abonnées
58	LicenseStatusNotification	Signaler l'état de la licence - nombre d'échantillons analysés
59	DataResetNotification	Signaler la réinitialisation des données
60	GetIocSummaryRequest	Obtenir les règles d'IOC agrégées par scores d'événements/de fichiers
61	FindAlertTemplatesByCriteriaRequest	Obtenir les modèles d'alerte rabbitmq par critères
62	SaveAlertTemplateRequest	Mettre à jour un modèle d'alerte
63	DeleteAlertTemplateRequest	Supprimer un modèle d'alerte
64	GetJobStatusRequest	Obtenir l'état du thread d'analyse de tâche en cours d'exécution

Serial #	Nom de l'opération	Signification
65	GetEventTypeCountSummaryRequest	Obtenir les nombres d'analyses d'événements par graphique de dates
66	Connexion	Connexion au service MA
67	Modifiée	Modification des changements de configuration
68	GetNextGenSummaryRequest	Obtenir les statistiques récapitulatives du tableau de bord nextgen

Interface utilisateur NetWitness Suite

Le tableau suivant répertorie les opérations consignées par le composant d'interface utilisateur de NetWitness Suite.

Serial #	Nom de l'opération	Signification
1	uploadTrialLicense	Télécharger la licence d'évaluation
2	LicenseEntitle	Attribuer des droits de licence
3	LicenseDeactivation	Désactiver une licence
4	ExpiredLicense	Licence expirée
5	LicenseOutOfComplianceAcknowledgement	Acceptation des CGU (conditions générales d'utilisation)
6	resetLicense	Réinitialiser une licence
7	usageDateExport	Utilisation des données de licence -csv/pdf
8	refreshLicense	Actualiser la licence LLS

Serial #	Nom de l'opération	Signification
9	LicenseOutOfCompliance	Non conforme
10	OOTBEntitlementOutOfCompliance	Sous licence d'évaluation OOTB non conforme
11	OOTBEntitlementFirstLoginTimeModified	Heure OOTB modifiée
12	OOTBEntitlementFileDeleted	Fichier OOTB supprimé
13	OOTBEntitlementDataTampering	Falsification des données OOTB
14	uploadOfflineResponse	Télécharger une réponse hors ligne
15	offlineDownloadCapRequest	Télécharger la demande hors ligne
16	movePerpetualToMetered	Passer d'une licence basée sur les services à une licence à suivi d'utilisation
17	moveMeteredToPerpetual	Passer d'une licence à suivi d'utilisation à une licence basée sur les services
18	mapServiceLicense	Mapper un service à une licence réelle
19	delete	Opération de suppression de modèles d'alerte.
20	HttpRequest	Opération de consignation des audits de l'URL utilisée.
21	Page consultée	Opération de consignation des audits de la page consultée.

Serial #	Nom de l'opération	Signification
22	Naviguer	Opération d'accès à la page consultée.
23	Événements	Opération d'affichage de la page d'événement consultée.
24	Recon	Opération de reconstruction d'événement demandée.
25	Services	Opération en lisant la liste des périphériques disponibles pour la procédure d'enquête.
26	Service	Opération liée à une liste de périphériques demandée à examiner.
27	Collectes	Opération d'affichage de la liste de collectes demandée.
28	Profils	Opération d'application d'un profil.
29	ColumnGroups	Opération d'application ou de lecture d'un groupe de colonnes.
30	ParallelCoordinates	Opérations liées au chargement de la navigation dans la vue Coordonnées.
31	Chronologie	Opérations liées au chargement de la navigation dans la vue Chronologie.

Serial #	Nom de l'opération	Signification
32	PrintView	Opérations d'ouverture d'une procédure d'enquête en mode Impression.
33	Préférences	Opérations liées à la demande Informateur.
34	import	Opérations liées à l'importation d'un groupe de colonnes ou de profils.
35	export	Opérations liées à l'exportation d'un groupe de colonnes, ou de profils.
36	Prédicat	Opérations liées aux requêtes (prédicats) utilisées pour la procédure d'enquête.
37	Langues	Opération pour la langue demandée à partir d'un périphérique.
38	CancelLanguageLoad	Opération pour le chargement de langue annulé dans la page de navigation.
39	summary	Opération pour un récapitulatif demandé à partir d'un périphérique.
40	languages	Opération pour une langue demandée à partir d'un périphérique.

Serial #	Nom de l'opération	Signification
41	aliases	Opération pour les alias de métadonnées demandés à partir d'un périphérique.
42	query	Opération pour une requête SDK demandée à partir d'un périphérique.
43	msearch	Opération pour une recherche de métadonnées demandée à partir d'un périphérique.
44	nodeListing	Liste des nœuds pour un nœud demandé à partir d'un périphérique.
45	content	Appel de contenu SDK demandé à partir d'un périphérique pour le téléchargement d'un fichier PCAP ou d'un log.
46	Exporter des fichiers	Liste de fichiers demandée pour une session en mode Fichiers ou des tâches d'extraction.
47	packets	Paquets demandés pour les sessions en mode Paquets ou des tâches d'extraction.
48	deleteEndpointCache	Opération d'effacement du cache de reconstruction d'un périphérique.

Serial #	Nom de l'opération	Signification
49	Connexion	Opération qui permet à l'utilisateur de se connecter à l'interface utilisateur NetWitness Suite.
50	Logoff	Opération qui permet à l'utilisateur de se déconnecter de l'interface utilisateur NetWitness Suite.
51	defaultDevice	Opération d'accès pour accéder au périphérique de l'interface utilisateur SA par défaut.
52	deleteDefaultDevice	Opération de suppression du périphérique de procédure d'enquête par défaut.
53	submitExtractFiles	Opération de soumission d'une demande d'extraction de fichiers depuis les sessions.
54	submitExtractLogs	Opération de soumission d'une demande d'extraction de logs depuis les sessions.
55	submitExtractPcap	Opération de soumission d'une demande d'extraction de logs depuis les sessions.
56	MetaGroup	Opérations liées aux groupes méta de l'interface utilisateur SA.

Serial #	Nom de l'opération	Signification
57	ExternalQuery	Opération lors du déclenchement d'une requête directe via une URL.
58	GeoMap	Opération d'accès à la vue de la carte géospatiale de procédure d'enquête.
59	SaveProfile	Opération d'enregistrement d'un profil de procédure d'enquête.
60	ApplyProfile	Opération d'application d'un profil de procédure d'enquête.
61	DeleteProfile	Opération d'application d'un profil de procédure d'enquête.
62	DeactivateProfile	Opération d'application d'un profil de procédure d'enquête.
63	VisualizePreferences	Opérations liées à la demande de visualisation Informateur.
64	ExportMetaGroup	Opérations d'exportation de plusieurs groupes méta de l'interface utilisateur SA.
65	userPredicates	Opérations d'exportation de plusieurs groupes méta de l'interface utilisateur SA.
66	FileView	Opération pour la demande de reconstruction pour le mode Fichiers.

Serial #	Nom de l'opération	Signification
67	resource.update	Opération lors du changement d'état d'abonnement Live.

Répondre

Le tableau suivant répertorie les opérations consignées par le composant RÉPONDRE.

Serial #	Nom de l'opération	Signification
1	update	Mettre à jour le paramètre de notification
2	update	Mettre à jour la configuration des paramètres d'intégration
3	delete	Supprimer les alertes
4	create	Créer un nouvel incident
5	update	Mettre à jour les détails de l'incident
6	read	Lire les détails de l'incident
7	delete	Supprimer les incidents
8	read	Lire les tâches de correction
9	delete	Supprimer les tâches de correction
10	update	Mettre à jour les tâches de correction
11	create	Création d'une règle :
12	update	Mettre à jour une règle d'alerte existante
13	reorder	Réorganiser la priorité des règles d'alerte

Emplacements des logs d'audit locaux

NetWitness Suite possède des fonctionnalités de consignation d'audit globale. Lorsque vous configurez une consignation d'audit globale, les logs d'audit de tous les composants NetWitness Suite effectuent la collecte dans un système centralisé, qui les convertit au format requis et les transfère à un serveur syslog tiers ou un Log Decoder.

Pour afficher les logs d'audit à partir des services individuels, vous pouvez consulter les emplacements des logs d'audit locaux. Le tableau suivant présente les chemins de répertoire locaux des logs d'audit pour l'interface utilisateur NetWitness Suite et les différents services NetWitness Suite.

Service/Module	Emplacement du log d'audit
NetWitness Suite Interface utilisateur (serveur Web NetWitness Suite)	L'interface utilisateur NetWitness Suite envoie des logs d'audit aux emplacements suivants : • **/var/lib/netwitness/uax/logs/audit/audit.log** (format lisible) • Syslog s'exécutant sur l'hôte local (format JSON) L'interface NetWitness Suite utilise la fonctionnalité AUTH de syslog pour écrire les logs d'audit dans syslog. Vous ne pouvez voir les logs d'audit que dans le premier emplacement (/var/lib/netwitness/uax/logs/audit/audit.log).
Services Core (Decoder, Log Decoder, Concentrator, Broker, and Archiver), Log Collector, Warehouse Connector, Workbench et IPDB Extractor	Les services Core et les services similaires envoient des logs d'audit à l'instance Syslog s'exécutant sur l'hôte local. Chemin : **/var/log/secure** (format JSON) Les services Core utilisent la fonctionnalité AUTHPRIV de Syslog pour écrire des logs d'audit dans Syslog.

Service/Module	Emplacement du log d'audit
Reporting Engine, Malware Analysis RÉPONDRE et Event Stream Analysis (ESA)	Ces services envoient des logs d'audit aux emplacements suivants : • **<application home directory>/logs/audit/audit.log** (format lisible) • Syslog s'exécutant sur l'hôte local (format JSON) Les éléments suivants sont les emplacements de log d'audit de ces services : Reporting Engine : **/home/rsasoc/rsa/soc/reporting-engine/logs/audit/audit.log** Serveur Respond /var/log/netwitness/respond-server/respond-server-audit.log Malware Analysis : **/var/lib/netwitness/rsamalware/spectrum/logs/audit/audit.log** Event Stream Analysis : **/opt/rsa/esa/logs/audit/audit.log** Ces services utilisent la fonctionnalité AUTH de syslog pour écrire des logs d'audit dans syslog. Vous ne pouvez afficher les logs d'audit que dans le premier emplacement (<application home directory>/logs/audit/audit.log).
Intégrité, Gestion des sources d'événements (ESM) et Appliance and Service Grouping (ASG)	Ces services envoient des logs d'audit aux emplacements suivants : • **/opt/rsa/sms/logs/audit/audit.log** (format lisible) • Syslog s'exécutant sur l'hôte local (format JSON) Ces services utilisent la fonctionnalité AUTH de syslog pour écrire des logs d'audit dans syslog. Vous ne pouvez afficher les logs d'audit que dans le premier emplacement (répertoire de base de l'application/logs/audit/audit.log).

Résolution des problèmes de configuration du système

Les rubriques de cette rubrique fournissent des informations de dépannage destinées aux administrateurs qui configurent les paramètres s'appliquant à l'ensemble du système de NetWitness Suite.

Résoudre les problèmes liés à la consignation globale des audits

Cette rubrique fournit des informations sur les problèmes potentiels que les utilisateurs de NetWitness Suite peuvent rencontrer lors de l'implémentation de la consignation globale des audits dans NetWitness Suite. Recherchez des explications et solutions dans cette rubrique.

Après avoir configuré la consignation globale des audits, il est recommandé de tester vos logs d'audit pour vous assurer qu'ils contiennent les événements d'audit tels que définis dans votre modèle de consignation des audits. Si vous ne pouvez pas afficher les logs d'audit sur votre serveur syslog ou Log Decoder tiers, ou si les logs d'audit n'apparaissent pas comme ils le devraient, passez en revue les suggestions de dépannage de base ci-dessous. Si vos problèmes persistent, consultez les suggestions de dépannage avancées.

Procédure de dépannage de base

Si vous ne pouvez pas afficher les logs d'audit sur un serveur syslog tiers ou Log Decoder :

- Vérifiez que RabbitMQ est opérationnel.
- Vérifiez la configuration du serveur de notification syslog et assurez-vous qu'il est activé. (Vous trouverez cette configuration dans Admin > Système > Notifications globales. Ne sélectionnez pas Notifications existantes.)
- Vérifiez la configuration de la consignation globale des audits.

Les rubriques Configurer la consignation globale des audits et Vérifier les logs d'audits globaux donnent des instructions. Si vous envoyez des logs d'audit vers un Log Decoder :

- Assurez-vous que le Log Decoder s'agrège au Concentrator sur le même hôte (Administration > Services > (sélectionnez Concentrator) >  > Afficher > Configuration).
- Vérifiez que le dernier parser CEF est déployé et activé.

- Vérifiez le modèle de notification pour la consignation des audits. Vous devez utiliser un modèle CEF et tous les logs arrivant au Log Decoder doivent utiliser un modèle CEF.

Si vous envoyez des logs d'audit à un serveur syslog tiers :

- Assurez-vous que le port de destination configuré pour le serveur syslog tiers n'est pas bloqué par un pare-feu.

Dépannage avancé

Pour pouvoir utiliser la consignation globale des audits sur votre réseau, RabbitMQ doivent être opérationnels.

Pour la consignation centralisée des audits, chaque service NetWitness Suite écrit des logs d'audit vers rsyslog en écoutant le port 50514 via UDP sur l'hôte local. Le plug-in rsyslog fournit dans le package de consignation des audits ajoute des informations supplémentaires et télécharge ces logs vers RabbitMQ. Logstash s'exécutant sur l'hôte Serveur NetWitness agrège les logs d'audit à partir de tous les services NetWitness Suite, les convertit au format requis, les envoie à un serveur syslog tiers ou Log Decoder pour une procédure d'enquête. Vous pouvez configurer le format des logs d'audits globaux et la destination utilisée par Logstash via l'interface utilisateur NetWitness Suite.

La rubrique Définir une configuration de consignation globale des audits fournit des instructions.

Vérifier les packages et services sur les hôtes

Hôte NetWitness Suite

Les packages ou services suivants doivent être présents sur l'hôte Serveur NetWitness :

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-1.5.4-1
- rsa-audit-plugins
- rabbitmq server

Services sur un hôte autre que l'hôte NetWitness Suite

Les packages et services suivants doivent être présents sur chacun des hôtes NetWitness Suite, outre l'hôte Serveur NetWitness :

- rsyslog-8.4.1
- rsa-audit-rt
- rabbitmq server

Log Decoder

Si vous transférez des logs d'audits globaux à un Log Decoder, le parser suivant doit être présent et activé :

- CEF

Problèmes possibles

Que faire si j'effectue une action sur un service mais les logs d'audit n'atteignent pas le serveur syslog tiers ou Log Decoder configuré ?

La cause possible peut être l'une des suivantes :

- Un service n'effectue pas la consignation sur le serveur syslog local.
- Les logs d'audit ne sont pas téléchargés vers RabbitMQ à partir du syslog local.
- Les logs d'audit ne sont pas agrégés sur l'hôte Serveur NetWitness.
- Les logs agrégés sur l'hôte Serveur NetWitness ne sont pas transférés vers le serveur Syslog ou le Log Decoder tiers configuré.
- Log Decoder n'est pas configuré pour recevoir des logs d'audit globaux au format CEF :
  - La capture Log Decoder n'est pas activée
  - Le Parser CEF n'est pas présent
  - Le Parser CEF n'est pas activé

Solutions possibles

Le tableau suivant propose des solutions possibles à ces problèmes.

Problème	Solutions possibles

Un service n'effectue pas la consignation sur le serveur syslog local.	• Vérifier que ce rsyslog est fonctionnel.
	Vous pouvez utiliser la commande suivante :
	`service rsyslog status`
	• Vérifier que ce rsyslog est à l'écoute sur le port 50514 à l'aide du protocole UDP.
	Vous pouvez utiliser la commande suivante :
	`netstat -tulnp|grep rsyslog`
	• Assurez-vous que l'application ou composant envoie les logs d'audit au port 50514. Exécutez l'utilitaire tcpdump sur l'interface locale pour le port 50514.
	Vous pouvez utiliser la commande suivante :
	`sudo tcpdump -i lo -A udp and port 50514`
	Voir la rubrique *« Exemples de solutions »* ci-après pour afficher les sorties de commande.

Les logs d'audit ne sont pas téléchargés vers RabbitMQ à partir du syslog local.	• Vérifier que le plug-in rsyslog est fonctionnel.
	Vous pouvez utiliser la commande suivante :
	`ps -ef|grep rsa_audit_onramp`
	• Vérifier que le serveur RabbitMQ est fonctionnel.
	Vous pouvez utiliser la commande suivante :
	`service rabbitmq-server status`
	Voir la rubrique « Exemples de solutions » pour afficher les sorties de commande.

Problème	Solutions possibles

Les logs d'audit ne sont pas agrégés sur l'hôte Serveur NetWitness.	• Vérifier que Logstash est opérationnel.
	Vous pouvez utiliser les commandes suivantes :
	`ps -ef|grep logstash`
	`service logstash status`
	• Vérifier que le serveur RabbitMQ est fonctionnel.
	Vous pouvez utiliser la commande suivante :
	`service rabbitmq-server status`
	• Vérifier que le serveur RabbitMQ est à l'écoute sur le port 5672.
	Vous pouvez utiliser la commande suivante :
	`netstat -tulnp|grep 5672`
	• Consulter les erreurs générées au niveau de Logstash.
	Vous pouvez utiliser la commande suivante pour l'emplacement des fichiers :
	`ls -l /var/log/logstash/logstash.*`
	Voir la rubrique « Exemples de solutions » pour afficher les sorties de commande.

Problème	Solutions possibles

Les logs agrégés sur l'hôte Serveur NetWitness ne sont pas transférés vers le serveur Syslog ou le Log Decoder tiers configuré.	• Vérifier que Logstash est opérationnel.
	Vous pouvez utiliser les commandes suivantes :
	`ps -ef|grep logstash`
	`service logstash status`
	• Consulter les erreurs générées au niveau de Logstash.
	Vous pouvez saisir la commande suivante pour l'emplacement des fichiers :
	`ls -l /var/log/logstash/logstash.`
	Voir la rubrique « Exemples de solutions » ci-après pour afficher les sorties de commande.
	• Vérifier que le service de destination est fonctionnel.
	• Vérifier que le service de destination écoute sur le port correct via le protocole correct.
	• Vérifier que le port configuré sur l'hôte de destination n'est pas bloqué.

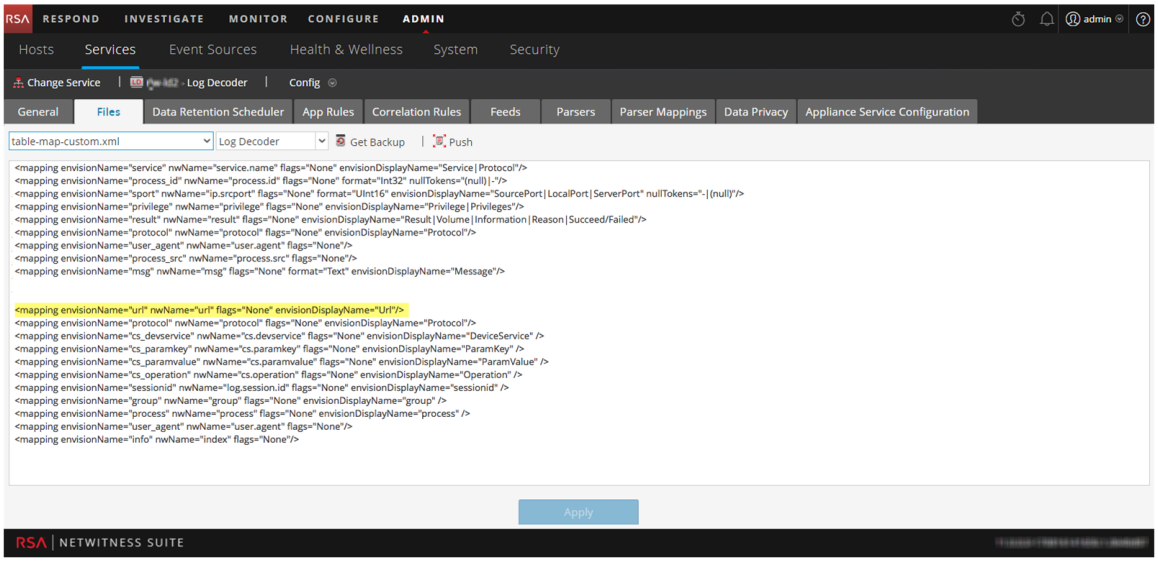
Les logs d'audit transférés de Logstash engendrent une défaillance de l'analyse au niveau du Log Decoder.	• Vérifier que le modèle de notification approprié est utilisé. Les logs d'audit analysés par un Log Decoder doivent être au format CEF. La destination à laquelle les logs d'audit arrivent directement ou indirectement au Log Decoder doit aussi utiliser un modèle CEF. • Le modèle de notification doit suivre la norme CEF. Suivez les étapes de ce guide pour utiliser soit le modèle CEF par défaut, soit créer un modèle CEF personnalisé en suivant des directives strictes. La rubrique Définir un modèle pour la consignation globale des audits fournit des informations supplémentaires. • Vérifier la configuration Logstash.

Pourquoi ne pouvons-nous pas voir les métadonnées personnalisées dans Investigation ?

Généralement, si une méta n'est pas visible dans Investigation, elle n'est pas indexée. Si vous avez besoin d'utiliser les clés méta personnalisées pour Investigation et Reporting, assurez-vous que les clés méta que vous avez sélectionnées sont indexées dans le fichier **table-map-custom.xml** sur Log Decoder. Suivez la procédure « Maintenir les fichiers de mappage des tables » pour modifier le fichier **table-map-custom.xml** sur Log Decoder.

Assurez-vous que les clés méta personnalisées sont également indexées dans **index-concentrator-custom.xml** sur le Concentrator. La rubrique « Modifier un fichier d'index de service » fournit des informations supplémentaires.

La figure suivante montre un exemple de fichier **table-map-custom.xml** dans Serveur NetWitness (ADMIN > Services > (sélectionnez le Log Decoder) >  >Vue > Config) avec l'exemple de méta personnalisé `url` mis en surbrillance.

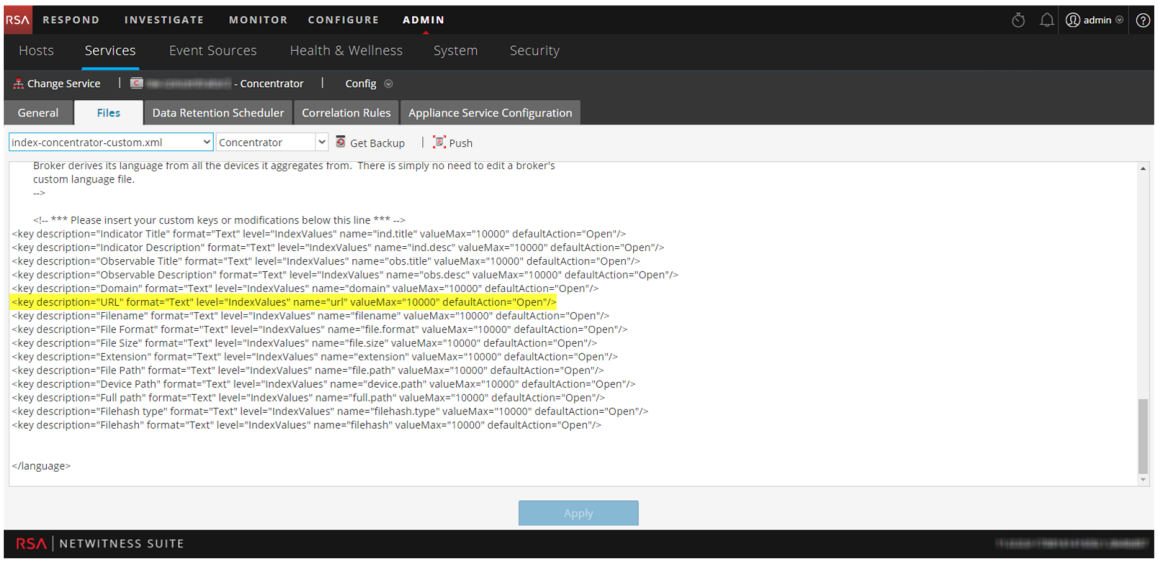


L'exemple de méta personnalisé `url` est mis en surbrillance dans l'échantillon de code suivant provenant du fichier **table-map-custom.xml** ci-dessus :

```
<mapping envisionName="url" nwName="url" flags="None"
envisionDisplayName="Url"/>
<mapping envisionName="protocol" nwName="protocol" flags="None"
envisionDisplayName="Protocol"/><mapping envisionName="cs_devservice"
nwName="cs.devservice" flags="None" envisionDisplayName="DeviceService"
/><mapping envisionName="cs_paramkey" nwName="cs.paramkey" flags="None"
envisionDisplayName="ParamKey" /><mapping envisionName="cs_paramvalue"
nwName="cs.paramvalue" flags="None" envisionDisplayName="ParamValue"
/><mapping envisionName="cs_operation" nwName="cs.operation"
flags="None" envisionDisplayName="Operation" /><mapping
```

```
envisionName="sessionid" nwName="log.session.id" flags="None"
envisionDisplayName="sessionid" /><mapping envisionName="group"
nwName="group" flags="None" envisionDisplayName="group" /><mapping
envisionName="process" nwName="process" flags="None"
envisionDisplayName="process" /><mapping envisionName="user_agent"
nwName="user.agent" flags="None"/><mapping envisionName="info"
nwName="index" flags="None"/>
```

La figure suivante montre un exemple de fichier **index-concentrator-custom.xml** dans Serveur NetWitness (ADMIN > Services > (sélectionnez le Concentrator) > > Vue > Config) avec l'exemple de méta personnalisé `url` mis en surbrillance.



