RSA NETWITNESS® SUITE

Guide de maintenance du 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

NetWitness Suite Maintenance du système

Ce guide englobe les tâches que les administrateurs effectuent après la configuration initiale du réseau pour permettre à NetWitness Suite de gérer les hôtes et les services du réseau, d'assurer le maintien en conditions opérationnelles et la surveillance du réseau, de gérer les tâches et d'optimiser les performances.

Le schéma suivant indique les différentes tâches de maintenance du système disponibles :

Les rubriques suivantes décrivent ces tâches :

- Bonnes pratiques
- Surveiller de l'intégrité dans NetWitness Suite
- Affichage des logs système et des logs de services
- Gestion des requêtes à l'aide de l'intégration d'URL
- Gestion des mises à jour de NetWitness Suite
- Prise en charge de FIPS
- Résoudre les problèmes de NetWitness Suite

Bonnes pratiques

Sauvegarde des ressources avec les stratégies fournies par RSA

Les stratégies de base RSA fournies avec NetWitness Suite ont pour but de vous aider à sauvegarder immédiatement les ressources de votre domaine NetWitness Suite (avant de configurer des règles propres à votre environnement et à votre stratégie de sécurité).

RSA vous recommande de configurer les notifications par e-mail aux propriétaires de ressource appropriés pour ces stratégies. Ils pourront ainsi être avertis lorsque les seuils de performance et de capacité sont atteints afin qu'ils puissent prendre des mesures immédiates.

RSA vous recommande également d'évaluer les stratégies de base et de désactiver une stratégie ou de modifier ses attributions de service ou de groupe en fonction de vos exigences de surveillance spécifiques.

Sauvegarde des ressources avec les stratégies basées sur votre environnement

Les stratégies de base RSA sont génériques et peuvent ne pas fournir une couverture de surveillance suffisante pour votre environnement. RSA vous recommande de collecter les problèmes non identifiés par les stratégies de base RSA sur une période donnée et de configurer des règles pour les prévenir.

Création judicieuse de règles et de notifications

Si possible, RSA vous recommande de vérifier que chaque règle ou stratégie est nécessaire avant de la mettre en œuvre. RSA vous recommande également de vérifier régulièrement la validité des stratégies mises en œuvre. Les alarmes et les notifications par e-mail non valides peuvent avoir un impact négatif sur l'objectif des propriétaires de ressources.

Résolution des problèmes

RSA vous recommande de consulter la rubrique Résolution des problèmes liés à l'intégrité et Résoudre les problèmes de NetWitness Suite lorsque vous recevez des messages d'erreur dans l'interface utilisateur et des fichiers log des hôtes et services.

Surveiller de l’intégrité dans NetWitness Suite

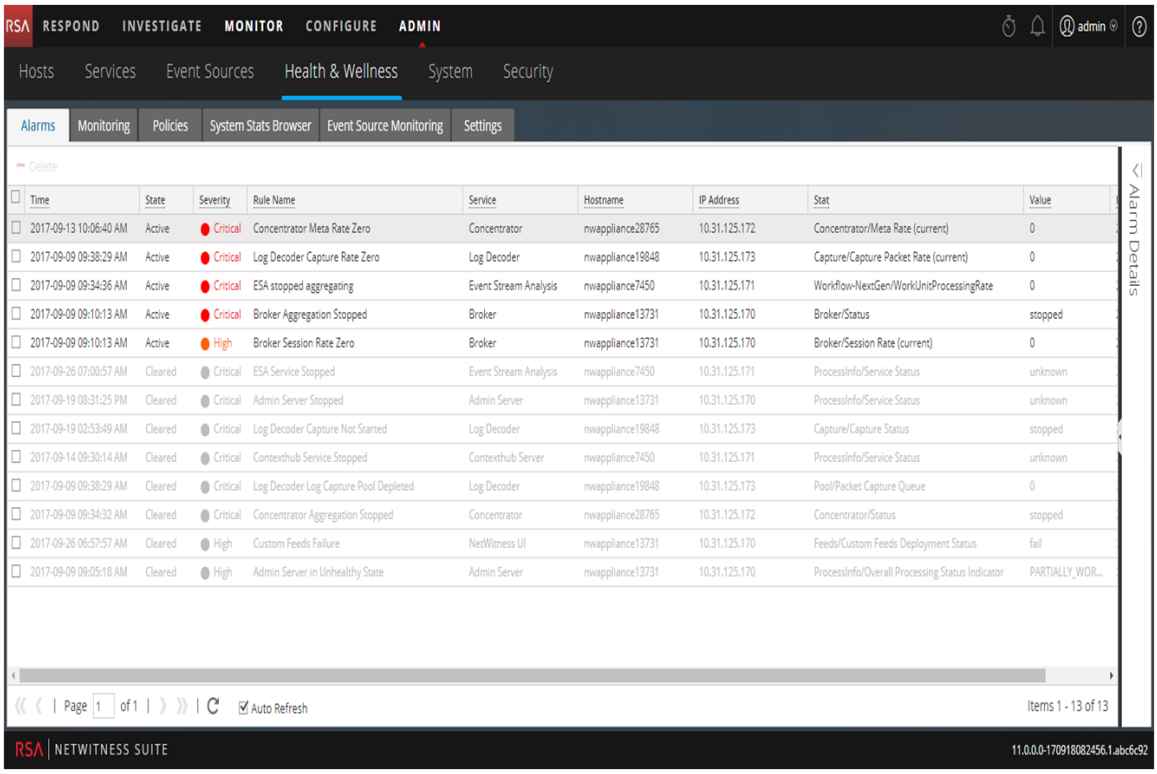
Le module Intégrité de NetWitness Suite permet de :

- Visualiser l'intégrité actuelle de tous les hôtes de tous les services exécutés sur les hôtes et divers aspects de l'état de santé des hôtes.
- Surveiller les hôtes et les services présents dans votre environnement réseau.
- Afficher les détails des différentes sources d'événements configurées avec NetWitness Suite.
- Afficher les statistiques système pour les hôtes sélectionnés en filtrant les vues si nécessaire.

De plus, vous pouvez configurer la surveillance d'Archiver et la surveillance de Warehouse Connector, utiliser les procédures de surveillance des statistiques des hôtes et tirer le meilleur parti des logs système pour surveiller NetWitness Suite.

Remarque : Par défaut, tous les utilisateurs sont autorisés à afficher l’intégralité de l’interface Intégrité. Les rôles Administrateur et Opérateur sont les seuls rôles pouvant gérer la vue Stratégies. Reportez-vous à la rubrique **Autorisations du rôle** dans le *Guide de la sécurité du système et de la gestion des utilisateurs* pour obtenir la liste complète des autorisations par défaut pour l’interface NetWitness Suite.

La figure illustre le module Intégrité de l'interface utilisateur NetWitness Suite et diverses sections de ce module.



Gérer les règles

Les stratégies peuvent être définies par l'utilisateur ou fournies par RSA. Une stratégie définit :

- Les services et hôtes auxquels s'applique la stratégie.
- Les règles spécifiant les seuils statistiques qui gouvernent les alarmes.
- Quand supprimer la stratégie.
- Qui informer lorsqu'une alarme se déclenche et quand envoyer les notifications.

Pour consulter des rubriques de référence connexes, référez-vous aux Règles prédéfinies NetWitness.

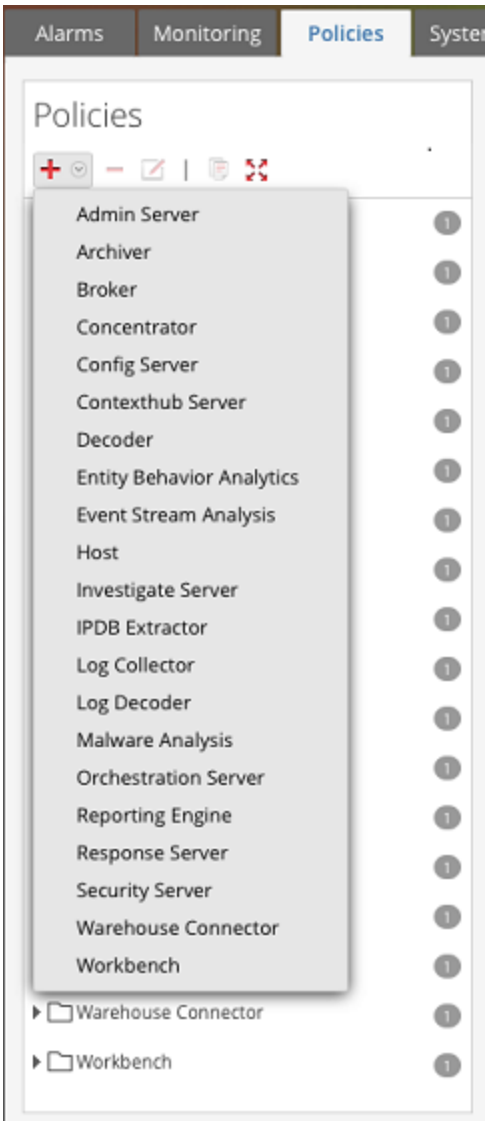
Remarque : Vous pouvez désormais configurer une stratégie pour informer de l'état d'expiration du certificat infrastructure à clé publique (PKI).

Ajouter une stratégie

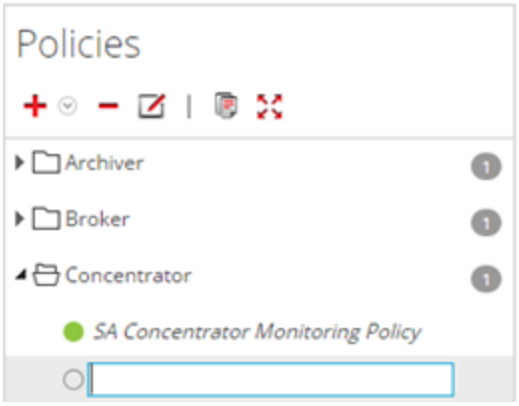
1. Accédez à **Administrateur** > **Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Cliquez sur  dans le panneau **Règles**.

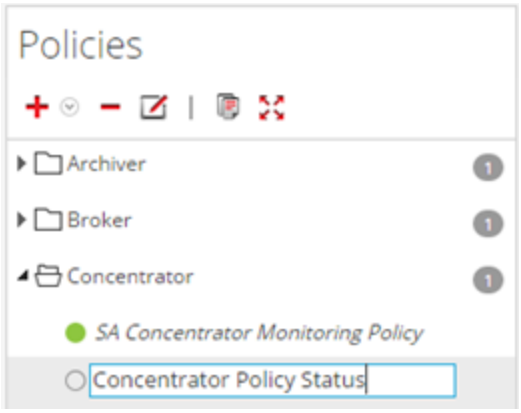
   La liste de vos hôtes et services s'affiche, pour laquelle vous pouvez créer des stratégies d'intégrité.



4. Sélectionnez un hôte ou un service (par exemple, **Concentrator**).
   Pour la stratégie d'infrastructure à clé publique, vous devez sélectionner un hôte (par exemple, Hôte).
   L'hôte ou le service s'affiche dans le panneau Règles avec le panneau Détails de la stratégie.



5. Saisissez un nom pour la stratégie (par exemple, **État de la stratégie Concentrator**) dans le panneau **Règles**.



Le nom (par exemple, **État de la stratégie Concentrator**) s'affiche maintenant en tant que nom de stratégie dans le panneau Détails de la stratégie.

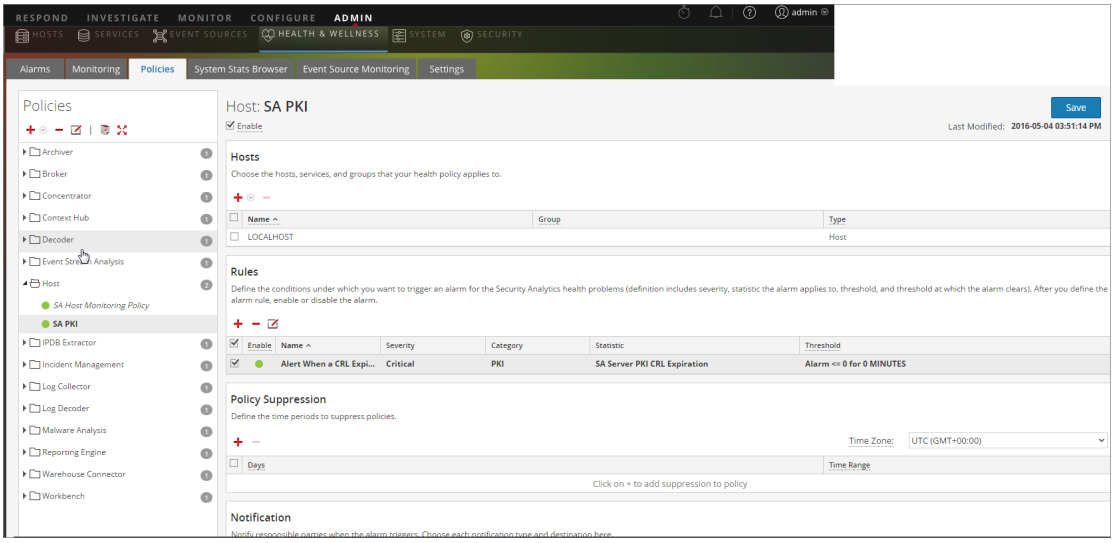
6. Créez une stratégie dans le panneau Détails de la stratégie :
   a. Cochez la case **Activer**.
   b. Ajoutez les services pertinents (dans cet exemple, tous les services Concentrator pertinents) que vous souhaitez surveiller pour les statistiques d'intégrité.
   Pour la stratégie d'infrastructure à clé publique, vous devez sélectionner LOCALHOST pour surveiller les statistiques d'intégrité.
   c. Ajoutez les conditions de règles pertinentes que vous souhaitez configurer pour la stratégie.
   d. Supprimez l'application de la stratégie pour la période que vous souhaitez.
   e. Ajoutez les notifications par e-mail que vous souhaitez pour la stratégie.
   f. Cliquez sur **Enregistrer** dans le panneau Détails de la stratégie.

La stratégie est ajoutée.

Ajouter un exemple de stratégie

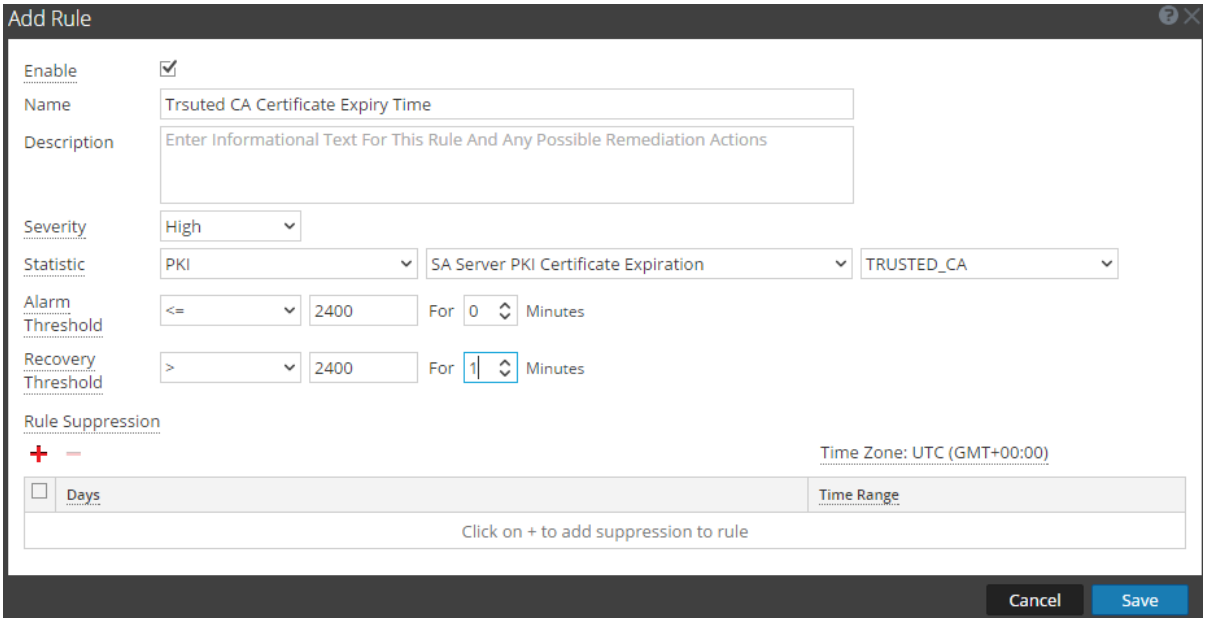
Vous trouverez ci-dessous un exemple général de configuration de la stratégie d'infrastructure à clé publique :

1. Ajouter une stratégie d'infrastructure à clé publique

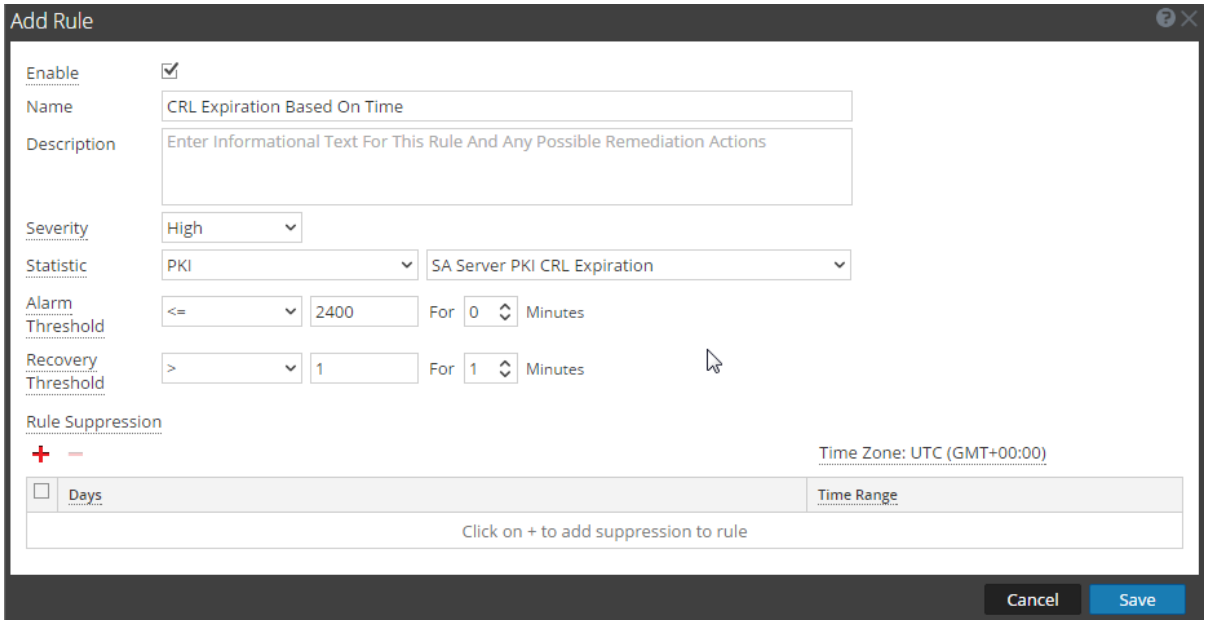


2. Ajouter une stratégie avec Statistiques :

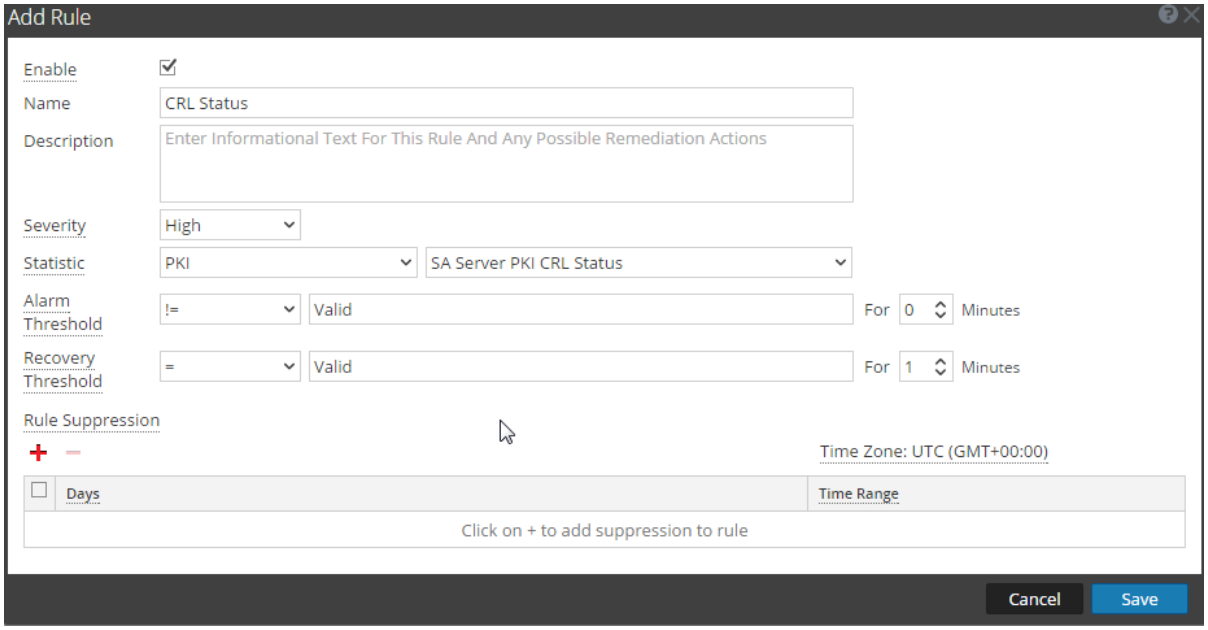
   - Pour l'expiration de l'autorité de certification



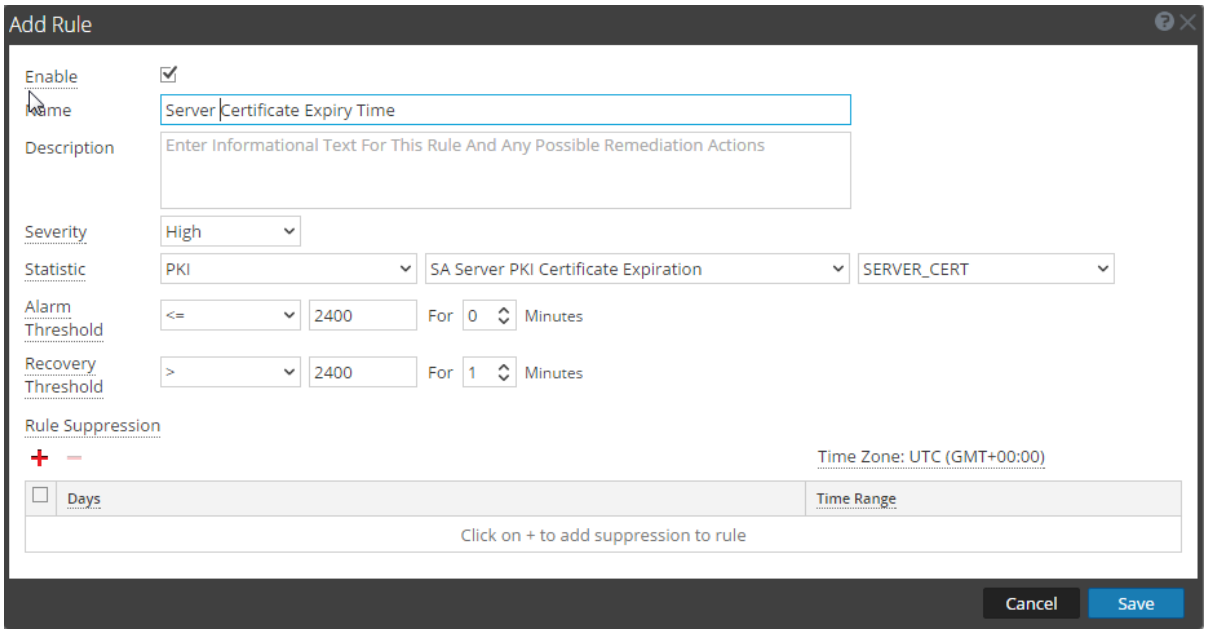
- Pour l'expiration de la liste de révocation des certificats



- Pour l'état de la liste de révocation des certificats



- Pour l'expiration du certificat de serveur



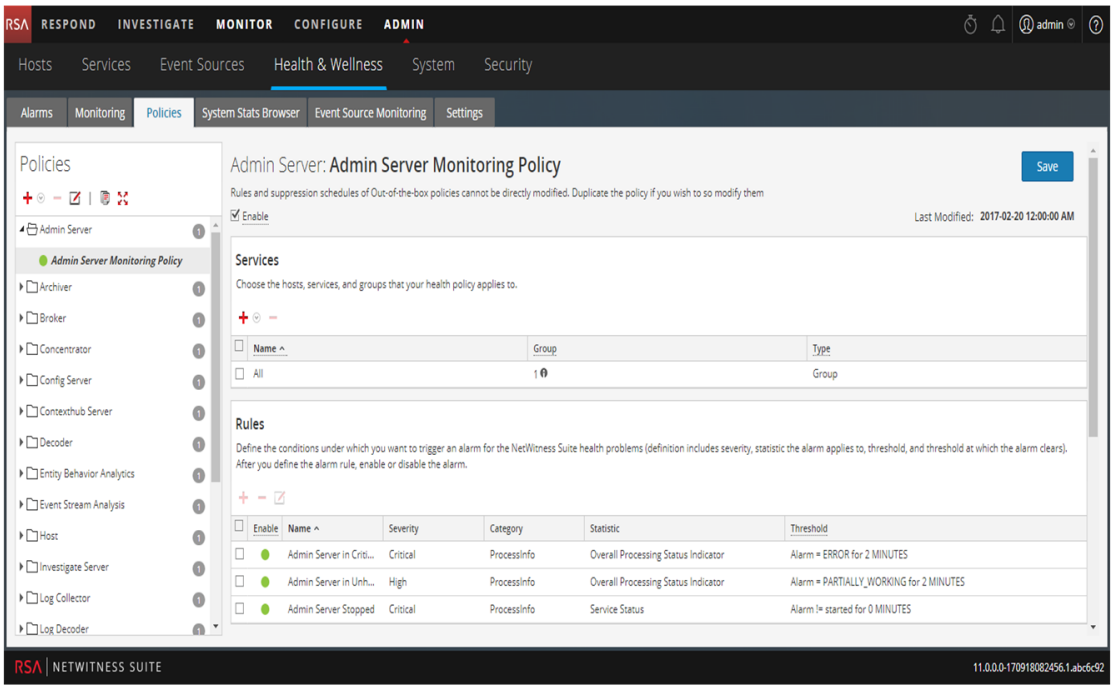
Modifier une stratégie

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie (par exemple, **État de la stratégie Concentrator**) sous un hôte ou un service.