L'exemple de méta personnalisé `url` est mis en surbrillance dans l'échantillon de code suivant provenant du fichier **index-concentrator-custom.xml** ci-dessus :

```
<key description="Severity" level="IndexValues" name="severity"
valueMax="10000" format="Text"/><key description="Result"
level="IndexValues" name="result" format="Text"/><key
level="IndexValues"  name="ip.srcport" format="UInt16"
description="SourcePort"/><key description="Process" level="IndexValues"
name="process" format="Text"/><key description="Process ID"
level="IndexValues" name="process_id" format="Text"/><key
description="Protocol" level="IndexValues" name="protocol"
format="Text"/><key description="UserAgent" level="IndexValues"
name="user_agent" format="Text"/><key description="DestinationAddress"
```

```
level="IndexValues" name="ip.dst" format="IPv4"/><key
description="SourceProcessName" level="IndexValues" name="process.src"
format="Text"/><key description="Username" level="IndexValues"
name="username"  format="Text"/><key description="Info"
level="IndexValues" name="index"  format="Text"/><key
description="customdevservice" level="IndexValues" name="cs.devservice"
format="Text"/>
<key description="url" level="IndexValues" name="url"  format="Text"/>
<key description="Custom Key" level="IndexValues" name="cs.paramkey"
format="Text"/><key description="Custom Value" level="IndexValues"
name="cs.paramvalue"  format="Text"/><key description="Operation"
level="IndexValues" name="cs.operation"  format="Text"/><key
description="CS Device Service" level="IndexValues" name="cs.device"
format="Text" valueMax="10000" defaultAction="Closed"/>
```

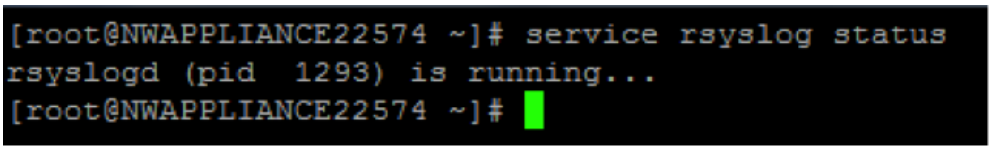
Exemples de solutions

Les exemples de solutions possibles qui suivent montrent les résultats des commandes citées en exemple. Consultez le tableau ci-dessous pour obtenir la liste complète des solutions possibles.

Vérifier que ce rsyslog est fonctionnel

Vous pouvez utiliser la commande suivante :

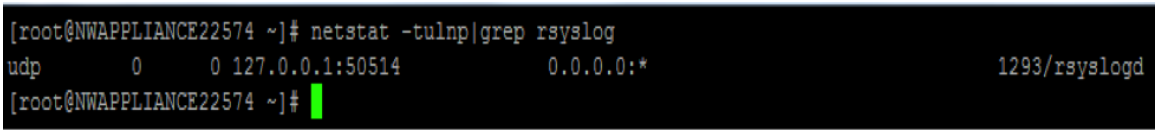
```
service rsyslog status
```



Vérifier que ce rsyslog est à l'écoute sur le port 50514 à l'aide du protocole UDP

Vous pouvez utiliser la commande suivante :

```
netstat -tulnp|grep rsyslog
```

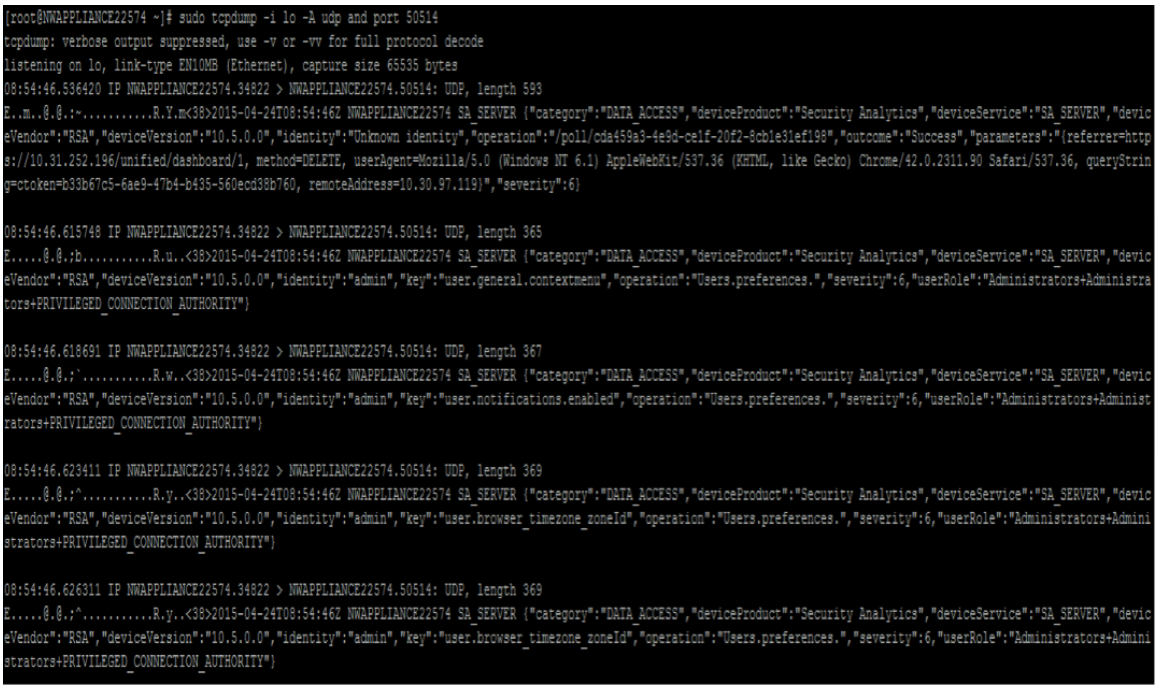


Vérifier que l'application ou le composant envoie les lots d'audit vers le port 50514

La figure suivante montre le résultat de l'exécution de l'utilitaire tcpdump sur l'interface locale pour le port 50514.

Vous pouvez utiliser la commande suivante :

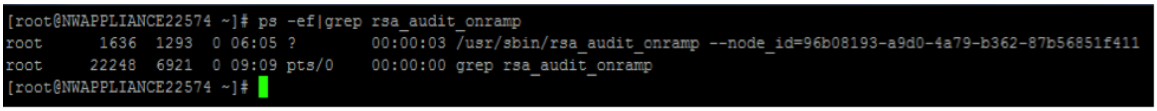
```
sudo tcpdump -i lo -A udp and port 50514
```



Vérifier que le plug-in rsyslog est fonctionnel

Vous pouvez utiliser la commande suivante :

```
ps -ef|grep rsa_audit_onramp
```



Vérifier que le serveur RabbitMQ est fonctionnel

Vous pouvez utiliser la commande suivante :

```
service rabbitmq-server status
```

```
[root@NWAPPLIANCE22574 ~]# service rabbitmq-server status
Status of node sa@localhost ...
[{pid,1862},
 {running_applications,
     [{rabbitmq_federation_management,"RabbitMQ Federation Management",
         "3.4.2"},
      {rabbitmq_management,"RabbitMQ Management Console","3.4.2"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.4.2"},
      {webmachine,"webmachine","1.10.3-rmq3.4.2-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.4.2-git680dba8"},
      {rabbitmq_federation,"RabbitMQ Federation","3.4.2"},
      {rabbitmq_stomp,"Embedded Rabbit Stomp Adapter","3.4.2"},
      {rabbitmq_management_agent,"RabbitMQ Management Agent","3.4.2"},
      {rabbit,"RabbitMQ","3.4.2"},
      {ssl,"Erlang/OTP SSL application","5.3.2"},
      {public_key,"Public key infrastructure","0.21"},
      {crypto,"CRYPTO version 2","3.2"},
      {asn1,"The Erlang ASN1 compiler version 2.0.4","2.0.4"},
      {os_mon,"CPO  CXC 138 46","2.2.14"},
      {inets,"INETS  CXC 138 49","5.9.7"},
      {mnesia,"MNESIA  CXC 138 12","4.11"},
      {amqp_client,"RabbitMQ AMQP Client","3.4.2"},
      {rabbitmq_auth_mechanism_ssl,
          "RabbitMQ SSL authentication (SASL EXTERNAL)","3.4.2"},
      {xmerl,"XML parser","1.3.5"},
      {sasl,"SASL  CXC 138 11","2.3.4"},
      {stdlib,"ERTS  CXC 138 10","1.19.4"},
      {kernel,"ERTS  CXC 138 10","2.16.4"}]},
 {os,{unix,linux}},
 {erlang_version,
     "Erlang R16B03 (erts-5.10.4) [source] [64-bit] [smp:2:2] [async-threads:30] [kernel-poll:true]\n"},
 {memory,
```

Vérifier que Logstash est opérationnel

Vous pouvez utiliser les commandes suivantes :

```
ps -ef|grep logstash
service logstash status
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep logstash
logstash  1583     1  0 06:05 ?        00:01:09 /usr/bin/java -Djava.io.tmpdir=/var/lib/logstash -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Djava.awt.headless=true -XX:C
MSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/jruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
.rb agent --pluginpath /opt/logstash -f /etc/logstash/conf.d -l /var/log/logstash/logstash.log
root      8509  6921  0 09:31 pts/0    00:00:00 grep logstash
[root@NWAPPLIANCE22574 ~]# service logstash status
logstash is running
[root@NWAPPLIANCE22574 ~]#
```

Vérifier que le serveur RabbitMQ est à l'écoute sur le port 5672

Par exemple, saisissez la commande suivante :

```
netstat -tulnp|grep 5672
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep 5672
tcp        0      0 127.0.0.1:5672              0.0.0.0:*                   LISTEN      1862/beam.smp
tcp        0      0 0.0.0.0:25672               0.0.0.0:*                   LISTEN      1862/beam.smp
[root@NWAPPLIANCE22574 ~]#
```

Consulter les erreurs générées au niveau de Logstash

Vous pouvez saisir la commande suivante pour l'emplacement des fichiers :

```
ls -l /var/log/logstash/logstash.*
```

```
[root@NWAPPLIANCE22574 ~]# ls -l /var/log/logstash/logstash.*
-rw-r--r--. 1 root     root        0 Apr 24 06:05 /var/log/logstash/logstash.err
-rw-r--r--. 1 logstash logstash 1043 Apr 24 06:04 /var/log/logstash/logstash.log
-rw-r--r--. 1 root     root       57 Apr 24 06:12 /var/log/logstash/logstash.stdout
[root@NWAPPLIANCE22574 ~]#
```

Consultez le tableau des solutions possibles ci-dessous pour obtenir la liste complète des problèmes et solutions possibles.

Dépanner la configuration du serveur NTP

Cette rubrique décrit les problèmes de configuration du serveur NTP que vous pouvez rencontrer et suggère des solutions à ces problèmes.

Problèmes identifiés par des messages dans le panneau Paramètres NTP ou fichiers logs

Cette rubrique donne des informations de dépannage pour des problèmes identifiés par l'affichage de messages NetWitness Suite dans le panneau Paramètres NTP et fichiers logs.

Message	Interface utilisateur : **Unexpected error occurred. First check the logs then contact Customer Care to resolve error.** **System Log:** **Timestamp Level Message** *yyyy-dd-mmThh:mm:ss:ms* ERROR com.rsa.smc.sa.adm.exception.MCOAgent Exception: No request sent, we did not discover any nodes
Cause probable	La configuration NetWitness Suite de bas niveau comporte une erreur ou le service de prise en charge ne fonctionne pas.
Solution	Contactez le Support Clients.
Message	Interface utilisateur : **Specified an invalid Hostname syntax**.
Cause probable	Le nom d'hôte du serveur NTP que vous avez saisi ne confirme pas d'adresse IP ou de syntaxe FQDN.
Solution	Saisissez de nouveau le nom d'hôte en utilisant la syntaxe correcte.
Message	Interface utilisateur : **Specified NTP server that already exists.**
Cause probable	Le nom d'hôte du serveur NTP que vous avez saisi est déjà défini dans NetWitness Suite.
Solution	Saisissez un nom d'hôte pour un serveur NTP qui n'est pas configuré dans NetWitness Suite.

Message	Interface utilisateur : **Cannot reach NTP server *hostname***. Please verify the server address and your firewall settings.
Cause probable	L'adresse du serveur ou les paramètres du pare-feu peuvent présenter une erreur.
Solution	Vérifiez l'adresse du serveur et les paramètres de votre pare-feu et corrigez-les si nécessaire.

Références

Cette rubrique fournit des supports de référence décrivant l'interface utilisateur de configuration des paramètres système de NetWitness Suite et définissant les paramètres. Les administrateurs utilisent des options de la vue Système d'administration pour configurer les paramètres du système. Chaque panneau est décrit dans une rubrique distincte.

- Panneau Configuration de la consignation globale des audits
- Panneau Notifications globales
  - Boîtes de dialogue Définir un serveur de notification
  - Boîtes de dialogue Définir une sortie de notification
  - Boîte de dialogue Définir un modèle de notification
  - Onglet Sortie
  - Onglet Serveurs
  - Onglet Modèles
- Panneau Paramètres proxy HTTP
- Panneau Configuration de l'e-mail
- Panneau Paramètres ESA
- Panneau Configuration des procédures d'enquête
- Panneau Configuration des services Live
- Panneau Paramètres NTP
- Panneau Actions des menus contextuels
- Panneau Configuration des notifications existantes

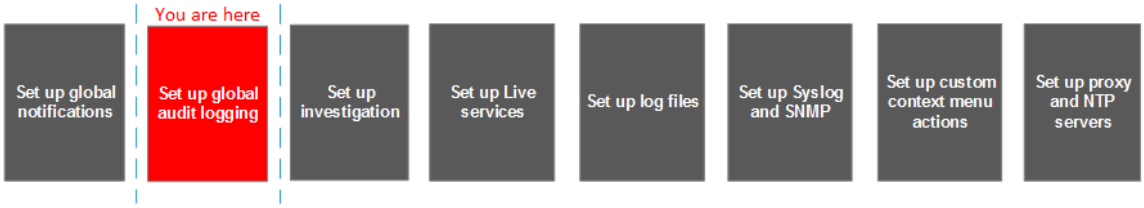
Panneau Configuration de la consignation globale des audits

Dans le panneau **Configurations de consignation globale des audits** (Admin > Système > Audit global), vous pouvez configurer la consignation d'audit globale en ajoutant des configurations qui définissent la façon dont les logs d'audit globaux sont transmis à des systèmes syslog externes. Les logs d'audit globaux sont transférés vers le Serveur de notifications sélectionné dans votre configuration de consignation d'audit globale à l'aide du modèle de Notification sélectionné.

La consignation globale des audits propose aux auditeurs une visibilité consolidée sur les activités des utilisateurs au sein de NetWitness Suite, en temps réel et à partir d'un emplacement centralisé.

Workflow

Ce workflow présente les procédures requises pour configurer et vérifier la consignation globale des audits.



Avant de pouvoir définir une configuration Consignation globale des audits, vous devez créer un serveur de notification Syslog dans l'onglet Notifications globales > Serveur. Le serveur de notification Syslog est la destination recevant les journaux d'audit globaux. Ensuite, vous devez sélectionner ou définir un modèle de consignation des audits dans la vue Notifications globales > onglet Modèles. Le modèle de consignation d'audit définit les champs format et message des logs d'audit envoyés au serveur Syslog tiers ou Log Decoder. Si vous utilisez un service Log Decoder, déployez l'analyseur Common Event Format sur votre service Log Decoder à partir de Live.

Remarque : Vous n'avez pas besoin de configurer l'onglet Notifications globales > Résultat pour la consignation globale des audits.

Après avoir ajouté la configuration de consignation globale des audits ici, les logs d'audit sont transférés au serveur de notification sélectionné dans la configuration. Vérifiez vos logs d'audit pour vérifier qu'ils affichent les événements tels que définis dans votre modèle de consignation des audits.

Que voulez-vous faire ?

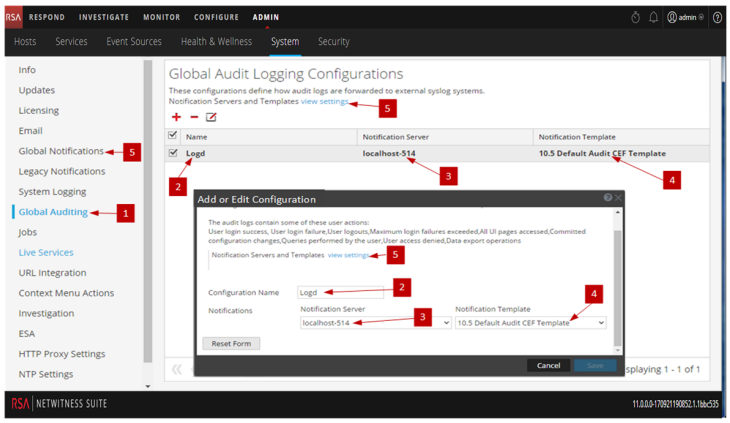
Rôle	Je souhaite...	Me montrer comment
Administrateur	Créer un serveur de notification Syslog.	Configurer une destination pour recevoir des logs d'audit globaux
Administrateur	Choisir un modèle de consignation des audits.	Définir un modèle pour la consignation globale des audits
Administrateur	Configurer la consignation globale des audits	Définir une configuration de consignation globale des audits Pour connaître la procédure complète, reportez-vous à section « Consignation globale des audits - Procédure générale » dans Configurer la consignation globale des audits.
Administrateur	Vérifier les logs d'audits globaux	Vérifier les logs d'audits globaux

Rubriques connexes

- Résoudre les problèmes liés à la consignation globale des audits
- Boîte de dialogue Ajouter une nouvelle configuration
- Métaclés CEF prises en charge
- Variables de métaclés prises en charge pour la consignation globale des audits
- Référence aux opérations de consignation globale des audits
- Emplacements des logs d'audit locaux

Aperçu rapide

L'exemple suivant illustre une configuration de consignation globale des audits. Ces configurations définissent la façon dont NetWitness Suite transmet les journaux d'audit aux systèmes Syslog externes.



1	Affiche le panneau Configurations de la consignation d'audit globale s'affiche.
2	Nom qui identifie la configuration de la consignation d'audit globale.
3	Serveur de notification affecté à la configuration de la consignation d'audit globale.
4	Modèle de notification affecté à la configuration de la consignation d'audit globale.
5	Affiche le panneau Notifications globales où vous configurez les serveurs et modèles requis pour définir une configuration de consignation globale des audits.

Barre d'outils

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

Icône	Description
+	Ajoute une configuration de consignation d'audit globale.
−	Supprime une configuration de consignation d'audit globale. La suppression d'une configuration globale des audits ne supprime pas le serveur et le modèle de notification associés. Après la suppression, le transfert des logs d'audits globaux, spécifiés dans cette configuration, est interrompu.
✎	Modifie une configuration de consignation d'audit globale. Vous pouvez changer la destination des logs d'audit globaux de vos audits d'utilisateur en sélectionnant un serveur de notification différent. Vous pouvez aussi modifier les champs de format et de message des entrées des logs d'audit en sélectionnant un modèle de notification différent. Vous ne pouvez pas modifier les types d'actions d'utilisateur NetWitness Suite qui sont consignés et envoyés dans les logs d'audit globaux.

Configurations

Le tableau ci-dessous décrit les configurations répertoriées.

Titre	Description
	Pour sélectionner une configuration individuelle, cochez la case près de la configuration. Pour sélectionner toutes les configurations, cochez la case dans la barre de titre de la table.
Nom	Affiche le nom de la configuration d'audit globale. Par exemple, vous pouvez nommer les configurations d'après la destination des logs d'audit globaux, tels que HQ SA et My Syslog Server.
Serveur de notification	Affiche le serveur de notification Syslog sélectionné en tant que destination pour les logs d'audit globaux. Si vous souhaitez transférer des logs d'audit globaux vers un Log Decoder, créez un type Syslog de serveur de notification. La section Configurer une destination pour recevoir des logs d'audit globaux fournit des instructions sur le mode de création d'un serveur de notification Syslog pour une consignation globale des audits.

Titre	Description
Modèle de notification	Affiche le modèle de notification de consignation des audits sélectionné pour la configuration. Il définit les champs de format et de message des entrées de log d'audit. Pour les services Log Decoder, utilisez le **modèle CEF d'audit par défaut**. Vous pouvez ajouter ou supprimer des champs dans le modèle CEF (Common Event Format) si vous avez des exigences spécifiques. Définir un modèle pour la consignation globale des audits fournit des instructions et Métaclés CEF prises en charge décrit les métaclés CEF disponibles. Pour les serveurs Syslog tiers, vous pouvez utiliser un modèle de consignation d'audit par défaut ou définir votre propre format (CEF ou non-CEF). La section Définir un modèle pour la consignation globale des audits fournit des instructions et la section Variables de métaclés prises en charge pour la consignation globale des audits décrit les variables de métadonnées disponibles.

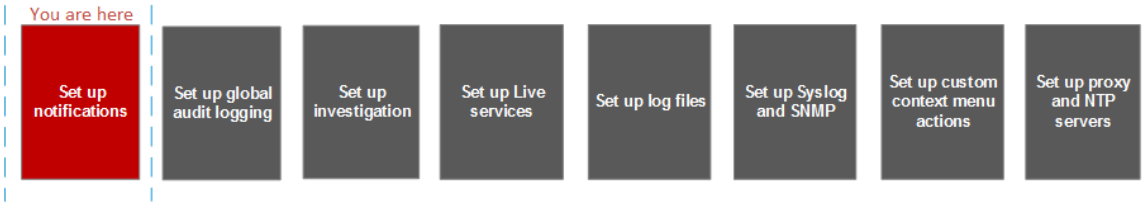
Panneau Notifications globales

Le panneau Notifications globales présente les fonctions permettant de configurer les paramètres de notification. Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE.

Dans le panneau Notifications globales, vous pouvez configurer les paramètres de notification globale suivants :

- Sorties de notification
- Serveurs de notification
- Modèles

Workflow



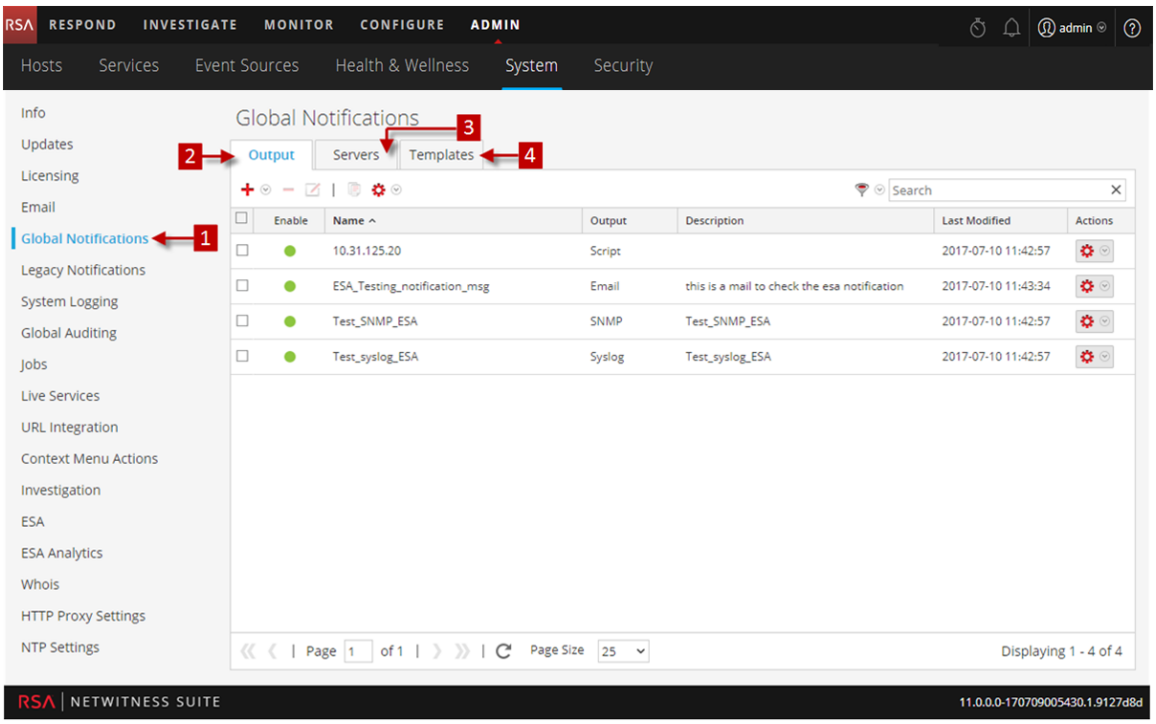
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer les serveurs de notification	Onglet Serveurs
Administrateur	Configurer les sorties de notification	Onglet Sortie
Administrateur	Configurer des modèles de notification	Onglet Modèles

Rubriques connexes

- Configurer un serveur de notification Syslog
- Configurer un script pour un serveur de notification

Aperçu rapide



1 Affiche le panneau Notification globale.

2 Affiche l'onglet Résultat

3 Affiche l'onglet Serveurs

4 Affiche l'onglet Modèles

Barre d'outils et fonctions

Le panneau Notifications globales comporte trois onglets : Sortie, Serveurs et Modèles.

Fonctionnalité	Description
Onglet Résultat	Cet onglet vous permet de configurer les sorties de notification. Reportez-vous à la section Onglet Résultat pour plus d'informations.
Onglet Serveurs	Cet onglet vous permet de configurer les serveurs de notification. Reportez-vous à la section Onglet Serveurs pour plus d'informations.
Onglet Modèles	Cet onglet vous permet de configurer des modèles de notification. Pour plus d'informations, reportez-vous à l'onglet Modèles.

Ce tableau décrit les colonnes dans la grille pour les Sorties de notification et Serveurs de notification.

Colonne	Description
	Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.
Activer	Indique si la configuration est activée. Un rond coloré en vert indique qu'une configuration est activée. Un rond blanc indique qu'aucune configuration n'est activée.
Nom	Nom qui identifie ou libelle la configuration.
Résultat	Sortie de la configuration. Les sorties sont E-mail, SNMP, Syslog et Script.
Description	Brève description de la configuration.
Dernière modification	Affiche la date et l'heure de la dernière modification de configuration.
Actions	Fournit un menu Actions  pour la configuration sélectionnée avec les actions qui peuvent être effectuées sur la configuration. Le menu Actions vous permet de supprimer, de modifier, de répliquer et d'exporter la configuration.

Ce tableau décrit les colonnes de la grille pour les Modèles de notification.

Colonne	Description
	Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.
Nom	Nom permettant d'identifier ou de libeller le modèle.
Type de modèle	Type de modèle. Les types sont Consignation des audits, Event Stream Analysis, Surveillance des sources d'événements et Alarmes d'intégrité.
Description	Brève description du modèle.

Colonne	Description
Actions	Fournit un menu Actions pour la configuration sélectionnée avec les actions qui peuvent être effectuées sur le modèle. Le menu Actions vous permet de supprimer, de modifier, de répliquer et d'exporter le modèle.

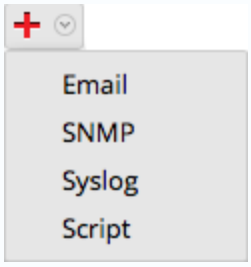
Barre d'outils du panneau Notifications globales

La barre d'outils du panneau Notifications globales se trouve en haut des onglets Sortie, Serveurs et Modèles.

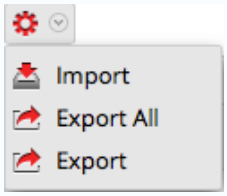
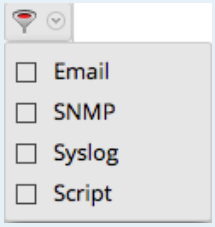
La figure suivante illustre la barre d'outils des onglets Sortie et Serveurs.

La figure suivante illustre la barre d'outils de l'onglet Général.

Le tableau suivant décrit les fonctions de la barre d'outils du panneau Notifications globales.

Fonctionnalité	Description
	Ajoute un serveur de notification sur l'onglet Serveurs, un résultat de notification (notification) sur l'onglet Résultat et un modèle de notification sur l'onglet Modèles. Sur les onglets Serveurs et Sortie, vous pouvez configurer les paramètres de notification par e-mail, SNMP, Syslog et Script.
	

Fonctionnalité	Description
	Supprime la configuration de notification sélectionnée. Vous ne pouvez pas supprimer les serveurs et les types de notification associés à des configurations de consignation globale d'audits. Si vous tentez de supprimer une sortie de notification (notification) utilisée par des alertes, un message vous avertit que les alertes qui utilisent la notification ne fonctionneront plus correctement. Le message indique le nombre d'alertes en cours. Vous pouvez également supprimer une configuration en la sélectionnant, puis en choisissant  > Supprimer dans la colonne Actions.
	Modifie une configuration de notification sélectionnée. Vous pouvez également supprimer une configuration en la sélectionnant, puis en choisissant  > Modifier dans la colonne Actions.
	Duplique la configuration de notification sélectionnée. Vous pouvez également dupliquer une configuration en la sélectionnant, puis en choisissant  > Dupliquer dans la colonne Actions.

Fonctionnalité	Description
	Affiche les options suivantes : • **Importer** : Importe un serveur, un type ou un modèle de notification. Par exemple, sur l'onglet Serveurs, vous pouvez importer une configuration de serveur de notification. • **Exporter tout** : Exporte toutes les configurations. Par exemple, sur l'onglet Serveurs, vous pouvez exporter toutes les configurations du serveur de notification. • **Exporter** : Exporte une configuration sélectionnée. Vous pouvez également exporter une configuration en sélectionnant une configuration, puis en sélectionnant  > Exporter dans la colonne Actions.
	Filtre par e-mail, SNMP, Syslog ou script.
	Recherche des configurations dans la grille.

Boîtes de dialogue Définir un serveur de notification

Cette rubrique décrit les boîtes de dialogue Définir un serveur de notification permettant de configurer les paramètres des différents types de serveurs de notification. Configurez les serveurs de notification dans Administration > Système > Notifications > onglet Serveurs.

Les notifications sont utilisées par plusieurs composants NetWitness Suite, tels que Event Stream Analysis (ESA), RÉPONDRE et Consignation globale des audits. Les paramètres de notification sont nommés Serveurs de notification. Sous l'onglet Serveurs - vue Administration-système - panneau Notifications, vous pouvez créer plusieurs configurations de serveur de notification.

Vous pouvez configurer les types de paramètres de serveur de notification suivants NetWitness Suite :

- E-mail
- SNMP
- Syslog
- Script

Pour la consignation globale des audits, seuls les serveurs de notification Syslog peuvent être utilisés.

Les procédures relatives aux serveurs de notification sont décrites dans la section Configurer les serveurs de notification.

Pour accéder aux boîtes de dialogue Définir une notification :

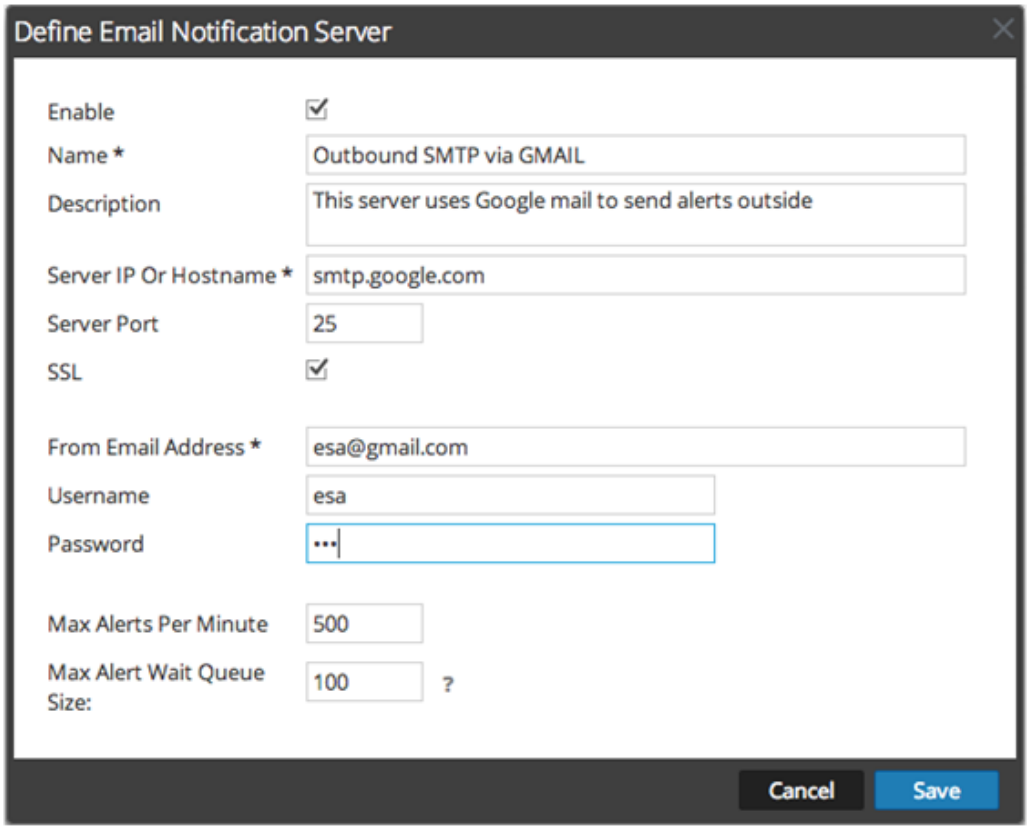
1. Accédez à **Administrateur > Système**.
2. Dans le volet de navigation de gauche, sélectionnez **Notifications globales**.
3. Sous l'onglet **Serveurs de notification**, cliquez sur  , puis sélectionnez un type de serveur de notification (E-mail, SNMP, Syslog ou script).
   La boîte de dialogue Définir un serveur de notification s'affiche pour vous permettre de choisir.

Quatre boîtes de dialogue de serveur de notification vous permettent de configurer les serveurs de notification.

E-mail

Les serveurs de notification par e-mail vous permettent de configurer les paramètres du serveur de messagerie afin d'envoyer des notifications d'alerte.

La figure suivante présente la boîte de dialogue Définir un serveur de notification par e-mail.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les serveurs de notification par e-mail.

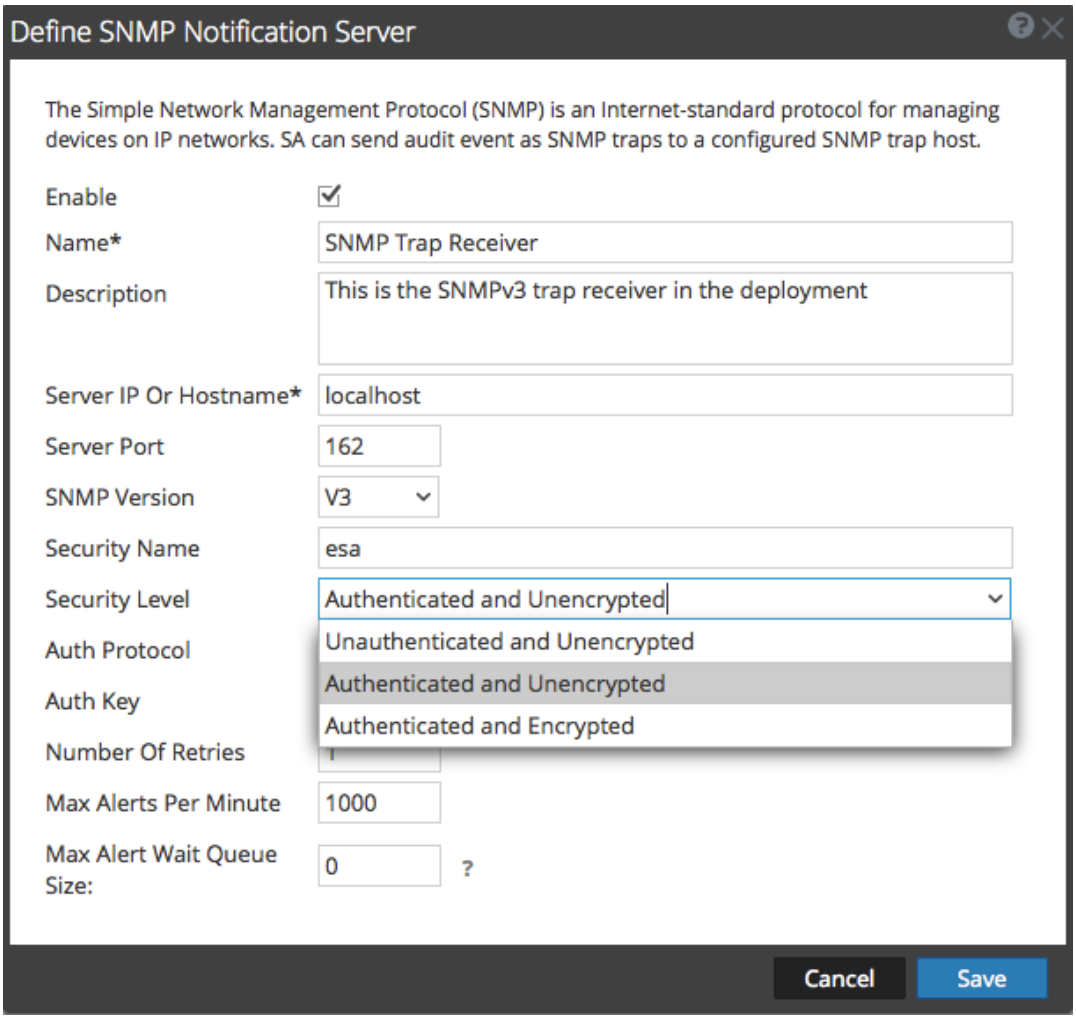
Parameters	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller le serveur de notification.
Description	Brève description du serveur de notification.
Adresse IP ou nom d'hôte du serveur	Nom d'hôte du serveur de messagerie. Pour les notifications ESM/SMS et ESA, vous devez spécifier uniquement le nom d'hôte/nom de domaine complet.
Port de serveur	Port de serveur.
SSL	Sélectionnez l'option si vous souhaitez que la communication soit établie via SSL.

Parameters	Description
Adresse de messagerie de l'expéditeur	Compte de messagerie à partir duquel vous souhaitez envoyer les notifications par e-mail.
Username	Nom d'utilisateur servant à se connecter au compte de messagerie si le serveur SMTP requiert une authentification pour relayer les e-mails correctement.
Mot de passe	Mot de passe servant à se connecter au compte de messagerie si le serveur SMTP requiert une authentification pour relayer les e-mails correctement.
Nombre maximal d'alertes par minute	Décrit le nombre maximal d'alertes par minute.
Taille maximale de la file d'attente des alertes	Décrit le nombre maximal d'alertes en file d'attente avant leur suppression.

SNMP

Les serveurs de notification SNMP vous permettent de configurer les paramètres des hôtes de trap SNMP en vue d'envoyer des notifications d'alerte.

La figure suivante présente la boîte de dialogue Définir un serveur de notification SNMP.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les serveurs de notification SNMP.

Parameters	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller le serveur de notification.
Description	Brève description du serveur de notification.
Adresse IP ou nom d'hôte du serveur	Adresse IP ou nom d'hôte de trap SNMP

Parameters	Description
Port de serveur	Numéro de port d'écoute sur l'hôte de trap SNMP.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>SNMP Version</td><td>Version SNMP. Les options sont les suivantes :
V1
V2C
V3
Si vous sélectionnez SNMP Version 3 (v3), les paramètres suivants s'affichent :

<table><tr><th>Paramètres</th><th>Description</th></tr><tr><td>Type de notification</td><td>En fonction du type de notification, des messages SNMP sont envoyés chaque fois qu'une alerte est générée. Les types de notification suivants ne sont pas pris en charge :
Notifier - interception avec accusé de réception. L'expéditeur permet d'obtenir un accusé de réception du destinataire.
Intercepter : notification sans accusé de réception</td></tr><tr><td>ID du moteur faisant autorité (Cette option est disponible uniquement pour le type de notification TRAP)</td><td>Identifiant permettant d'identifier les agents. L'ID du moteur faisant autorité, ainsi que le nom d'utilisateur permettent d'identifier l'agent de façon unique.</td></tr><tr><td>Niveau de sécurité</td><td>Définit le niveau de sécurité. Les options sont les suivantes :
Non authentifié(e) ni déchiffré(e)
Authentifié(e) et déchiffré(e)
Authentifié(e) et chiffré(e)</td></tr></table></td></tr>
</table>

Parameters	Description
	Protocole d'autorisation (Cette option est disponible uniquement pour le niveau de sécurité Authentifié(e) et déchiffré(e) et Authentifié(e) et chiffré(e)) — Protocole d'authentification permettant de valider un utilisateur avant de fournir un accès au serveur. Les options sont les suivantes : • SHA • MD5
	Clé d'authentification (Cette option est disponible uniquement pour le niveau de sécurité Authentifié(e) et déchiffré(e) et Authentifié(e) et chiffré(e)) — Mot de passe que vous souhaitez utiliser pour l'authentification.
	Protocole de confidentialité (cette option est disponible uniquement pour le niveau de sécurité Authentifié(e) et chiffré(e)) — Le protocole de confidentialité est une technique de chiffrement pour la communication des données.
	Clé privée (Cette option est disponible uniquement pour le niveau de sécurité Authentifié(e) et chiffré(e)) — Mot de passe que vous souhaitez utiliser pour le chiffrement.
Communauté	Chaîne de communauté utilisée pour l'authentification sur l'hôte de trap SNMP. La valeur par défaut est **public**.

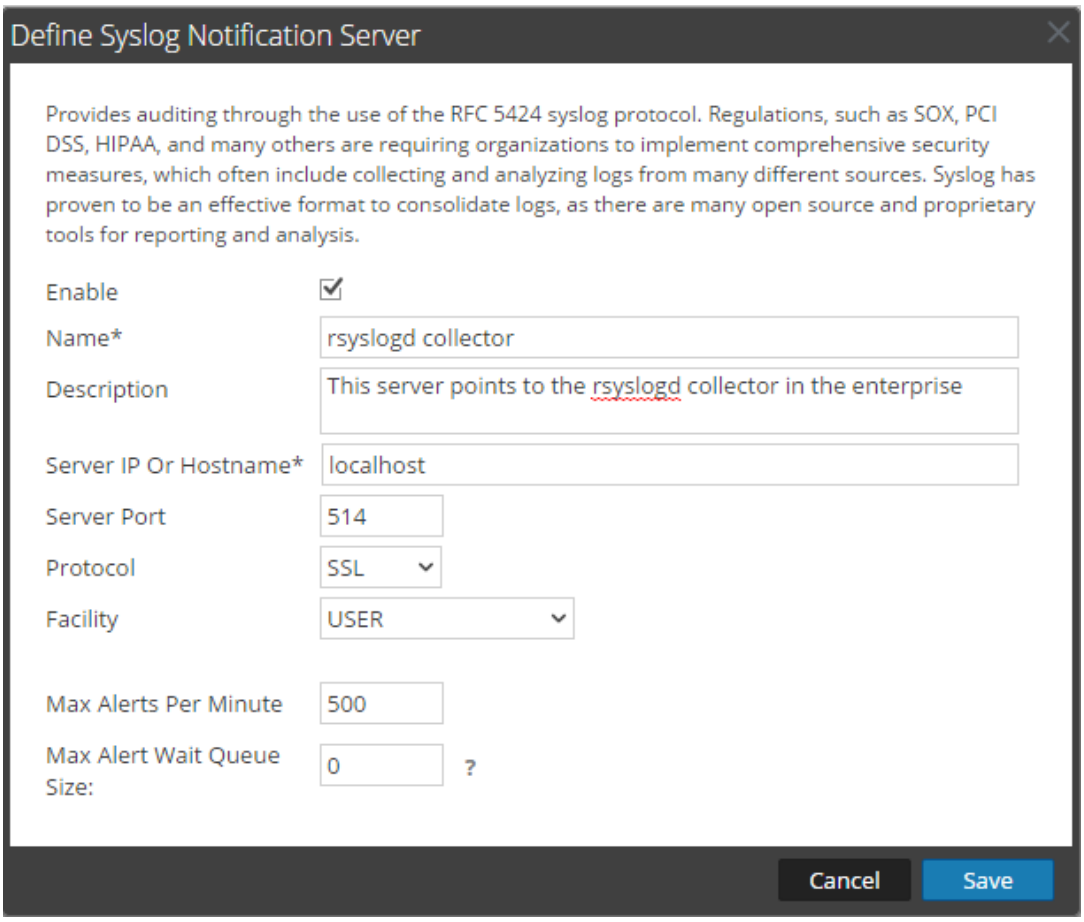
Parameters	Description
Nombre de nouvelles tentatives	Nombre de tentatives liées à la trap.
Nombre maximal d'alertes par minute	Nombre maximal d'alertes par minute.
Taille maximale de la file d'attente des alertes	Nombre maximal d'alertes à placer en file d'attente avant d'être supprimées.

Syslog

Les serveurs de notification Syslog vous permettent de configurer les paramètres Syslog en vue d'envoyer des notifications. En cas d'activation, Syslog propose l'audit via l'utilisation du protocole Syslog RFC 5424. Le format Syslog a fait la preuve de son efficacité pour consolider les logs car il existe de nombreux outils open source et propriétaires pour le reporting et l'analyse.

Vous ne pouvez pas désactiver les serveurs de notification associés aux configurations de consignation globale des audits.

La figure suivante présente la boîte de dialogue Définir un serveur de notification Syslog.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les serveurs de notification Syslog.

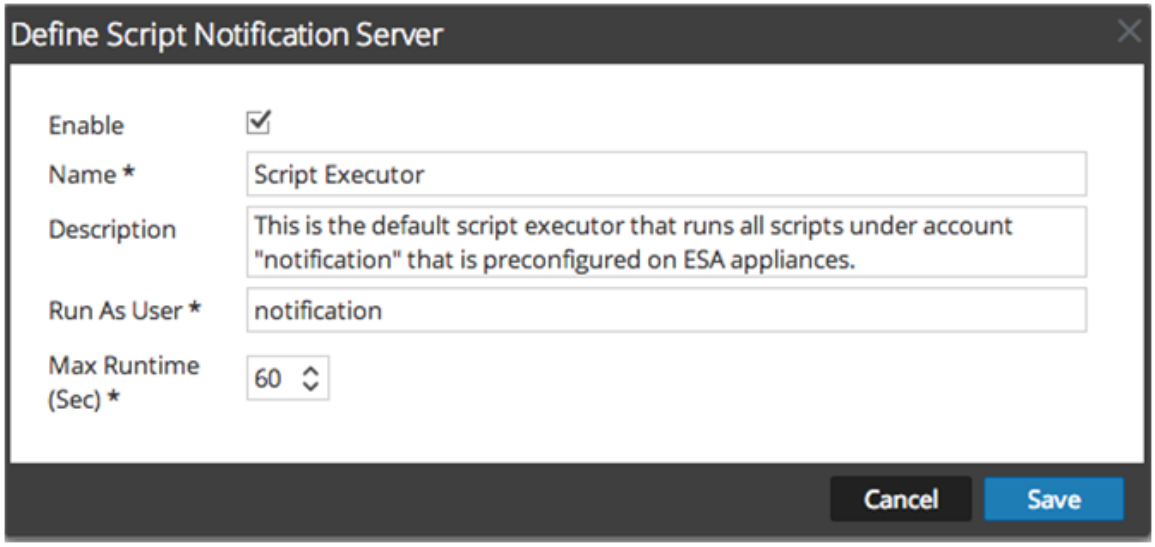
Parameters	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller le serveur de notification.
Description	Brève description du serveur de notification.
Adresse IP ou nom d'hôte du serveur	Nom de l'hôte où le processus Syslog cible est en cours d'exécution.
Port de serveur	Numéro du port où s'effectue l'écoute par le processus Syslog cible.

Parameters	Description
Protocole	Protocole à utiliser pour transférer les fichiers Syslog.
Site	Fonctionnalité Syslog désignée à utiliser pour tous les messages sortants. Elle permet de spécifier le type de programme qui se connecte au message. Voici quelques valeurs possibles : KERN, USER, MAIL et DAEMON. Cela permet au fichier de configuration de spécifier que les messages des différentes fonctionnalités seront gérés différemment.
Nombre maximal d'alertes par minute	Nombre maximal d'alertes par minute. Ce champ n'est pas utilisé pour la consignation des audits globaux.
Taille maximale de la file d'attente des alertes	Nombre maximal d'alertes à placer en file d'attente avant d'être supprimées. Ce champ n'est pas utilisé pour la consignation des audits globaux.

Script

Les serveurs de notification par script vous permettent de configurer un script pour un serveur de notification.

La figure suivante présente la boîte de dialogue Définir un serveur de notification par script.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les serveurs de notification par script.

Parameters	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Nom	Nom permettant d'identifier ou de libeller le serveur de notification.
Description	Brève description du serveur de notification.
Exécuter en tant qu'utilisateur	Nom de l'identité de l'utilisateur sous laquelle le script est exécuté. L'identité de l'utilisateur par défaut est **notification**. Pour ESA, vous ne pouvez pas définir cette option dans un autre cadre, sauf si vous avez créé le compte sur l'hôte ESA.
Temps d'exécution max (sec)	Durée maximale (en secondes) pendant laquelle le script est autorisé à s'exécuter.

Boîtes de dialogue Définir une sortie de notification

Cette section décrit les différentes boîtes de dialogue de sortie de notification. Configurez les sorties de notification dans ADMIN > Système > Notifications > onglet Résultat. Les notifications sont tout simplement les destinations utilisées pour l'envoi des notifications. Pour ESA, les notifications vous permettent de définir la façon dont vous souhaitez recevoir les alertes ESA. Voici les différentes notifications prises en charge par NetWitness Suite :

- E-mail
- SNMP
- Syslog
- Script

Les procédures relatives aux notifications sont décrites dans Configurer les résultats de notification.

Pour accéder aux boîtes de dialogue Définir une notification :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Sous l'onglet **Sortie**, cliquez sur +, puis sélectionnez une sortie de notification (E-mail, SNMP, Syslog ou script).
   La boîte de dialogue Définir une notification s'affiche pour vous permettre de choisir.

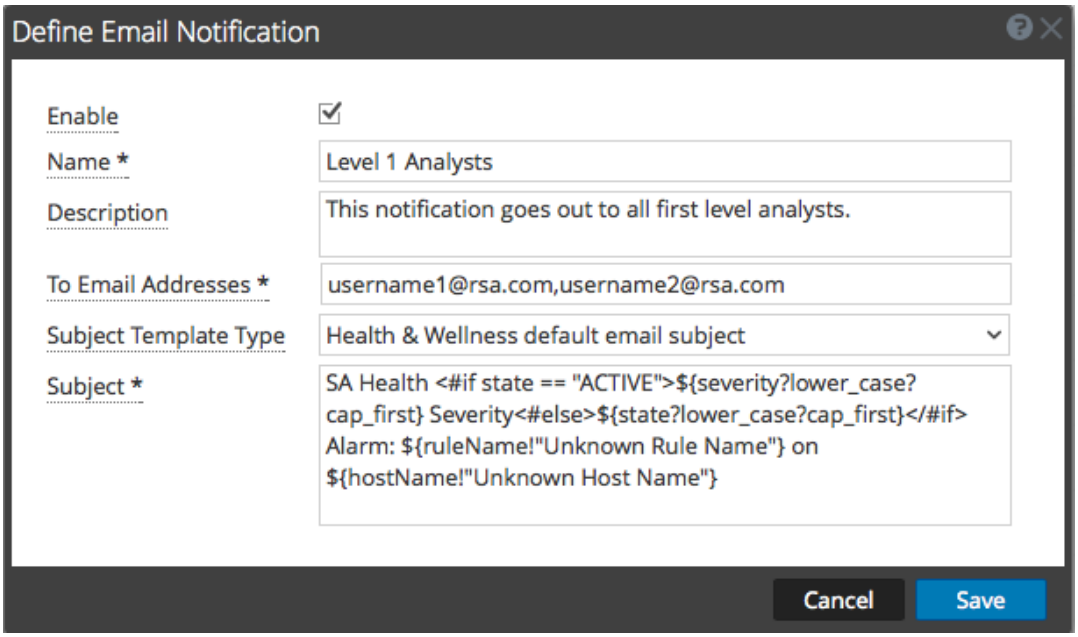
Fonctionnalités

Quatre boîtes de dialogue de notification vous permettent de configurer les sorties de notification.