   La vue Détails de la stratégie s'affiche.
4. Cliquez sur .

   Le nom de la stratégie (par exemple, **Stratégie de surveillance du serveur administrateur**) et le panneau de détails de la stratégie deviennent modifiables.



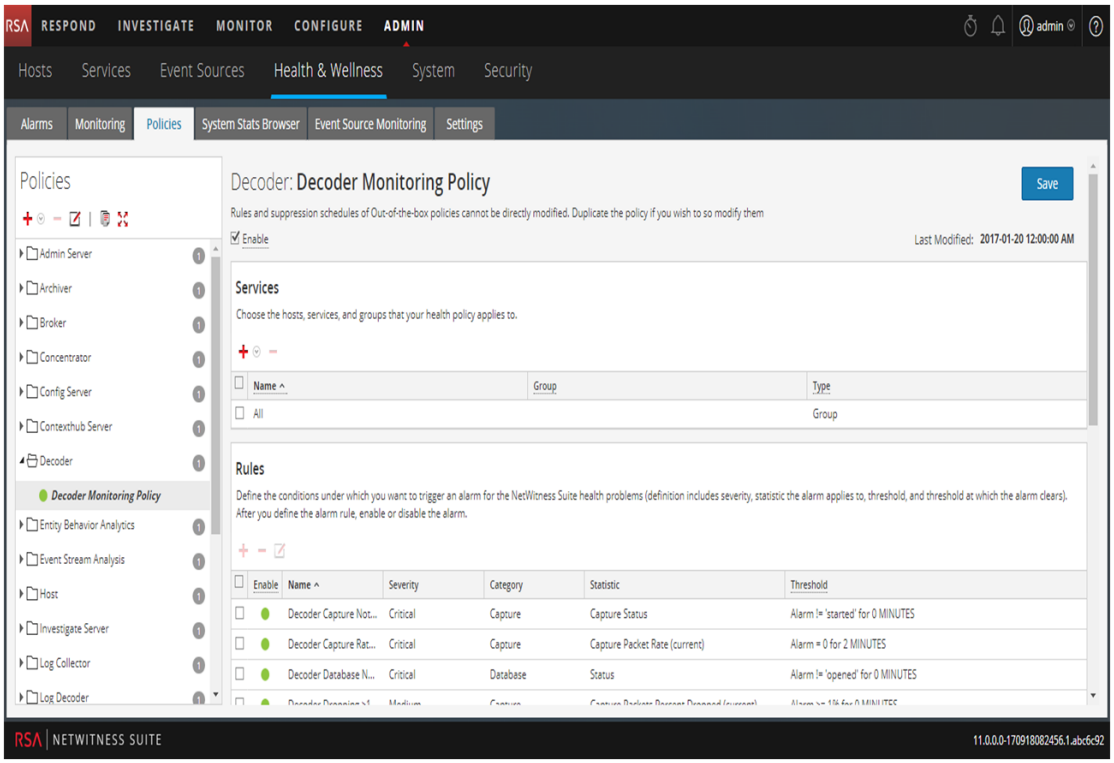
5. Procédez aux modifications requises et cliquez sur **Enregistrer** dans le panneau Détails de la stratégie. Vous pouvez :
   - Modifier le nom de la stratégie.
   - Activer ou désactiver la stratégie.
   - Ajouter ou supprimer des hôtes et des services dans la stratégie.
   - Ajouter, supprimer ou modifier des règles dans la stratégie.
   - Ajouter, modifier ou supprimer des suppressions dans la stratégie.
   - Ajouter, modifier ou supprimer des notifications dans la stratégie.

Remarque : La fonction **Enregistrer** s'applique aux règles de stratégies basées sur la sélection du mode activation ou désactivation. Elle réinitialise également les compteurs des conditions de règles pour les règles modifiées, ainsi que l'intégralité de la stratégie.

Dupliquer une stratégie

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.
3. Sélectionnez une stratégie (par exemple, **État de la stratégie Concentrator**) sous un hôte ou un service.
4. Cliquez sur . NetWitness Suite copie la stratégie et la répertorie en ajoutant **(1)** à son

nom d'origine.



5. Cliquez sur et renommez la stratégie. Par exemple, remplacez **Stratégie de surveillance Decoder(1)** par **État de la nouvelle stratégie Concentrator**.

> **Remarque :** La stratégie dupliquée est désactivée par défaut, et les attributions de l'hôte et du service ne sont pas dupliquées. Attribuez les hôtes et services pertinents à la stratégie dupliquée avant de l'utiliser pour surveiller l'intégrité de l'infrastructure NetWitness Suite.

Attribuer des services ou des groupes

Pour attribuer des hôtes ou services à une stratégie :

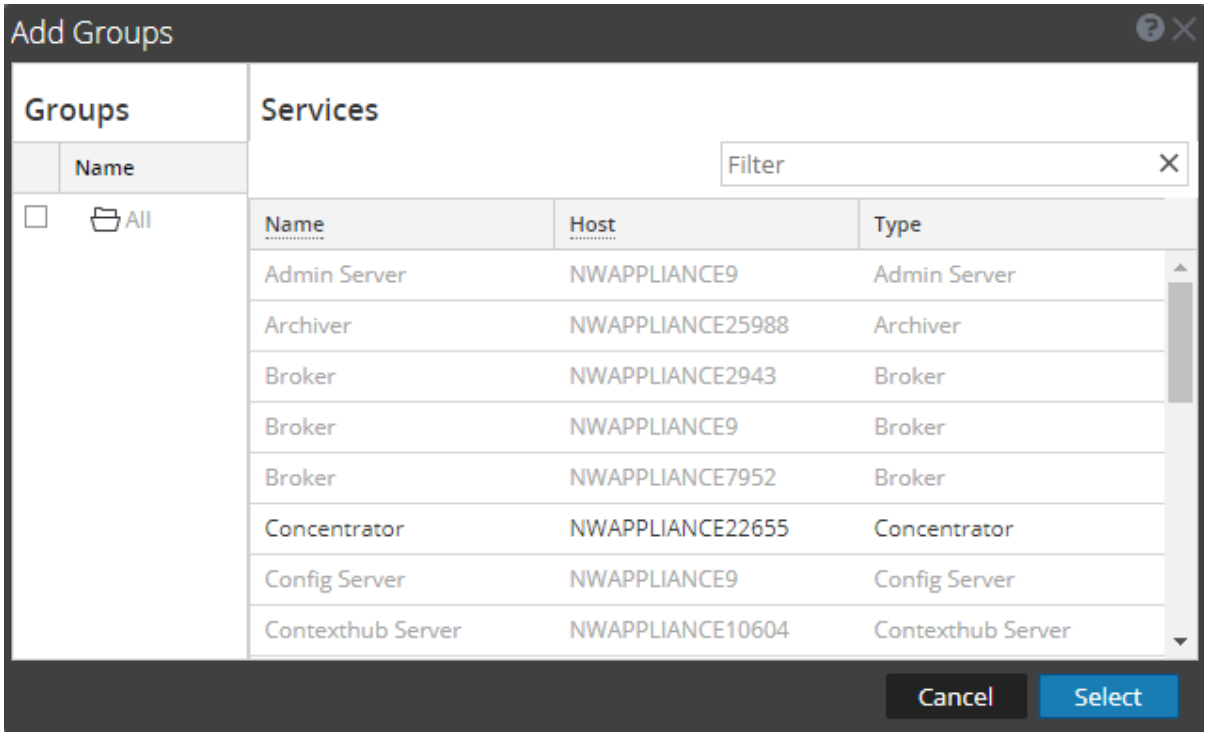
1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie (par exemple, **Première stratégie**) sous un hôte ou un service.

   La vue Détails de la stratégie s'affiche.
4. Cliquez sur dans la barre d'outils de la liste des services et des groupes.
5. Procédez de l'une des manières suivantes :

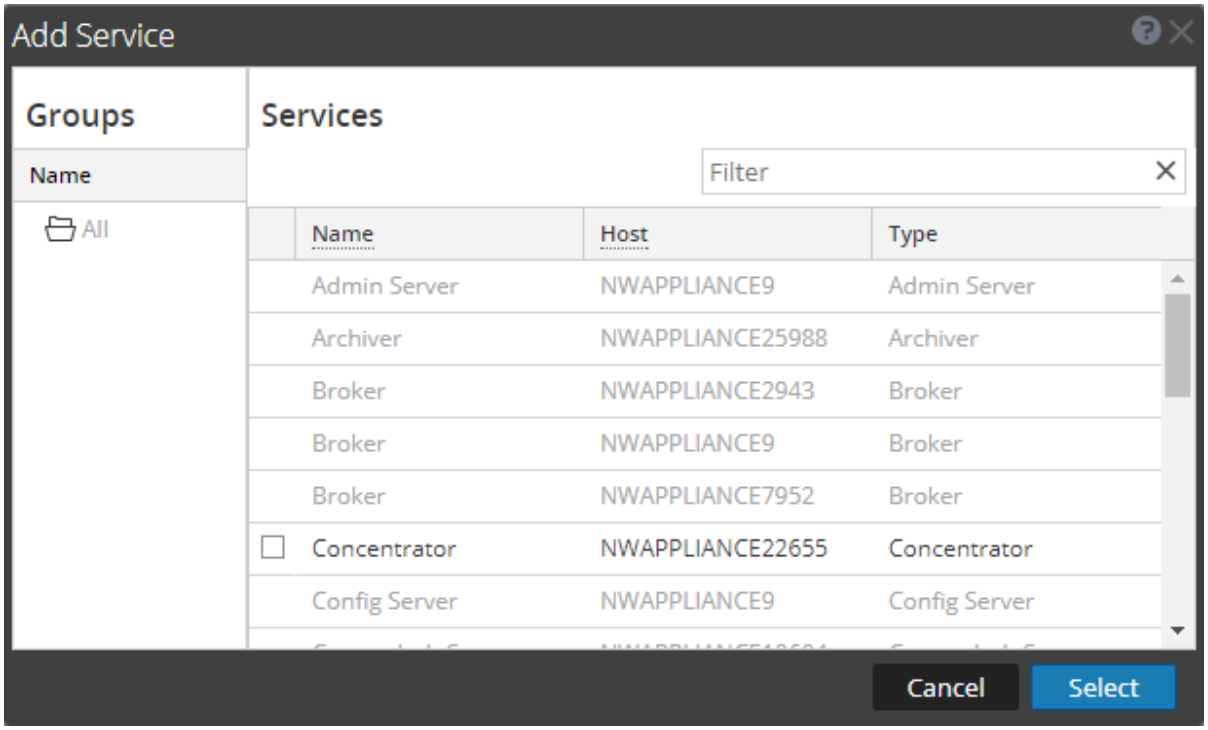
- Pour les hôtes, sélectionnez **Groupes** ou **Hôtes** dans le menu de sélection.
- Pour les services, sélectionnez **Groupes** ou **Services** dans le menu de sélection.

6. Selon que vous allouez des services ou des groupes, effectuez l'une des actions suivantes :
   - **Groups**, la boîte de dialogue **Groupes** s'affiche pour vous permettre de sélectionner des groupes d'hôtes ou de services prédéfinis.



   - **Services**, la boîte de dialogue **Services** s'affiche pour vous permettre de sélectionner

chaque service.



7. Cochez la case en regard des groupes ou services que vous souhaitez attribuer à la stratégie, cliquez sur **Sélectionner** dans la boîte de dialogue, puis cliquez sur **Enregistrer** dans le panneau Détails de la stratégie.

Remarque : Les services sont filtrés pour la sélection en fonction du type de politiques. Par exemple, vous ne pouvez sélectionner que des services Concentrator pour une stratégie de type Concentrator.

Supprimer des services ou des groupes

Pour supprimer un hôte ou un service à partir d'une stratégie :

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie sous un service.

   La vue Détails de la stratégie s'affiche.
4. Sélectionnez un hôte ou un service.

5. Cliquez sur − .

   L'hôte ou le service est supprimé de la stratégie.

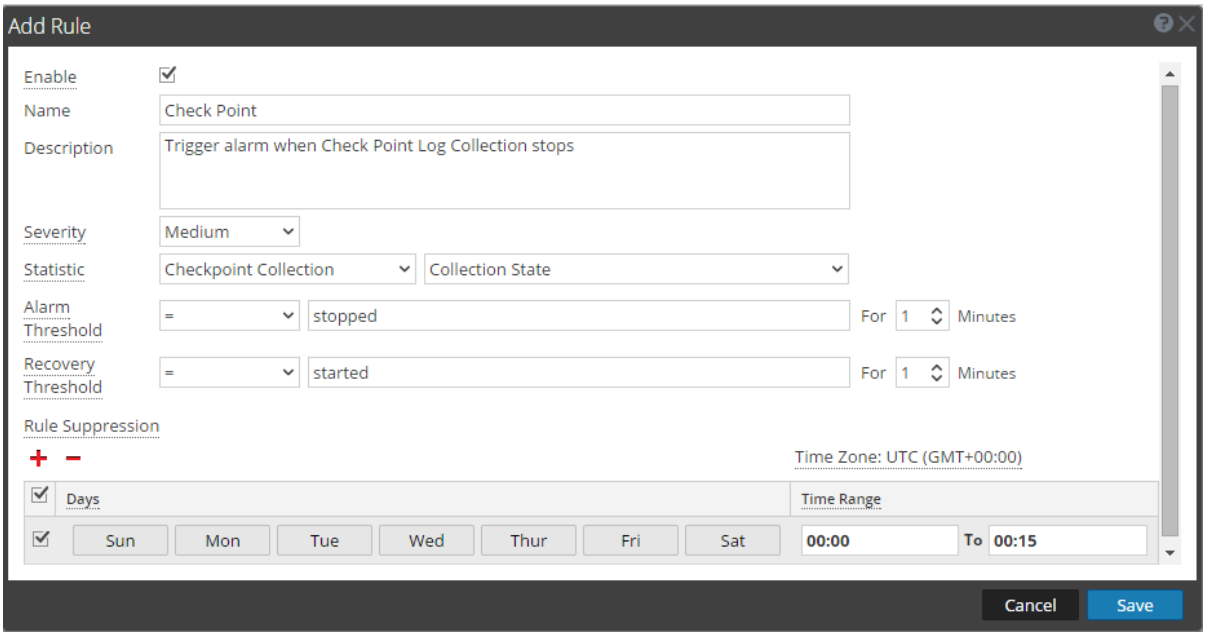
Ajouter ou modifier une règle

Pour ajouter une règle à une stratégie :

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie (par exemple, **Checkpoint**) sous un hôte ou un service.

   La vue Détails de la stratégie s'affiche.
4. Selon que vous modifiez une règle existante ou que vous ajoutez une nouvelle règle, procédez comme suit :
   - Pour ajouter : Cliquez sur + dans la barre d'outils de la liste Règles.
   - Pour modifier : Sélectionnez une règle dans la liste Règles et cliquez sur .
5. Renseignez les champs de la boîte de dialogue pour définir ou mettre à jour la règle.
6. Ajoutez le champ **Description** comme illustré dans l'exemple suivant.



7. Cliquez sur **OK**.

   La règle est ajoutée à la stratégie ou est mise à jour.

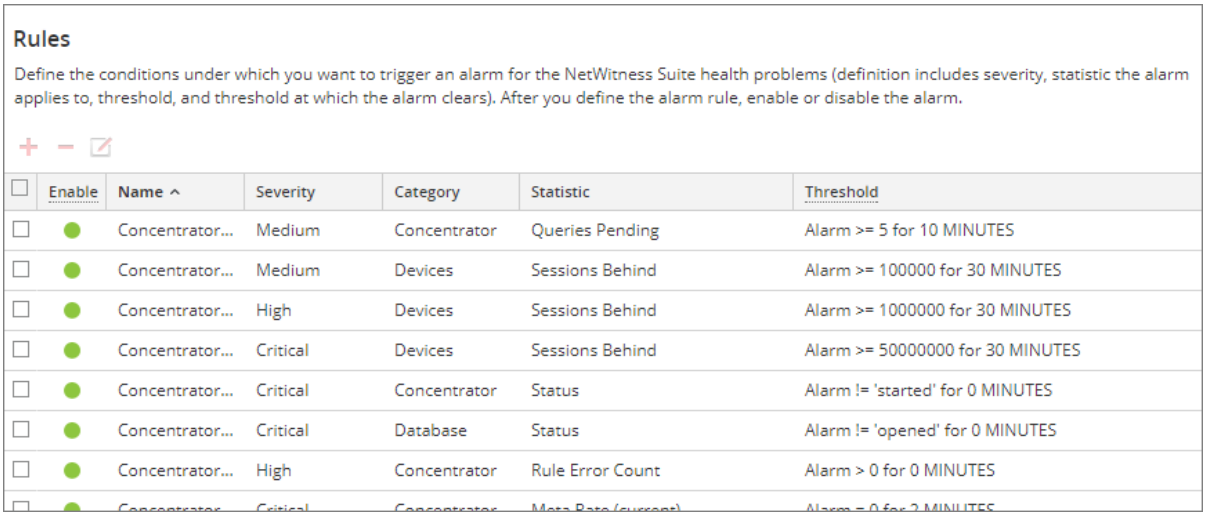
Masquer ou afficher les colonnes de conditions de règle

Pour masquer ou afficher les colonnes de conditions de règle dans le panneau Règles :

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie sous un service.

   La vue Détails de la stratégie s'affiche.
4. Accédez au panneau **Règles**.



5. Cliquez sur **v** à droite de **Catégorie**, sélectionnez **Colonnes** et décochez les conditions de règle **Statique** et **Seuil**.

   Vous pouvez cocher ou décocher les colonnes de Règles pour les afficher ou les masquer. Le panneau **Règles** s'affiche sans les conditions de règle.

Supprimer une règle

Pour supprimer un hôte ou un service à partir d'une stratégie :

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

   La vue Stratégies s'affiche.
3. Sélectionnez une stratégie sous un service.

   La vue Détails de la stratégie s'affiche.
4. Sélectionnez une règle dans la liste **Règles** (par exemple, **Checkpoint**).

5. Cliquez sur .
   La règle est supprimée de la stratégie.

Éliminer une règle

1. Cliquez sur l'onglet **Stratégies**.
   La vue Stratégies s'affiche.
2. Sélectionnez une stratégie sous un service.
   La vue Détails de la stratégie s'affiche. Vous pouvez spécifier des périodes pour la suppression de la règle lors de son ajout initial, ou bien modifier la règle et spécifier les périodes de suppression.
3. Ajoutez ou modifiez une règle.
4. Dans le panneau **Suppression de règle** de la boîte de dialogue **Ajouter** ou **Modifier une règle**, spécifiez les périodes et les jours au cours desquels vous souhaitez que la règle soit supprimée.

Supprimer une stratégie

1. Ajoutez ou modifiez une stratégie.
   La vue Stratégies s'affiche.
2. Dans le panneau **Suppression de stratégie** :
   a. Sélectionnez un fuseau horaire dans la liste déroulante **Fuseau horaire**.
      Ce fuseau horaire s'applique à l'intégralité de la stratégie (suppression de politique et suppression de règle).
   b. Cliquez sur  dans la barre d'outils.
   c. Spécifiez les périodes et jours au cours desquels vous voulez que la stratégie soit supprimée.

Ajouter une notification par e-mail

Pour ajouter une notification par e-mail à une stratégie :

1. Ajoutez ou modifiez une stratégie.
   La vue Stratégies s'affiche.
2. Dans le panneau **Notification** :
   a. Cliquez sur  dans la barre d'outils.
      Une ligne vide s'affiche pour la notification par e-mail.

b. Sélectionnez l'e-mail :

- Types de notification dans la colonne Destinataire (voir **Configurer les sorties de notification** dans le *Guide de configuration système NetWitness Suite* pour la source des valeurs dans cette liste déroulante).
- Serveur de notification dans la colonne Serveur de notification (voir **Configurer les serveurs de notification** dans le *Guide de configuration système NetWitness Suite* pour la source des valeurs dans cette liste déroulante).
- Serveur de modèle dans la colonne Modèle (voir **Configurer des modèles de notification** dans le *Guide de configuration système NetWitness Suite* pour la source des valeurs dans cette liste déroulante).

Remarque : Reportez-vous à **Inclure la ligne d'objet de l'e-mail par défaut** si vous souhaitez inclure la ligne d'objet de l'e-mail par défaut du modèle de type Intégrité dans vos notifications par e-mail Intégrité pour des destinataires spécifiés.

Supprimer une notification par e-mail

Pour ajouter une notification par e-mail à une stratégie :

1. Ajoutez ou modifiez une stratégie.
   La vue Stratégies s'affiche.
2. Dans le panneau **Notification** :
   a. Sélectionnez une notification par e-mail.
   b. Cliquez sur .
      La notification est supprimée.

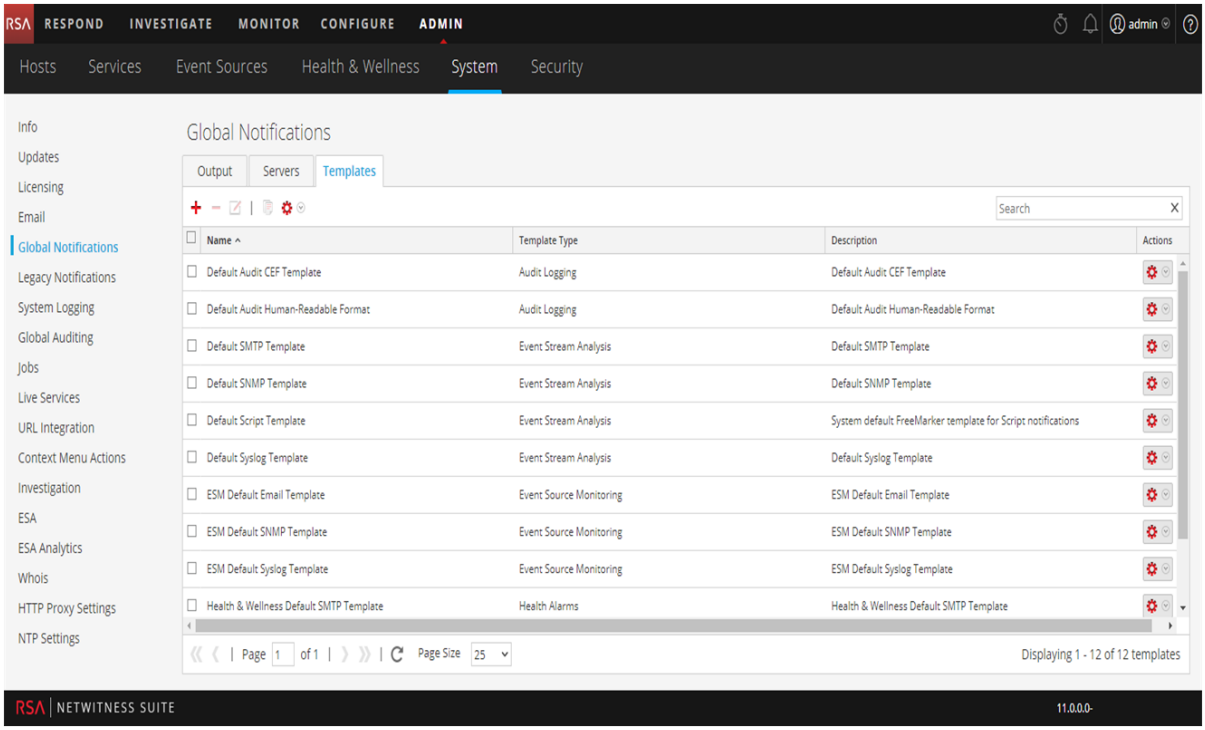
Inclure la ligne d'objet de l'e-mail par défaut

Les e-mails générés par les notifications configurées pour les stratégies n'incluent pas la ligne d'objet des modèles de notification par e-mail par défaut de type Intégrité. Vous devez spécifier la ligne d'objet dans les lignes d'objet à exclure. Cette procédure vous indique comment insérer une ligne d'objet dans les modèles.

Pour les rubriques de référence connexes, consultez la Vue Règles et Règles prédéfinies NetWitness.