E-mail

Les notifications par e-mail vous permettent de définir l'adresse e-mail de destination à laquelle vous pouvez envoyer les alertes. Cette boîte de dialogue vous permet également d'ajouter une description personnalisée dans l'objet de l'e-mail et de définir plusieurs destinataires.

La figure suivante présente la boîte de dialogue Définir une notification par e-mail.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les notifications par e-mail.

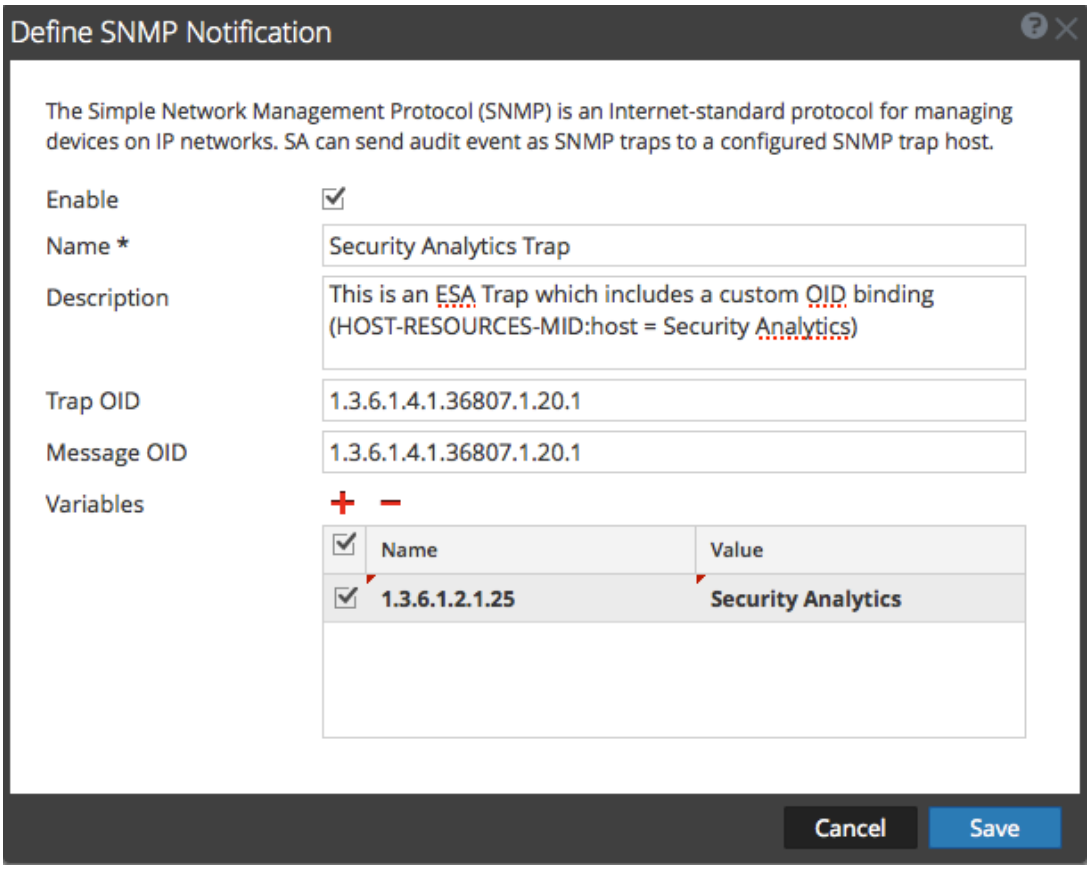
Paramètre	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller la notification.
Description	Brève description de la notification
Adresses e-mail des destinataires	Décrit les adresses e-mail de destination auxquelles l'alerte doit être envoyée. **Remarque :** Vous pouvez en définir plusieurs.
Type de modèle d'objet	Répertorie les modèles disponibles pour créer un objet. Lorsque vous choisissez un modèle, le champ Objet est automatiquement rempli avec le code de votre modèle choisi.

Paramètre	Description
Sujet	Description personnalisée de l'alerte déclenchée. Ces informations sont automatiquement remplies si vous choisissez l'un des modèles prédéfinis du menu déroulant Type de modèle d'objet. **Remarque :** Pour fournir un objet personnalisé, reportez-vous à la rubrique Inclure la ligne d'objet de l'e-mail par défaut dans le *Guide de maintenance du système*.

SNMP

Les notifications SNMP vous permettent de définir les paramètres SNMP servant à envoyer des notifications d'alerte.

La figure suivante présente la boîte de dialogue Définir une notification SNMP.



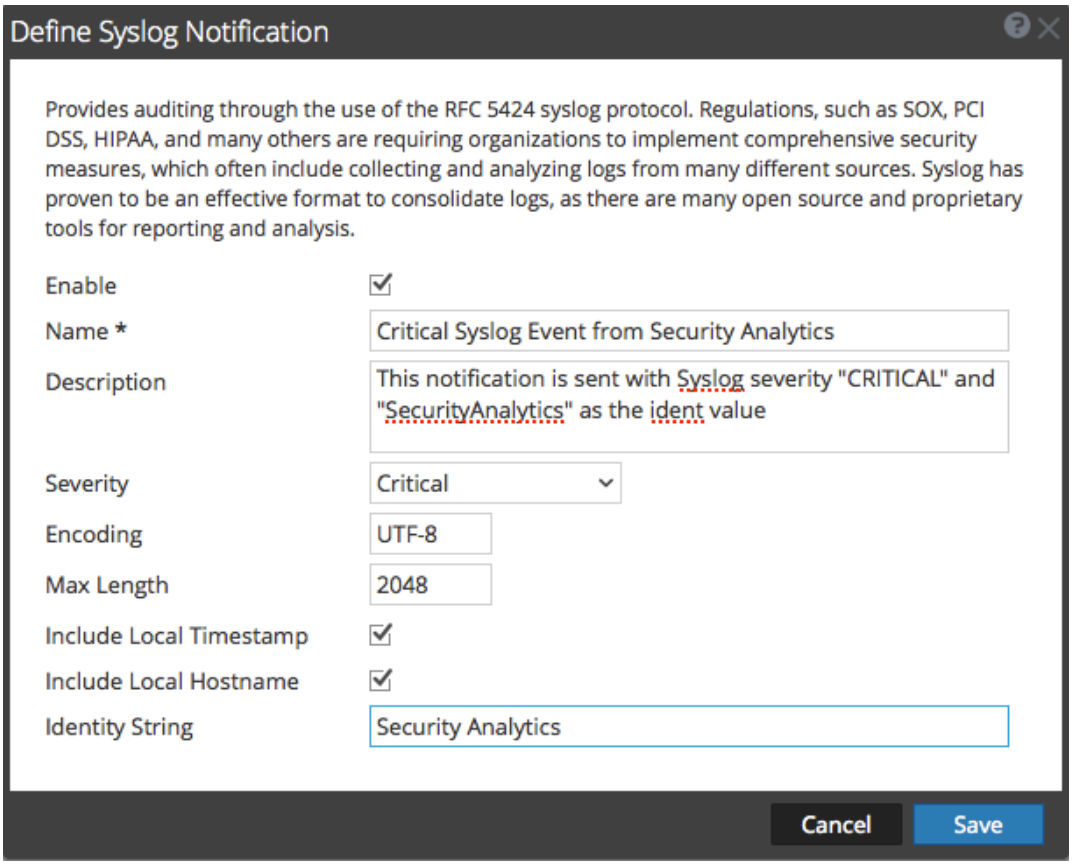
Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les notifications SNMP.

Paramètre	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller la notification.
Description	Brève description de la notification
ID d'objet de trap	L'ID d'objet pour le trap SNMP sur l'hôte de trap qui reçoit l'événement. La valeur par défaut est **1.3.6.1.4.1.36807.1.20.1**. Cette valeur est un nom hiérarchique qui représente le système qui génère le trap. 1.3.6.1.4.1 est le préfixe commun pour toutes les entreprises et 36807.1.20.1 identifie NetWitness Suite.
ID d'objet de message	L'identifiant d'objet de message pour le trap SNMP.
les variables.	Informations supplémentaires à inclure au trap. Il s'agit d'une variable qui est une paire nom/valeur.

Syslog

Les notifications Syslog vous permettent de définir les paramètres Syslog permettant d'envoyer des notifications d'alerte.

La figure suivante présente la boîte de dialogue Définir une notification Syslog.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les notifications Syslog.

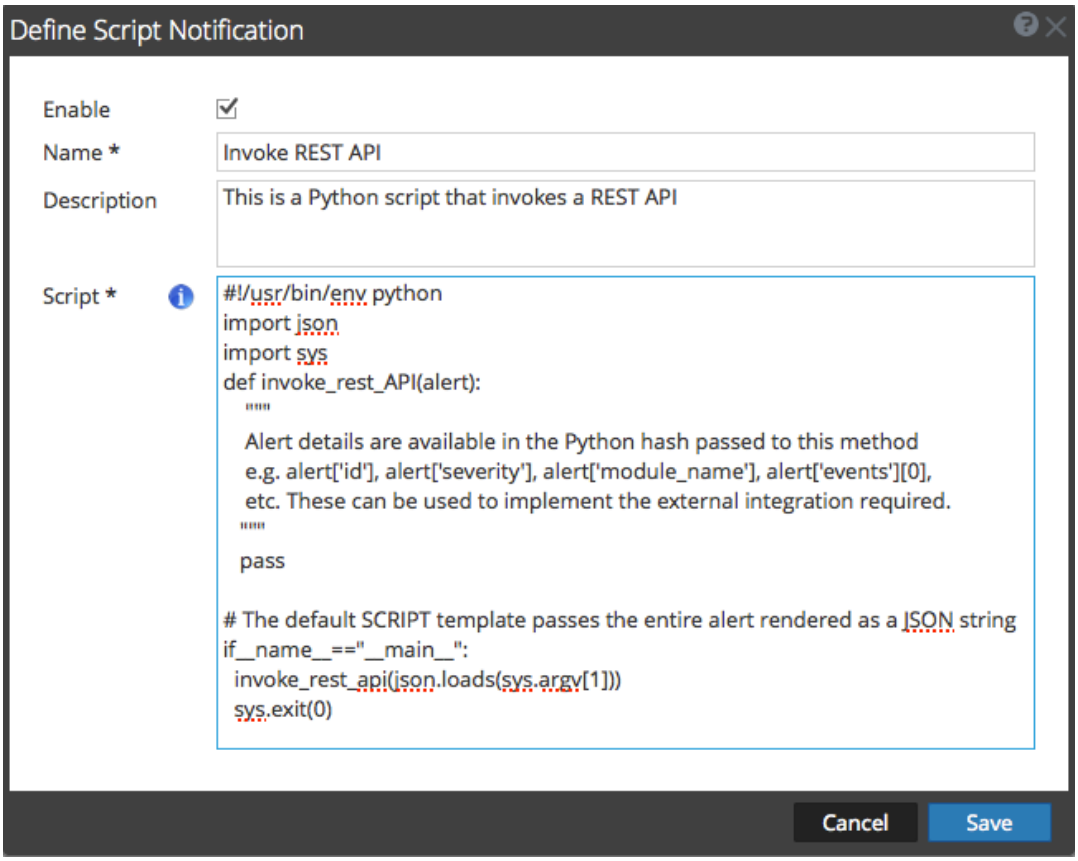
Paramètre	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller la notification.
Description	Brève description de la notification
Gravité	Définit la sévérité de l'alerte.
Encoding	Définit le format d'encodage. Dans certains environnements où aucun jeu de caractères normaux n'est utilisé (par exemple, caractères japonais), ce champ aidera à sélectionner le bon encodage des caractères.

Paramètre	Description
Longueur max.	La longueur maximale d'un message Syslog en octets. La valeur par défaut est **2048**. Les messages qui dépassent la longueur maximale sont tronqués lorsque la case à cocher **Tronquer les messages Syslog trop longs** est activée (dans Administration > Système > Notifications héritées). La section Panneau Configuration des notifications existantes fournit des informations supplémentaires.
Inclure l'horodatage local	À sélectionner pour inclure l'horodatage local aux messages.
Inclure le nom d'hôte local	À sélectionner pour inclure le nom d'hôte local aux messages Syslog.
Identifier la chaîne	Une chaîne d'identité à ajouter comme préfixe à chaque alerte Syslog. Si la chaîne est vierge, aucune chaîne d'identité n'est ajoutée comme préfixe aux alertes Syslog sortantes. Vous pouvez utiliser cette chaîne pour identifier les alertes d'ESA.

Script

Les notifications par script vous permettent de définir le script qui s'exécutera en réponse à l'alerte. Vous pouvez utiliser n'importe quel script pour les notifications ESA.

La figure suivante présente la boîte de dialogue Définir une notification par script.



Le tableau suivant répertorie les divers paramètres dont vous avez besoin pour définir les notifications par script.

Paramètre	Description
Activer	Sélectionnez le serveur de notification pour l'activer.
Name	Nom permettant d'identifier ou de libeller la notification.
Description	Brève description de la notification
Script	Définit le script.

Boîte de dialogue Définir un modèle de notification

Dans le panneau Notifications globales, vous pouvez configurer les paramètres de notification globale des serveurs, sorties et modèles de notification. Sous l'onglet Modèles, vous pouvez configurer les modèles de différentes notifications. Le modèle de notification définit les champs de format et de message des notifications. Vous pouvez sélectionner un modèle par défaut ou utiliser la boîte de dialogue Définir un modèle pour configurer et modifier des modèles.

Vous pouvez définir les types de modèles suivants :

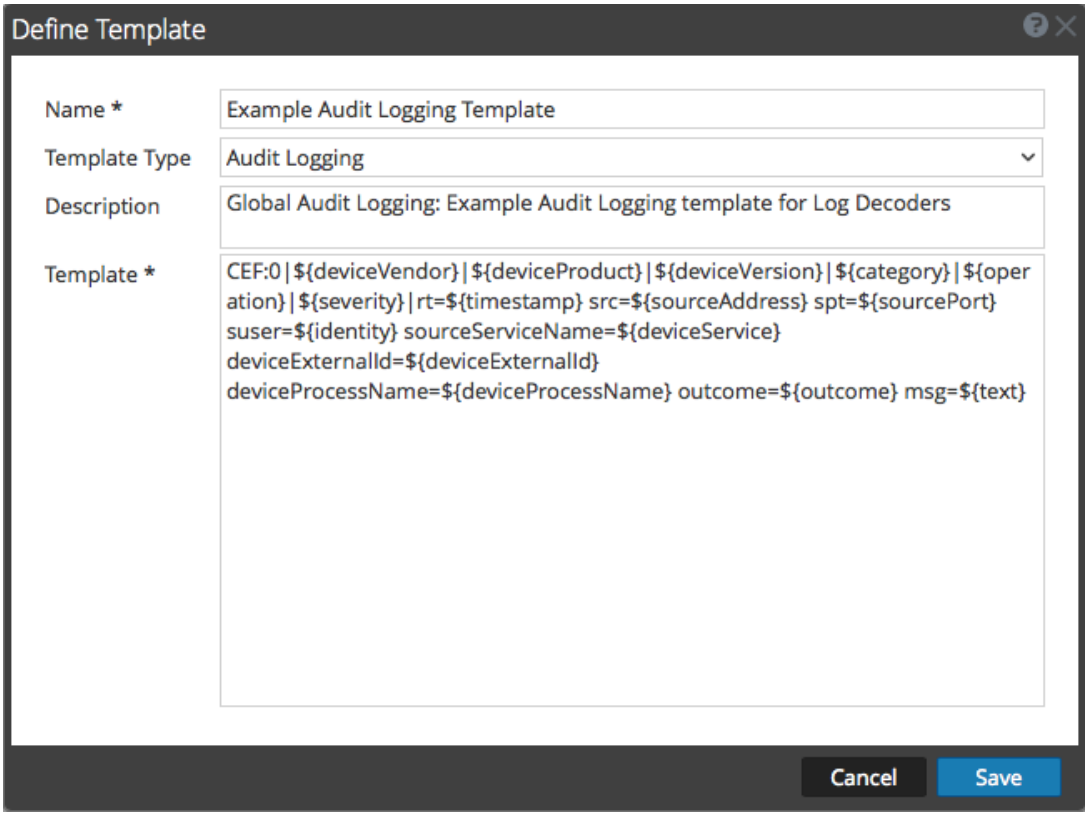
- Consignation des audits
- Event Stream Analysis
- Surveillance des sources d'événements
- Alarmes d'intégrité

Les procédures liées au modèle de notification sont décrites dans la section Configurer des modèles pour les notifications.

Pour accéder à la boîte de dialogue Définir un modèle :

1. Accédez à **ADMIN > Système**.
2. Dans le volet de navigation de gauche, sélectionnez **Notifications globales > onglet Modèle**.
3. Dans le panneau **Configurations des notifications**, cliquez sur  ou sélectionnez une configuration, puis cliquez sur  .

La boîte de dialogue **Définir un modèle** s'affiche.



Fonctionnalités

Le tableau suivant décrit les fonctionnalités de la boîte de dialogue Définir un modèle.

Champ	Description
Nom	Saisissez un nom unique pour le modèle de notification.
Type de modèle	Sélectionnez le type de modèle à créer. • **Consignation des audits** : Utilisez ce modèle pour la consignation globale des audits. • **Event Stream Analysis** : Utilisez ce type de modèle pour les notifications d'alerte ESA. • **Surveillance des sources d'événements** : Utilisez ce type de modèle pour les notifications d'alerte ESM. • **Alarmes d'intégrité** : Utilisez ce type de modèle pour les notifications d'intégrité.

Champ	Description
Description	Ajoutez une description au modèle. Par exemple, si vous créez un modèle de notification pour les Log Decoders à utiliser dans le cadre de la consignation globale des audits, vous pouvez mentionner cette information dans la description.
Modèle	Indiquez le format du modèle. Définir un modèle pour la consignation globale des audits fournit des instructions sur la façon de définir un modèle de consignation d'audit à utiliser pour la consignation globale des audits. Pour définir un modèle Event Stream Analysis (ESA), reportez-vous à la section Définir un modèle pour les notifications d'alerte ESA.

Onglet Sortie

Dans le panneau **Notifications globales**, sous l'onglet **Résultat** (Admin > Système > Notifications > Résultat), configurez les sorties de notification. Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE.

Les configurations des **sorties de notification** définissent les lignes de l'adresse e-mail et de l'objet, les paramètres OID de trap SNMP, les paramètres de sortie Syslog et le code du script.

Les notifications sont les destinations configurées pour les notifications d'alerte envoyées par le service ESA. Vous pouvez configurer les éléments suivants comme destinations à l'aide de l'onglet Sortie :

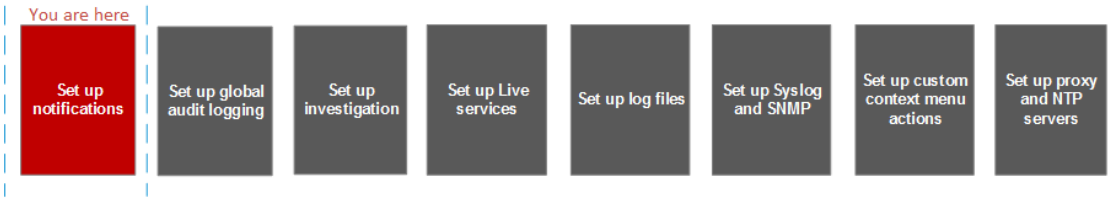
- E-mail
- SNMP
- Syslog
- Script

Remarque : Vous n'avez pas besoin de configurer l'onglet Sortie pour la consignation globale des audits. Pour connaître le détail des étapes, Configurer la consignation globale des audits.

Workflow

Ce workflow affiche les procédures nécessaires afin de configurer et vérifier le résultat pour les notifications globales. Vous pouvez effectuer les opérations suivantes :

- Configurer les paramètres E-mail pour les notifications.
- Configurer les paramètres SNMP pour les notifications.
- Configurer les paramètres Syslog pour les notifications.
- Configurer un script pour les notifications.



Que voulez-vous faire ?

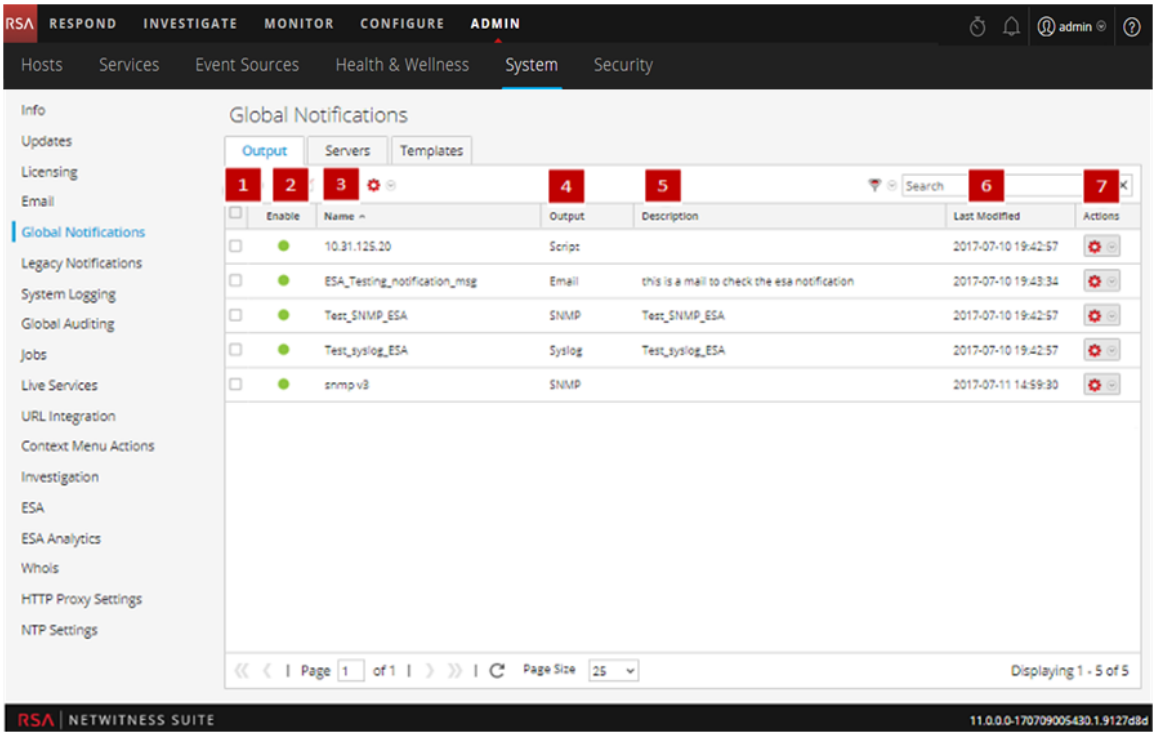
Rôle	Je souhaite...	Me montrer comment
Administrateur	Définir les sorties de notification.	Configurer les résultats de notification

Rubriques connexes

- Présentation des résultats de notification
- Configurer la messagerie en tant que méthode de notification
- Configurer un script en tant que méthode de notification
- Configurer le protocole SNMP en tant que méthode de notification
- Configurer Syslog en tant que méthode de notification

Aperçu rapide

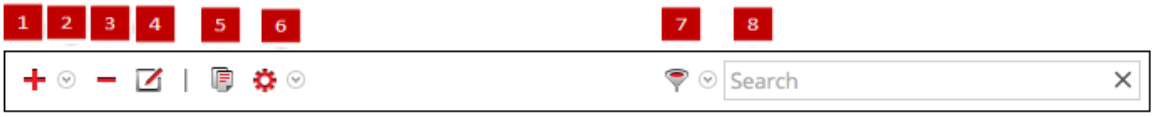
L'exemple suivant illustre la configuration des sorties de notifications globales.



1 Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.

2	Indique si la configuration est activée. Un rond coloré en vert indique qu'une configuration est activée. Un rond blanc indique qu'aucune configuration n'est activée.
3	Identifie ou étiquette la configuration.
4	Identifie le résultat de la configuration. Les sorties sont E-mail, SNMP, Syslog et Script.
5	Décrit la configuration du stockage.
6	Affiche la date et l'heure de la dernière modification de configuration.
7	Fournit un menu Actions pour la configuration sélectionnée avec les actions qui peuvent être effectuées sur la configuration. Le menu Actions vous permet de supprimer, de modifier, de répliquer et d'exporter la configuration.

La barre d'outils du panneau Notifications globales figure en haut de la balise Résultat et fournit les options suivantes :



1	Ajoute un résultat de notification
2	Configure les paramètres de notification par E-mail, SNMP, Syslog et Script.
3	Supprime la configuration de notification sélectionnée. Vous ne pouvez pas supprimer les serveurs et les types de notification associés à des configurations de consignation globale d'audits. Si vous tentez de supprimer une sortie de notification (notification) utilisée par des alertes, un message vous avertit que les alertes qui utilisent la notification ne fonctionneront plus correctement. Le message indique le nombre d'alertes en cours. Vous pouvez également supprimer une configuration en la sélectionnant, puis en choisissant > Supprimer dans la colonne Actions.
4	Modifie une configuration de notification sélectionnée. Vous pouvez également supprimer une configuration en la sélectionnant, puis en choisissant > Modifier dans la colonne Actions.
5	Duplique la configuration de notification sélectionnée. Vous pouvez également dupliquer une configuration en la sélectionnant, puis en choisissant > Dupliquer dans la colonne Actions.
6	Affiche les options suivantes :

- **Importer** : Importe un serveur, un type ou un modèle de notification. Par exemple, sur l'onglet Serveurs, vous pouvez importer une configuration de serveur de notification.
- **Exporter tout** : Exporte toutes les configurations. Par exemple, sur l'onglet Serveurs, vous pouvez exporter toutes les configurations du serveur de notification.
- **Exporter** : Exporte une configuration sélectionnée. Vous pouvez également exporter une configuration en sélectionnant une configuration, puis en sélectionnant  > Exporter dans la colonne Actions.

7 Filtre par e-mail, SNMP, Syslog ou script.

8 Recherche des configurations dans la grille.

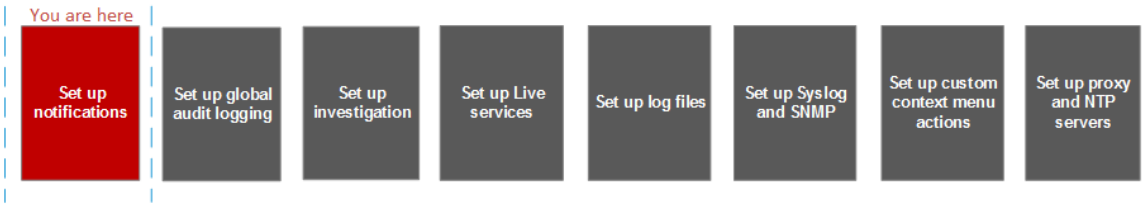
Onglet Serveurs

Cette section décrit les composants de l'onglet Notifications globales > Serveurs. Cet onglet vous permet de configurer les serveurs de notification. Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE.

Configurez les **serveurs de notification** dans l'onglet Serveurs. Sous l'onglet **Serveurs**, ajoutez les serveurs depuis lesquels vous souhaitez recevoir les notifications issues du système. Pour la consignation globale des audits, définissez des Log Decoders pour les serveurs de notification Syslog.

Event Stream Analysis peut envoyer des notifications aux utilisateurs par e-mail, SNMP ou Syslog lorsqu'une alerte est déclenchée sur le service ESA. Ces expéditeurs de notifications d'alerte sont appelés des serveurs de notification. Vous pouvez configurer différents paramètres de notification et les utiliser lors de la définition d'une règle ESA. Par exemple, vous pouvez configurer plusieurs serveurs de messagerie ou serveurs Syslog et utiliser leurs paramètres pour définir une règle ESA.

Workflow



Le workflow affiche les procédures nécessaires afin de configurer et vérifier les serveurs pour les notifications globales. Vous pouvez effectuer les opérations suivantes :

- Configurer les paramètres E-mail d'un serveur de notification.
- Configurer les paramètres SNMP d'un serveur de notification.
- Configurer les paramètres Syslog d'un serveur de notification.
- Configurer un script pour un serveur de notification.

Que voulez-vous faire ?

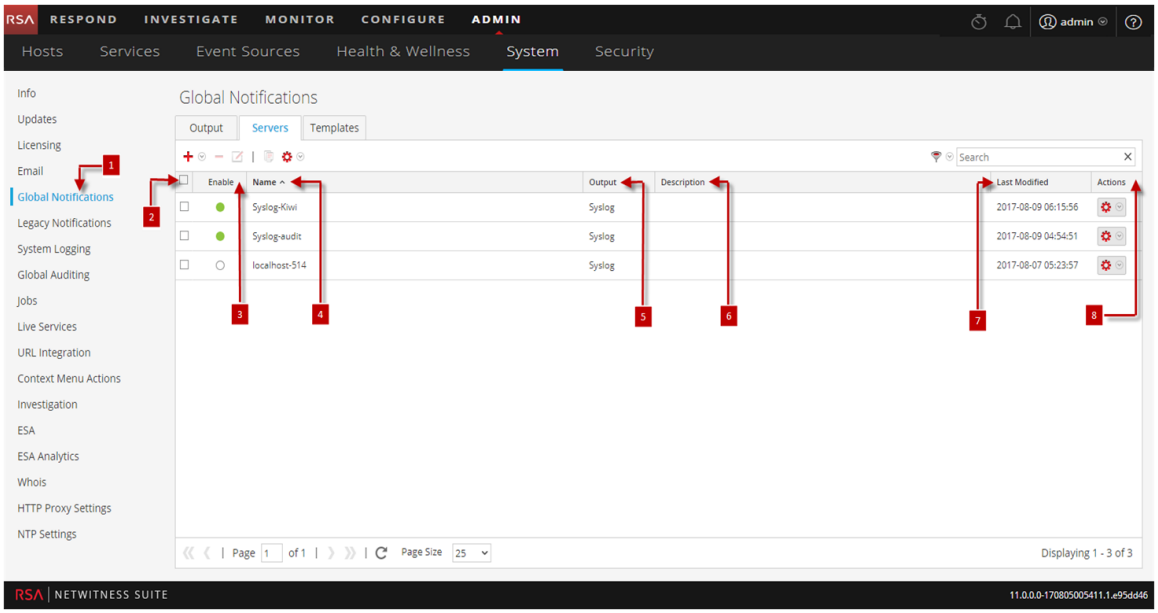
Rôle	Je souhaite...	Me montrer comment
Administrateur	Définir des serveurs de notification	Configurer les serveurs de notification

Rubriques connexes

- Présentation des serveurs de notification
- Configurer les paramètres de messagerie d'un serveur de notification
- Configurer un script pour un serveur de notification
- Configurer les paramètres SNMP d'un serveur de notification
- Configurer un serveur de notification Syslog

Aperçu rapide

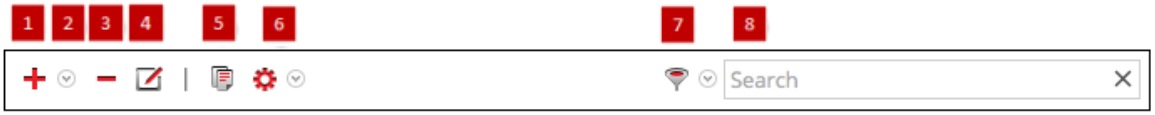
L'exemple suivant illustre la configuration globale des serveurs de notification.



1	Affiche le panneau de l'onglet Serveur.
2	Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.
3	Indique si la configuration est activée. Un rond coloré en vert indique qu'une configuration est activée. Un rond blanc indique qu'aucune configuration n'est activée.
4	Identifie ou étiquette la configuration.
5	Identifie le résultat de la configuration. Les sorties sont E-mail, SNMP, Syslog et Script.
6	Décrit la configuration du stockage.
7	Affiche la date et l'heure de la dernière modification de configuration.

8	Fournit un menu Actions pour la configuration sélectionnée avec les actions qui peuvent être effectuées sur la configuration. Le menu Actions vous permet de supprimer, de modifier, de répliquer et d'exporter la configuration.

La barre d'outils du panneau Notifications globales figure en haut de la balise Résultat et fournit les options suivantes :



1	Ajoute un résultat de notification
2	Configure les paramètres de notification par E-mail, SNMP, Syslog et Script.
3	Supprime la configuration de notification sélectionnée. Vous ne pouvez pas supprimer les serveurs et les types de notification associés à des configurations de consignation globale d'audits. Si vous tentez de supprimer une sortie de notification (notification) utilisée par des alertes, un message vous avertit que les alertes qui utilisent la notification ne fonctionneront plus correctement. Le message indique le nombre d'alertes en cours. Vous pouvez également supprimer une configuration en la sélectionnant, puis en choisissant > Supprimer dans la colonne Actions.
4	Modifie une configuration de notification sélectionnée. Vous pouvez également modifier une configuration en la sélectionnant, puis en choisissant > Modifier dans la colonne Actions.
5	Duplique la configuration de notification sélectionnée. Vous pouvez également dupliquer une configuration en la sélectionnant, puis en choisissant > Dupliquer dans la colonne Actions.
6	Affiche les options suivantes : • **Importer** : Importe un serveur, un type ou un modèle de notification. Par exemple, sur l'onglet Serveurs, vous pouvez importer une configuration de serveur de notification. • **Exporter tout** : Exporte toutes les configurations. Par exemple, sur l'onglet Serveurs, vous pouvez exporter toutes les configurations du serveur de notification.

- **Exporter** : Exporte une configuration sélectionnée. Vous pouvez également exporter une configuration en sélectionnant une configuration, puis en sélectionnant  > Exporter dans la colonne Actions.

7 Filtre par e-mail, SNMP, Syslog ou script.

8 Recherche des configurations dans la grille.

Onglet Modèles

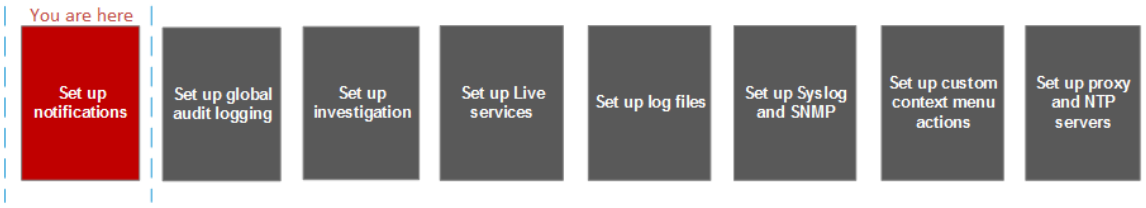
Les modèles de notification permettent de configurer les modèles de notification. Les configurations de notifications globales définissent les paramètres des notifications pour les composants Gestion des sources d'événements, Intégrité, Consignation globale des audits, Event Stream Analysis (ESA) et RÉPONDRE. Les modèles de notification définissent les champs de format et de message des notifications.

Sélectionnez un modèle par défaut ou configurez des modèles pour E-mail, SNMP, Syslog et Script selon le type de modèle. Pour les modèles Event Stream Analysis (ESA), configurez Email, SNMP, Syslog et Script. Pour les modèles de consignation des audits, configurez Syslog.

Les modèles Event Stream Analysis ne sont pas spécifiques à un type de notification d'alerte, autrement dit, le même modèle peut être utilisé pour tous les types de notifications.

Lors de la mise à niveau de NetWitness Suite 10.4, tous les modèles de notification existants migrent vers le type de modèle Event Stream Analysis.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Définir des modèles de notification	Configurer des modèles pour les notifications

Rubriques connexes

Configurer des modèles de notification globale

Configurer un modèle

Définir un modèle pour les notifications d'alerte ESA

Supprimer un modèle

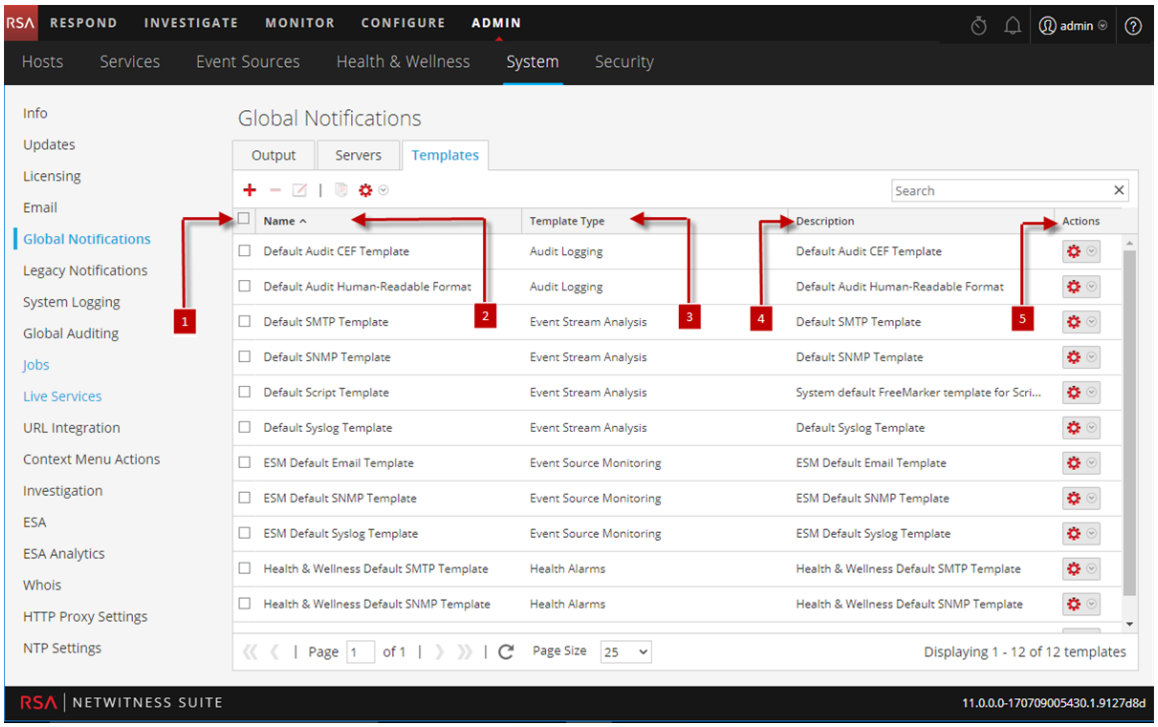
Dupliquer un modèle

Modifier un modèle

Importer et exporter un modèle de notifications global

Aperçu rapide

L'exemple suivant illustre l'onglet Modèles de notification globale.



1	Permet de sélectionner une ligne pour effectuer une action dans la barre d'outils. Cochez la case dans le titre de la colonne pour sélectionner ou désélectionner toutes les lignes de la grille.
2	Identifie ou libelle les modèles
3	Permet de choisir un type de modèle
4	Décrit les modèles
5	Fournit un menu Actions pour les modèles sélectionnés avec les actions qui peuvent être effectuées sur les modèles. Le menu Actions vous permet de supprimer, de modifier, de répliquer et d'exporter la configuration.

Panneau Paramètres proxy HTTP

Le panneau Paramètres proxy HTTP présente les fonctionnalités de prise en charge du proxy dans la vue Système d'administration > panneau Paramètres proxy HTTP.

Remarque : La prise en charge du proxy ne concerne que les proxies HTTP et HTTPS et non SOCKS5.

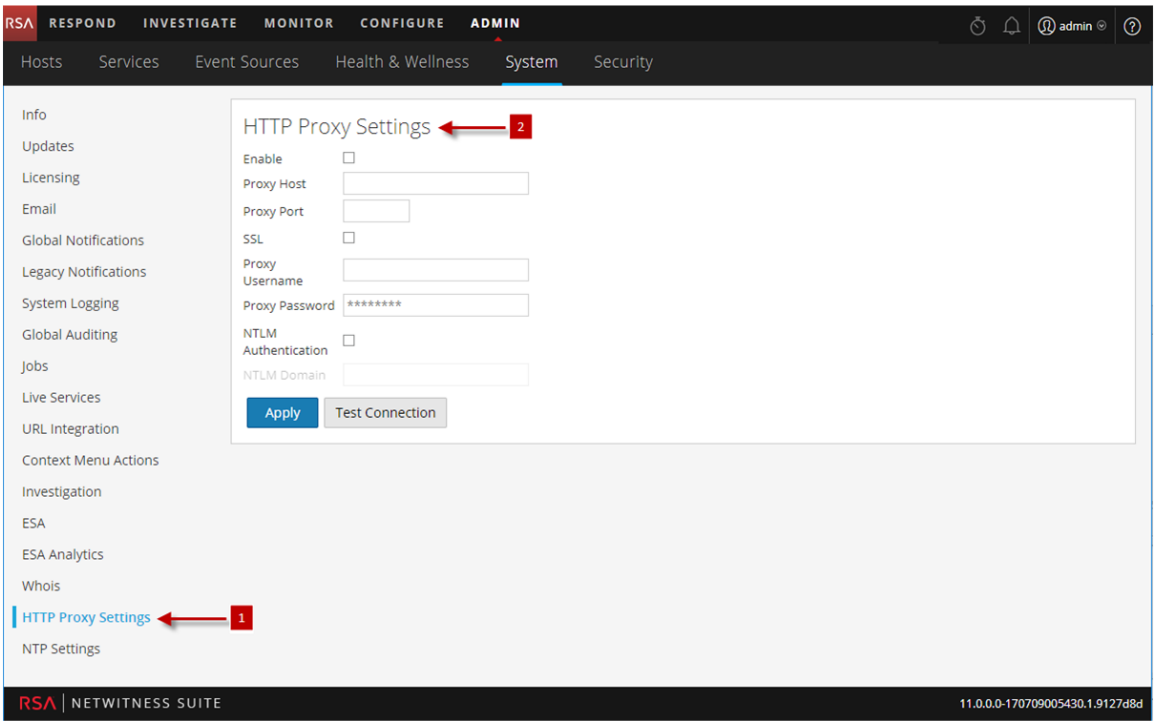
Le panneau Paramètres proxy HTTP fournit une interface utilisateur permettant de configurer un proxy à utiliser dans les modules et services NetWitness Suite. Les paramètres proxy configurent un proxy à utiliser lorsque cela est nécessaire dans NetWitness Suite. Les paramètres contenus dans ce panneau remplacent les paramètres proxy configurés pour un service individuel tel que Malware Analysis ou Live.

Rubriques connexes

Configurer le proxy pour NetWitness Suite

Aperçu rapide

L'exemple suivant illustre le panneau Paramètres proxy HTTP.



1 Affiche le panneau Paramètres Proxy HTTP.

2 Permet à l'utilisateur de configurer les paramètres du proxy HTTP.

Barre d'outils et fonctions

Ce tableau décrit les fonctions de la section Paramètres proxy.

Fonctionnalité	Description
Activer	Permet d'activer la configuration du proxy système à utiliser dans NetWitness Suite.
Hôte proxy	Nom d'hôte de l'hôte proxy.
Port du proxy	Port utilisé pour la communication sur l'hôte proxy.
Nom d'utilisateur proxy	(Facultatif) Nom d'utilisateur permettant de se connecter à l'hôte proxy si le proxy requiert une authentification.
Mot de passe du proxy	(Facultatif) Mot de passe utilisateur permettant de se connecter à l'hôte proxy si le proxy requiert une authentification.
Utiliser l'authentification NTLM	Permet d'utiliser l'authentification NT LAN Manager et les protocoles de sécurité de session.
Domaine NTLM	Nom du domaine NTLM.
Use SSL	(Facultatif) Permet d'activer la communication via une connexion SSL.
Appliquer	Applique les modifications effectuées afin qu'elles prennent effet immédiatement.

Panneau Configuration de l'e-mail

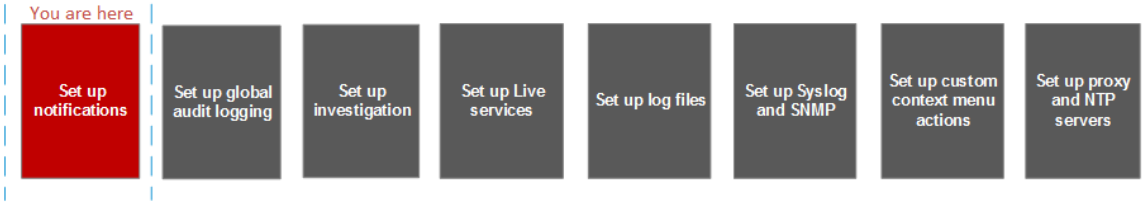
Le panneau Configuration de l'e-mail fournit des informations sur les paramètres de configuration dans la vue système > Panneau Configuration de l'e-mail. RSA NetWitness® Suite envoie des notifications aux utilisateurs par e-mail concernant les différents événements système. Pour pouvoir configurer ces notifications par e-mail, vous devez d'abord configurer le serveur de messagerie SMTP (reportez-vous à la section Configurer les serveurs de messagerie et les comptes de notification).

Le panneau Configuration de l'e-mail permet de :

- Configurer le serveur de messagerie.
- Configurer un compte de messagerie pour recevoir les notifications.
- Afficher les statistiques des opérations liées à la messagerie.

Workflow

Ce workflow présente les procédures requises pour configurer et vérifier le panneau E-mail.



Que voulez-vous faire ?

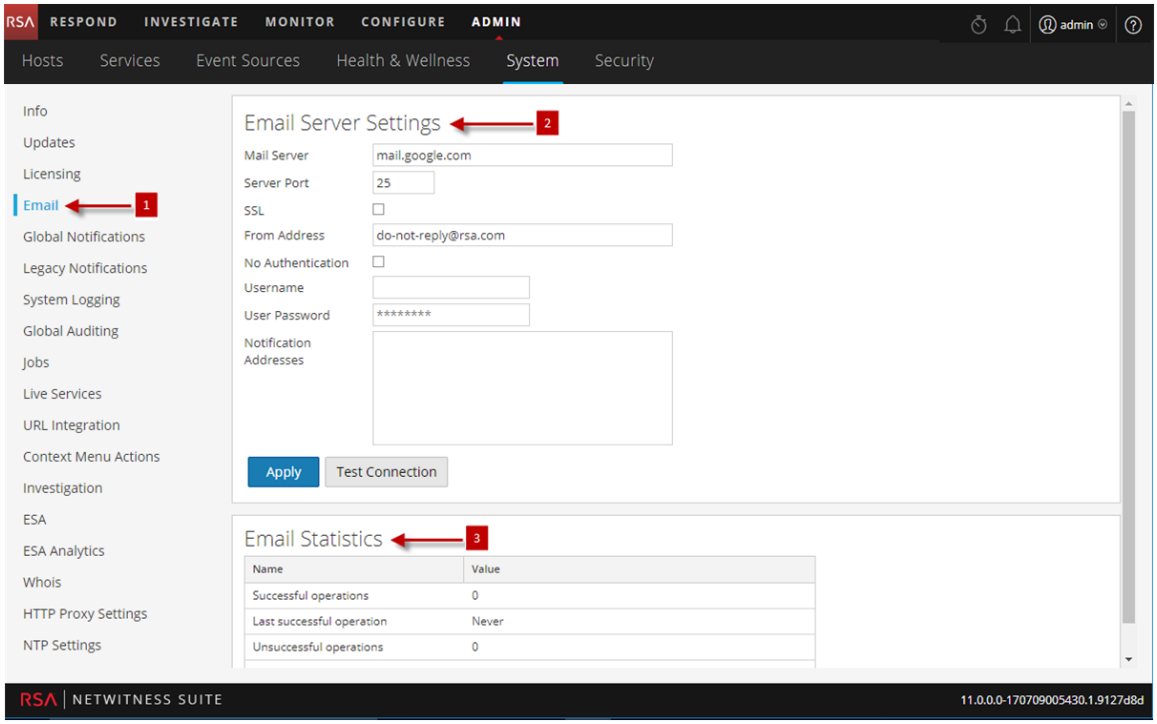
Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer le service de messagerie SMTP	Configurer les serveurs de messagerie et les comptes de notification
Administrateur	Paramètres de messagerie en tant que serveur de notification	Configurer les paramètres de messagerie d'un serveur de notification
Administrateur	Configurer, vérifier et activer le compte de messagerie	Recevoir une notification par e-mail

Rubriques connexes

- Configurer les paramètres de messagerie d'un serveur de notification
- Configurer la messagerie en tant que méthode de notification
- Configurer les serveurs de messagerie et les comptes de notification

Aperçu rapide

L'exemple suivant illustre une configuration de la messagerie. La configuration définit le mode de notification des événements par e-mail.



1	Affiche le panneau Configuration par e-mail.
2	Permet à l'utilisateur de configurer les paramètres du serveur de messagerie.
3	Fournit des informations sur les opérations de messagerie.

Barre d'outils et fonctions

Le panneau **Configuration de l'e-mail** contient deux sections : **Paramètres du serveur de messagerie** et **Statistiques de la messagerie**.

Paramètres du serveur de messagerie

Dans la section **Paramètres du serveur de messagerie**, configurez les paramètres ci-dessous.

Fonctionnalité	Description
Serveur de messagerie	Nom du serveur de messagerie. La valeur par défaut est **mail.google.com**.
Port de serveur	Port de serveur utilisé pour envoyer et recevoir des e-mails. La valeur par défaut est **25**.
Utiliser SSL	Préférence d'utilisation de SSL dans les communications entre le serveur de messagerie et NetWitness Suite. Par défaut, l'option est désactivée.
Adresse de l'expéditeur	Adresse qui apparaît dans tous les e-mails de NetWitness Suite. L'adresse de l'expéditeur par défaut pour les e-mails est **do-not-reply@rsa.com**.
Nom d'utilisateur	Nom d'utilisateur permettant d'accéder au serveur de messagerie. La valeur par défaut est **vide**.
Mot de passe d'utilisateur	Mot de passe d'utilisateur permettant d'accéder au serveur de messagerie. La valeur par défaut est **vide**.
Tester la connexion	Teste la connexion au serveur de messagerie.
Appliquer	Applique la configuration de la messagerie à cette instance de NetWitness Suite.

Statistiques relatives à la messagerie

La section Statistiques relatives à la messagerie fournit des informations sur le nombre d'opérations liées à la messagerie ayant réussi ou échoué, ainsi que l'heure de la dernière opération liée à la messagerie ayant réussi ou échoué. Pour chaque statistique, le nom et la valeur sont affichés.

Panneau Paramètres ESA

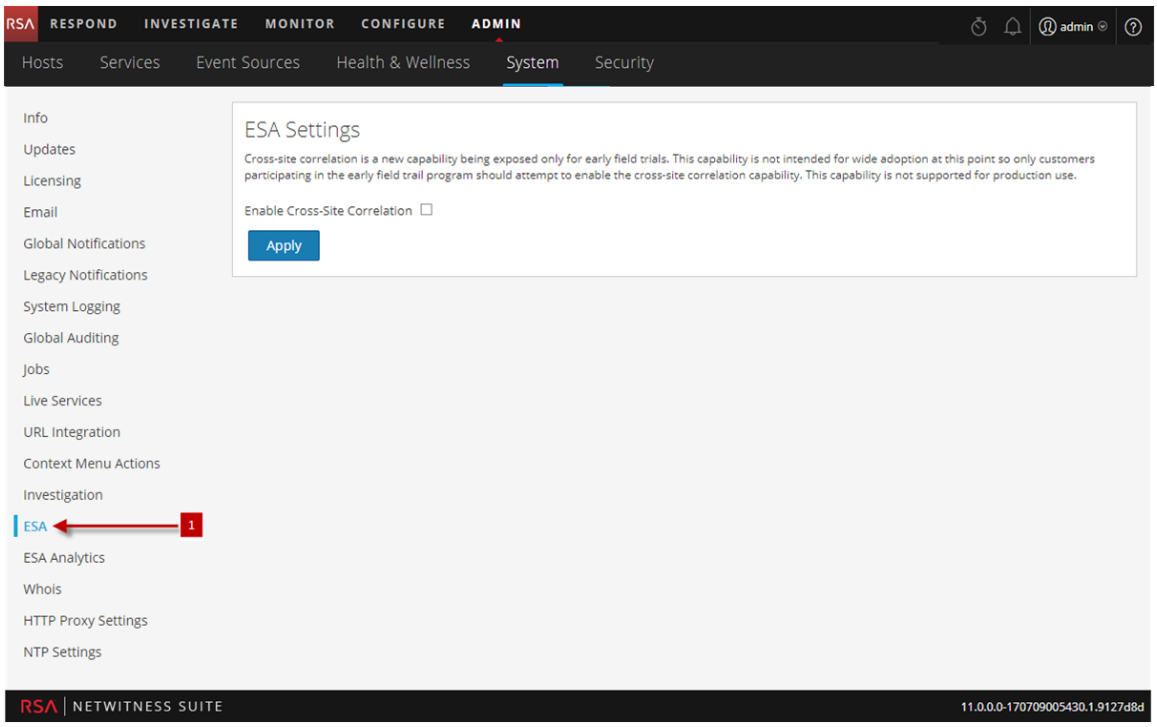
Le panneau Paramètres ESA est l'emplacement dans lequel vous activez et désactivez la corrélation entre les sites. La corrélation entre les sites est une nouvelle fonctionnalité uniquement disponible pour les évaluations anticipées sur site. Cette fonctionnalité n'est pas conçue pour être adoptée de manière généralisée.