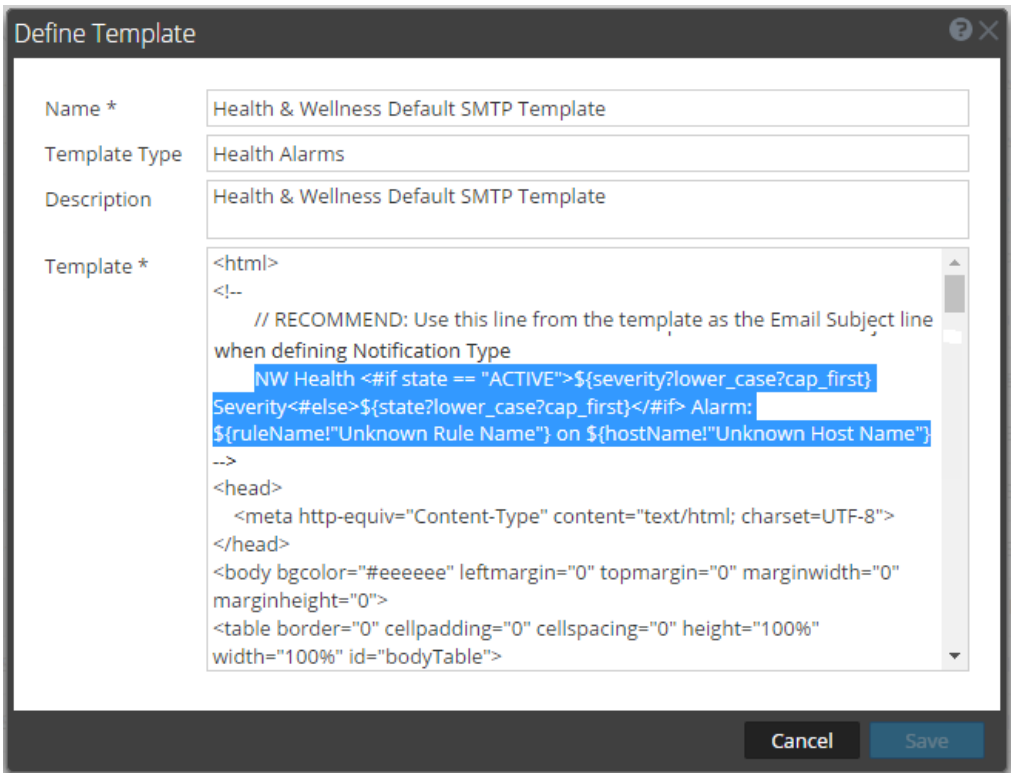
Pour inclure la ligne d'objet d'un modèle d'e-mail de type Intégrité dans votre notification par e-mail :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, sélectionnez **Notifications globales**.
3. Sélectionnez un modèle d'e-mail de type Intégrité (par exemple, **Modèle SMTP par défaut d'intégrité**).



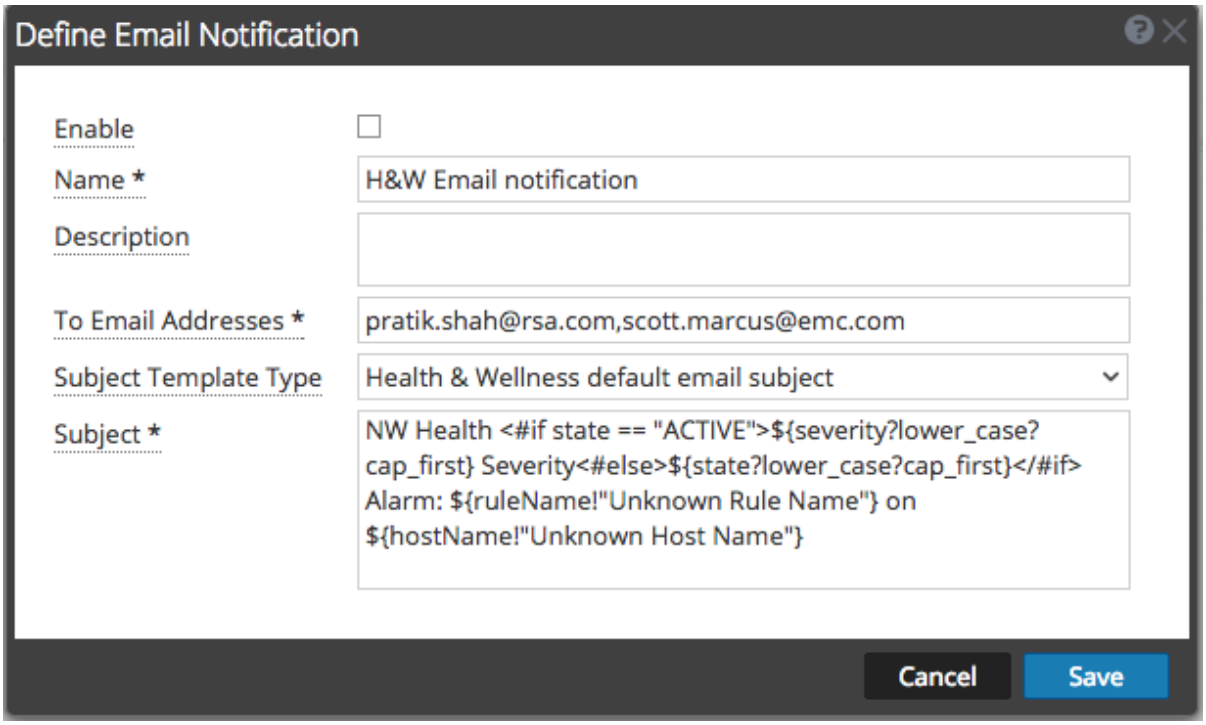
La boîte de dialogue Définir un modèle s'affiche.

4. Cliquez sur , puis, dans le champ **Modèle**, copiez la ligne d'objet (mettez en surbrillance la ligne d'objet et appuyez sur Ctrl+C) dans la mémoire tampon.



5. Cliquez sur **Annuler** pour fermer le modèle.
6. Cliquez sur l'onglet **Sortie** et sélectionnez une notification (par exemple, **Intégrité**).
7. Cliquez sur .

   La boîte de dialogue **Définir une notification par e-mail** s'affiche.
8. Remplacez la valeur de la zone de texte **Objet** par la ligne d'objet contenue dans la mémoire tampon (mettez en surbrillance le texte existant et appuyez sur Ctrl-V).



9. Cliquez sur **Enregistrer**.

Surveiller les statistiques du système

Le Navigateur Stat. système filtre les statistiques par hôte sélectionné, composant s'exécutant sur l'hôte, catégorie statistique, statistique individuelle ou toute combinaison d'hôtes, de composants, de catégories et de statistiques. Vous pouvez également choisir l'ordre d'affichage des informations.

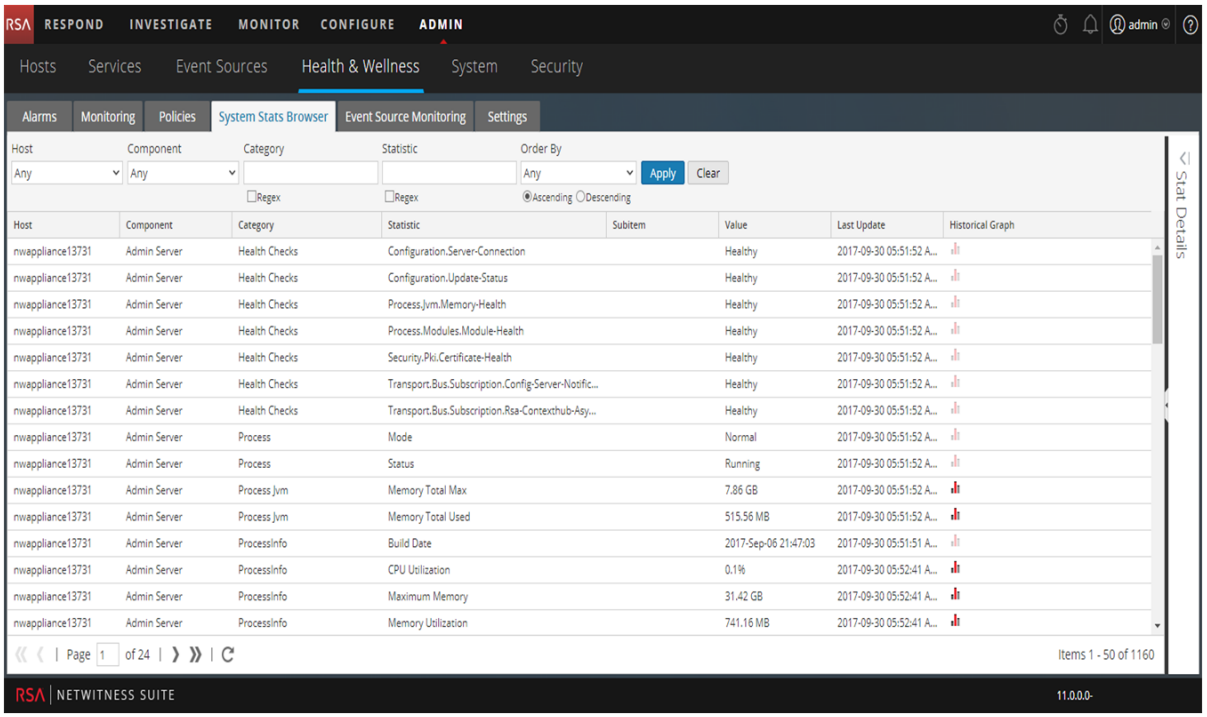
Pour accéder au Navigateur Stat. système :

1. Accédez à **Administrateur** > **Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

2. Cliquez sur l'onglet **Navigateur Stat. système**.

L'onglet Navigateur Stat. système s'affiche.



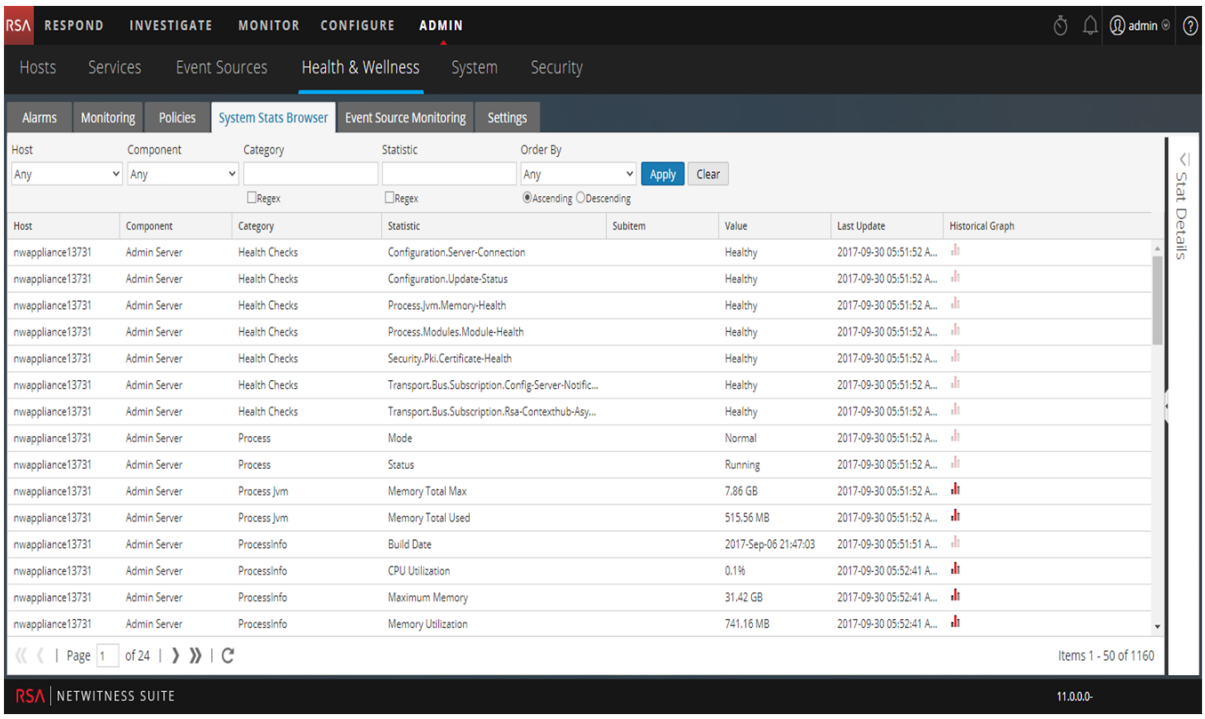
Filtrer les statistiques du système

Vous pouvez filtrer les statistiques système de l'une des manières suivantes afin de surveiller :

- les statistiques collectées pour un hôte donné ;
- les statistiques collectées pour un composant donné ;
- les statistiques collectées pour un type donné ou appartenant à une certaine catégorie ;
- les statistiques répertoriées en fonction de la sélection.

Pour filtrer la liste des statistiques système :

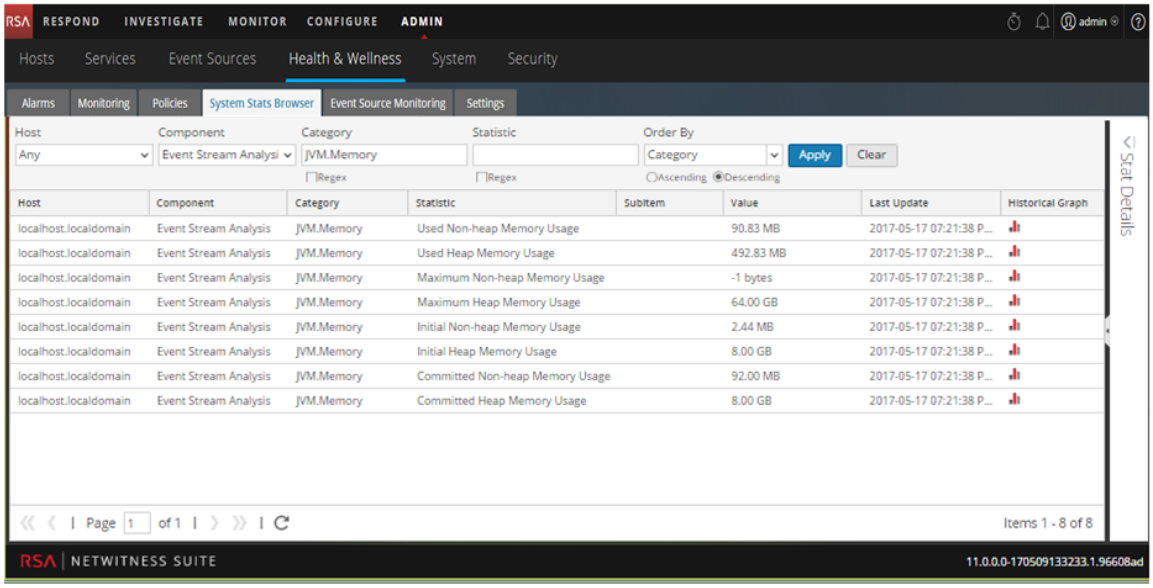
1. Accédez à **Administrateur > Intégrité**.
   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.
2. Cliquez sur **Navigateur Stat. système**.
   L'onglet Navigateur Stat. système s'affiche.



Filtrez les statistiques système de l'une des manières suivantes :

- Pour afficher les statistiques système d'un hôte donné, sélectionnez ce dernier dans la liste déroulante **Hôte**.
  Les statistiques système de l'hôte sélectionné s'affichent.
- Pour afficher les statistiques système d'un composant donné, sélectionnez ce dernier dans la liste déroulante **Composant**.
  Les statistiques système du composant sélectionné s'affichent.
- Pour afficher les statistiques système d'une catégorie donnée, saisissez le nom de cette dernière dans le champ **Catégorie**.
  Sélectionnez **Regex** pour activer ce filtre. Il effectue une recherche des expressions régulières dans du texte et répertorie la catégorie spécifiée. Si Regex n'est pas sélectionné, il prend en charge la mise en correspondance des schémas de globbing.
  Les statistiques système de la catégorie sélectionnée s'affichent.
- Pour trier les statistiques dans l'ordre de votre choix, vous pouvez définir cet ordre dans la colonne **Trier par**.
- Pour afficher une statistique donnée sur les différents hôtes, saisissez son nom dans le champ **Statistiques**.
  Sélectionnez **Regex** pour activer ce filtre. Il effectue une recherche des expressions régulières dans du texte et répertorie la catégorie spécifiée. Si Regex n'est pas sélectionné, il prend en charge la mise en correspondance des schémas de globbing.
  Les statistiques système pour les statistiques sélectionnées s'affichent.

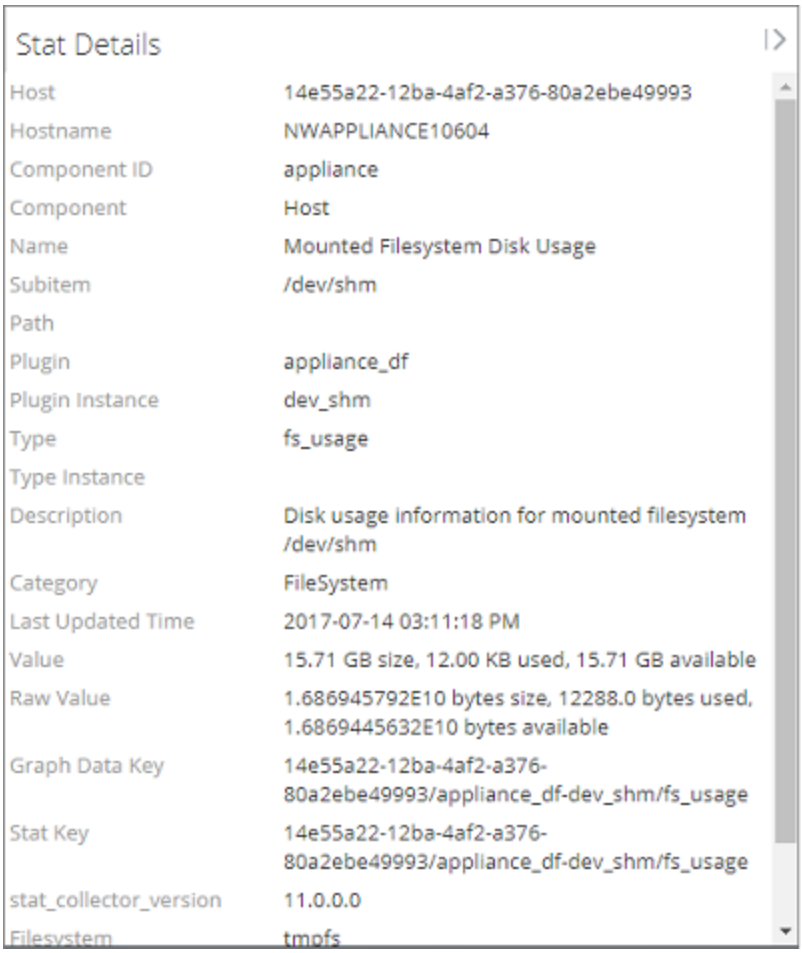
La figure suivante illustre le Navigateur Stat. système filtré par l'hôte NWAPPLIANCE10604 et classé par ordre décroissant des catégories de statistiques.



3. Pour afficher les détails d'une statistique donnée :

   a. Sélectionnez une ligne pour choisir une statistique.

   b. Cliquez sur <|.
   La section Détails stat. s'affiche.



Pour plus de détails sur les différents paramètres de **Administrateur** > **Intégrité** > vue **Navigateur Stat. système**, reportez-vous à la Vue Navigateur Stat. système.

Afficher un graphique de l'historique des statistiques du système

Le graphique de l'historique des statistiques système collectées vous donne des informations sur la variation des statistiques sur une période sélectionnée.

Pour afficher un graphique de l'historique :

1. Accédez à **Administrateur > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

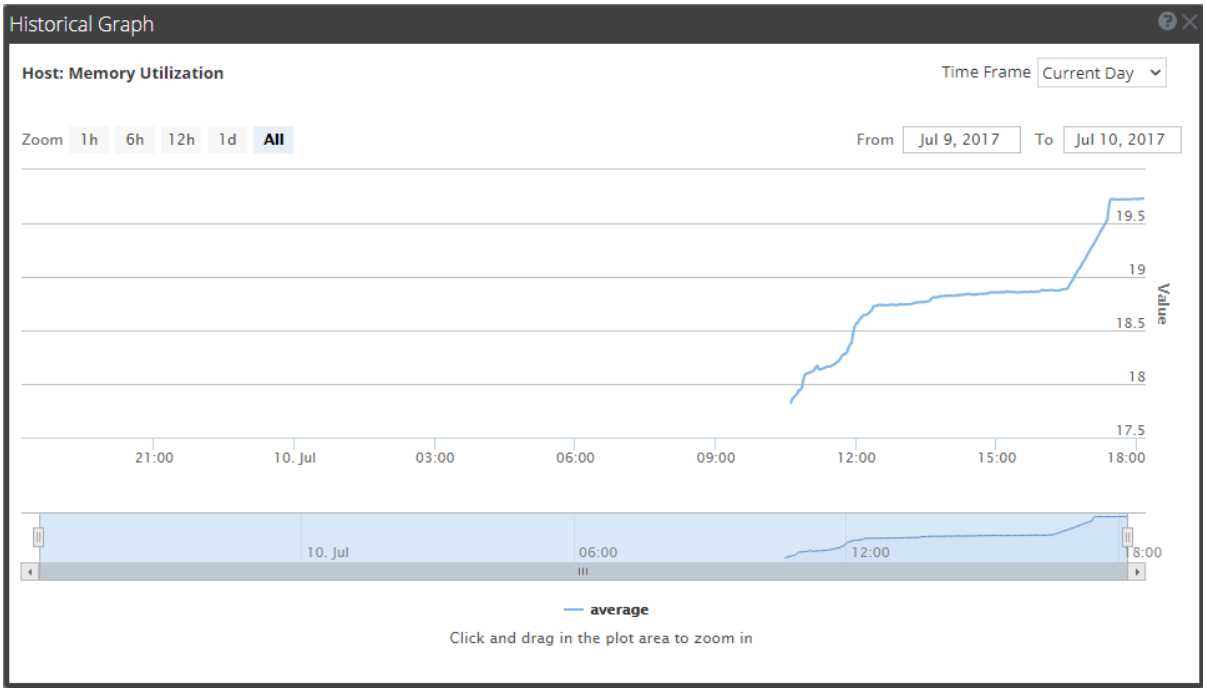
2. Cliquez sur l'onglet **Navigateur Stat. système**.

3. Dans l'onglet Navigateur Stat. système, spécifiez les critères de filtre pour afficher les statistiques souhaitées.

4. Dans la colonne **Graphique de l'historique**, sélectionnez .

   Le graphique de l'historique pour la statistique sélectionnée s'affiche.

La figure ci-dessous montre un exemple de graphique de l'historique pour la statistique Utilisation de mémoire d'un hôte.



La vue graphique est personnalisée pour afficher les statistiques collectées pour le jour actuel et les valeurs sont analysées pour un intervalle d'une heure (10h15 - 11h15). Placez le pointeur de la souris sur le graphique pour afficher les détails à un instant donné. Par exemple, la figure indique l'utilisation de la mémoire à 11h00.

Remarque : Vous pouvez personnaliser la vue du graphique en sélectionnant Délai et Période. Vous pouvez effectuer une analyse détaillée en définissant une valeur, une heure ou en cliquant simplement sur la zone de traçage du graphique Pour plus d'informations sur les paramètres à personnaliser et sur les fonctions d'analyses délimitées, reportez-vous à la rubrique Graphique de l'historique relatif aux statistiques du système. Toute interruption ou tout écart dans la ligne du graphique indique une panne du service ou de l'hôte à ce moment.

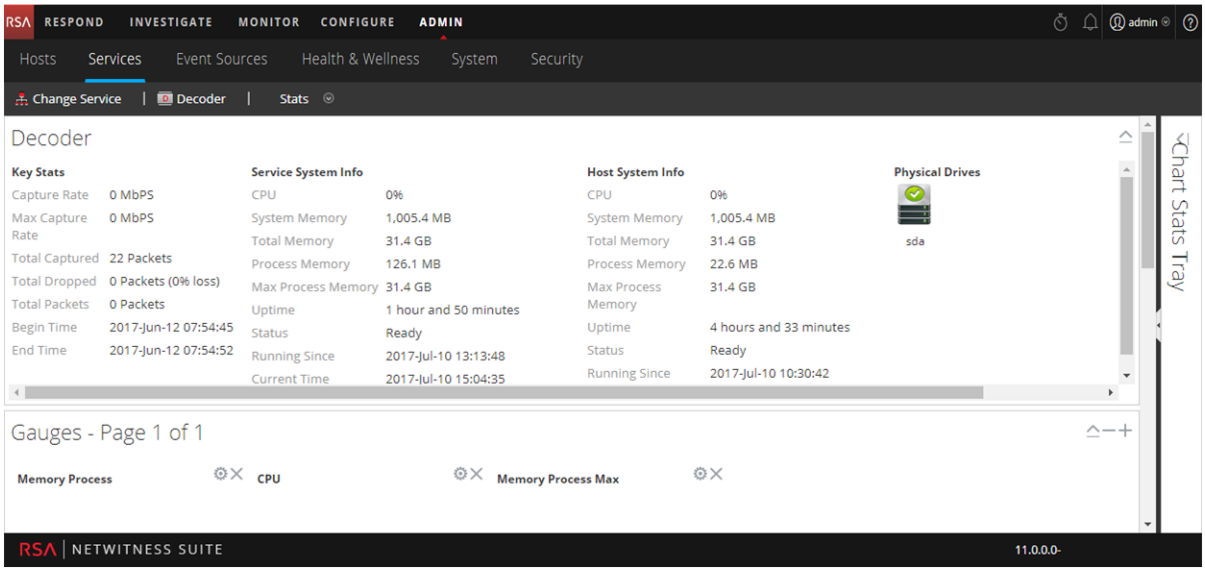
Surveiller les statistiques liées aux services

NetWitness Suite permet de surveiller l'état et les opérations d'un service. La vue Statistiques des services affiche les statistiques clés, les informations du système de services et les informations du système d'hôtes pour un périphérique. En outre, plus de 80 statistiques peuvent être affichées sous forme de jauges et dans des graphiques chronologiques. Seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés sous forme de graphiques chronologiques et historiques.

Bien que différentes statistiques soient disponibles pour différents types de services, certains éléments sont communs à chaque périphérique Core.

Pour surveiller les statistiques des services dans NetWitness Suite :

1. Accédez à **Administrateur > Services**.
   La vue Services s'affiche.
2. Sélectionnez un service, puis **Vue > Statistiques** dans la colonne Actions.



3. Pour personnaliser la vue : Développez ou réduisez les graphiques, par exemple développez la barre de statistiques graphiques pour afficher les graphiques disponibles. Déplacez une section vers le haut ou le bas pour modifier l'ordre. Par exemple, faites glisser la section Jauges vers le haut pour qu'elle se trouve au-dessus de la section Statistiques de synthèse.

Ajouter des statistiques à une jauge ou un graphique

Dans la vue Statistiques des services, vous pouvez personnaliser les statistiques surveillées pour les différents services. La barre de statistiques graphiques répertorie toutes les statistiques disponibles pour le service. Le nombre de statistiques varie en fonction du type de service en cours de surveillance. Toute statistique de la barre de statistiques graphiques peut être affichée sous forme de graphique en jauge ou chronologique. Seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés sous forme de graphiques chronologiques et historiques.

Créer une jauge pour une statistique

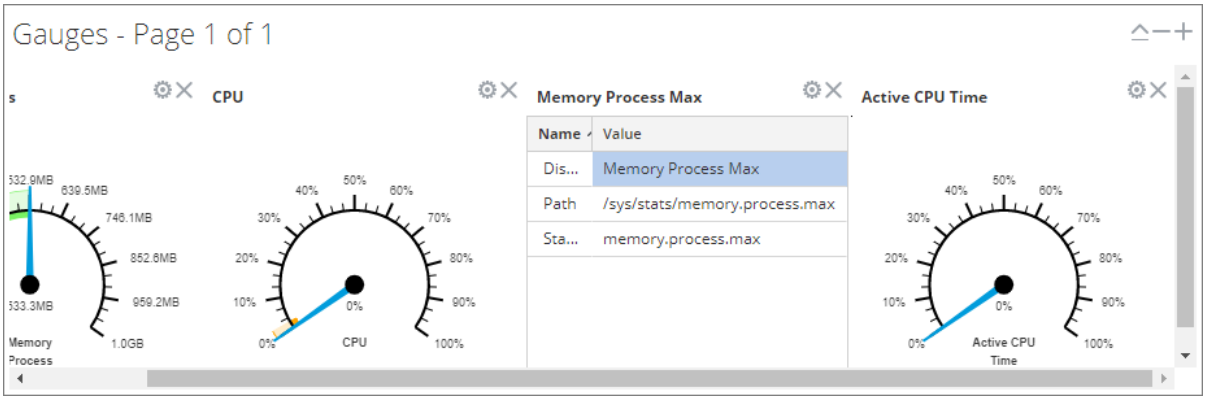
Pour créer une jauge pour une statistique dans la vue Statistiques des services :

1. Accédez à **ADMIN > Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service, puis **Vue > Statistiques** dans la colonne Actions.

La barre de statistiques graphiques s'affiche sur la droite.

3. Si cette barre est réduite, cliquez sur pour consulter la liste des statistiques disponibles.
4. Dans la **barre de statistiques graphiques**, cliquez sur une statistique, puis faites-la glisser dans la section **Jauges**.

   Une jauge est alors créée pour la statistique. Si l'espace manque pour placer la jauge, une nouvelle page est créée dans la section Jauges. La nouvelle jauge est alors ajoutée à la nouvelle page. Dans cet exemple, le graphique Temps CPU actif a été ajouté à la section Jauges par glisser-déplacer depuis la barre de statistiques graphiques.

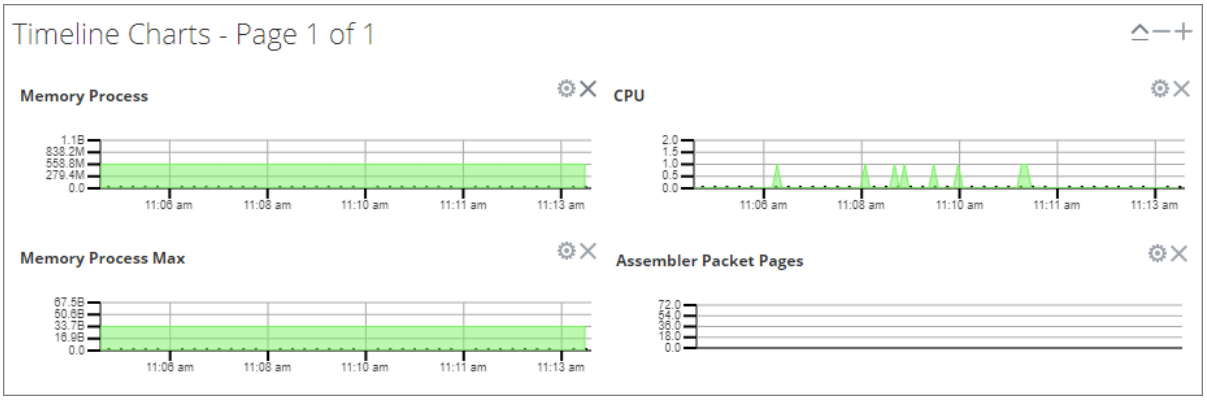


Créer un graphique chronologique pour une statistique

Pour créer une chronologie pour une statistique :

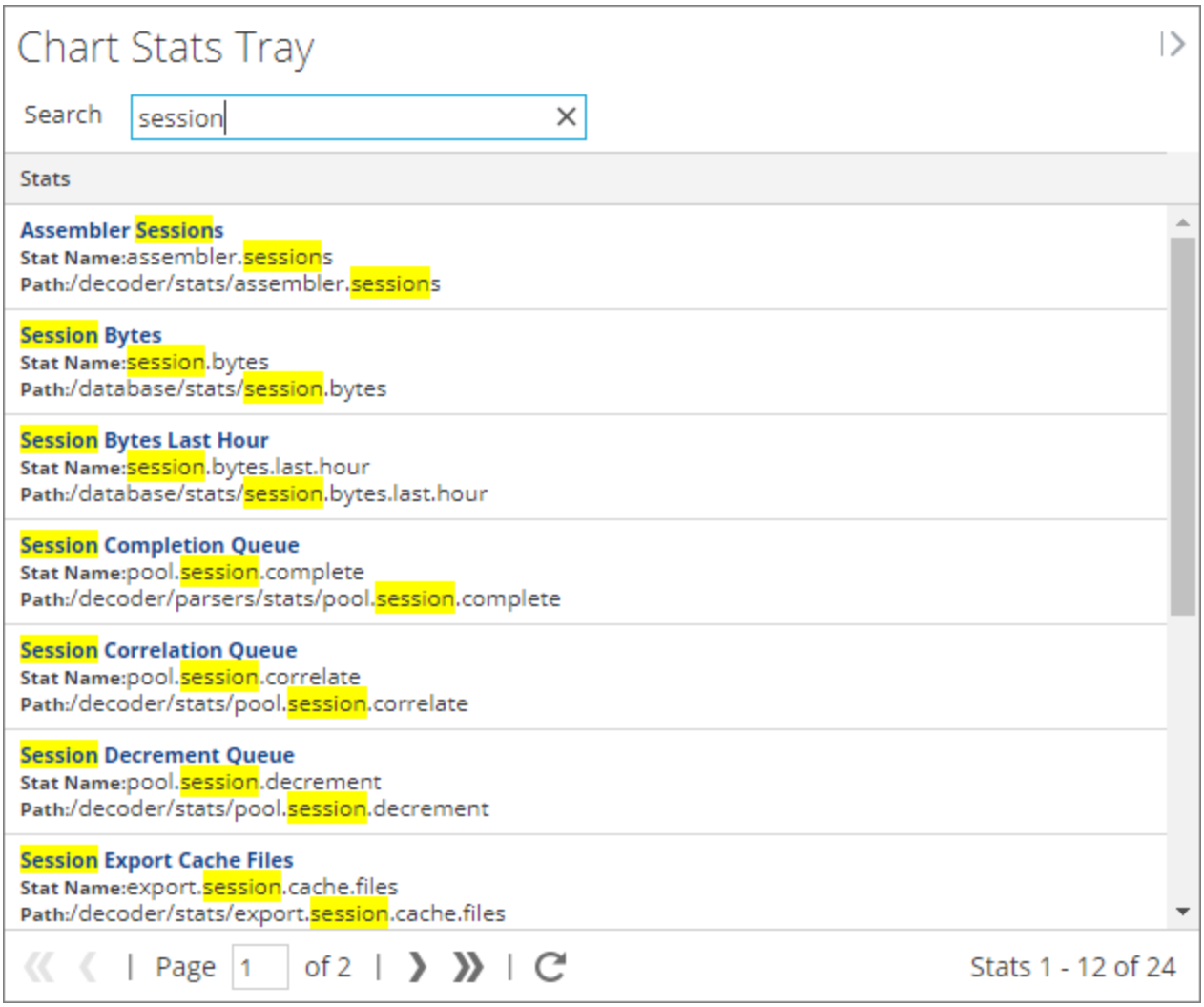
Dans la **barre de statistiques graphiques**, cliquez sur une statistique, puis faites-la glisser dans la section **Graphiques chronologiques** ou **Graphiques chronologiques de l'historique**.

Un graphique chronologique est alors créé pour la statistique. Si l'espace manque pour placer ce graphique, une nouvelle page est créée dans la section Graphiques chronologiques. Le nouveau graphique est alors ajouté à la nouvelle page. Dans cet exemple, le graphique Pages de paquets de l'assembleur a été ajouté à la section Graphiques chronologiques par glisser-déplacer depuis la barre de statistiques graphiques.



Rechercher une statistique dans la barre de statistiques graphiques

Pour rechercher une statistique, saisissez un terme de recherche, par exemple **session**, dans le champ de recherche, puis appuyez sur la touche **RETOUR**. Lorsque les statistiques correspondent, le mot correspondant s'affiche en surbrillance.



Modifier les propriétés des jauges de statistiques

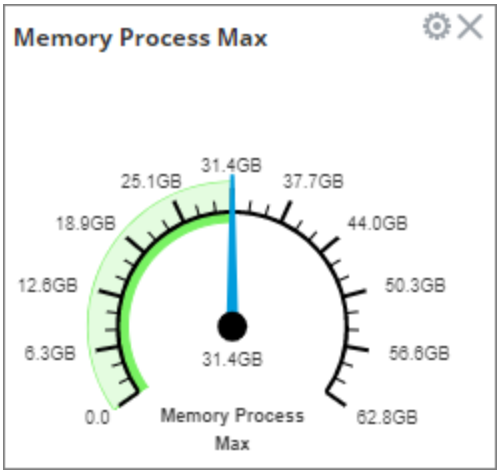
La section Jauges de la vue Statistiques des services présente les statistiques sous la forme d'une jauge analogique. Les propriétés de chaque jauge sont modifiables, comme leur titre, mais aussi, pour certaines d'entre elles, d'autres propriétés encore.

Modifier les propriétés d'une jauge

1. Accédez à **Administrateur > Services**

   Les services Administrateur s’affichent.

2. Sélectionnez un service, puis **Vue > Statistiques** dans la colonne Actions.
   La vue Statistiques des services contient la section Jauges.
3. Accédez à la jauge dont vous souhaitez modifier les propriétés (par exemple, **Processus mémoire**).



4. Cliquez sur l'icône Propriétés ( ) pour afficher les noms et les valeurs des paramètres.
5. Pour mettre en surbrillance la valeur du champ **Nom d'affichage**, double-cliquez sur la valeur ; par exemple, **Processus mémoire**.

   Remarque : Un clic sur les deux autres valeurs n'a aucun effet, car les propriétés ne sont pas modifiables dans la jauge.

6. Saisissez une nouvelle valeur pour le nom d'affichage et cliquez sur l'icône **Propriétés** ( ).
   Le nouveau titre remplace **Processus mémoire**.

Ajouter des statistiques à la section Jauges

Vous pouvez ajouter d'autres jauges en faisant glisser une statistique de la **barre de statistiques graphiques** vers la section **Jauges**.

1. Pour développer la barre de statistiques graphiques, cliquez sur .
2. Faites défiler vers le bas et sélectionnez une statistique, par exemple, **Débit de session (maximal)**.
3. Faites glisser la statistique vers la section **Jauges**.
   La nouvelle jauge s'affiche dans la section Jauges.

Modifier les propriétés des graphiques chronologiques

Les graphiques chronologiques affichent les statistiques au fil du temps. La vue Statistiques des services contient deux types de chronologies : actuelle et historique. Vous pouvez faire glisser les statistiques disponibles dans la barre de statistiques graphiques vers la section Graphiques chronologiques. Seules les statistiques relatives à la taille des sessions, aux sessions et aux paquets peuvent être affichés sous forme de graphiques chronologiques et historiques. Les propriétés de chaque graphique chronologique sont modifiables, comme leur titre, mais aussi, pour certains d'entre eux, d'autres propriétés encore.

Pour accéder aux graphiques :

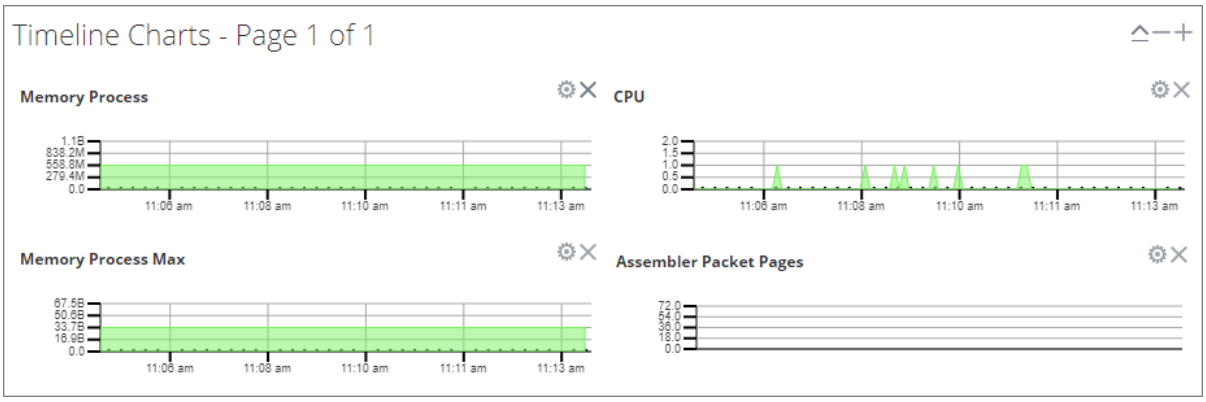
1. Accédez à **Administrateur > Services**.
2. Sélectionnez un service et cliquez sur **Stats**.

   La vue Statistiques des services s'affiche. Les graphiques sont affichés dans cette vue.

Modifier les propriétés d'une chronologie

Pour modifier les propriétés d'un graphique chronologique :

1. Accédez au graphique dont vous voulez modifier les propriétés (par exemple, **Processus mémoire**).



2. Cliquez sur l'icône **Propriétés** ( ) pour afficher les noms et les valeurs des paramètres.
3. Double-cliquez sur une valeur (par exemple, le champ **Nom d'affichage**) pour rendre cette valeur modifiable.

   Remarque : Rien ne se passe si vous cliquez sur les deux autres valeurs, car les propriétés ne peuvent pas être modifiées dans le graphique.

4. Saisissez une nouvelle valeur, puis cliquez sur l'icône **Propriétés** ( ).

   Le graphique chronologique qui s'affiche reprend les nouvelles valeurs.

Modifier les propriétés d'une chronologie historique

Pour modifier les propriétés d'un graphique chronologiques de l'historique :

1. Accédez à Graphiques chronologiques de l'historique.
2. Cliquez sur l'icône **Propriétés** ( ) pour afficher les noms et les valeurs des paramètres.
3. Cliquez sur une valeur (par exemple, **27/01/2015** dans le champ **Date de début**) pour rendre cette valeur modifiable.
4. Saisissez une nouvelle valeur.
5. Si nécessaire, modifiez la valeur des champs **Date de fin** et **Nom d'affichage**.
6. Cliquez sur l'icône **Propriétés** ( ).
   La chronologie de l'historique qui s'affiche reprend les nouvelles valeurs.

Remarque : Pour rétablir les propriétés par défaut du graphique chronologique de l'historique afin que les valeurs soient mises à jour de façon dynamique, supprimez les dates de début et de fin, placez le curseur dans le champ Date de début, puis actualisez votre navigateur.

Ajouter des statistiques à des graphiques chronologiques

Vous pouvez ajouter des graphiques chronologiques en faisant glisser une statistique de la barre de statistiques graphiques vers la section Chronologies.

1. Pour développer la barre de statistiques graphiques, cliquez sur .
2. Sélectionnez une statistique dans la liste, par exemple, **Débit de session (maximum)**.
3. Faites glisser cette statistique dans la **section Chronologies**.
   La nouvelle chronologie s'affiche dans la section Chronologies.

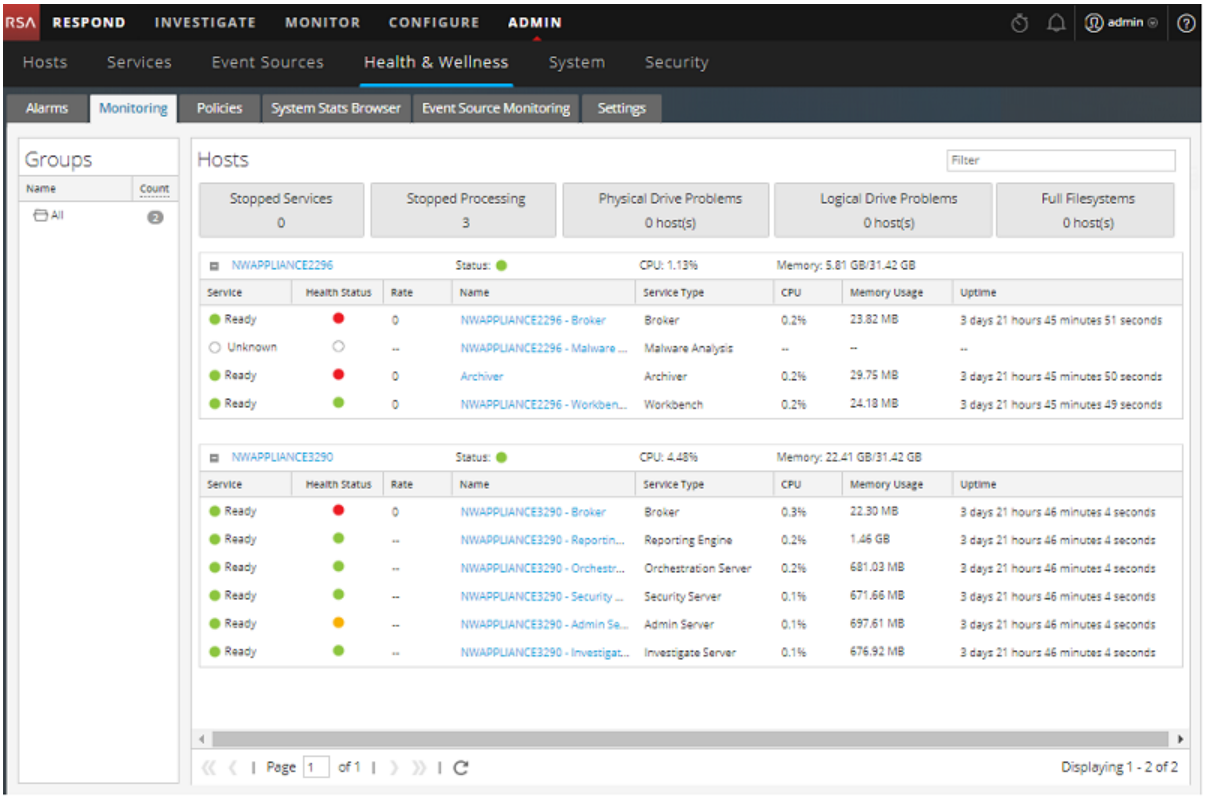
Surveiller les hôtes et les services

NetWitness Suite permet de surveiller l'état des hôtes et services installés. Vous pouvez afficher l'état d'intégrité actuel de tous les hôtes et des services qu'ils exécutent, l'utilisation du processeur et la mémoire utilisée, ainsi que des informations détaillées sur les hôtes et les services.

Pour surveiller les hôtes et les services dans NetWitness Suite :

1. Accédez à **Administrateur > Intégrité**.
   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.
2. Sélectionnez l'onglet **Surveillance**.
   La liste de tous les hôtes et des services associés appartenant au groupe **Tous** s'affiche par défaut.
   L'état de fonctionnement, l'utilisation du processeur et l'utilisation de la mémoire s'affichent

pour chaque hôte.



Cliquez sur ⊞ à gauche d'un hôte (⊞ apparaît lorsque des services sont installés sur l'hôte).

3. La liste des services installés sur l'hôte sélectionné s'affiche.
   Le nom, l'état de fonctionnement, le processeur utilisé, la mémoire utilisée et la durée de fonctionnement pour chaque service s'affichent.

Filtrer les hôtes et les services dans la vue Surveillance

Vous pouvez filtrer les hôtes et les services dans la vue Surveillance en procédant de l'une des manières suivantes :

- Hôtes appartenant à un groupe donné
- Hôte donné et services associés
- Hôtes dont les services ont été arrêtés
- Hôtes dont le traitement des services a été arrêté ou désactivé
- Hôtes présentant des problèmes de lecteurs physiques

- Hôtes présentant des problèmes de lecteurs logiques
- Hôtes disposant de systèmes de fichiers complets

Pour consulter la rubrique de référence connexe, reportez-vous à la rubrique Vue Surveillance.

Pour filtrer les hôtes et les services :

1. Accédez à **Administrateur > Intégrité**.

   Par défaut, la vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

2. Sélectionnez l'onglet **Surveillance**.

3. Filtre les hôtes et les services de l'une des manières suivantes :

   - Pour afficher la liste des hôtes et services associés qui appartiennent à un groupe donné, sélectionnez le groupe en question dans le panneau Groupes.

     Tous les hôtes et services associés appartenant au groupe indiqué sont affichés dans le panneau Hôtes.

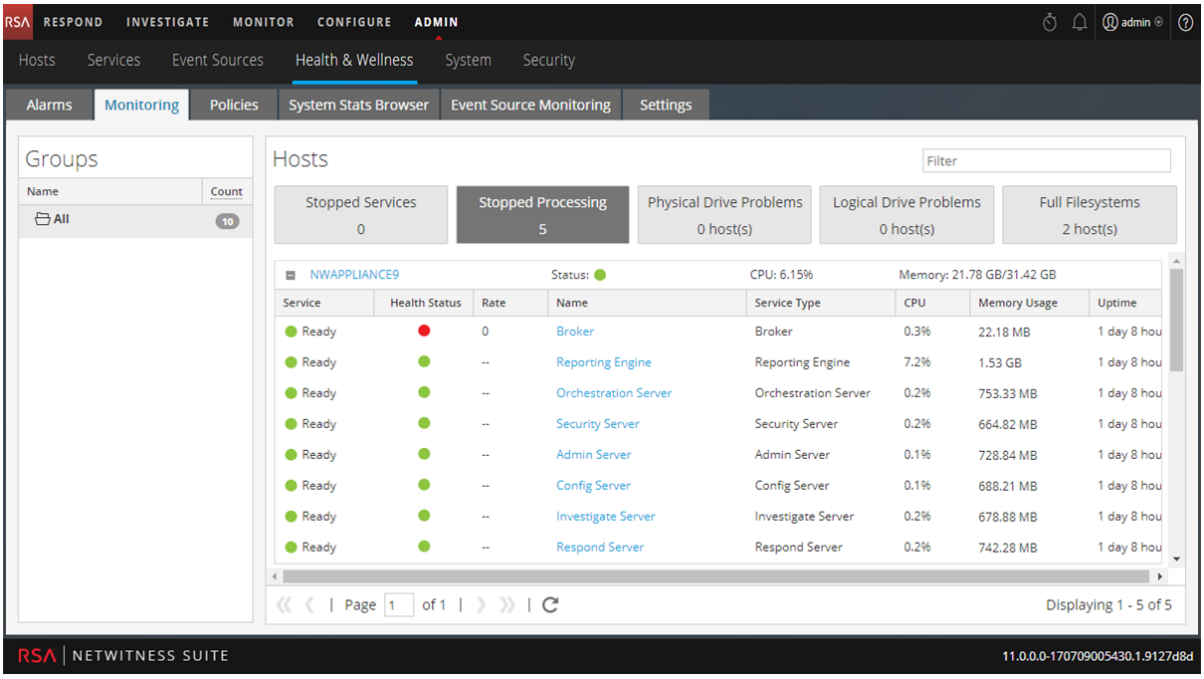
     Remarque : Le regroupement des hôtes est dérivé des groupes créés sur la page Administration. Tous les groupes créés sur la page Administration sont affichés ici.