Attention : Seuls les clients participant au programme d'évaluation anticipée sur site peuvent tenter d'activer la fonctionnalité de corrélation entre les sites. Cette fonctionnalité n'est pas prise en charge pour une utilisation en production.

Rubriques connexes

- Définir un modèle pour les notifications d'alerte ESA
- Guide Investigation et Malware Analysis
- Guide de configuration de Context Hub

Aperçu rapide



1	Affiche le panneau Paramètres ESA.

Barre d'outils et fonctions

Les fonctions du panneau Paramètres ESA sont les suivantes :

- Case à cocher Activer la corrélation intersite : lorsque cette option est activée, la corrélation intersite dans ESA l'est également. Lorsque vous ajoutez un déploiement dans ADMIN > Alertes > Configurer, vous pouvez déployer le même ensemble de règles sur plusieurs services ESA pour un traitement centralisé des règles.
- Bouton Appliquer : il active votre sélection.

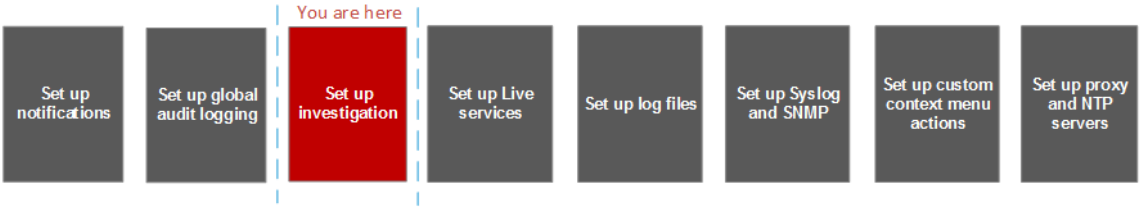
Panneau Configuration des procédures d'enquête

La vue Système > Panneau Configuration des procédures d'enquête, qui est l'interface utilisateur des administrateurs pour configurer les paramètres de l'ensemble du système que NetWitness Suite Investigation utilise lors de l'analyse des données et de la reconstruction d'un événement.

Les paramètres de configuration des procédures d'enquête permettent à un administrateur de gérer les performances d'application des procédures d'enquête. Alors que les analystes procèdent à l'analyse et la reconstruction de sessions sur lesquelles ils enquêtent, les opérations de chargement, recherche, visualisation et reconstruction de grandes quantités de données peuvent avoir un effet sur les performances.

Remarque : Les analystes peuvent également définir les préférences individuelles d'Investigation dans la vue Profils et la vue Navigation.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer les paramètres Naviguer, Événements et Recherche contextuelle	Configurer les paramètres du module Investigation
Administrateur	Effacer le cache de reconstruction pour les services	Configurer les paramètres du module Investigation

Rubriques connexes

- Procédures standard

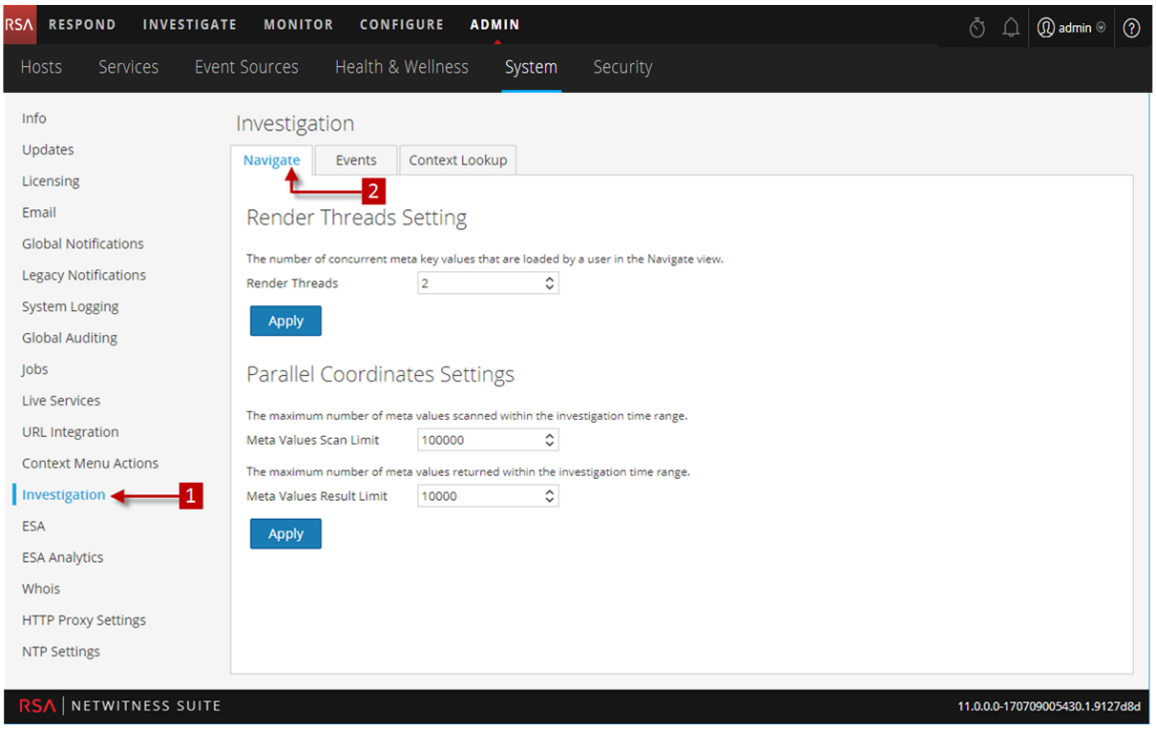
Aperçu rapide

Le panneau Configuration des procédures d'enquête compte trois onglets : Naviguer, Événements et Recherche contextuelle.

Bien que la plupart des champs des onglets disposent d'une liste de sélection avec des incréments spécifiques aux valeurs possibles, vous pouvez saisir manuellement une valeur dans la plage autorisée. Lorsqu'une valeur n'est pas valide, le champ apparaît en surbrillance de couleur rouge. Lorsque des valeurs valides sont sélectionnées, cliquez sur Appliquer dans une section donnée pour que la modification prenne effet immédiatement.

Onglet Naviguer

La figure ci-dessous présente l'onglet Naviguer.



1 Le panneau Configuration des procédures d'enquête s'affiche.

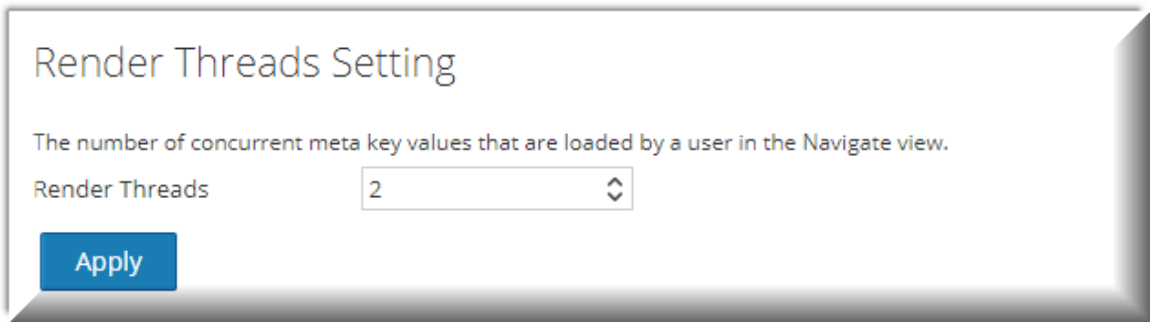
2 Affiche l'onglet Naviguer.

Barre d'outils et fonctions

L'onglet Naviguer présente deux sections : Paramètre Générer les threads et Paramètres de coordonnées parallèles.

Générer les paramètres de threads

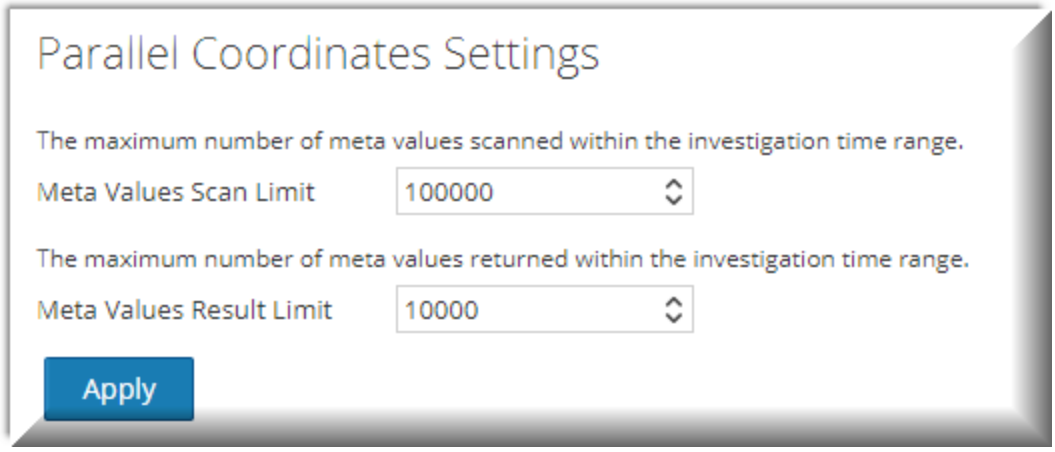
Le Paramètre Générer les paramètres de threads est une valeur sélectionnable entre 1 et 20, qui détermine le nombre de charges (valeurs) simultanées dans la vue Naviguer. La valeur par défaut est 1.



Paramètres de coordonnées parallèles

Les Paramètres de coordonnées parallèles s'appliquent à la visualisation des coordonnées parallèles dans la vue Naviguer. Il existe une limite fixe pour la quantité de données qui peut être affichée sous la forme d'un graphique de coordonnées parallèles. Dans NetWitness Suite, l'administrateur peut configurer des limites de coordonnées parallèles ici.

Remarque : Pour de meilleures performances, les paramètres recommandés sont **Limite d'analyse de valeurs méta : 100000** et **Limite de résultat de valeurs méta : 1000-10000**.



Le tableau suivant décrit les Paramètres de coordonnées parallèles.

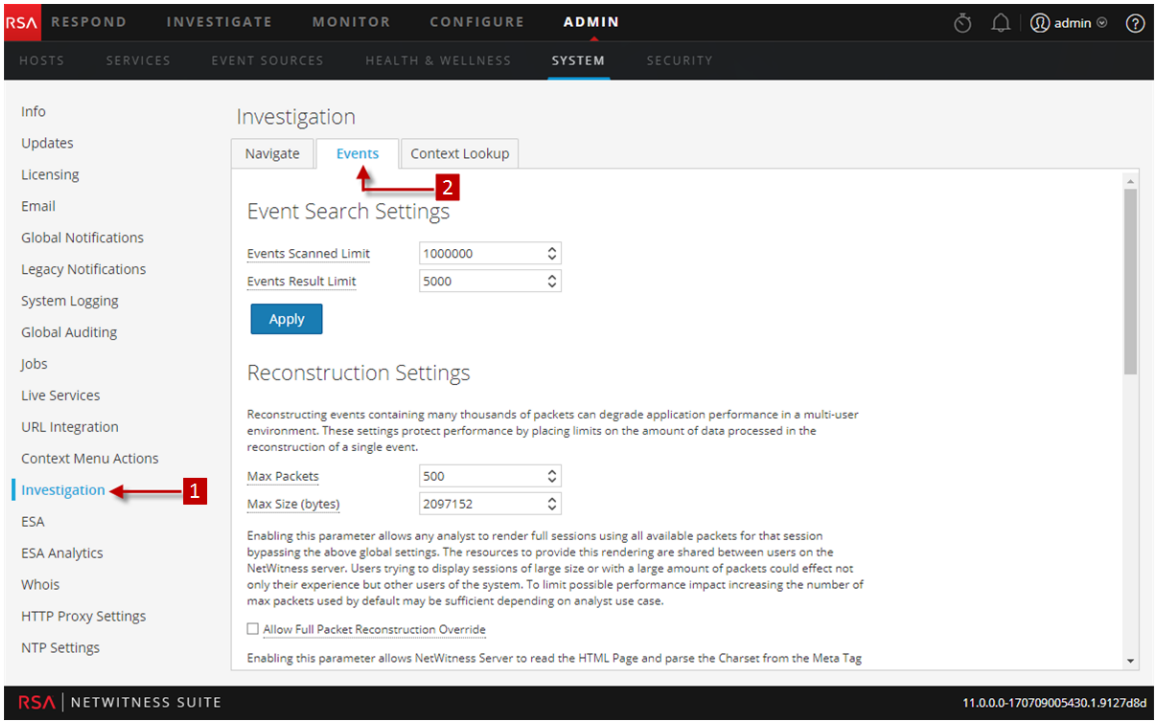
Paramètre	Description
Limite d'analyse de valeurs méta	Nombre maximum de valeurs méta analysées dans la période Investigation sélectionnée par l'analyste dans la vue Naviguer. Les valeurs possibles se situent dans une plage entre 1 000 et 10 000 000. La valeur par défaut est 100 000.

Paramètre	Description
Limite de résultat de valeurs méta	Nombre maximum de valeurs méta renvoyées dans la période Investigation sélectionnée par l'analyste dans la vue Naviguer. Les valeurs possibles se situent dans une plage entre 100 et 1 000 000 000. La valeur par défaut est 10 000.

Aperçu rapide

Onglet Événements

La figure ci-dessous présente l'onglet Événements.



Les procédures associées à ce panneau sont présentées dans la section Procédures standard.

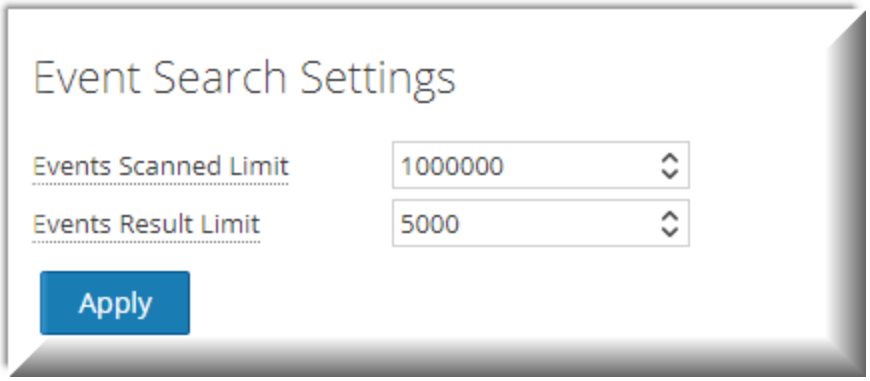
1. Le panneau Configuration des procédures d'enquête s'affiche.
2. Affiche l'onglet Événements.

Barre d'outils et fonctions

L'onglet Événements propose des paramètres configurables qui ont un impact sur la procédure d'enquête des événements. Cet onglet présente quatre sections : Paramètres de recherche d'événements, Paramètres de reconstruction, Paramètres de reconstruction de la vue Web et Paramètres du cache de reconstruction.

Paramètres de recherche d'événements

Les Paramètres de recherche d'événements aident à limiter le nombre d'événements analysés lors de la recherche dans la vue Événements.



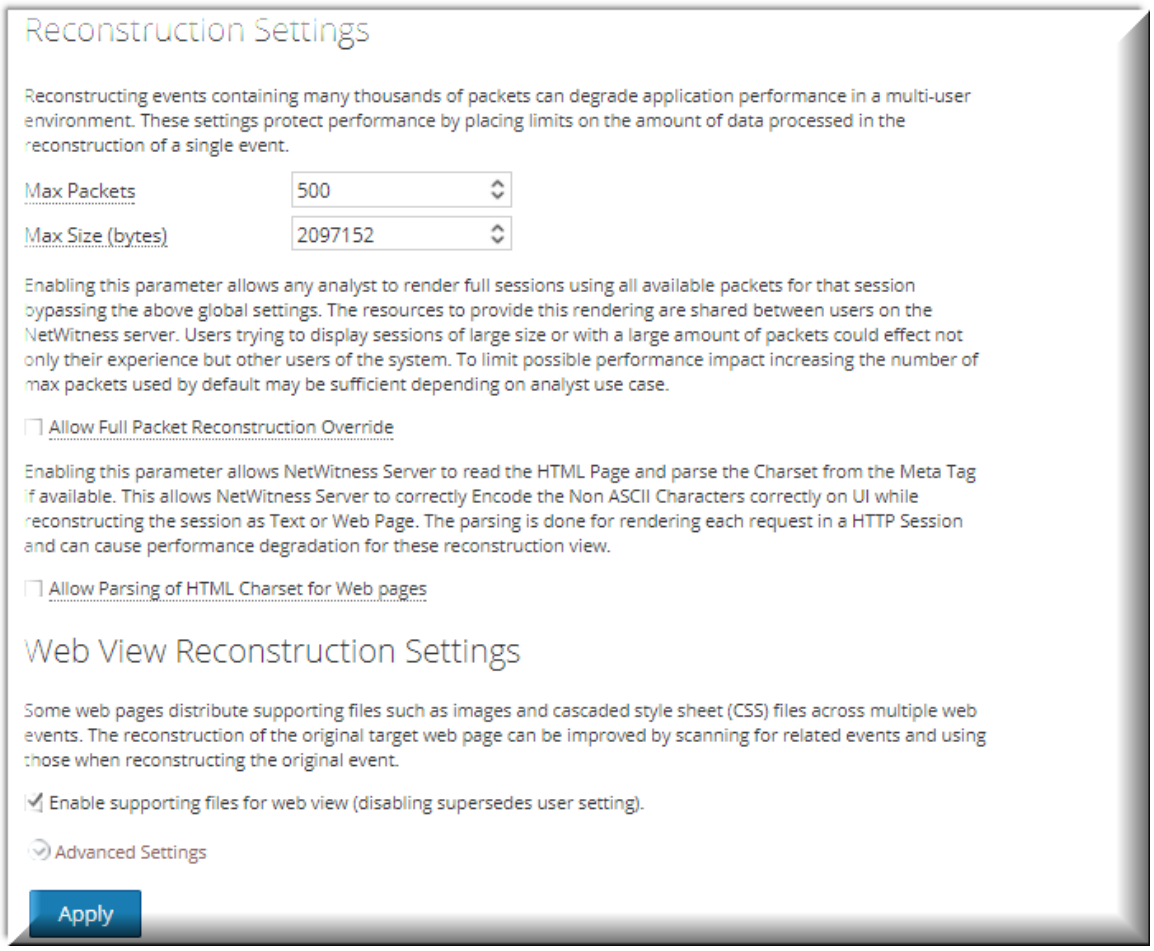
Le tableau suivant décrit les Paramètres de recherche d'événements.

Paramètre	Description
Limite des événements analysés	Nombre maximum d'événements à analyser lors de la recherche dans la vue Événements.
Limite des résultats d'événements	Nombre maximum de résultats à renvoyer lors de la recherche dans la vue Événements.

Paramètres de reconstruction

Alors que les analystes reconstruisent des sessions sur lesquelles ils enquêtent, certains événements peuvent être très volumineux et contenir des milliers de paquets source. La reconstruction de ces sessions peut avoir un effet négatif sur les performances de l'application, en particulier dans un environnement avec de multiples utilisateurs. Les paramètres de reconstruction permettent à un administrateur de limiter le nombre de paquets et la taille d'un événement unique au cours de la reconstruction.

Remarque : Le remplacement de la section Paramètres de reconstruction est configurable pour la vue Web (dans Paramètres de reconstruction de la vue Web).



Le tableau suivant décrit les fonctions des Paramètres de reconstruction.

Paramètre	Description
Nombre maximum de paquets pour un seul événement	Ce paramètre protège les performances en imposant une limite au nombre de paquets traités pour la reconstruction d'un seul événement. Les valeurs possibles se situent dans une plage de 100 à 10 000 paquets, qu'il est possible de saisir manuellement ou de sélectionner dans la liste de sélection par incréments de 100. La valeur par défaut est 100 paquets.

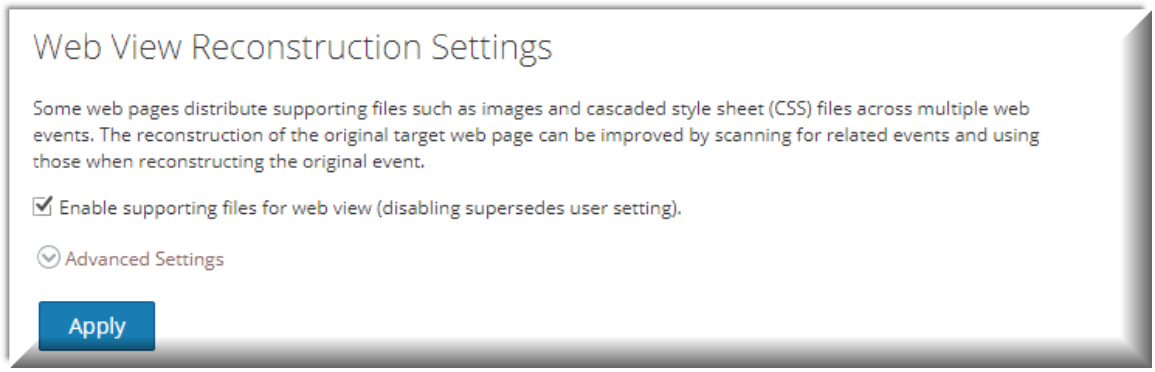
Paramètre	Description
Taille maximum en octets d'un seul événement	Ce paramètre protège les performances en imposant une limite à la taille maximum, en octets, pour la reconstruction d'un seul événement. Les valeurs possibles se situent dans une plage de 102 400 à 104 857 600 octets, qu'il est possible de saisir manuellement ou de sélectionner dans la liste de sélection par incréments de 10 240. La valeur par défaut est 2 097 152 octets.
Autoriser le remplacement par la reconstruction complète des paquets	Lorsque cette case est cochée, les analystes disposent d'un bouton Utiliser plus de paquets dans le panneau Reconstruction. Cela permet au serveur NW de régénérer les événements en utilisant tous les paquets disponibles dans l'événement.
Autoriser l'analyse du jeu de caractères HTML pour les pages Web	Cette option permet au Serveur NetWitness d'identifier le codage des pages Web défini dans la balise Méta HTML au lieu de l'en-tête HTTP. Par défaut, cet élément est désactivé.

Paramètres de reconstruction de la vue Web

Les Paramètres de reconstruction de la vue Web permettent à un administrateur de configurer les paramètres qui améliorent la reconstruction d'une vue Web en analysant et reconstruisant les événements connexes qui contiennent les mêmes fichiers de prise en charge. Lorsque NetWitness Suite reconstruit une vue Web qui couvre plusieurs événements, il est possible d'améliorer la reconstruction de l'événement cible en analysant et en reconstruisant les événements connexes qui contiennent les mêmes fichiers de prise en charge, comme des images et des fichiers de feuilles de style en cascade (CSS).

- Les seuls événements connexes qui sont analysés sont les événements de type service HTTP avec la même adresse source que l'événement cible, et un horodatage au sein d'une période spécifiée avant et après l'événement cible.
- Le nombre maximum d'événements connexes à analyser est configurable.

Cliquez sur l'option Paramètres avancés pour afficher tous les paramètres configurables de cette section.



Le tableau suivant décrit les Paramètres de reconstruction de la vue Web.