     Par exemple, si vous sélectionnez le groupe **Groupe_LC** dans le panneau Groupes, tous les hôtes appartenant à ce groupe sont affichés.

   - Pour afficher la liste de tous les services dont le traitement a été arrêté, cliquez sur **Traitement arrêté** dans le panneau Hôtes.

     Tous les hôtes pour lesquels le traitement d'au moins un service a été arrêté sont affichés.

     Remarque : Les boutons supérieurs permettent d'afficher les statistiques système de tous les hôtes configurés dans NetWitness Suite et ne changent pas avec l'application des filtres sur les groupes.



Remarque : De la même manière, vous pouvez filtrer la liste des hôtes et des services associés en choisissant le filtre approprié
. Cliquez sur Services arrêtés pour afficher la liste de tous les services dont le traitement a été arrêté.
- Cliquez sur Problème de disque physique pour afficher la liste des hôtes présentant de tels problèmes.
- Saisissez un nom d'hôte dans la zone de filtre pour afficher uniquement l'hôte et les services exécutés sur l'hôte.

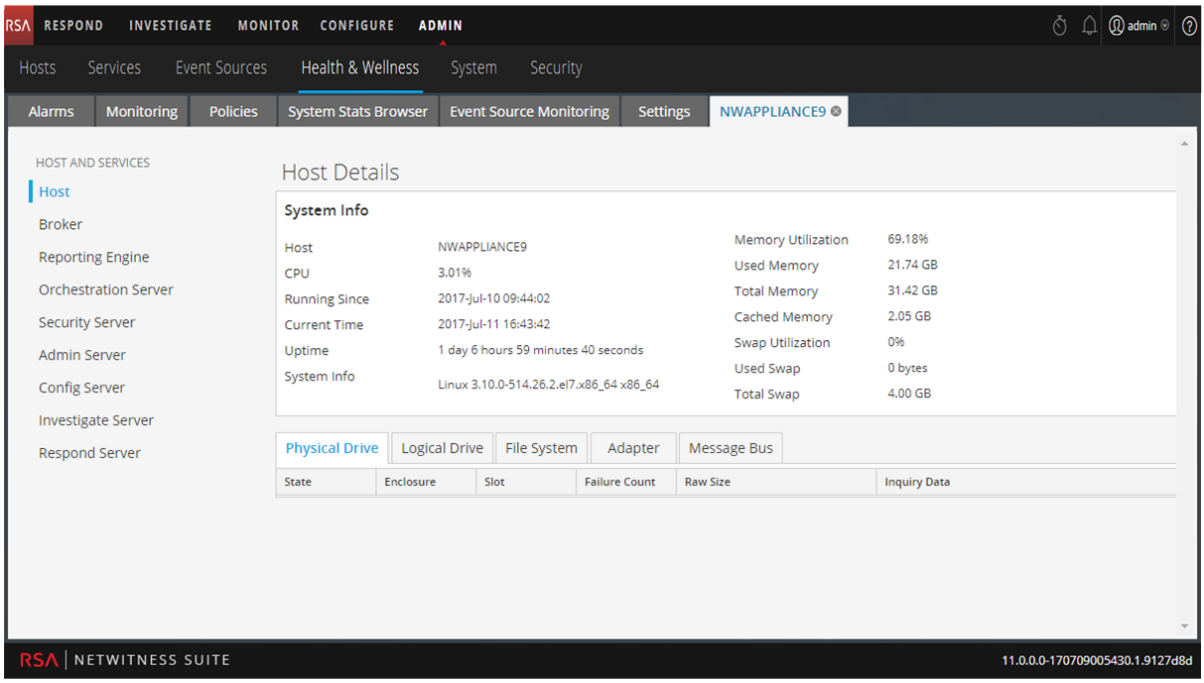
Surveiller les détails d'un hôte

Vous pouvez afficher les détails de l'hôte, le taux d'utilisation de sa mémoire et du CPU, des informations système, le lecteur physique, le disque logique et des informations sur le système de fichiers pour enquêter plus avant si vous rencontrez des problèmes avec l'hôte.

Pour afficher les détails de l'hôte :

1. Accédez à **Administrateur > Intégrité**.
   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.
2. Sélectionnez l'onglet **Surveillance**.
3. Cliquez sur un hôte dans le panneau **Hôtes**.

La vue Détails de l'hôte s'affiche dans une nouvelle page.



Surveiller les détails d'un service

Vous pouvez afficher les détails d'un service, sa mémoire et l'utilisation du CPU, les informations système et divers détails selon le service sélectionné.

Pour afficher les détails d'un service :

1. Accédez à **Administrateur > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

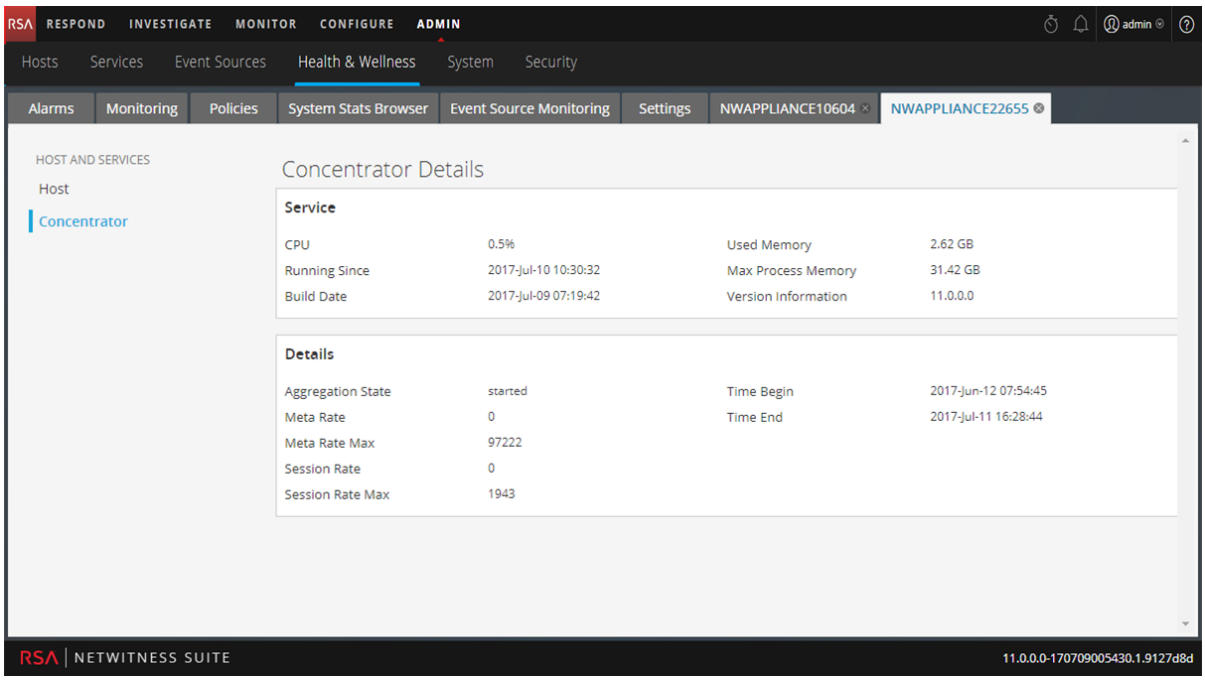
2. Sélectionnez l'onglet **Surveillance**.

3. Cliquez sur ⊞ pour un hôte du panneau Hôtes.

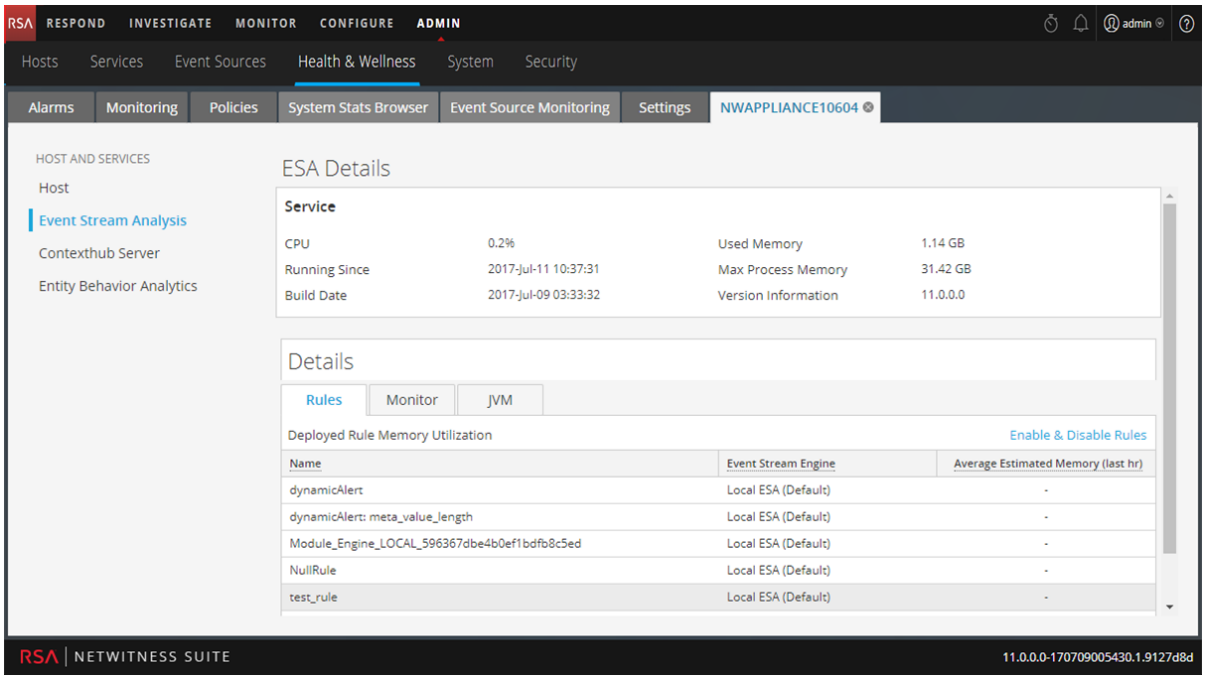
   La liste des services en cours d'exécution sur l'hôte s'affiche.

4. Cliquez sur un service.

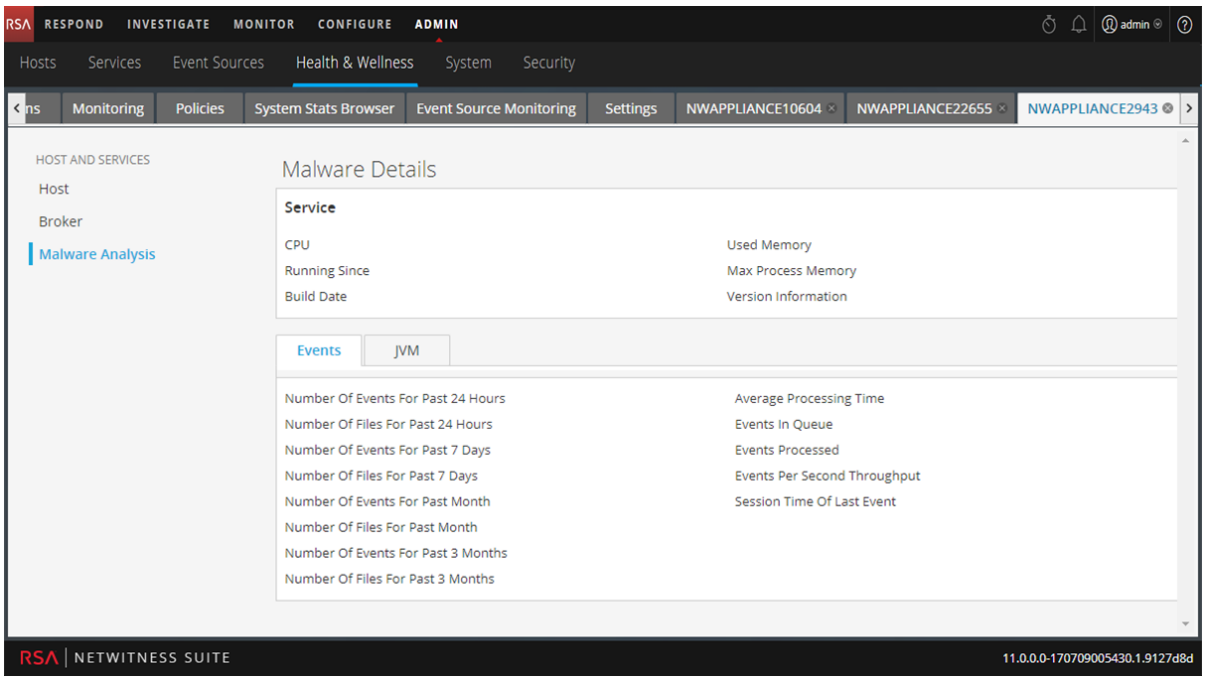
   La vue des détails du service s'affiche comme nouvelle page. Les vues des détails des services Archiver, Broker, Concentrator et Decoder contiennent les panneaux **Service** et **Détails**.



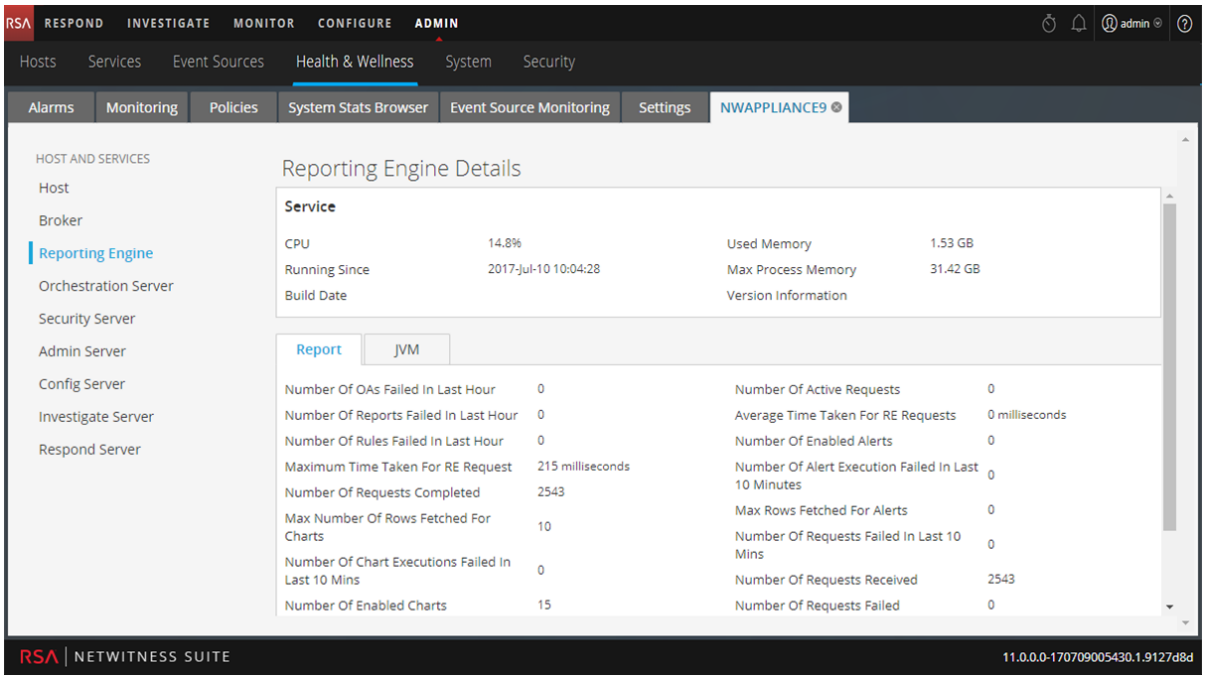
La vue des détails du service Event Stream Analysis (ESA) contient les panneaux **Service** et **Détails** ainsi que les onglets **Surveiller** et **JVM** qui affichent des statistiques supplémentaires.



La vue des détails du service Malware Analysis contient le panneau **Service** ainsi que les onglets **Règles, Événements** et **JVM** qui affichent des statistiques supplémentaires.



La vue des détails du service Reporting Engine contient le panneau **Service** plus les onglets **Rapport** et **JVM** qui affichent des statistiques supplémentaires.



Remarque : Vous pouvez également accéder à la page des détails des services en cliquant sur les services répertoriés dans le panneau des options de la vue Détails de l'hôte.

Reportez-vous à la Vue Surveillance pour une description détaillée de la vue Détails de chaque service.

Surveiller des sources d'événements

La fonction de surveillance des sources d'événement de NetWitness Suite propose les fonctionnalités suivantes :

- Prise en charge de basculement sur incident
- Fourniture d'une liste consolidée des sources d'événement et de leurs périphériques associés Collector et Log Decoder
- Prise en charge de Regex pour les règles
- Décommission
- Fonctions de filtrage
- Graphique de l'historique

En outre, vous pouvez surveiller des sources d'événement, contrôler le nombre d'événements générés par un type de source et afficher le graphique de l'historique des événements collectés. Pour surveiller les sources d'événements, vous devez configurer les sources d'événements afin qu'elles génèrent et envoient des notifications en cas de besoin.

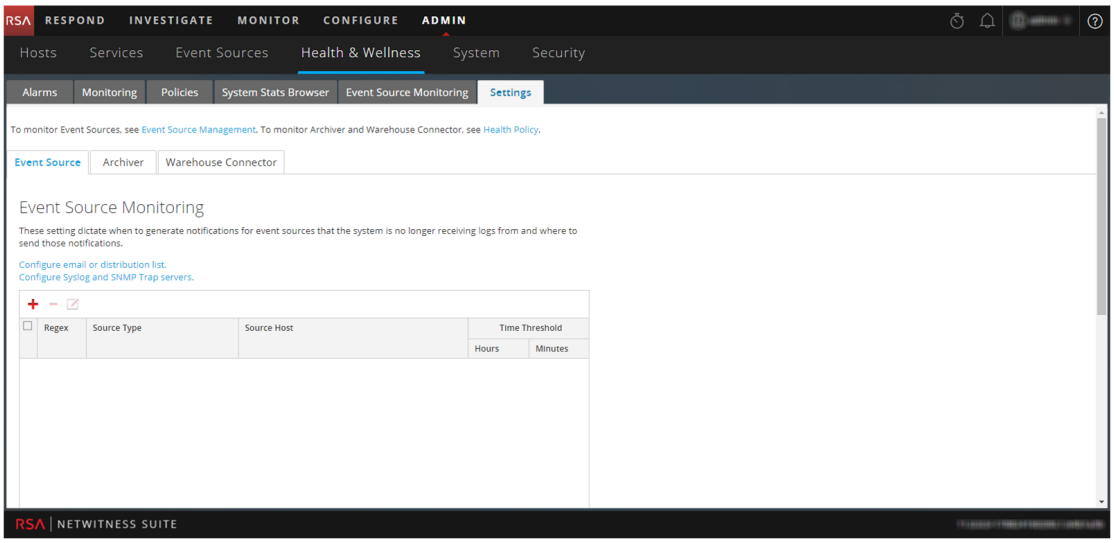
Configurer la surveillance des sources d'événements

Pour surveiller les sources d'événements, vous devez configurer les sources d'événements afin qu'elles génèrent et envoient des notifications en cas de besoin. Pour consulter la rubrique référencée associée, reportez-vous à Vue Paramètres d'intégrité - Sources d'événements.

Pour configurer et activer la surveillance des événements dans NetWitness Suite :

1. Accédez à **Administrateur** > **Intégrité**.
2. Sélectionnez **Paramètres** > **Source d'événement**.

   L'onglet Source d'événement s'affiche.

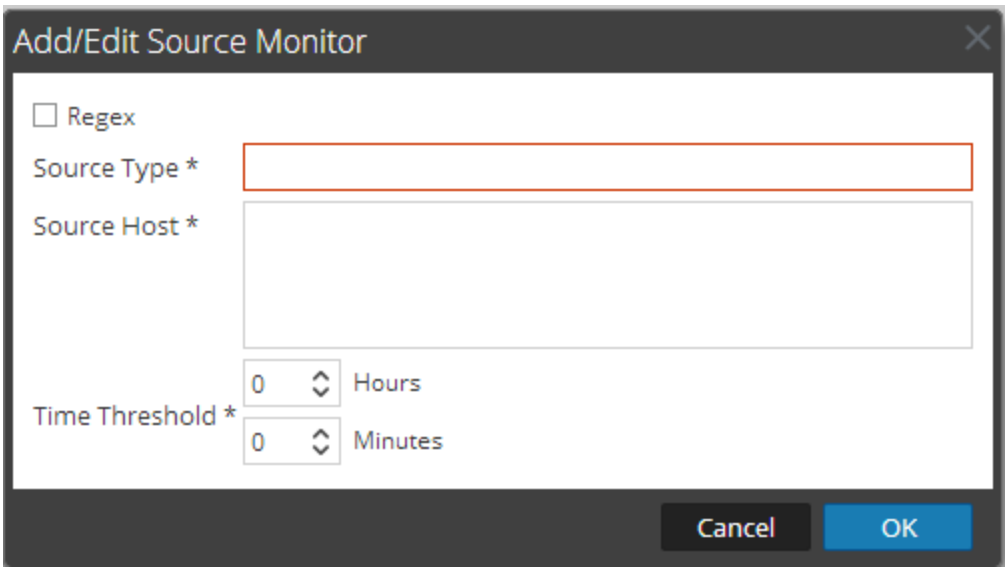


3. Sous **Surveillance des sources d'événements**, cliquez sur +.

   La boîte de dialogue Ajouter/modifier la surveillance des sources s'affiche.

4. Définissez le **Type de source**, l'**Hôte source** et le **Seuil de délai d'attente** de la source d'événement que vous souhaitez surveiller pour détecter le moment où NetWitness Suite cesse d'en recevoir des logs. Si vous ne spécifiez pas de **Seuil de délai d'attente**, NetWitness Suite surveille la source d'événement jusqu'à ce que vous définissiez un seuil.

   Remarque : Pour le **Type de source** et l'**Hôte source**, vous devez spécifier les valeurs que vous avez configurées pour la source de l'événement sous l'onglet **Sources d'événements** de la vue **Administration** > **Services** > Service Log Collector > **Vue** > **Config**. Vous pouvez ajouter ou modifier les sources d'événements que vous souhaitez surveiller. Les deux paramètres qui identifient une source d'événement sont **Type de source** et **Hôte source**. Vous pouvez utiliser **globbing** (association de motifs et caractères génériques) pour spécifier le **Type de source** et l'**Hôte source** des sources d'événements



5. Cliquez sur **OK**.

   La source d'événement s'affiche dans le panneau.

6. Configurez la méthode de notification en procédant comme suit :

   - Sélectionnez **Configurer l'e-mail ou la liste de distribution**.

     Le panneau Administrateur > Système > Configuration de l'e-mail s'affiche, de sorte que vous pouvez spécifier à qui les notifications sont envoyées.

   - Sélectionnez **Configurer des serveurs de traps Syslog et SNMP**.

     Le panneau Administration > Configuration d'audit système s'affiche, de sorte que vous pouvez configurer le Syslog et les traps SNMP auxquels les notifications sont envoyées.

7. Cliquez sur **Appliquer**.

   NetWitness Suite commence par envoyer des notifications lorsqu'il cesse de recevoir des événements de cette source d'événements une fois le délai de seuil écoulé.

Pour plus de détails sur les paramètres de la vue des paramètres Surveillance des sources d'événements, consultez la Vue Contrôle des sources d'événements.

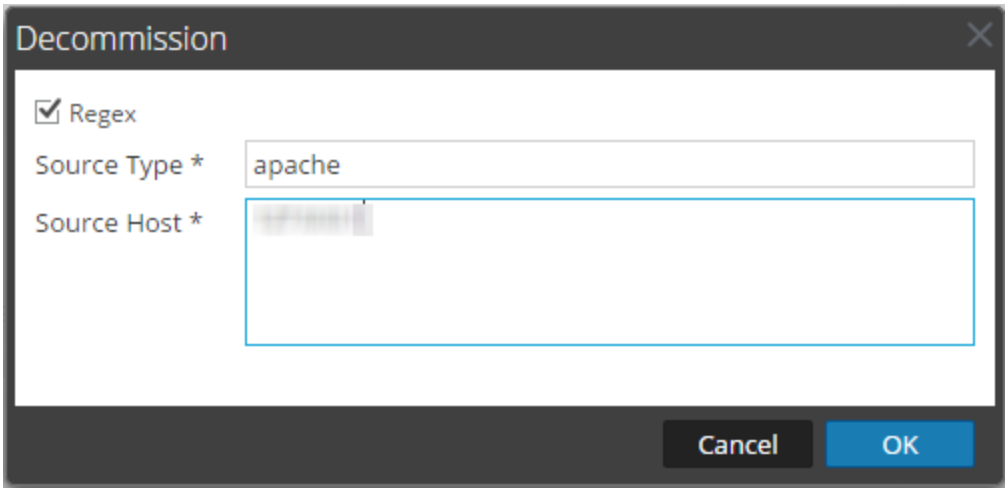
Abandonner la surveillance des sources d'événements

Si un service Log Collector (Local Collector ou Remote Collector) pour lequel vous configurez la surveillance de source d'événement devient inutilisable, NetWitness Suite continue de vous notifier que vous n'en recevrez pas d'événements avant d'avoir décommissionné le collecteur.

Attention : Si vous avez configuré un Local Collector de basculement sur incident pour un Remote Collector et que le Local Collector bascule vers un Log Decoder en veille, vous devez abandonner le Local Collector pour arrêter les notifications.

Pour abandonner la surveillance pour une source d'événement :

1. Accédez à **Administrateur** > **Intégrité**.
2. Sélectionnez **Paramètres** > **Source d'événement**.
   L'onglet **Source d'événement** s'affiche.
3. Sous **Décommissionner**, cliquez sur +.
   La boîte de dialogue **Décommissionner** s'affiche.
4. Définissez le **Type de source** et l'**Hôte source** pour la source pour laquelle vous souhaitez abandonner les notifications de surveillance d'événement.



Filtrer des sources d'événements

Vous pouvez choisir le filtre à afficher.

- Événements appartenant à une source d'événements donnée
- Événements appartenant à des types de sources d'événements donnés
- Événements collectés auprès d'un Collector Log donné
- Événements triés par deux sources d'événements, Log Collector, Log Decoder ou Heure du dernier événement.

Pour filtrer la liste des sources d'événements :

1. Accédez à **Administrateur > Intégrité**.
2. Cliquez sur **Surveillance des sources d'événements**.
3. Filtrez la liste de l'une des manières suivantes :

- Pour consulter les événements générés par une source d'événements donnée, saisissez la source demandée dans le champ **Source de l'événement**. Sélectionnez **Regex** pour activer ce

filtre, puis cliquez sur **Appliquer**. Une recherche des expressions régulières est effectuée dans du texte et la catégorie spécifiée est répertoriée. Ce champ prend également en charge la mise en correspondance des schémas de globbing.
Tous les événements générés par la source d'événement spécifiée s'affichent.

- Pour consulter les événements collectés auprès d'un Log Collector donné, sélectionnez ce dernier dans la liste déroulante, puis cliquez sur **Appliquer**.
La liste de tous les événements collectés auprès du Log Collector indiqué, dans différentes sources d'événements sont affichés.

Remarque : Vous pouvez également choisir les filtres suivants :
- Pour consulter les événements appartenant à un type de source d'événements, sélectionnez ce type, puis cliquez sur **Appliquer**.
- Pour consulter les événements reçus au cours d'une période donnée, sélectionnez cette période, puis cliquez sur **Appliquer**. Vous pouvez affiner les résultats de la requête pour qu'ils ne contiennent que les sources d'événements dont les logs ont été reçus dans le délai sélectionné ou uniquement les sources d'événements dont les logs n'ont pas été reçus dans le délai sélectionné

Pour plus d'informations sur les différents paramètres et pour obtenir leur description, reportez-vous à la rubrique Vue Contrôle des sources d'événements.

Afficher le graphique de l'historique des événements collectés pour une source d'événement

Le graphique de l'historique des événements collectés à partir d'une source d'événement vous donne des informations sur la variation de la collecte sur une période sélectionnée.

Pour afficher un graphique de l'historique :

1. Accédez à **Administrateur > Intégrité**.
La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.
2. Cliquez sur **Surveillance des sources d'événements**.
La vue Surveillance des sources d'événements s'affiche.
3. Dans la colonne **Graphique de l'historique**, sélectionnez .
Le graphique de l'historique pour la source d'événement sélectionnée s'affiche.
La figure ci-dessous montre un exemple de graphique de l'historique pour le type de source d'événement **winevent_snare**.

La vue graphique est personnalisée pour afficher les événements collectés pour le jour actuel et les valeurs sont analysées pour un intervalle d'une heure (9h05 - 10h05). Placez le pointeur de la souris sur le graphique pour afficher les détails à un instant donné. Par exemple, la figure indique le taux moyen de collecte à 9h30.

Remarque : Vous pouvez personnaliser la vue du graphique en sélectionnant Délai et Période. Vous pouvez effectuer une analyse détaillée en définissant une valeur, une heure ou en cliquant simplement sur la zone de traçage du graphique Pour plus d'informations sur les paramètres à personnaliser et sur les fonctions d'analyses délimitées, reportez-vous à la rubrique Graphiques de l'historique d'intégrité collectés à partir d'une source d'événement.
Si le graphique ne présente aucune donné, cela peut être dû aux raisons suivantes :
-la source d'événement est en panne.
-la source d'événement n'effectue aucun traitement pour le moment.

Surveiller les alarmes

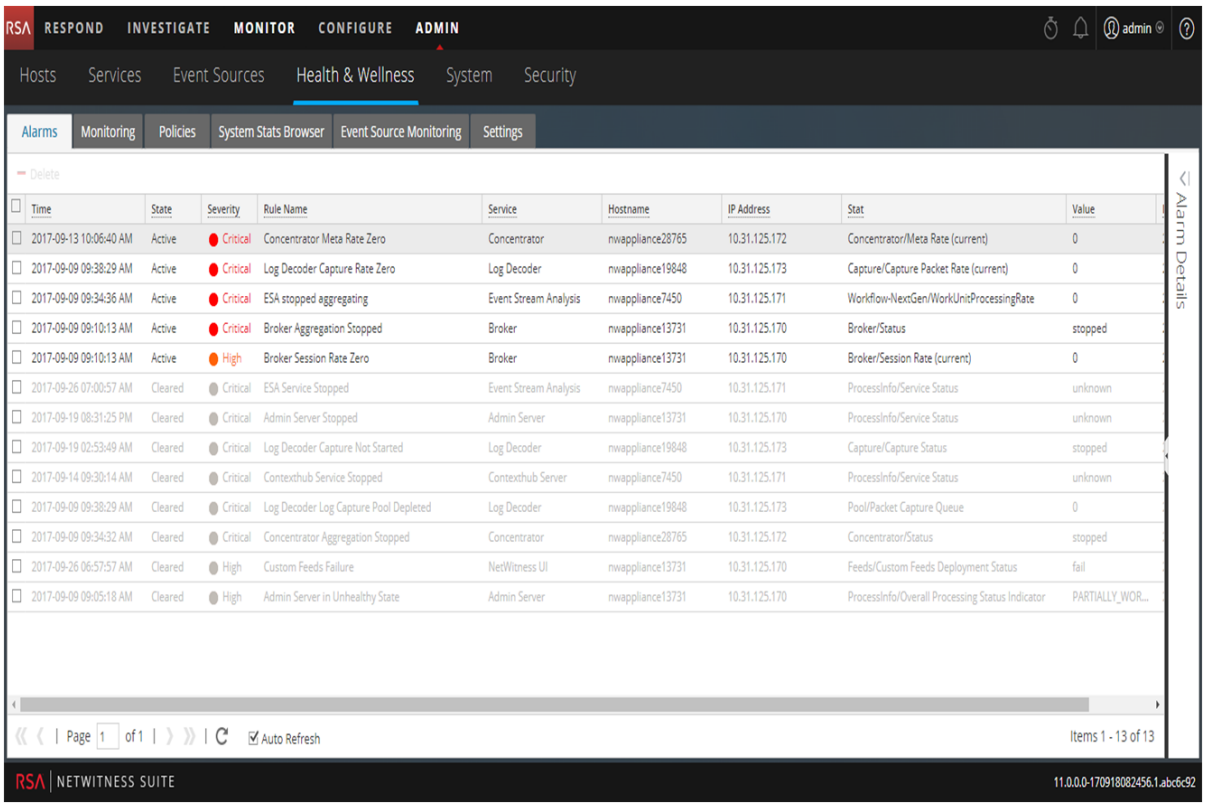
Vous pouvez configurer les alarmes et les surveiller dans l'interface Intégrité pour les hôtes et les services présents dans votre domaine NetWitness Suite. Les alarmes s'affichent dans la vue comme **Active** lorsque les seuils statistiques définis par les règles pour les hôtes et les services ont été franchis. Les alarmes sont grisées et passent à l'état **Effacée** lorsque le seuil d'effacement a été franchi.

Vous configurez les paramètres des alarmes dans Gérer les règlesGérer les règles Pour consulter la rubrique référencée associée, reportez-vous à Vue Intégrité - Vue Alarmes.

Pour surveiller les alarmes configurées dans NetWitness Suite :

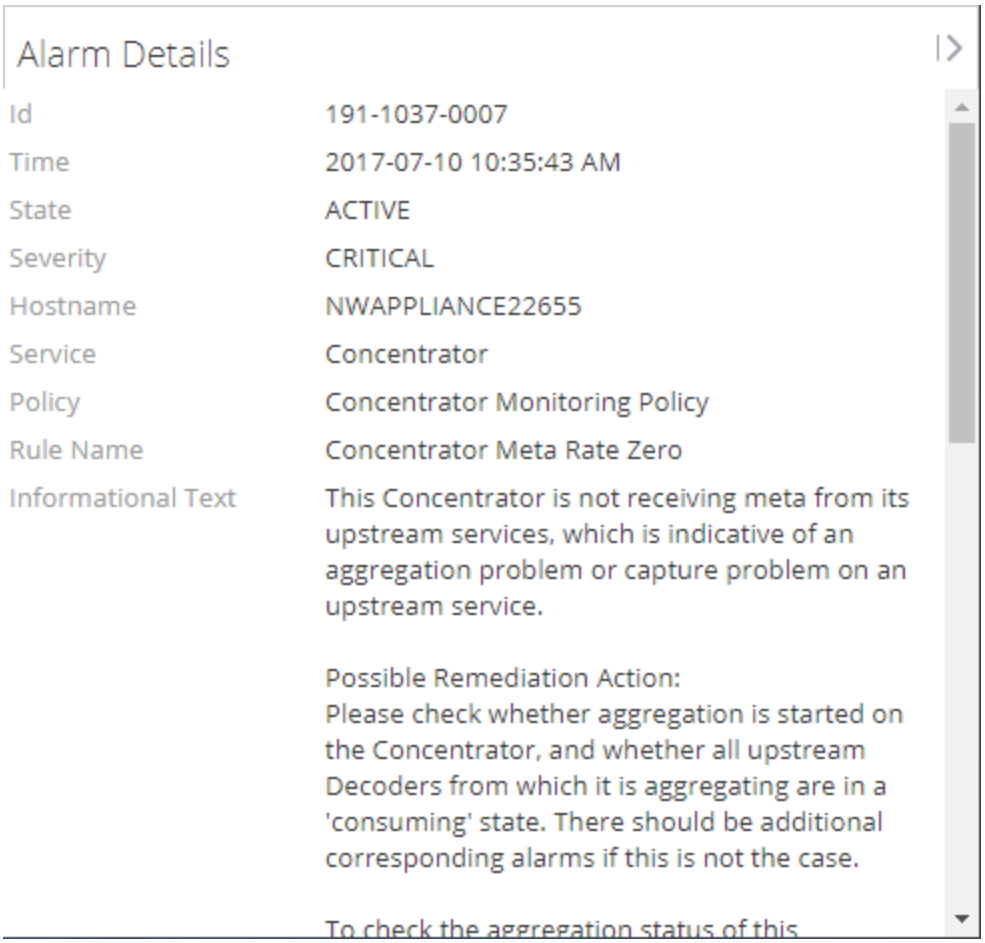
1. Accédez à **Administrateur > Intégrité**.

   Par défaut, la vue Intégrité s'affiche avec l'onglet Alarmes ouvert.



2. Cliquez sur l'alarme dont vous souhaitez afficher les détails dans le panneau Détails.

3. Cliquez sur  (Développer) pour afficher les détails de l'alarme que vous avez sélectionnée.



Surveiller l'intégrité à l'aide des alertes SNMP

Vous pouvez surveiller un composant Serveur NetWitness en utilisant une alerte de manière proactive grâce au protocole SNMP (Simple Network Management Protocol) basé sur les seuils ou les pannes du système.

Vous pouvez surveiller ce qui suit pour les composants NetWitness Suite :

- Utilisation du CPU qui atteint un seuil défini.
- Utilisation de mémoire qui atteint un seuil défini.
- Utilisation du disque qui atteint un seuil défini.

SNMP Configuration

Les Serveur NetWitness peuvent être configurés pour envoyer des traps de seuil et des traps de surveillance SNMPv3. Les traps de seuils sont envoyés en conjonction avec les seuils de nœuds configurés par les applications NetWitness Suite Core elles-mêmes. Les traps de surveillance sont envoyés par le processus SNMP lui-même pour les éléments indiqués dans son fichier de configuration. Le client doit configurer le processus SNMP sur un autre service pour recevoir les traps SNMP à partir de NetWitness Suite. Vous pouvez configurer le processus SNMP sur NetWitness Suite lors de la configuration de Serveur NetWitness. Pour plus d'informations, reportez-vous à la section **Paramètres de configuration des services** dans le *NetWitness SuiteGuide de mise en route des hôtes et des services* concernant l'hôte spécifique.

Seuils

Les seuils peuvent être définis dans les statistiques de service qui acceptent le message setLimit. Vous pouvez récupérer les seuils en cours à l'aide du message getLimit. Pour définir une limite, vous pouvez utiliser une valeur de seuil inférieure ou supérieure.

Lorsque la valeur des statistiques dépasse le seuil inférieur ou supérieur, une trap SNMP est déclenchée indiquant que le seuil est dépassé. La trap n'est pas déclenchée si la valeur est inférieure ou supérieure à celle définie, mais une autre trap est déclenchée si la valeur revient à la normale (au-dessus de la valeur inférieure et en dessous de la valeur supérieure).

Vous devez définir le seuil pour le service à l'aide de la vue Explorer les services ou de l'API REST.

Voici un exemple de seuil pour la surveillance de l'utilisation du CPU (inférieure à 10 % ou supérieure à 90 %) :

```
/sys/stats/cpu setLimit low=10 high=90
```

Voici un exemple de définition du seuil à l'aide de l'API REST :

```
http://<log decoder>:50102/sys/stats/cpu?msg=setLimit&low=10&high=90
```

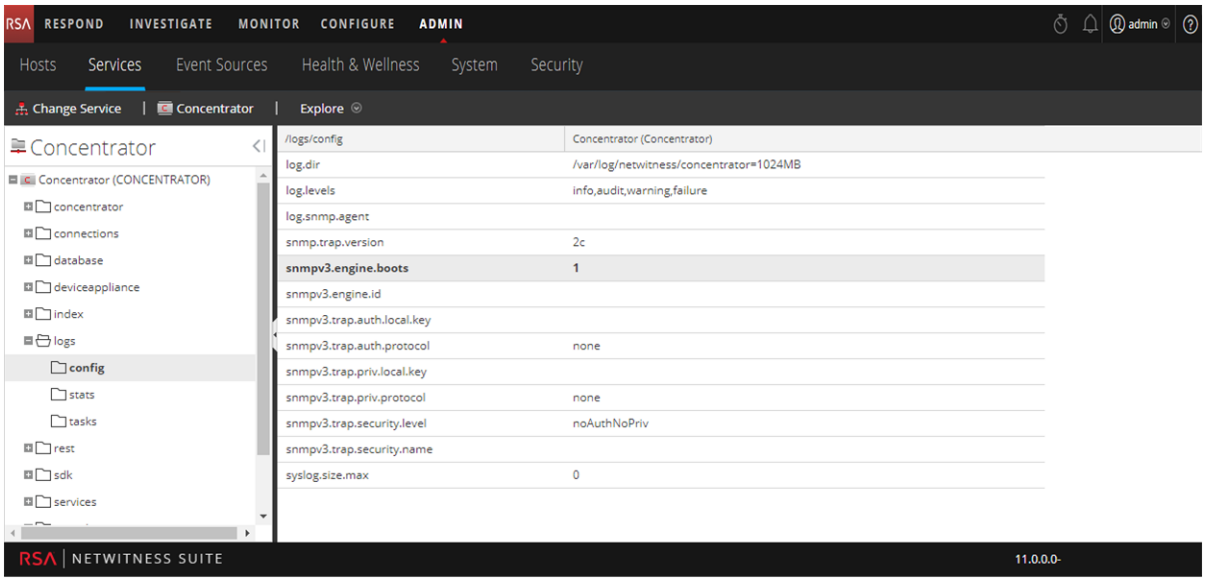
Si l'utilisation du CPU atteint 90 % ou plus, une trap SNMP est générée :

```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu
old=77% new=91
```

Configurer SNMPv3 pour un hôte

1. Accédez à **Administrateur > Services**.
   La vue Services s'affiche.
2. Sélectionnez le service.
3. Dans la colonne Actions, sélectionnez **Vue > Explorer**.
4. Dans la liste des nœuds, développez la liste et sélectionnez le dossier config. Par exemple, log > config

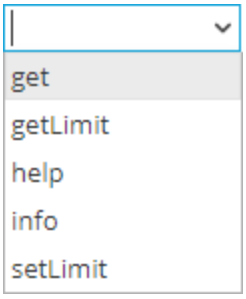
5. Définissez la configuration SNMPv3.



Définir le seuil d'un service

1. Accédez à **Administrateur > Services**.
   La vue Services s'affiche.
2. Sélectionnez le service.
3. Dans la colonne Actions, sélectionnez **Vue > Explorer**.
4. Dans la liste des nœuds, développez la liste et sélectionnez le dossier stats.
5. Sélectionnez par exemple, cpu, puis cliquez dessus avec le bouton droit de la souris.
6. Dans le menu déroulant, sélectionnez **Propriétés**.

   Le panneau Propriétés s'affiche : Le volet Propriétés est doté d'une liste déroulante de messages disponibles pour le paramètre.



7. Sélectionnez setLimit.
8. Spécifiez les valeurs inférieure et supérieure.

Résolution des problèmes liés à l'intégrité

Problèmes communs à tous les hôtes et services

Vous pouvez voir des statistiques erronées dans l'interface Intégrité si :

- certains ou l'ensemble des hôtes et des services ne sont pas correctement provisionnés et activés ;
- votre déploiement repose sur plusieurs versions (c'est-à-dire que les hôtes sont mis à jour vers différentes versions de NetWitness Suite) ;
- les services de support ne sont pas en cours d'exécution.

Problèmes identifiés par des messages dans l'interface ou par des fichiers logs

Cette section fournit des informations de dépannage pour les problèmes identifiés par des messages que NetWitness Suite affiche dans l'interface Intégrité ou inclut dans les fichiers log d'intégrité.

Message	Interface utilisateur : **Impossible de se connecter au service de gestion du système**
	Logs du service de gestion du système :
	
	`Caught an exception during connection recovery!`
	`java.io.IOException`
	`at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:106)`
	`at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:102)`
	`at com.rabbitmq.client.impl.AMQConnection.start (AMQConnection.java:346)`
	`at com.rabbitmq.client.impl.recovery.RecoveryAwareAMQConnectionFactory.newConnection(RecoveryAwareAMQConnectionFactory.java:36)`

```
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
recoverConnection(AutorecoveringConnection.java:388)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
beginAutomaticRecovery(AutorecoveringConnection.java:360)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.acc
ess$000(AutorecoveringConnection.java:48)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection$1.
shutdownCompleted(AutorecoveringConnection.java:345)
 at
com.rabbitmq.client.impl.ShutdownNotifierComponent.notifyListe
ners(ShutdownNotifierComponent.java:75)
 at com.rabbitmq.client.impl.AMQConnection$MainLoop.run
(AMQConnection.java:572)
 at java.lang.Thread.run(Thread.java:745)
 Caused by: com.rabbitmq.client.ShutdownSignalException:
connection error
 at com.rabbitmq.utility.ValueOrException.getValue
(ValueOrException.java:67)
 at
com.rabbitmq.utility.BlockingValueOrException.uninterruptibleG
etValue(BlockingValueOrException.java:33)
 at
com.rabbitmq.client.impl.AMQChannel$BlockingRpcContinuation.ge
tReply
(AMQChannel.java:343)
 at com.rabbitmq.client.impl.AMQConnection.start
(AMQConnection.java:292)
 ... 8 more
 Caused by: java.net.SocketException: Connection reset
 at java.net.SocketInputStream.read
```

	(SocketInputStream.java:189) at java.net.SocketInputStream.read (SocketInputStream.java:121) at java.io.BufferedInputStream.fill (BufferedInputStream.java:246) at java.io.BufferedInputStream.read (BufferedInputStream.java:265) at java.io.DataInputStream.readUnsignedByte (DataInputStream.java:288) at com.rabbitmq.client.impl.Frame.readFrom(Frame.java:95) at com.rabbitmq.client.impl.SocketFrameHandler.readFrame (SocketFrameHandler.java:139) at com.rabbitmq.client.impl.AMQConnection$MainLoop.run (AMQConnection.java:532)
Cause probable	Le service RabbitMQ n'est pas en cours d'exécution sur Serveur NetWitness.

Solution	Redémarrez le service RabbitMQ, SMS et les services NetWitness Suite avec les commandes suivantes.
	`systemctl restart rabbitmq-server`
	`systemctl restart rsa-sms`
	`systemctl restart jetty`

Message/ Problème	Interface utilisateur : **Impossible de se connecter au service de gestion du système**
Cause	Le service de gestion du système, le service RabbitMQ ou le service Mongo n'est pas en cours d'exécution.
Solution	Exécutez les commandes suivantes sur le serveur Serveur NetWitness pour vérifier que ces services sont en cours d'exécution. `[root@nwserver ~]# systemctl status rsa-sms`

	RSA NetWitness SMS :: Server is not running. [root@nwserver ~]# systemctl start rsa-sms Starting RSA NetWitness SMS :: Server... [root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is running (5687). [root@nwserver ~]# systemctl status mongod mongod (pid 2779) is running... systemctl status rabbitmq-server Status of node nw@localhost ... [{pid,2501}, {running_applications, [{rabbitmq_federation_management,"RabbitMQ Federation Management", "3.3.4"},

Message/ Problème	Interface utilisateur : **Impossible de se connecter au service de gestion du système**
Cause probable	L'utilisation de la partition `/var/lib/rabbitmq` est de 70 % ou plus.
Solution	Contactez le Support Clients.

Message/ Problème	Interface utilisateur : **Échec de la migration d'hôte.**
Cause probable	Un ou plusieurs services NetWitness Suite peuvent se trouver à l'état **arrêté**.
Solution	Assurez-vous que les services suivants sont en cours d'exécution, puis redémarrez Serveur NetWitness : Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, serveur Répondre, IPDB Extractor, Log Collector, Log Decoder, Malware

	Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problème	Interface utilisateur : **serveur indisponible.**
Cause probable	Un ou plusieurs services NetWitness Suite peuvent se trouver à l'état **arrêté**.
Solution	Assurez-vous que les services suivants sont en cours d'exécution, puis redémarrez Serveur NetWitness : Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, serveur Répondre, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Message/ Problème	Interface utilisateur : **Serveur non disponible**
Cause probable	Le service de gestion du système, le service RabbitMQ ou le service Mongo n'est pas en cours d'exécution.

Solution 1	Exécutez les commandes suivantes sur le serveur Serveur NetWitness pour vérifier que ces services sont en cours d'exécution.
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is not running.`
	`[root@nwserver ~]# systemctl start rsa-sms`
	`Starting RSA NetWitness SMS :: Server...`
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is running (5687).`
	`[root@nwserver ~]# systemctl status mongod`
	`mongod (pid 2779) is running...`
	`systemctl status rabbitmq-server`
	`Status of node nw@localhost ...`
	`[{pid,2501},`

	{running_applications, [{rabbitmq_federation_management,"RabbitMQ Federation Management", "3.3.4"},
Solution 2	Vérifiez que la partition /var/lib/rabbitmq est à moins de 75 % de sa capacité maximale.
Solution 3	Consultez les erreurs liées aux fichiers log Serveur NetWitness (var/lib/netwitness/uax/logs/nw.log).

Message/ Problème	ContextHub s'arrête et ne permet pas d'ajouter ou de modifier des sources de données et des listes.
Cause probable	Le stockage est rempli à 95 % ou plus.
Solution 1	Augmentez l'espace de stockage en mettant à jour le fichier YML, situé à l'emplacement /etc/netwitness/contexthub-server/contexthub-server.yml. Par exemple, pour augmenter l'espace de stockage de 120 à 150 Go, saisissez une valeur (en octets) en modifiant le paramètre approprié : rsa.contexthub.data.disk-size: 161061273600
Solution 2	Supprimez une longue liste indésirable ou inutilisée.
Solution 3	Configurer l'index TTL de la liste pour supprimer automatiquement les données STIX et TAXI, nettoyant ainsi l'espace de stockage.

Message/ Problème	Context Hub s'exécute sur une mémoire morte et 50 % sont réservés pour le cache. Lorsque le cache est rempli à 100 %, la réponse du cache s'arrête. Pour toutes les nouvelles recherches, les temps de réponse seront ralentis.
Cause probable	Le cache est rempli à 50 % ou plus.
Solution 1	Par défaut, Context Hub nettoie le cache toutes les 30 minutes. Réduisez le

	délai d'expiration du cache des sources de données.
Solution 2	Désactivez le cache pour les sources de données.
Solution 3	Augmentez la mémoire RAM du processus CH Java en modifiant l'option -Xmx disponible dans le fichier /etc/netwitness/contexthub-server/contexthub-server.conf. Dans JAVA_OPTS, recherchez l'option -Xmx. Par exemple, modifiez l'entrée comme suit : -Xmx8G où 8G représente 8 Go d'espace. Redémarrez ensuite le service Context Hub. **Remarque :** La mémoire est inférieure à la mémoire système disponible. N'oubliez pas qu'il y a beaucoup d'autres services s'exécutant sur l'hôte.