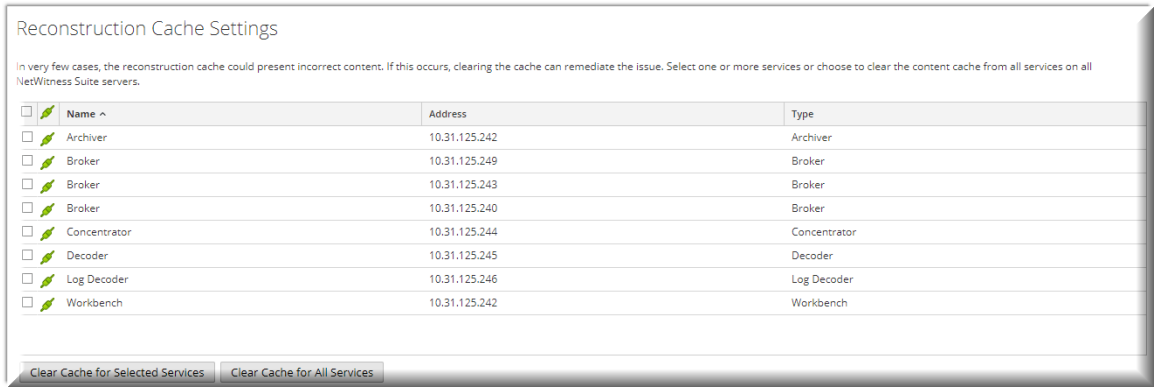
Paramètre	Description
Activer la prise en charge des fichiers pour la vue Web	Cette option détermine comment les vues Web qui ont des données connexes dans d'autres sessions sont reconstruites. Le paramètre par défaut est activé. Lorsque ce paramètre est activé, les fichiers de prise en charge provenant d'événements connexes peuvent être utilisés dans la reconstruction des vues Web. Dans cette section, d'autres paramètres pour la calibration des performances sont activés, et les analystes ont la possibilité d'activer l'utilisation des CSS dans les reconstructions. Si le paramètre est désactivé, les fichiers de prise en charge provenant d'événements connexes ne sont pas utilisés et le paramètre permettant aux analystes d'activer les CSS dans les reconstructions est désactivé.
Période pour analyser les événements connexes	Disponible lorsque l'option **Activer la prise en charge des fichiers pour la vue Web** est cochée. Configure la période pendant laquelle NetWitness Suite analyse les événements connexes qui sont de type de service HTTP et ont la même adresse source que l'événement cible. C'est une valeur comprise entre 0 et 60. • Secondes avant l'événement cible • Secondes après l'événement cible

Paramètre	Description
Limiter le nombre d'événements connexes traités	Permet la configuration du nombre maximum d'événements connexes analysés par NetWitness Suite dans la plage spécifiée pour découvrir les fichiers de prise en charge pour l'événement cible. Par défaut, cette option est désactivée. Lorsqu'elle est activée, le champ Maximum d'événements connexes devient actif.
Maximum d'événements connexes	Lorsque l'option **Limiter le nombre d'événements traités** est activée, ce champ spécifie le nombre maximum d'événements connexes que NetWitness Suite analyse dans la période de temps spécifiée pour découvrir les fichiers de prise en charge pour l'événement cible. Il s'agit d'une valeur sélectionnable entre 10 et 1 000, avec des incréments de 100. La valeur par défaut est 100.
Limiter le nombre de paquets et la taille de chaque événement connexe	Remplace les paramètres généraux du nombre maximum de paquets et de la taille maximum (en octets) pour les événements individuels connexes.
Nombre maximum de paquets pour un seul événement connexe	Les valeurs possibles se situent dans une plage de 100 à 10 000 paquets, par incrément de 100 à partir de la liste de sélection. La valeur par défaut est 100 paquets.

Paramètre	Description
Taille maximale, en octets, d'un seul événement connexe	Les valeurs possibles se situent dans une plage de 102 400 à 104 857 600 octets, par incrément de 10 240 à partir de la liste de sélection. La valeur par défaut est 524 288 octets.

Paramètres du cache de reconstruction

Dans certains cas, le cache de reconstruction peut présenter du contenu incorrect. Pour cette raison, NetWitness Suite supprime du cache les reconstructions qui datent de plus d'un jour. Le cache est vidé tous les jours à minuit. Entre les vidages de cache quotidiens, certaines actions peuvent engendrer l'utilisation d'entrées de cache périmées pour une reconstruction, et en cas de besoin, les administrateurs peuvent vider le cache manuellement pour un ou plusieurs services connectés au serveur Serveur NetWitness actuel.



Le tableau suivant décrit les fonctions des Paramètres du cache de reconstruction.

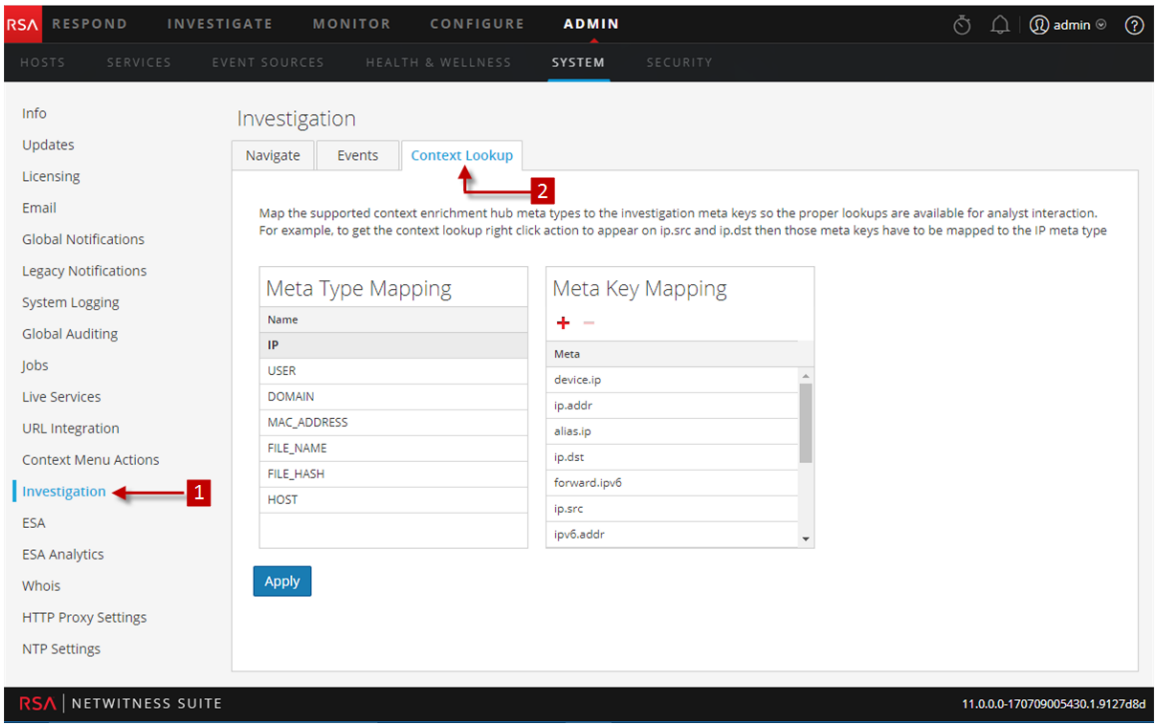
Fonctionnalité	Description
Boîte de sélection	La zone de sélection au niveau des lignes individuelles et dans la barre de titre permet la sélection d'un, de plusieurs ou de tous les services dont le cache doit être vidé manuellement.
Effacer le cache pour les services sélectionnés	Vide le cache de reconstruction pour chaque service sélectionné.

Fonctionnalité	Description
Effacer le cache pour tous les services	Vide le cache de reconstruction pour tous les services.

Aperçu rapide

Onglet Recherche contextuelle

La figure ci-dessous illustre l'onglet Recherche contextuelle.



Les procédures associées à ce panneau sont fournies dans Gérer le mappage du type de méta et de la clé méta dans le *Guide de configuration de Context Hub*.

1. Le panneau Configuration des procédures d'enquête s'affiche.
2. Affiche l'onglet Recherche contextuelle.

Barre d'outils et fonctions

L'onglet Recherche contextuelle permet à l'administrateur de configurer le mappage des clés méta et du type de méta dans Investigation. L'administrateur peut ajouter ou supprimer les clés méta trouvées dans Investigation dans la liste des types de méta pris en charge par le service Context Hub.

Le tableau suivant décrit les fonctions de l'onglet Recherche contextuelle.

Fonctionnalité	Description
+	Ajoute une clé méta au type de méta sélectionné pris en charge par Context Hub.
−	Supprime la clé méta du type de méta sélectionné.
Appliquer	Enregistre les modifications apportées à l'onglet Recherche contextuelle.

Panneau Configuration des services Live

Le panneau Configuration des services Live présente les fonctionnalités permettant de configurer votre compte Live et la connexion au serveur CMS.

Le Compte Live se compose de deux sections État Live RSA et Télécharger les logs d'activité Live Feedback. **Connectez-vous** en saisissant les informations d'identification de votre compte Live pour pouvoir accéder aux services Live. Pour activer votre compte Live pour NetWitness Suite, veuillez contacter le Support Clients RSA. Lorsque vous aurez obtenu confirmation que votre compte Live a été configuré, vous pourrez configurer la connexion au serveur CMS comme décrit dans la section Configurer les paramètres des services Live.

Le panneau Services Live fournit l'interface utilisateur permettant d'accéder à ce qui suit :

- Le compte Live
- Calendrier des mises à jour du contenu Live et préférences de notification des mises à jour
- Participation à Live Feedback
- Partage des détails d'utilisation du contenu Live
- RSA Live Connect (Bêta)

Boîte de dialogue Nouvelles fonctions activées

Lorsque vous vous connectez à NetWitness Suite pour la première fois, la boîte de dialogue **Nouvelles fonctions activées** s'affiche.

Fonctionnalité	Description
Accepter	Cliquer sur Accepter indique que vous vous engagez à ce qui suit : • Participer à Live Feedback. • Autoriser NetWitness Suite à envoyer à RSA les metrics d'utilisation et la version des hôtes NW concernant votre environnement, à condition qu'un compte Live soit configuré. • Recevoir les données de renseignements sur les menaces provenant de Live Connect.
Afficher les paramètres	Cliquer sur **Afficher les paramètres** vous redirige vers l'interface utilisateur des services Live pour afficher les paramètres. Si vous n'avez pas encore configuré votre compte Live, un écran masqué est affiché.

Pour plus d'informations sur Live Feedback, reportez-vous à la rubrique Présentation de Live Feedback

Pour plus d'informations sur les comportements d'analystes et partage de données, voir le « **NetWitness Suite Feedback et Data Sharing** » section dans les *Guide de gestion des Services live*.

Pour plus d'informations sur Live Connect Threat Insights, reportez-vous à la section Configurer les paramètres des services Live

Workflow

Que voulez-vous faire ?

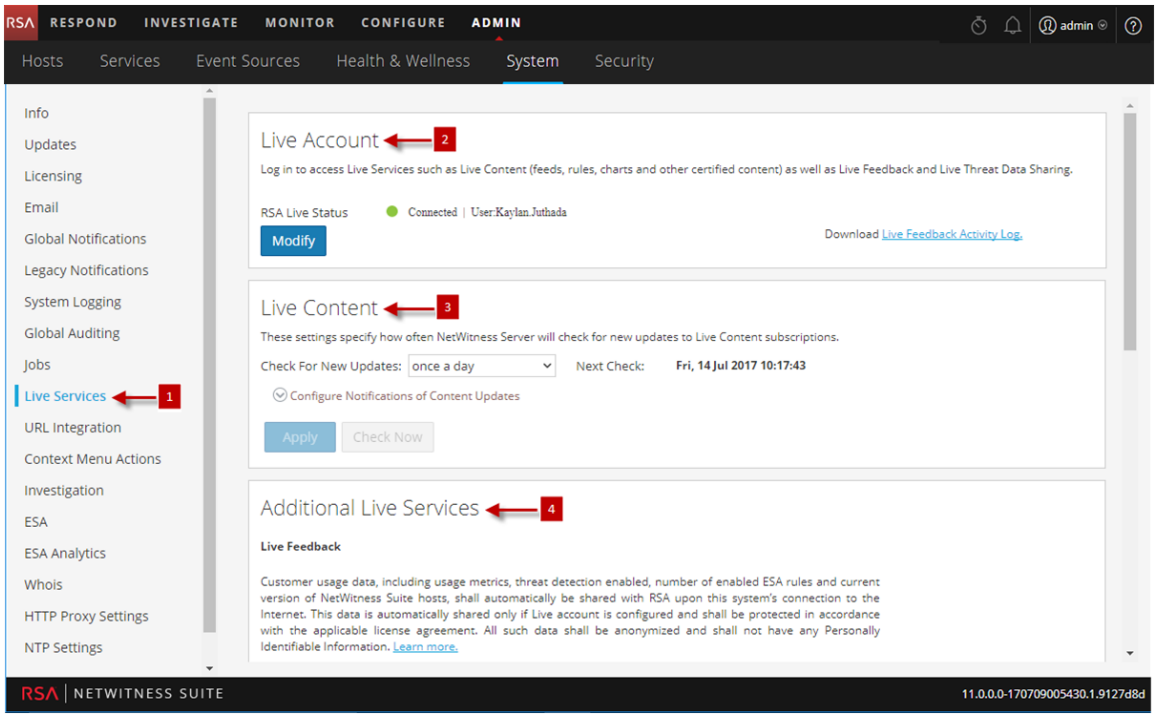
Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer le compte Live, Connexion au serveur CMS	Configurer les paramètres de messagerie d'un serveur de notification
Administrateur	Télécharger des données vers RSA pour Live Feedback	Télécharger des données vers RSA pour Live Feedback
Administrateur	Configuration, Panneau de configuration du service Live	Panneau Configuration des services Live
Administrateur	Présentation de Live Feedback	Présentation de Live Feedback

Rubriques connexes

- Présentation de Live Feedback
- Configurer les paramètres des services Live
- Télécharger des données vers RSA pour Live Feedback
- Guide de gestion des services Live

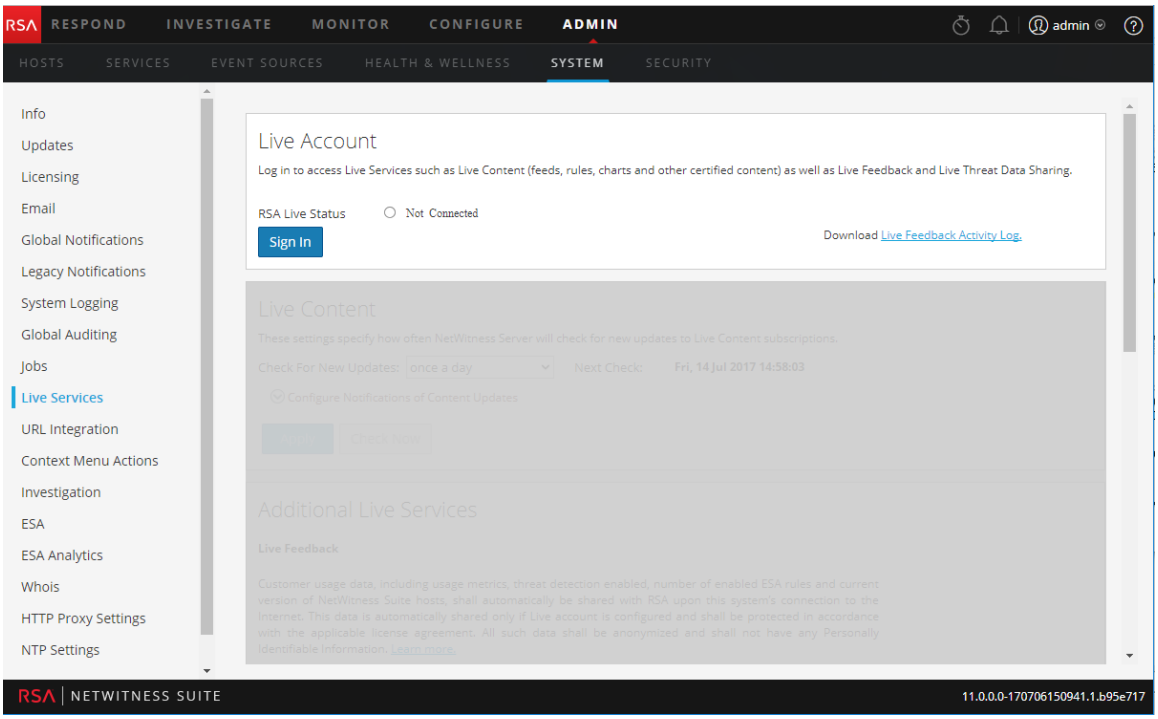
Aperçu rapide des services Live

Accédez à cette vue dans le menu **ADMIN > SYSTÈME > Services Live**.



Remarque : Si vous ne vous connectez pas avec les informations d'identification de votre compte Live, un écran masqué s'affiche.

1	Affiche le panneau Configuration des services Live
2	Permet de saisir les informations d'identification du compte Live avec l'aide du Support client.
3	Fournit la mise à jour sur le Contenu Live
4	D'autres services Live fournissent Live Feedback



Barre d'outils et fonctions

Le panneau Configuration de Live comporte trois sections : Compte Live, Contenu Live et Services Live supplémentaires.

Section Compte Live

Dans la section **Compte Live**, vous devez saisir les informations d'identification Live. Les informations requises pour configurer le compte Live de l'utilisateur sont le nom d'utilisateur, le mot de passe et l'URL Live pour le système de gestion de contenu (CMS) RSA. Ces informations sont fournies par le Service client.

Le tableau suivant décrit les fonctions de la section Compte Live.

Fonctionnalité	Description
Hôte	L'URL Live pour le Content Management System. La valeur par défaut pointe vers le RSA CMS avec l'URL **cms.netwitness.com**.
Port	Le port de communication permettant à Live d'envoyer des requêtes au Content Management System. La valeur par défaut de ce champ est **443**, qui est le port de communication de Content Management System.
SSL	Autorise l'utilisateur à communiquer via une connexion SSL.
Username	Le nom d'utilisateur lié au compte Live et fourni par le Support Clients RSA.

Fonctionnalité	Description
Mot de passe	Le mot de passe lié au compte Live et fourni par le Support Clients RSA.
Tester la connexion	Teste si la connexion est réussie ou non.
Appliquer	Enregistre et applique la configuration.

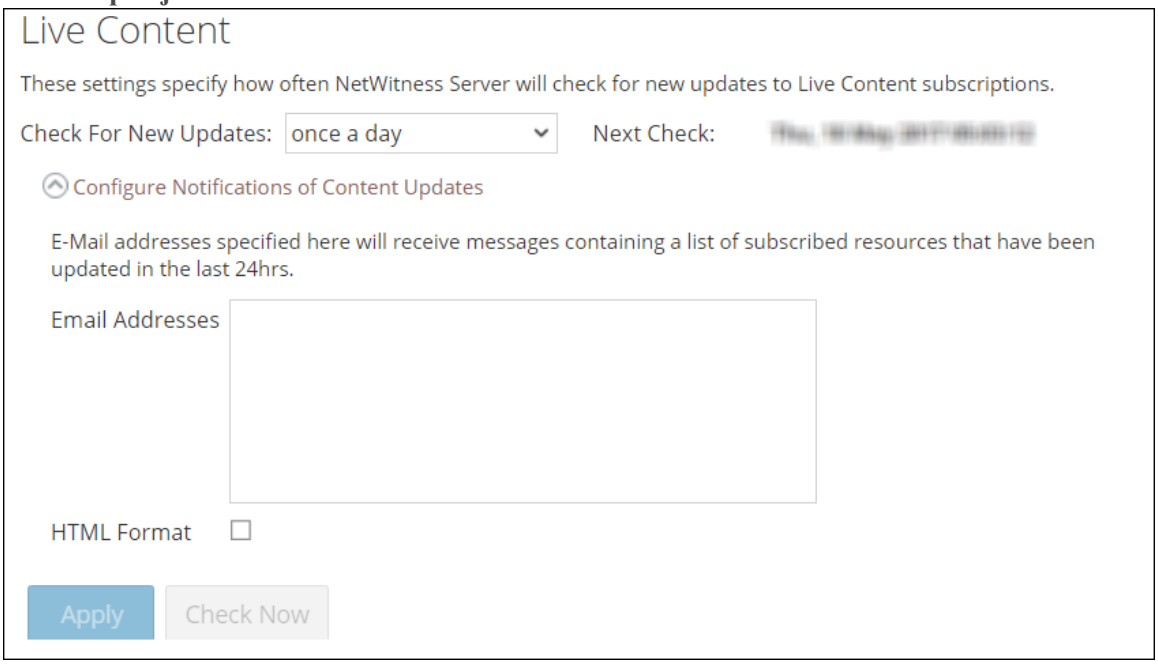
La section Compte Live comporte une option pour télécharger et partager les données historiques de Live Feedback en cliquant sur les logs d'activité Live Feedback.

Pour plus d'informations sur la façon de télécharger les données d'un historique, reportez-vous à la section Télécharger des données vers RSA pour Live Feedback

Section Contenu Live

Vous pouvez configurer l'intervalle de synchronisation du Contenu Live et la notification de fréquence à laquelle NetWitness Suite recherche les nouvelles mises à jour du Contenu Live :

Utilisez le champ **Rechercher de nouvelles mises à jour** pour modifier l'intervalle. Sélectionnez un intervalle dans la liste déroulante. La valeur par défaut pour ce paramètre est **une fois par jour**.



Le tableau suivant décrit les fonctions du Contenu Live.

Fonctionnalité	Description
Rechercher de nouvelles mises à jour	Ce paramètre indique à quelle fréquence NetWitness Suite doit rechercher de nouvelles mises à jour pour les abonnements Live et synchroniser les ressources et les balises souscrites : • une fois par jour • deux fois par jour • quatre fois par jour • toutes les heures • toutes les deux heures • toutes les demi-heures La valeur par défaut pour ce paramètre est Une fois par jour.
Next Check	Affiche l'heure et la date de la prochaine synchronisation Live planifiée, en fonction de l'intervalle configuré pour la vérification.
Adresses e-mail	Les adresses e-mail spécifiées ici recevront des messages contenant la liste des ressources souscrites ayant été mises à jour au cours des dernières 24 heures.
Format HTML	Indique le format des e-mails. • Activé = HTML • Désactivé = texte
Vérifier maintenant	Au lieu d'attendre le prochain cycle de ressources planifié, cette option contraint Live à démarrer la synchronisation immédiate des ressources souscrites dans cette instance de NetWitness Suite. **Attention :** Utilisez cette fonction avec prudence car la synchronisation peut entraîner une recharge du parser si un Lua Parser ou un Flex Parser est déployé dans le cycle de mise à jour. Cela est acceptable une ou deux fois par jour, mais trop de recharges du parser dos à dos peut provoquer la perte de paquets au niveau du décodeur. S'il s'agit de la configuration initiale et que vous n'avez pas encore configuré les abonnements de ressources Live, n'effectuez pas la synchronisation maintenant. Attendez de configurer les abonnements.

Fonctionnalité	Description
Appliquer	Applique le changement de configuration au comportement de synchronisation des abonnements. Les modifications prennent effet immédiatement. Le champ **La nouvelle synchronisation Live est planifiée pour** est mis à jour si l'heure a changé.

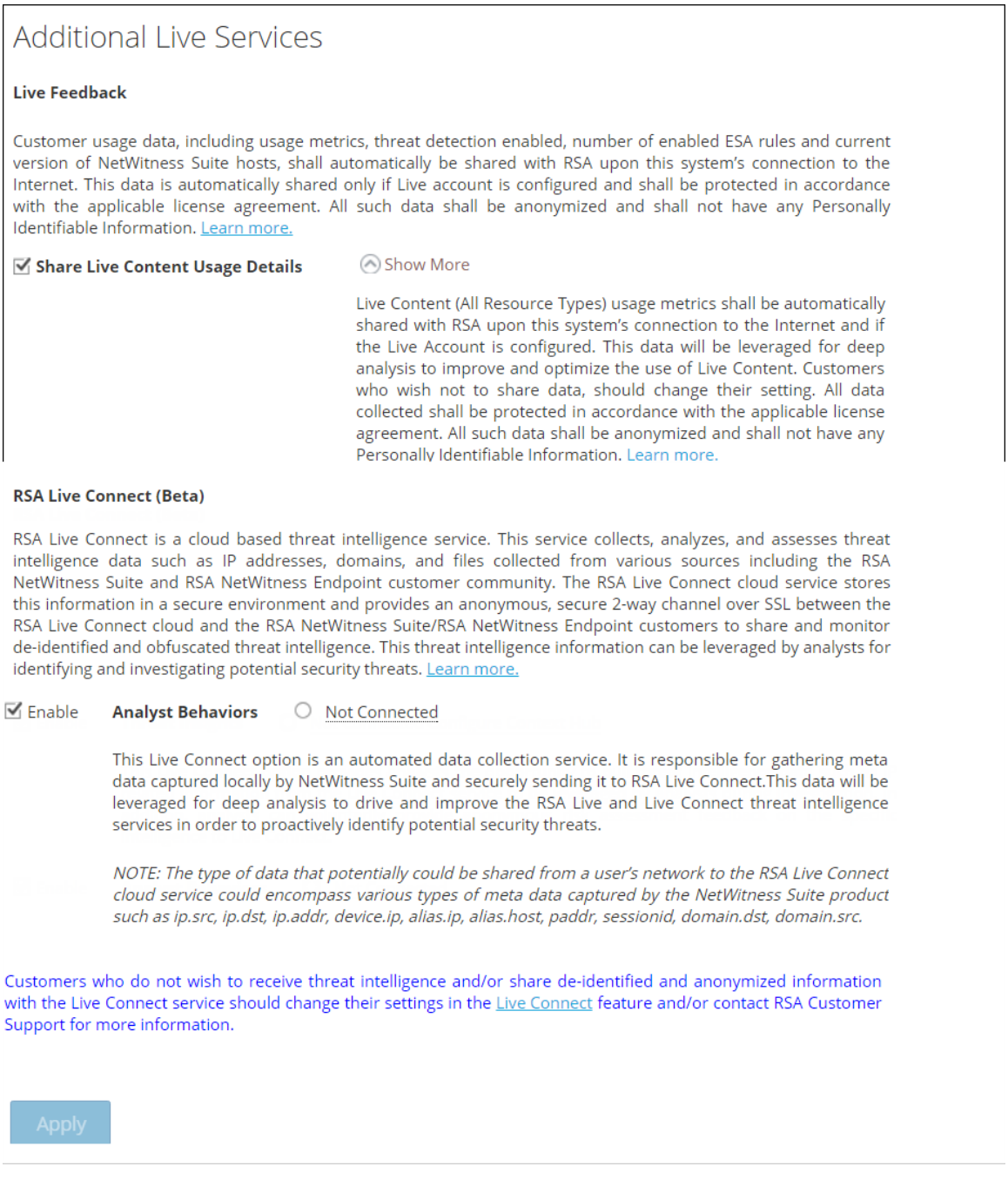
Forcer la synchronisation immédiate

Pour forcer la synchronisation immédiate, cliquez sur **Vérifier maintenant**. NetWitness Suite recherche les mises à jour dans les ressources souscrites.