Message/ Problème	La source de données de liste affiche des statistiques ou un état non opérationnel.
Cause probable 1	Il est impossible de : • accéder à la source de données • analyser ou lire un fichier CSV • afficher un schéma correspondant au fichier CSV
Cause probable 2	L'authentification est impossible lors de l'accès à la source de données.
Solution 1	Veillez à enregistrer le fichier CSV au bon emplacement, par exemple /var/lib/netwitness/contexthub-server/data/ et à vérifier les autorisations de lecture requises.
Solution 2	Assurez-vous que le schéma de fichier CSV spécifié pendant la configuration de la source de données correspond. Dans le cas contraire, créez une nouvelle source de données avec un nouveau schéma, ou modifiez le fichier CSV afin qu'il corresponde au schéma. Par exemple, admettons que vous configurez une Source de données de liste avec un schéma comportant column1, column2 et column3. Lors de la prochaine mise à jour du fichier CSV, le nombre de colonnes augmente ou diminue,

Solution 3	ou l'ordre des colonnes est modifié. Dans ce cas, le schéma ne correspond plus et la source de données de liste configurée s'affichera comme étant « non opérationnelle » dans les statistiques d'Intégrité.
	Assurez-vous que le mot de passe est correct. Pour confirmer la modification de la source de données, entrez le mot de passe et cliquez sur Tester la connexion. Pour plus d'informations liées aux solutions ci-dessus, reportez-vous à la rubrique Configurer des listes en tant que sources de données dans le *Guide de Configuration de Context Hub*.

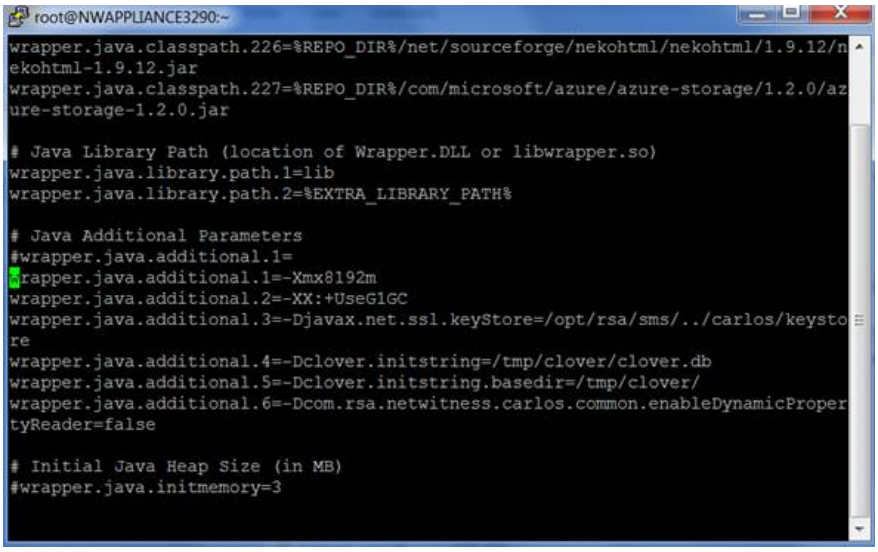
Problèmes non identifiés par l'interface utilisateur ou les logs

Cette section fournit des informations de dépannage pour les problèmes non identifiés par des messages que NetWitness Suite affiche dans l'interface Intégrité ou inclut dans les fichiers log d'Intégrité. Par exemple, vous pouvez voir des statistiques incorrectes dans l'interface.

Problème	Statistiques incorrectes affichées dans l'interface Intégrité.
Cause probable	Le service SMS n'est pas en cours d'exécution. Le service SMS doit être en cours d'exécution sur Serveur NetWitness.
Solution	Redémarrez le service SMS.

Problème	NetWitness Suite n'affiche pas la version vers laquelle vous avez mis à niveau tant que vous n'avez pas redémarré jettysrv (serveur jeTTy).
Cause probable	Lorsque NetWitness Suite vérifie une connexion, il interroge un service toutes les 30 secondes pour voir s'il est actif. Durant ces 30 secondes, si le service est à nouveau opérationnel, il ne recevra pas la nouvelle version.
Solution	1. Arrêtez le service manuellement. 2. Attendez qu'il passe hors ligne. 3. Redémarrez le service. NetWitness Suite affiche la version correcte.

Problème	Serveur NetWitness n'affiche pas la page **Service non disponible**.
Cause probable	Après avoir effectué la mise à niveau vers NetWitness Suite version 10.5, JDK 1.8 n'est pas la version par défaut et le jettysrv (serveur jeTTy) ne parvient pas à démarrer. Sans le serveur jeTTy, le serveur NetWitness Suite ne peut pas afficher la page **Service non disponible**.
Solution	Redémarrez jettysrv.

Problème	Le service SMS est arrêté et le message d'erreur suivant s'affiche dans le fichier log : `java.lang.OutOfMemoryError: Java heap space`
Solution	Vous pouvez utiliser la solution suivante afin d'augmenter la quantité de mémoire en fonction de vos besoins. 1. Ouvrez /opt/rsa/sms/conf/wrapper.conf  2. Remplacez `wrapper.java.additional.1=-Xmx8192m` par : `wrapper.java.additional.1=-Xmx16g` 3. Redémarrez le service SMS : `systemctl start rsa-sms`

Gestion des mises à jour de NetWitness Suite

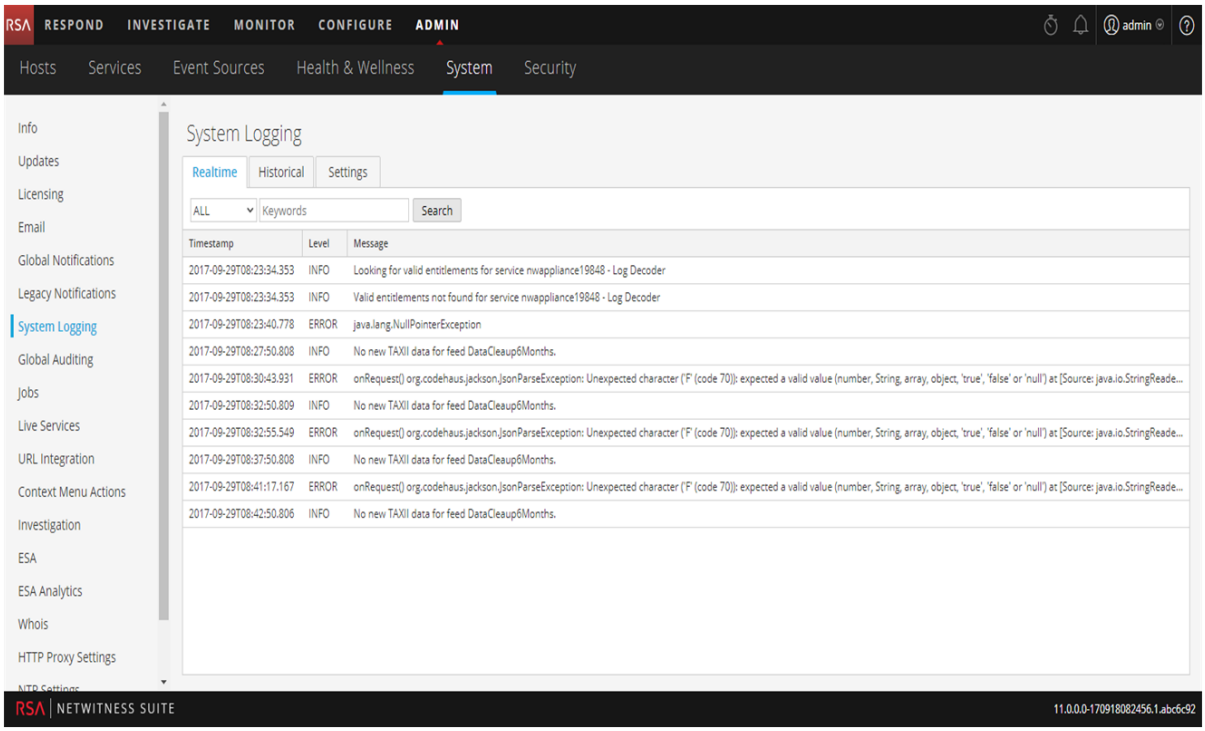
RSA publie régulièrement des mises à jour de la version du logiciel NetWitness Suite, dans le but d'améliorer en permanence le produit. Une mise à jour de version logicielle comprend une version, un service pack ou un correctif (y compris le correctif de sécurité) et un logiciel connexe dont dépend la version, le service pack ou le correctif. Des guides d'utilisation sont fournis pour chaque mise à jour de version du logiciel, ce qui inclut les étapes détaillées pour l'installation de la mise à jour. Il est important de télécharger le guide de mise à jour de la version à partir de RSA Link (https://community.rsa.com/community/products/netwitness) et de suivre les étapes qui y sont décrites. Des informations complémentaires sont disponibles dans la rubrique « Mettre à jour l'hôte vers une nouvelle version » dans le *Guide de mise en route des hôtes et des services* et le Panneau Mises à jour système - Onglet Paramètres.

Affichage des logs système et des logs de services

NetWitness Suite fournit des vues des logs système et des logs de service. Lorsque vous affichez les logs de service, vous pouvez également sélectionner des messages pour le service ou l'hôte.

Afficher les logs système

1. Accédez à **Administrateur > Système**.
2. Dans le panneau des options, sélectionnez **Consignation système**.

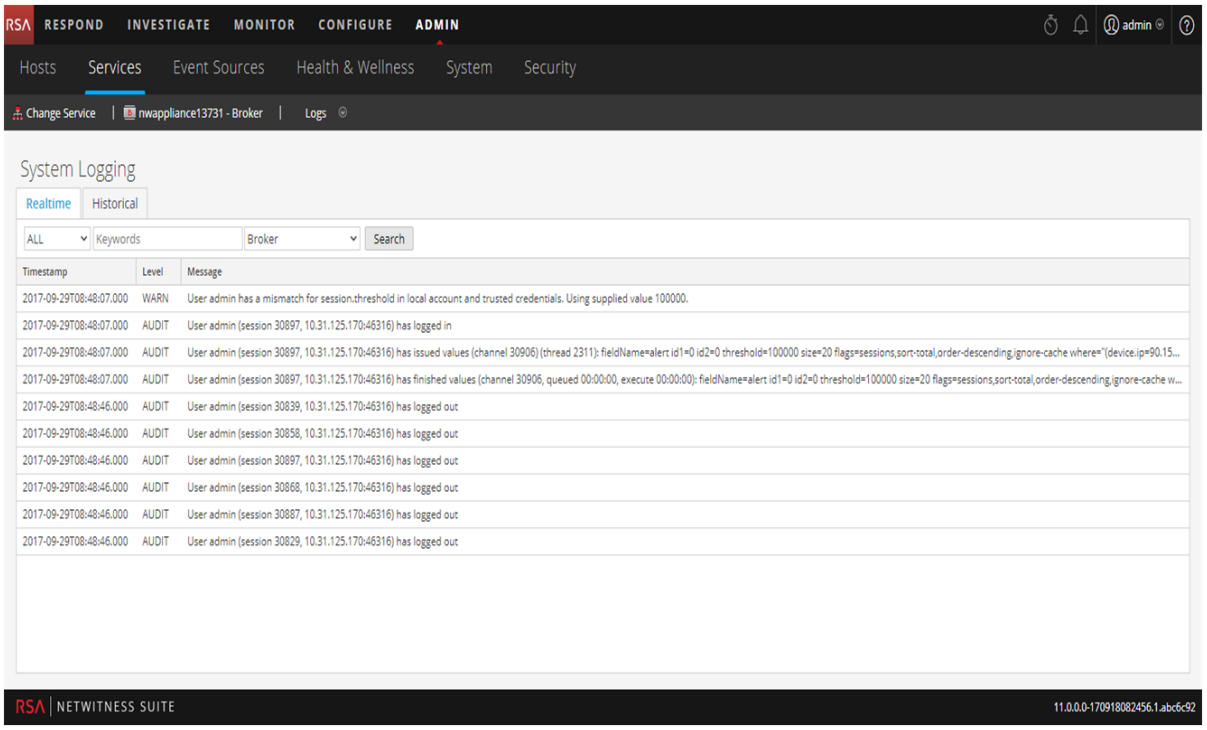


Afficher les logs de service

Pour afficher les logs de service NetWitness Suite :

1. Accédez à **Administrateur > Services**.
2. Dans la grille **Services**, sélectionnez un service.

3. Dans la colonne **Actions**, sélectionnez **Vue > Logs**.



Filtrer les entrées de log

Pour filtrer les résultats affichés sous l'onglet En temps réel :

1. (Facultatif) Pour les logs de système et de service, sélectionnez le **Niveau du log** et un **Mot clé**, ou les deux. Les logs système disposent de sept niveaux de consignation. Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. La valeur par défaut est **TOUTES** les entrées de log.
2. (Facultatif) Pour les logs de service, sélectionnez le service : hôte ou service.
3. Cliquez sur **Filtre**.

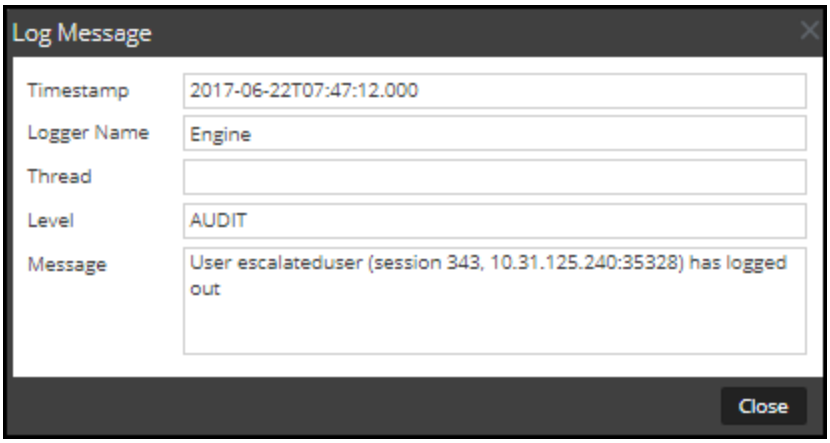
   La vue est réinitialisée avec les 10 entrées les plus récentes qui correspondent à votre filtre. Alors que de nouvelles entrées de log correspondantes deviennent disponibles, la vue est mise à jour pour afficher ces entrées.

Afficher les détails d'une entrée de log

Chaque ligne de la grille de log sous l'onglet En temps réel propose des informations de synthèse sur l'entrée de log. Pour afficher les détails complets :

1. Cliquez deux fois sur une entrée de log.

   La boîte de dialogue **Message log**, qui contient l'horodatage, le nom de l'enregistreur, le thread, le niveau et le message s'affiche.



2. Après la consultation, cliquez sur **Fermer**.

Accéder au fichier log de Reporting Engine

Tous les fichiers log

Le Reporting Engine stocke les fichiers log suivants dans le répertoire **rsasoc/rsa/soc/reporting-engine/log** :

- Fichiers log actuels du fichier **reporting-engine.log**.
- Copies de sauvegarde des fichiers log précédents du fichier **reporting-engine.log.***.
- Tous les fichiers log de script UNIX dans les fichiers ayant la syntaxe suivante : **reporting-engine.sh_*timestamp*.log** (par exemple, **reporting-engine.sh_20120921.log**).

Le Reporting Engine écrit rarement des messages d'erreur de ligne de commande dans le fichier **rsasoc/nohup.out** .

Logs upstart

Le Reporting Engine ajoute les messages log, la sortie de log écrits par upstart daemon et les commandes utilisées pour démarrer le Reporting Engine dans le répertoire **/var/log/secure**.

Le fichier log upstart est un fichier log système. Seul l'utilisateur root peut donc le lire. Le Reporting Engine génère les fichiers log, conserve des copies de sauvegarde des fichiers log précédents, stocke les fichiers log de script UNIX et ajoute les fichiers log upstart à un autre répertoire.

Rechercher et exporter des logs d'historique

NetWitness Suite fournit une vue du log NetWitness Suite dans laquelle une recherche peut être effectuée, ou le log de service dans un format paginé. Lors du chargement initial, la grille affiche la dernière page des entrées de log pour le système ou le service. Vous pouvez exporter des logs à partir de la vue en cours.

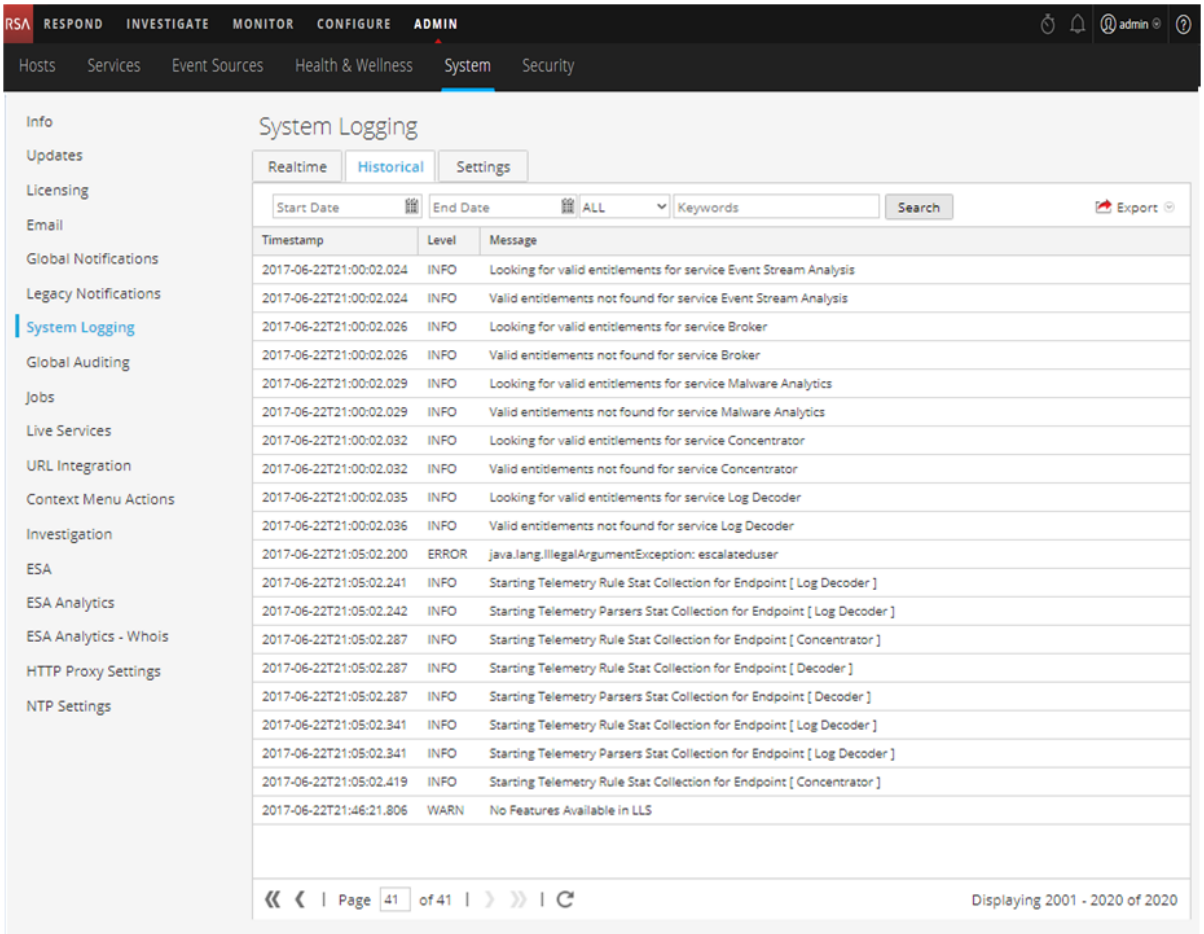
Afficher le log de système historique

Pour afficher le log historique pour le système :

1. Accédez à **Administrateur > Système**.
2. Dans le panneau des options, sélectionnez **Consignation système**.

   Le panneau Consignation système s'ouvre sur l'onglet En temps réel par défaut.
3. Cliquez sur l'onglet **Historique**.

   Une liste des logs historiques pour le système s'affiche.



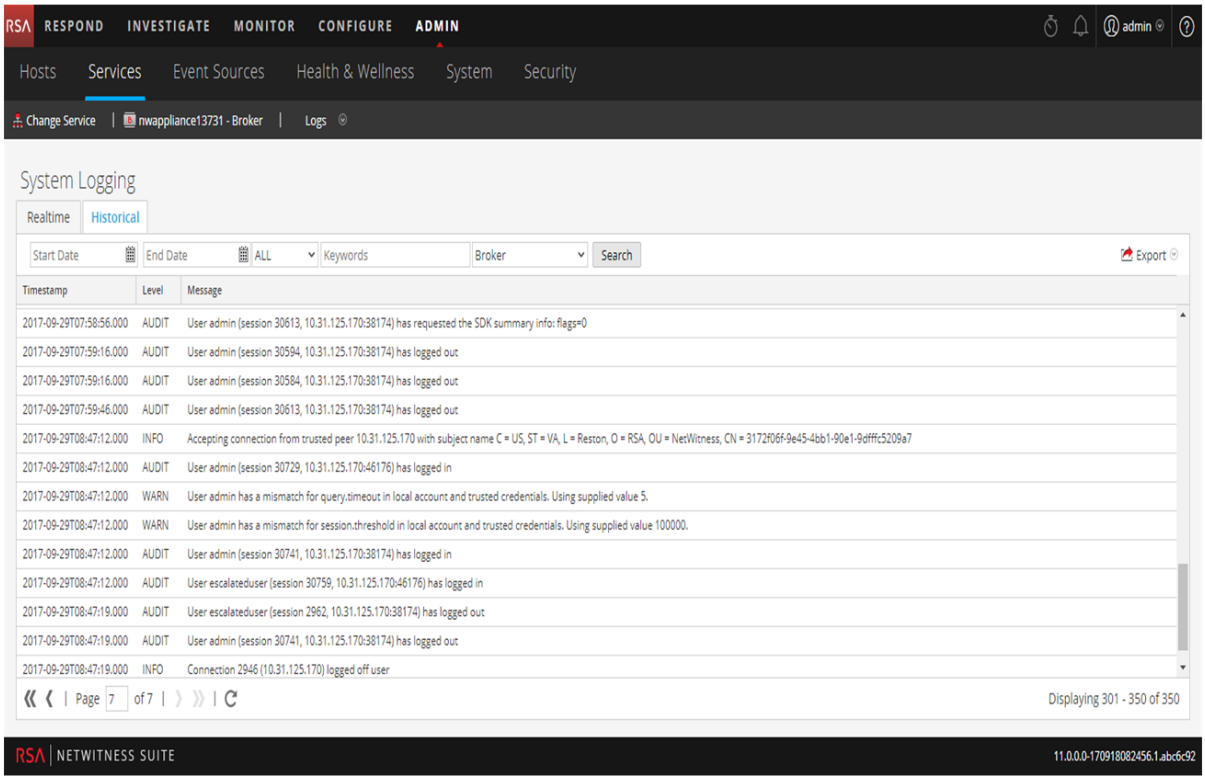
Afficher un log de service historique

Pour afficher le log historique pour les services :

1. Sélectionnez **Administrateur > Services**.
2. Sélectionnez un service.
3. Dans la colonne **Actions**, sélectionnez **Vue > Logs**.

   La vue Logs de service s'ouvre sur l'onglet En temps réel.
4. Cliquez sur l'onglet **Historique**.

   Une liste des logs historiques pour le service sélectionné s'affiche.



Rechercher les entrées de log

Pour rechercher les résultats affichés sous l'onglet **Historique** :

1. (Facultatif) Sélectionnez une **Date de début** et une **Date de fin**. Éventuellement, sélectionnez une **Heure de début** et une **Heure de fin**.
2. (Facultatif) Pour les logs de système et de service, sélectionnez le **Niveau du log** et un **Mot clé**, ou les deux. Les logs système disposent de sept niveaux de consignation. Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. La valeur par défaut est **TOUTES** les entrées de log.
3. (Facultatif) Pour les logs de service, sélectionnez le Service : hôte ou service.

4. Cliquez sur **Rechercher**.

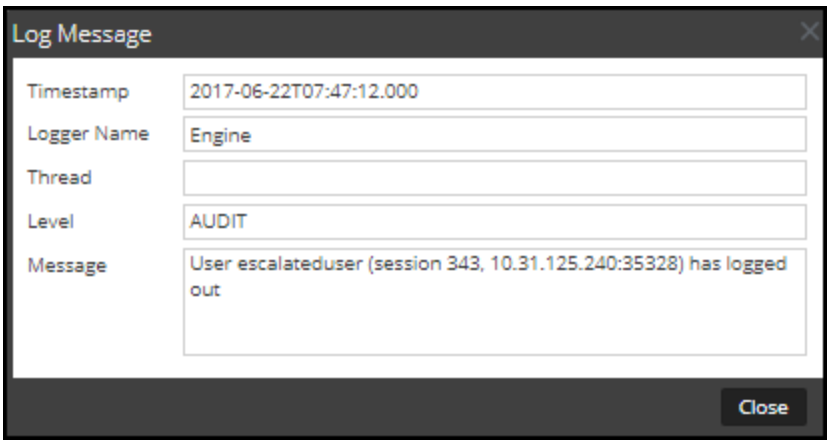
   La vue est réinitialisée avec les 10 entrées les plus récentes qui correspondent à votre filtre. Alors que de nouvelles entrées de log correspondantes deviennent disponibles, la vue est mise à jour pour afficher ces entrées.

Afficher les détails d'une entrée de log

Chaque ligne de la grille de log sous l'onglet **Historique** propose des informations de synthèse sur l'entrée de log. Pour afficher tous les détails pour un message de log :

1. Cliquez deux fois sur une entrée de log.

   La boîte de dialogue **Message log**, qui contient l'horodatage, le nom de l'enregistreur, le thread, le niveau et le message, s'affiche.