Au lieu d'attendre le prochain cycle de ressources planifié, cette option contraint Live à démarrer la synchronisation immédiate des ressources souscrites dans cette instance de NetWitness Suite. Vous pouvez utiliser cette option pour voir l'impact immédiat d'une modification de configuration. Par exemple, si un nouveau service a été ajouté ou si de nouvelles ressources ont été basculées vers le déploiement automatique. La synchronisation planifiée pourrait avoir lieu plusieurs heures plus tard si Services Live est configuré pour se synchroniser quelques fois par jour.

Attention : La synchronisation peut entraîner une recharge du parser si un Flex Parser est déployé dans le cycle de mise à jour. Cela est acceptable une ou deux fois par jour, mais trop de recharges du parser dos à dos peut provoquer la perte de paquets au niveau du décodeur. S'il s'agit de la configuration initiale et que vous n'avez pas encore configuré les abonnements de ressources Live, n'effectuez pas la synchronisation maintenant. Attendez de configurer les abonnements.

Services Live supplémentaires



Remarque : Cliquez sur En savoir plus sur les données que RSA collecte. Pour plus d'informations, reportez-vous à la section Présentation de Live Feedback

Le tableau suivant décrit les fonctions de Services Live supplémentaires.

Fonctionnalité	Description

Live Feedback	Affiche les types de données que RSA collecte :
	• Nom du produit
	• Version du produit
	• Instance du produit
	• Clé d'activation
	• Informations détaillées sur chaque composant, notamment :
	  • ID
	  • Name
	  • Version
	  • ID de l'instance
	• Metrics pour chaque composant

Partager les détails d'utilisation du contenu Live)	Permet à NetWitness Suite d'envoyer des données techniques anonymes sur les metrics d'utilisation du contenu à RSA. Cette option est activée par défaut.
RSA Live Connect	Fournit plus d'informations sur le service Live Connect et la configuration des services Live.
Activer (Threat Insights)	Active la fonctionnalité Threat Insights où Live Connect est ajouté en tant que source de données pour le service Context Hub et que l'analyste peut extraire des données relatives aux renseignements sur les menaces au cours de la procédure d'enquête. Assurez-vous que ce service Context Hub est déjà configuré avant d'activer cette fonctionnalité. Cette option est activée par défaut (cochée)
Activer (Analyst Behaviors)	Permet à NetWitness Suite d'envoyer des données anonymes, techniques relatives à votre environnement à RSA. Cette option est activée par défaut (cochée)

Fonctionnalité	Description
Appliquer	Applique les modifications configurées. Les modifications prennent effet immédiatement. **Remarque :** Cette option est applicable uniquement pour les fonctionnalités Threat Insights et Analyst Behaviors.

À propos de la participation à Live Feedback

Lorsque vous participez à Live Feedback, les informations pertinentes sont collectées en vue de procéder à des améliorations. Pour plus d'informations sur Live Feedback, reportez-vous à la rubrique Présentation de Live Feedback.

Lorsque vous installez NetWitness Suite, l'application vous invite à participer à Live Feedback. Pour plus d'informations, consultez Configurer les paramètres des services Live.

Si nécessaire, vous pouvez télécharger manuellement les données d'utilisation historiques et les partager avec RSA. Pour plus d'informations sur la façon de télécharger les données d'utilisation historiques et les partager avec RSA, reportez-vous à la rubrique Télécharger des données vers RSA pour Live Feedback.

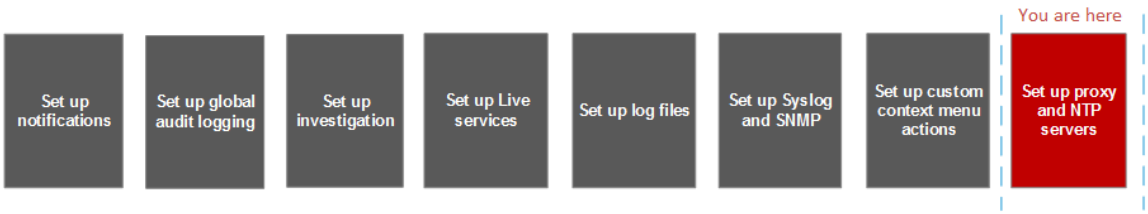
Panneau Paramètres NTP

Le panneau Paramètre NTP est un protocole conçu pour synchroniser les horloges des ordinateurs hôtes sur un réseau. Pour plus d'informations sur le protocole NTP, consultez la page d'accueil du site http://www.ntp.org/.

Remarque : Les hôtes NetWitness Suite Core doivent pouvoir communiquer avec l'hôte SA associé au port UDP 123 pour la synchronisation horaire NTP.

Utilisez la vue **Administration** > **Système** > **Paramètres NTP** pour configurer un ou plusieurs serveurs NTP. Après avoir configuré un serveur NTP, NetWitness Suite utilise le protocole NTP pour synchroniser les horloges des machines hôtes. Configurez plusieurs serveurs NTP à des fins de basculement sur incident.

Workflow



Que devez-vous faire ?

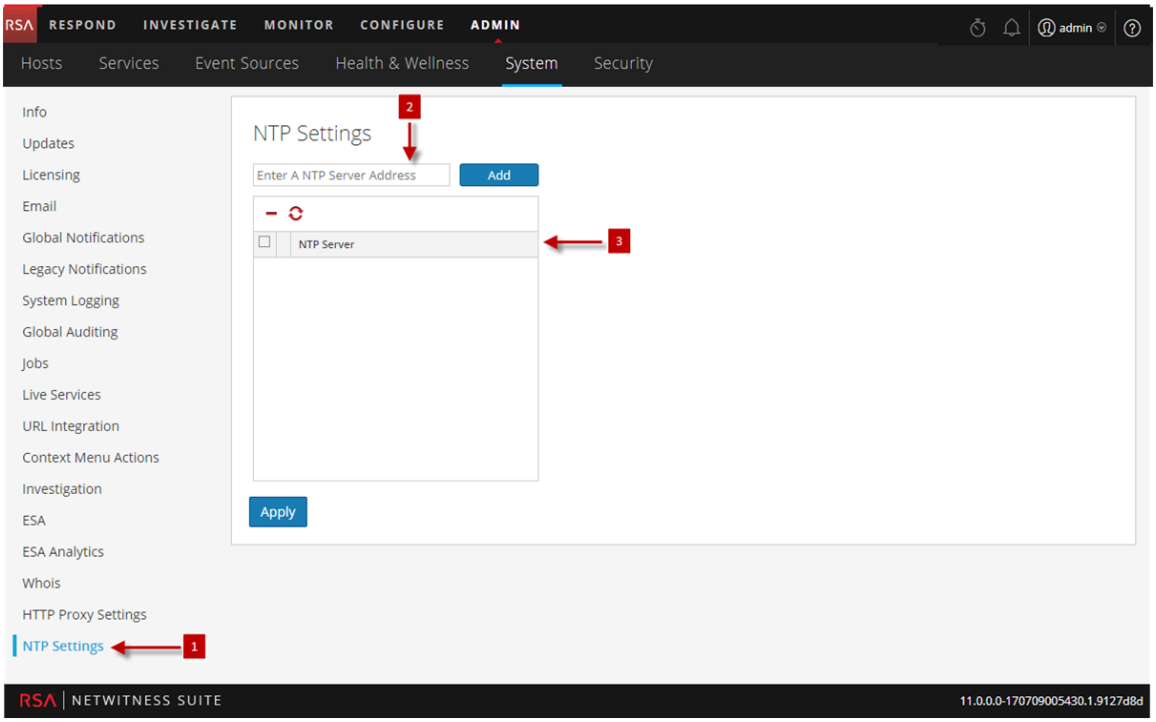
Rôle	Je souhaite...	Me montrer comment
Administrateur	Ajouter ou modifier un serveur NTP	Configurer les serveurs NTP

Rubriques connexes

- Configurer les serveurs NTP
- Dépanner la configuration du serveur NTP

Aperçu rapide

L'exemple suivant illustre un panneau de configuration NTP. Le panneau définit le mode d'ajout d'un serveur NTP au panneau Configuration NTP.



1 Affiche le panneau Configuration NTP

2 Permet de saisir l'adresse IP ou le nom d'hôte du serveur NTP.

3 Permet de cliquer sur un nom d'hôte existant

Barre d'outils et fonctions

Le tableau suivant décrit les paramètres du panneau Paramètres NTP.

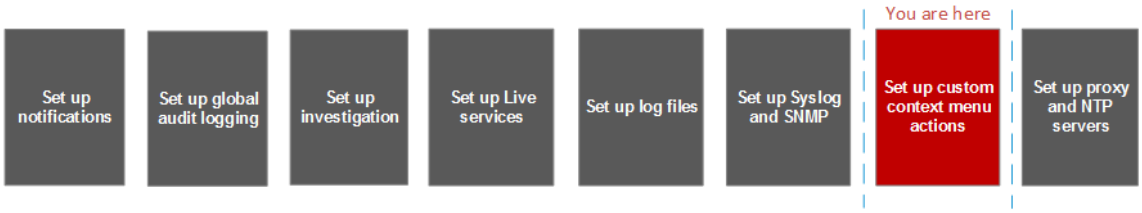
Paramètre	Description
	Permet de saisir l'adresse IP ou le nom d'hôte du serveur NTP.
Ajouter	Ajoute le serveur NTP à NetWitness Suite.
	Supprime le serveur NTP sélectionné.
	Synchronise le serveur NTP sélectionné.
	Sélectionne le serveur NTP que vous souhaitez supprimer ou synchroniser.

Paramètre	Description
Serveur NTP	Adresse IP ou nom d'hôte du serveur NTP. Si vous cliquez sur un nom d'hôte existant, NetWitness Suite rend le nom d'hôte modifiable et affiche les boutons de commande suivants : • **Mettre à jour** - Applique vos modifications. • **Annuler** - Annule vos modifications.
Appliquer	Applique les paramètres du serveur NTP et synchronise les horloges des machines hôtes sur la base du protocole NTP.

Panneau Actions des menus contextuels

Dans le panneau Actions des menus contextuels, les administrateurs peuvent afficher des actions de menu contextuel intégrées, et ajouter, modifier ou supprimer des actions de menu contextuel personnalisées qui apparaissent sous forme d'options dans un menu contextuel.

Workflow



Que voulez-vous faire ?

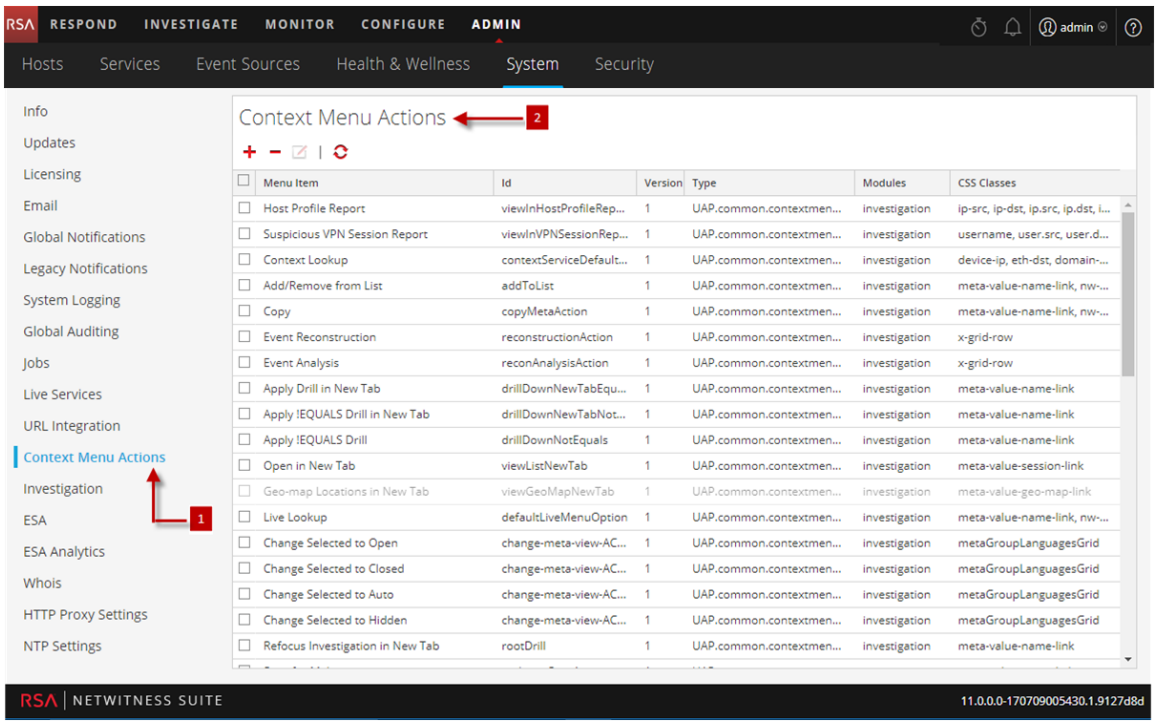
Rôle	Je souhaite...	Me montrer comment
Administrateur	Panneau Actions des menus contextuels personnalisés	Actions du menu Ajouter un contexte personnalisé.

Rubriques connexes

- Actions du menu Ajouter un contexte personnalisé

Aperçu rapide

La figure suivante est un exemple du panneau Actions des menus contextuels.



1	Affiche le panneau Actions des menus contextuels
2	La barre d'outils permet à l'utilisateur d'ajouter, de modifier, de supprimer des actions des menus contextuels

Barre d'outils et fonctions

Le panneau Actions des menus contextuels contient une grille et une barre d'outils. Le tableau suivant décrit la barre d'outils et les fonctions des grilles.

Fonctions	Description
+	Affiche la boîte de dialogue Configuration des menus contextuels qui vous permet de créer une action contextuelle.
↻	Actualise la liste.
−	Supprime les actions contextuelles sélectionnées. NetWitness Suite ne demande pas confirmation que vous souhaitez supprimer l'action. Les actions sélectionnées sont immédiatement supprimées sans aucune possibilité d'annulation.

Fonctions	Description
	Affiche la boîte de dialogue Modifier l'action contextuelle qui vous permet de modifier une action contextuelle existante.
Élément du menu	L'élément de menu apparaît dans le menu contextuel. Lors de la création d'une action de menu contextuel, le paramètre est `displayName`. Voici un échantillon de ligne de code : `"displayName": "User Agent String Lookup”`
ID	ID unique pour l'action contextuelle. Lors de la création d'une action de menu contextuel, le paramètre est `id`. Voici un échantillon de ligne de code : `"id": "UserAgentStringAction"`
Version	Numéro de version de l'action contextuelle. Lors de la création d'une action de menu contextuel, le paramètre est `version`. Voici un échantillon de ligne de code : `"version": "1"`
Type	Type d'action contextuelle. Lorsque vous créez une action de menu contextuel, le paramètre est `type`.. Tous les types d'action de contexte NetWitness Suite commencent par cette chaîne : `UAP.common.contextmenu.actions`. La dernière partie de la chaîne identifie le menu au sein de NetWitness Suite, par exemple, `URLContextAction` ou `LivePostContextAction`. Voici un échantillon de ligne de code : `"type": "UAP.common.contextmenu.actions.URLContextAction"`

Fonctions	Description

Modules	Noms des modules dans lesquels l'action contextuelle est disponible. Pour le moment, toutes les actions intégrées des menus contextuels s'appliquent au module Investigation.
	Lors de la création d'une action de menu contextuel, le paramètre est `modules`.
	Voici un échantillon de ligne de code :
	`"modules": [`
	`"investigation"`
	`],`

Classes de modules	Les classes CSS qui identifient les noms des vues des modules dans lesquels l'action contextuelle est disponible. Pour le moment, toutes les actions intégrées au menu contextuel concernent le module Investigation et les classes de module des clés non-méta sont décrites ci-dessous en détails.
	Voici un échantillon de quelques ligne de code :
	`"moduleClasses": [`
	`"UAP.investigation.navigate.view.NavigationPanel”,`
	`<-- Enabled in Navigate pane-->`
	`“UAP.investigation.events.view.EventGrid”`
	`],`

Classes CSS	Classes CSS auxquelles l'action de menu contextuel s'applique. Les classes CSS définissent l'endroit où le menu contextuel apparaît dans Investigation lorsque vous cliquez avec le bouton droit. Lors de la création d'une action de menu contextuel, le paramètre est `cssClasses`.
	Voici un échantillon de ligne de code :
	`"cssClasses": [`
	`“client”`
	`]`
	La plupart des classes CSS que vous pouvez ajouter sont des clés méta. Vous pouvez également ajouter certaines classes CSS de clés non-méta. Vous trouverez ci-dessous des détails supplémentaires et des exemples.

Classes CSS et exemples

Les classes CSS peuvent être des clés méta et des clés non-méta.

Classes CSS de clés méta

Les clés méta sont un type de classe CSS que vous pouvez ajouter. Pour les clés méta qui présentent une période, remplacez la période par un tiret lors de la définition d'une classe CSS. Par exemple, la clé méta `alias.host` devient la classe CSS `alias-host`. La clé méta `ip.src` devient la classe CSS `ip-src`.

Classes CSS non-méta

Les classes CSS de clés non-méta sont également disponibles. Les classes du tableau suivant définissent les actions et les parties de l'interface utilisateur où l'action est disponible.

Classe CSS	Type	Description
`meta-value-session-link`	Action	Ouvrir dans le décompte des sessions méta
`meta-value-name-link`	Action	Ouvrir dans le nom de la valeur méta
`nw-event-value`	Action	Utiliser pour les actions de contexte pour la reconstruction dans la valeur méta
`UAP.investigation.navigate.view. NavigationPanel`	Interface utilisateur	S'applique à la vue Naviguer
`UAP.investigation.events.view. EventGrid`	Interface utilisateur	S'applique à la vue Événement
`UAP.investigation.reconstruction.view. content.ReconstructedEventDataGrid`	Interface utilisateur	S'applique à la vue Reconstruction d'événement

Exemple

Exemple commenté d'une action de menu contextuel permettant de valider l'agent utilisateur à partir de la clé méta de l'application client (client). Les commentaires sont supprimés automatiquement une fois l'action appliquée dans la vue Système d'administration. Le nouvel élément du menu s'affiche après le redémarrage du navigateur.

```
{
     "displayName": "User Agent String Lookup”, <!-- What name shows up
in NW UI -->
     "cssClasses": [
         “client”  <!-- What meta key to launch from -->
     ],
     "description": "",
     "type": "UAP.common.contextmenu.actions.URLContextAction",
     "version": "1",
     "modules": [
         "investigation"
     ],
     "local": "false",
     "groupName": "externalLookupGroup”, <!-- What group to show link
in. Remove line to show in main list -->
     "urlFormat": "http://www.useragentstring.com/?uas={0}&getText=all”, <!-- The
{0} gets replaced with whatever was right clicked on -->
     "disabled": "",
     "id": "UserAgentStringAction",
    "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel”, <-- Enabled
in Navigate pane-->
        “UAP.investigation.events.view.EventGrid” <-- Enabled in Event
View pane -->
     ],
     "openInNewTab": "true",
     "order": "15"
 }
```

Panneau Configuration des notifications existantes

Le panneau de configuration des notifications existantes permet de configurer le syslog et les paramètres de notification SNMP. Ces configurations permettent de contrôler les habilitations, Gestion de la source d'événements (ESM) d'ancienne génération, Warehouse Connector et Archiver.

Les procédures liées à ces paramètres sont décrites dans Configurer les paramètres Syslog et SNMP.

Workflow

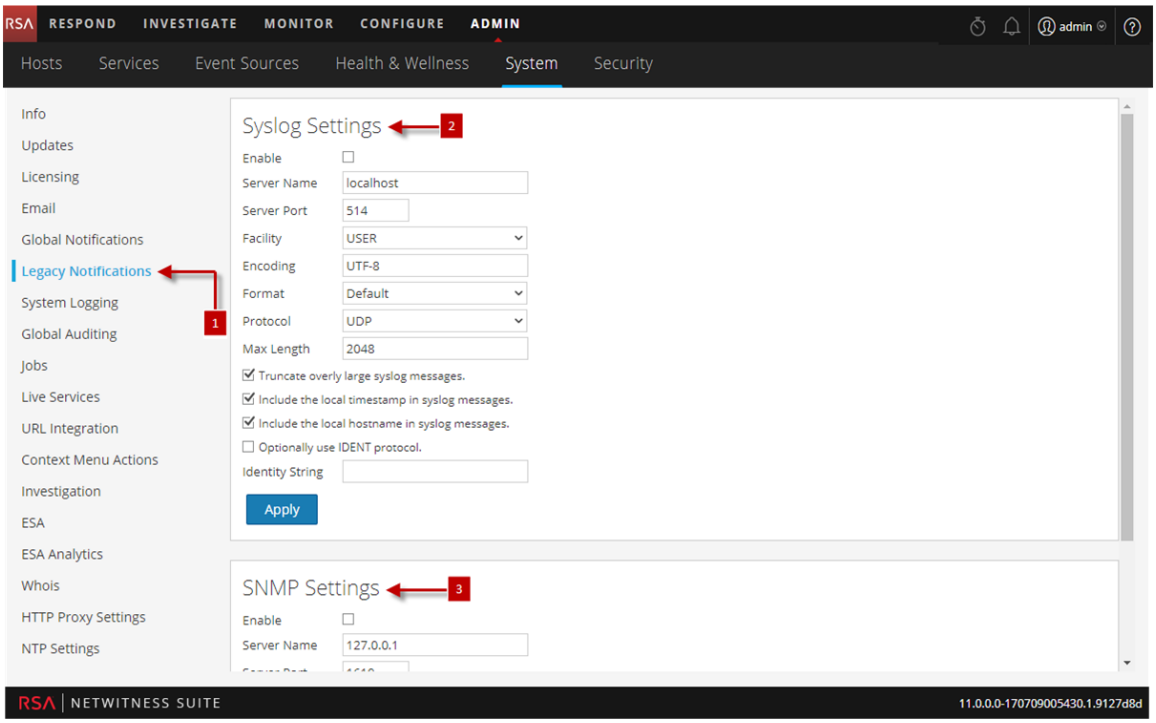
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer les paramètres syslog	Configurer les paramètres Syslog et SNMP
Administrateur	Configurer les paramètres SNMP	Configurer les paramètres Syslog et SNMP

Rubriques connexes

- Configurer les paramètres Syslog et SNMP

Aperçu rapide



1	Affiche le panneau Configuration des notifications existantes.
2	Permet à l'utilisateur de configurer les notifications Syslog pour le contrôle des habilitations, de la Gestion des sources d'événements (ESM) existantes, du service Warehouse Connector et du service Archiver.
3	Permet à l'utilisateur de configurer les notifications SNMP pour le contrôle des habilitations, de la Gestion des sources d'événements (ESM) existantes, du service Warehouse Connector et du service Archiver.

Barre d'outils et fonctions

Le panneau de configuration des notifications existantes se compose de deux sections : Paramètres Syslog et paramètres SNMP.

Paramètres Syslog

Le tableau suivant décrit les options disponibles pour la configuration des notifications syslog pour contrôler les Habilitations, Gestion de la source d'événements (ESM) d'ancienne génération, Warehouse Connector et Archiver.

Fonctionnalité	Description
Activer	Active les paramètres syslog configurés ici.
Nom du serveur	Indique l'hôte sur lequel le processus Syslog cible est en cours d'exécution.
Port de serveur	Indique le port sur lequel le processus Syslog cible est en cours d'écoute.
Site	Indique la fonctionnalité Syslog désignée pour utiliser tous les messages sortants. Les valeurs possibles sont KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL1 via LOCAL7.
Encodage	Indique l'encodage à utiliser pour le texte dans les messages syslog, par exemple UTF-8.
Format	Indique le format du message. Les valeurs possibles sont les suivantes : Défaut, PCI DSS ou SEC.
Protocole	Indique le protocole de communications utilisé lors de l'envoi de syslogs : UDP ou TCP. Par défaut, le protocole UDP est sélectionné.
Longueur maximale	Indique la longueur maximale en octets de tout message syslog. La valeur par défaut est **2048**. Les messages qui dépassent la longueur maximale sont tronqués lorsque la case **Tronquer les messages Syslog trop volumineux** est cochée.
Tronquer les messages Syslog trop volumineux	Lorsque cette case est cochée, tous les messages dépassant la longueur maximale sont tronqués.
Inclure l'horodatage local dans les messages Syslog	Lorsque cette case est cochée, NetWitness Suite comprend l'horodatage local dans des messages.
Inclure le nom d'hôte local dans les messages Syslog	Lorsque cette case est cochée, NetWitness Suite comprend le nom d'hôte local dans des messages syslog.

Fonctionnalité	Description
(Facultatif) Utiliser le protocole IDENT	Lorsque cette case est cochée, NetWitness Suite ajoute comme préfixe la chaîne d'identité aux alertes syslog sortantes.
Identifier la chaîne	Il s'agit d'une chaîne d'identité à ajouter comme préfixe à chaque alerte syslog. Si la chaîne est vierge, aucune chaîne d'identité n'est ajoutée comme préfixe aux alertes syslog sortantes. Vous pouvez l'utiliser pour identifier la source de l'alerte. Les utilisateurs le définissent généralement sur le nom du programme qui envoie le message syslog.
Appliquer	Applique les paramètres de configuration syslog.

Paramètres SNMP

Le tableau suivant décrit les options disponibles pour la configuration des notifications SNMP pour contrôler les Habilitations, Gestion de la source d'événements (ESM) d'ancienne génération, Warehouse Connector et Archiver.

Fonctionnalité	Description
Activer	Active les paramètres SNMP configurés ici.
Nom du serveur	Indique l'hôte de trap SNMP.
Port de serveur	Indique le port d'écoute sur l'hôte de trap SNMP
Version SNMP	Spécifie la version SNMP, **v1** ou **v2c**.
ID d'objet de trap	Indique l'ID d'objet pour le trap SNMP sur l'hôte trap qui reçoit l'événement d'audit. La valeur par défaut est **0.0.0.0.0.1**.
Communauté	Indique la chaîne de communauté utilisée pour l'authentification sur l'hôte de trap SNMP ; la valeur par défaut est **public**.
Activer	Active les notifications SNMP telles que configurées ici.
Appliquer	Applique les paramètres de configuration SNMP.