2. Après la consultation, cliquez sur **Fermer**.

   La boîte de dialogue se ferme.

Parcourir les entrées de log

Pour parcourir les différentes pages de la grille, utilisez les commandes de pagination en bas de la grille, comme suit :

- Utilisez les boutons de navigation
- Saisissez manuellement le nombre de pages que vous souhaitez afficher, puis appuyez sur **ENTRÉE**.

Exporter un fichier log

Pour exporter les logs dans la vue actuelle :

Cliquez sur **Exporter**, et sélectionnez l'une des options de la liste déroulante : **Format CSV** ou **Séparé par des tabulations**.

Le fichier est téléchargé avec un nom de fichier qui identifie le type de log et le séparateur de champ. Par exemple, un log système NetWitness Suite exporté avec des valeurs séparées par des virgules est nommé **UAP_log_export_CSV.txt**, et un log hôte exporté avec des valeurs séparées par des tabulations est nommé **APPLIANCE_log_export_TAB.txt**.

Gestion des requêtes à l'aide de l'intégration d'URL

L'intégration d'une URL permet de représenter le chemin de navigation ou le chemin de requête utilisé lors de la recherche active d'un service dans la vue Navigation. Vous n'avez pas besoin d'afficher ni de modifier ces objets souvent.

L'intégration d'une URL permet d'effectuer le mappage à un ID unique qui est automatiquement créé chaque fois que vous cliquez sur un lien de navigation dans la vue Navigation pour effectuer une recherche verticale parmi les données. À la fin de la recherche verticale, l'URL reflète les ID de requête du point de recherche verticale. Le Nom d'affichage s'affiche dans le chemin de navigation, dans la vue Navigation.

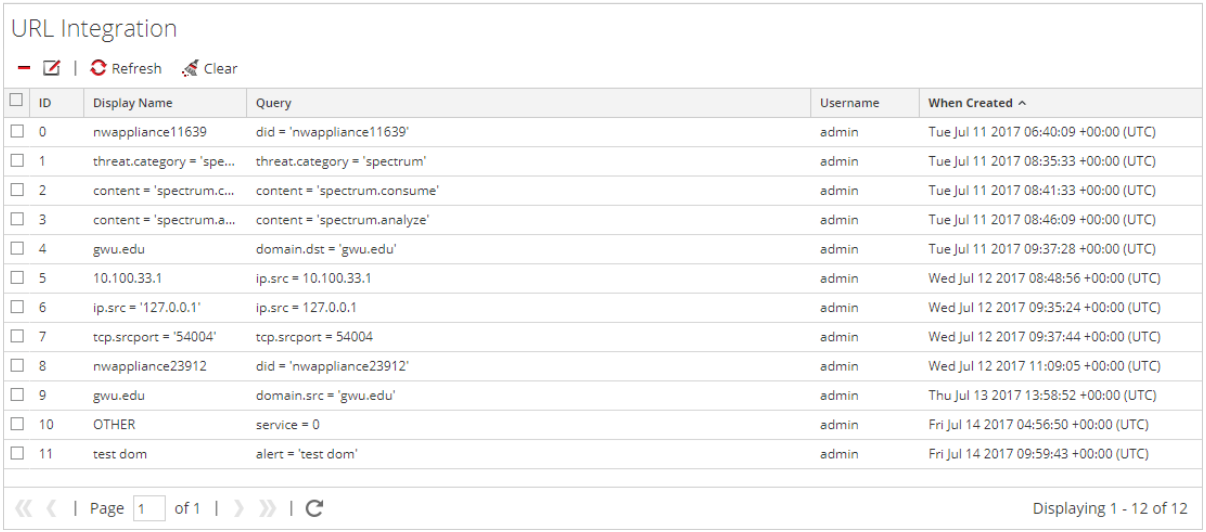
Le panneau **Intégration d'URL** fournit la liste des requêtes et permet aux utilisateurs disposant des autorisations appropriées de modifier cette source de données sous-jacente et d'analyser les modèles de requête des autres utilisateurs du système NetWitness Suite. Le panneau vous permet d'effectuer les opérations suivantes :

- Actualiser la liste.
- Modifier une requête.
- Supprimer une requête.
- Effacer toutes les requêtes de la liste.

Attention : Lorsqu'une requête est supprimée du système, les URL d'Investigation comprenant l'ID de cette requête ne fonctionnent plus.

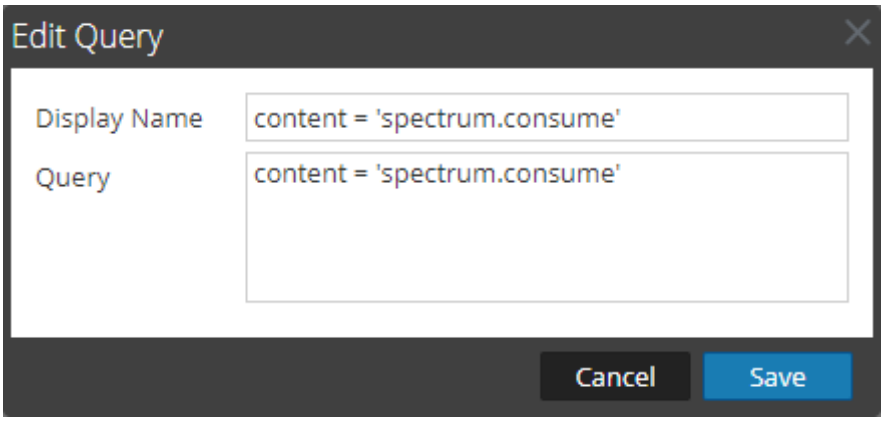
Modifier une requête

1. Accédez à **Administrateur > Système**.
2. Dans le panneau des options, sélectionnez **Intégration d'URL**.



3. Sélectionnez la ligne dans la grille et double-cliquez sur la ligne ou cliquez sur .

   La boîte de dialogue **Modifier la requête** s'affiche.



4. Modifiez les champs **Nom d'affichage** et **Requête**, mais ne laissez aucun champ vide.
5. Pour enregistrer les modifications, cliquez sur **Enregistrer**.

Supprimer une requête

Attention : Lorsqu'une requête est supprimée du système, les URL d'Investigation comprenant l'ID de cette requête ne fonctionnent plus.

Pour supprimer entièrement une requête à partir de NetWitness Suite :

1. Sélectionnez la requête.
2. Cliquez sur

Une boîte de dialogue vous demande de confirmer que vous souhaitez bien supprimer la requête.

3. Cliquez sur **Oui**.

Effacer toutes les requêtes

Pour effacer toutes les requêtes de la liste :

- Cliquez sur 

  La liste entière est effacée.

Utiliser une requête dans un URI

La fonction Intégration d'URL facilite les intégrations aux produits tiers en permettant d'effectuer une recherche en fonction de l'architecture NetWitness Suite. En utilisant une requête dans un URI, vous pouvez pivoter directement d'un produit qui autorise les liens personnalisés vers un point de recherche verticale spécifique dans la vue Investigation de NetWitness Suite.

Le format de saisie d'un URI à l'aide d'une requête chiffrée au format URL est le suivant :

http://<nw host:port>/investigation/<serviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>

où

- **<nw host: port>** est l'adresse IP ou DNS, avec ou sans port, le cas échéant (SSL ou non). Cette désignation est nécessaire uniquement si l'accès est configuré sur un port non standard via un proxy.
- **<serviceId>** est l'ID de service interne dans l'instance de NetWitness Suite pour le service à interroger. L'ID de service ne peut être représenté que sous la forme d'un nombre entier. Vous pouvez visualiser l'ID de service approprié à partir de l'URL lors de l'accès à la vue Investigation au sein de NetWitness Suite. Cette valeur change en fonction du service auquel elle est connectée pour analyse.
- **<encoded query>** est la requête NetWitness Suite chiffrée au format URL. La longueur de la requête est limitée par les restrictions d'URL HTML.
- **<start date>** et **<end date>** définissent la période pour la requête. Le format est le suivant : <aaaa-mm-jj>H<hh:mm>. Les dates de début et de fin sont obligatoires. Les plages relatives (par exemple, Dernière heure) ne sont pas prises en charge dans cette version. Toutes les heures sont exécutées au format UTC.

Par exemple :
http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00/2012-10-31T00:00

Exemples

Voici des exemples de requêtes où le serveur Serveur NetWitness est 192.168.1.10 et où serviceID est identifié par la valeur 2.

Toute l'activité du 03/12/2013 entre 5h00 et 6h00 avec un nom d'hôte enregistré

- Custom Pivot: alias.host exists
- https://192.168.1.10/investigation/2...13-03-12T06:00

Toute l'activité du 03/12/2013 entre 17h00 et 17h10 avec trafic http vers et à partir de l'adresse IP 10.10.10.3

- Custom Pivot: service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- Encoded Pivot Dissected:
  - service=80 => service&3D80
  - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - https://192.168.1.10/investigation/2...13-03-12T17:10

Remarques supplémentaires

Certaines valeurs peuvent ne pas être chiffrées dans le cadre de la requête. Par exemple l'IP src et dst est utilisé pour ce point d'intégration. Dans le cas de l'exploitation d'une application tierce pour l'intégration de cette fonctionnalité, il est possible d'y faire référence sans appliquer de chiffrage.

Prise en charge de FIPS

NetWitness Suite 11.0 est fourni avec des modules de chiffrement FIPS 140-2 qui prennent en charge toutes les opérations de chiffrement dans NetWitness Suite. NetWitness Suite s'appuie sur deux modules qui prennent en charge une assurance conception de niveau 3 :

- RSA BSAFE Crypto-J
- OpenSSL avec BSAFE (OWB)

Les deux modules ont été certifiés compatibles avec un environnement opérationnel comparable à la configuration standard NetWitness Suite.

Par défaut, les modules de chiffrement imposent l'utilisation de suites de chiffrement certifiées FIPS dès que possible. Pour les exceptions, consultez les informations suivantes et les notes de mise à jour. Pour plus d'informations sur les modules FIPS, consultez http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Le numéro de certificat FIPS de RSA BSAFE Crtypo-J est 2468, et le certificat FIPS OWB est inclus dans RSA BSAFE Crypto-C Micro Edition avec un numéro de certificat de 2300.

Dans la version 11.0.0.0, FIPS est activé sur tous les services à l'exception du Log Collector. Cela inclut le Log Decoder et Decoder s'ils étaient compatibles avec FIPS dans la version 10.6.4.x. FIPS ne peut être désactivé sur aucun service à l'exception du Log Collector, Log Decoder et Decoder.

Remarque : Pour une nouvelle installation de la version 11.0.0.0, par défaut, tous les services Core utiliseront FIPS, à l'exception du Log Collector et Log Decoder. FIPS ne peut être désactivé sur aucun service à l'exception du Log Collector, Log Decoder et Packet Decoder.

Remarque : Pour les mises à niveau de la version 10.6.4.x à la version 11.0.0.0, les conditions suivantes s'appliquent pour les services Log Collector, Log Decoder et Decoder :
- FIPS n'est pas activé pour le service Log Collector après la mise à niveau vers la version 11.0.0.0, même s'il l'était dans la version 10.6.4.x. Vous devez activer la prise en charge FIPS après la mise à niveau vers la version 11.0.0.0. Reportez-vous aux instructions Prise en charge de FIPS pour les Log Collectors.
- Si FIPS a été activé pour les services Log Decoder et Packet Decoder dans la version 10.6.4.x, il reste activé dans la version 11.0.0.0. Toutefois, si FIPS n'est pas activé pour les services Log Decoder et Packet Decoder dans la version 10.6.4.x, il ne sera pas activé dans la version 11.0.0.0. Vous pouvez alors activer manuellement FIPS pour ces services si nécessaire. Reportez-vous aux instructions Prise en charge de FIPS pour les Log Decoders et Decoders.

Prise en charge de FIPS pour les Log Collectors

Pour activer FIPS pour les Log Collectors :

1. Arrêtez le service Log Collector.
2. Ouvrez le fichier `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Modifiez la valeur de la variable suivante en **off** comme décrit ici :
   `Environment="OWB_ALLOW_NON_FIPS=on"`
   devient
   `Environment="OWB_ALLOW_NON_FIPS=off"`
4. Rechargez le processus du système en exécutant la commande suivante :
   `systemctl daemon-reload`
5. Redémarrez le service Log Collector.
6. Définissez le mode FIPS pour le service Log Collector dans l'interface utilisateur :

   Remarque : Cette étape n'est pas requise si vous mettez à niveau de la version 10.6.4 à la version 11.0.0.0 et si FIPS a été activé dans la version 10.6.4.

   a. Accédez à **Administrateur** > **Services**.
   b. Sélectionnez le service Log Collector, puis accédez à **Vue** > **Config**.
   c. Dans le Mode SSL FIPS, cochez la case sous Valeur de configuration, puis cliquez sur **Appliquer**.

Prise en charge de FIPS pour les Log Decoders et Decoders

Pour activer FIPS pour les Log Decoders et Decoders pour lesquels le mode FIPS était désactivé dans la version 10.6.4.x :

1. Accédez à **Administrateur** > **Services** et sélectionnez un service Log Decoder ou Packet Decoder.
2. Sélectionnez **Vue** > **Config** puis, dans **Configuration système**, activez le **Mode SSL FIPS** en cochant la case dans la colonne **Valeur de configuration**.
3. Redémarrez le service.
4. Cliquez sur **Appliquer**.

Résoudre les problèmes de NetWitness Suite

Pour plus d'informations sur la résolution des problèmes liés à NetWitness Suite, consultez les rubriques suivantes :

- Informations de débogage
- Notification des erreurs
- Conseils divers
- NwLogPlayer
- Résoudre les problèmes liés aux feeds

Informations de débogage

NetWitness SuiteFichiers log

Les fichiers suivants contiennent des informations de log NetWitness Suite.

Composant	Fichier
rabbitmq	/var/log/rabbitmq/nw@localhost.log /var/log/rabbitmq/nw@localhost-sasl.log
collectd	/var/log/messages
nwlogcollector	/var/log/messages
nwlogdecoder	/var/log/messages
sms	/opt/rsa/sms/wrapper.log
sms	/opt/rsa/sms/logs/sms.log
sms	/opt/rsa/sms/logs/audit/audit.log
NetWitness Suite	/var/lib/netwitness/uax/logs/nw.log
NetWitness Suite	/var/lib/netwitness/uax/logs/ audit/audit.log
NetWitness Suite	/opt/rsa/jetty9/logs

Fichiers intéressants

Les fichiers suivants sont utilisés dans les principaux composants NetWitness Suite et peuvent être utiles lorsque vous essayez d'analyser divers problèmes.

Composant	Fichier	Description
rabbit	/etc/rabbitmq/rabbitmq.config	Fichier de configuration RabbitMQ. Ce fichier de configuration régit partiellement le comportement de RabbitMQ, notamment en ce qui concerne les paramètres réseau/SSL.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	Fichier de configuration d'environnement RabbitMQ. Ce fichier indique le nom du nœud RabbitMQ et l'emplacement du fichier des plug-in activés.
rabbit	/etc/rabbitmq/rsa_enabled_plugins	Ce fichier répertorie les plug-in activés dans RabbitMQ. Ce fichier est géré par le serveur RabbitMQ, via la commande rabbitmq-plugins. Ce fichier remplace le chemin /etc/rabbitmq/enabled_plugins afin de contourner les problèmes liés à la mise à niveau du Log Collector à partir des versions précédentes.

Composant	Fichier	Description
rabbit	/etc/rabbitmq/ssl/truststore.pem	Le magasin d'approbations RabbitMQ. Ce fichier contient une séquence de certificats x.509 au format d'encodage PEM, représentés par des AC de confiance. Tout client qui se connecte à RabbitMQ et présente un certificat signé par une AC de cette liste est considéré comme un client de confiance.

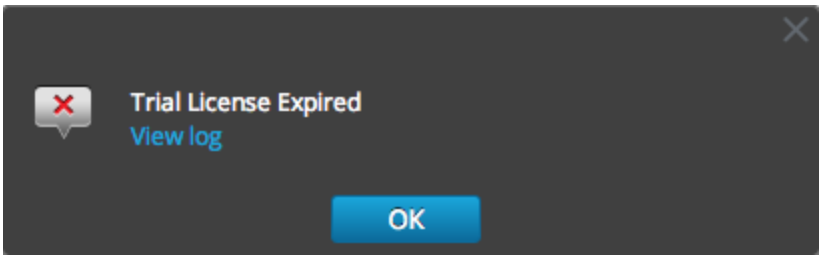
Composant	Fichier	Description
rabbit	/var/log/rabbitmq/mnesia/nw@localhost	Le répertoire Mnesia RabbitMQ. Mnesia est la technologie de base de données Erlang/OTP qui permet de stocker des objets Erlang de manière permanente. RabbitMQ utilise cette technologie pour stocker des informations telles que l'ensemble actuel de politiques, les files d'attente et les échanges permanents, etc. Plus important, les répertoires msg_store_persistent et msg_store_transient sont ceux dans lesquels RabbitMQ stocke les messages qui ont été mis en file d'attente sur le disque, par exemple, si des messages sont publiés en tant que messages permanents ou s'ils ont été paginés vers le disque à cause de limitations de la mémoire. Surveillez ce répertoire si des alarmes de disque ou de mémoire ont été déclenchées dans RabbitMQ. **Attention :** Ne supprimez pas ces fichiers manuellement. Utilisez les outils RabbitMQ pour purger ou supprimer des files d'attente. La modification manuelle de ces fichiers peut rendre votre

Composant	Fichier	Description
		instance RabbitMQ inopérable.

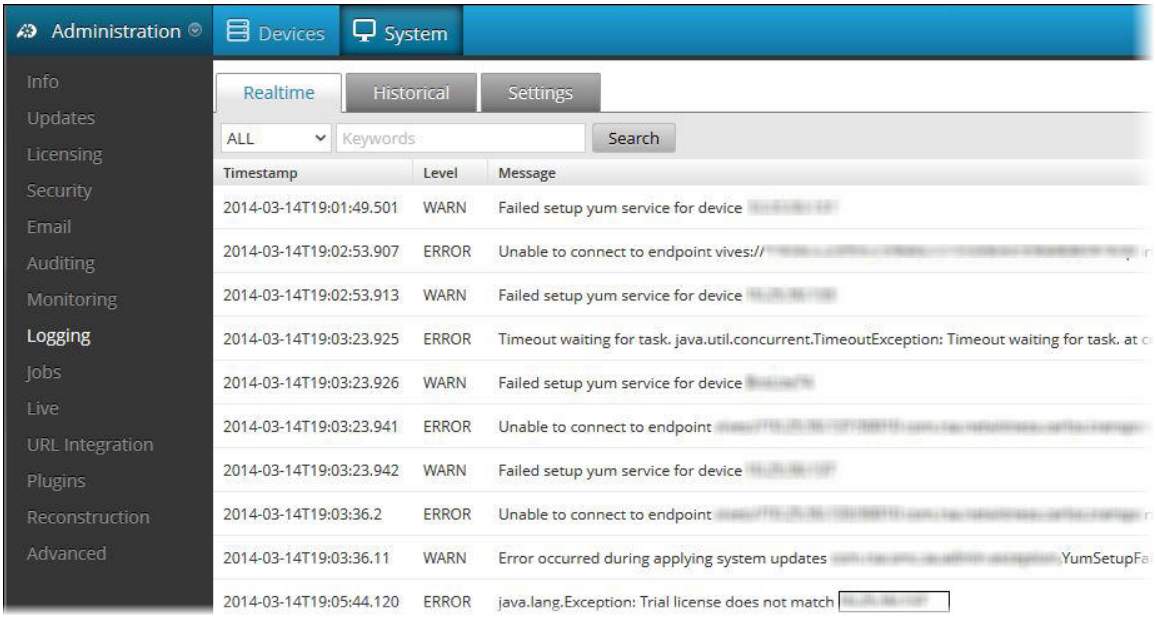
Notification des erreurs

NetWitness Suite possède un ensemble de types de messages d'erreur associées à différents composants et opérations. NetWitness Suite affiche les commentaires sous la forme d'une notification d'erreur simple et d'une entrée de log.

Lorsqu'une boîte de dialogue de notification d'erreur s'affiche, vous avez deux options : acquitter simplement le message ou afficher le log du système pour obtenir un complément d'informations.



Si vous souhaitez afficher le log du système pour obtenir un complément d'informations lors de l'affichage d'une notification d'erreur, cliquez sur **Afficher le log**. Le log s'ouvre dans la vue **Administration** > **Système** avec une liste de messages. L'horodatage et le niveau du message sont également mentionnés.



Conseils divers

Renforcer le compte administrateur

Le Guide du renforcement STIG présent dans la NetWitness SuiteDocumentation sur RSA Link (https://community.rsa.com/docs/DOC-64211) comprend ces informations.

Messages du log d'audit

Il peut être utile de voir quelles actions de l'utilisateur génèrent des types de messages logs dans le fichier de messages **/var/log/**.

La feuille de calcul des catégories d'événements incluses dans le package d'analyseurs de logs de l'archive NetWitness Suite Parser v2.0.zip répertorie les catégories d'événements et les lignes de l'analyseur d'événements pour faciliter la génération de rapports, d'alertes et de requêtes.

NwConsole pour Intégrité

RSA a ajouté la commande **logParse** à **NwConsole**. Cette commande prend en charge l'analyse de logs, une méthode permettant de vérifier l'analyseur de logs sans configurer l'intégralité du système pour l'analyse des logs. Pour plus d'informations sur la commande **logParse**, dans la ligne de commande, tapez `help logParse`.

Erreur de client Thick : entrée du périphérique de contenu distant introuvable

Erreur :« *L'entrée du périphérique de contenu distant est introuvable* », générée pour une règle de corrélation appliquée à un service Concentrator.

Problème : dans le module Investigation, si vous cliquez sur la valeur méta `correlation-rule-name` dans la métaclé Alerte, vous n'obtenez aucune information de session.

Solution : Au lieu d'utiliser des règles de corrélation sur les Decoders et les Concentrators, utilisez des règles ESA. Ces règles **enregistrent** les sessions de corrélation correspondant à la règle ESA.

Afficher les analyseurs d'exemple

Comme les analyseurs flex et lua sont chiffrés quand ils sont livrés par Live, il est difficile d'en consulter le contenu.

Toutefois, certains exemples en texte brut sont disponibles ici :**https://community.emc.com/docs/DOC-41108**.

Configurer les sources d'événements WinRM

L'article Inside EMC suivant contient une vidéo qui présente la procédure de configuration de la collecte Windows RM (Remote Management) :**https://inside.emc.com/docs/DOC-122732**.

Par ailleurs, il contient deux scripts permettant d'accéder rapidement aux procédures décrites dans le « Guide de configuration des sources d'événements Windows ».

NwLogPlayer

NwLogPlayer est un utilitaire qui simule le trafic syslog. Dans l'environnement hébergé, `NwLogPlayer.exe` est un utilitaire de ligne de commande situé sur l'ordinateur client RSA NetWitness® Suite dans le répertoire suivant :

```
C:\Program Files\NetWitness\NetWitness 9.8
```

NwLogPlayer est également présent sur l'hôte Log Decoder sous `/usr/bin`.

Utilisation

Sur la ligne de commande, saisissez `nwlogplayer.exe -h` pour répertorier les options disponibles, comme indiqué ici :

`--priority arg`	permet de définir le niveau de priorité du log
`-h [ --help ]`	permet d'afficher ce message
`-f [ --file ] arg (=stdin)`	message d'entrée ; affiche par défaut la valeur **stdin**
`-d [dir ] arg`	répertoire d'entrée
`-s [ --server ] arg (=localhost)`	serveur distant ; affiche par défaut la valeur **localhost**
`-p [ --port ] arg (=514)`	port distant ; affiche par défaut la valeur **514**

`-r [ --raw ] arg (=0)`	Détermine le mode Raw. • 0 = ajouter une marque de priorité (valeur par défaut) • 1= le contenu du fichier sera copié ligne par ligne sur le serveur. • 3 = détection automatique • 4 = flux enVision • 5 = objet binaire
`-m [ --memory ] arg`	Mode test de vitesse. Permet de lire jusqu'à 1 mégaoctet de messages à partir du contenu du fichier et de relectures.
`--rate arg`	Décompte d'événements par seconde. Cet argument n'a aucun effet si le **taux** est supérieur au nombre d'événements par seconde que le programme peut traiter en mode continu.
`--maxcnt arg`	nombre maximal de messages à envoyer
`-c [ --multiconn ]`	connexion multiple
`-t [ --time ] arg`	permet de simuler l'heure de l'horodatage ; le format est `yyyy-m-d-hh:mm:ss`
`-v [ --verbose ]`	Si la valeur est **true**, la sortie est détaillée
`--ip arg`	permet de simuler une balise IP
`--ssl`	permet d'utiliser SSL pour se connecter
`--certdir arg`	répertoire de l'autorité de certification OpenSSL
`--clientcert arg`	permet d'utiliser ce certificat client SSL codé PEM
`--udp`	permet d'effectuer un envoi en UDP

Résoudre les problèmes liés aux feeds

Présentation

L'objectif du générateur de flux est de générer le mappage d'une source d'événement sur la liste de groupes auxquels elle appartient.

Si vous disposez d'une source d'événement à partir de laquelle vous collectez des messages qui ne figure pas encore dans les groupes de sources d'événement appropriés, cette rubrique fournit des références et des informations générales pour vous aider à traquer le problème.

Détails

Le feed ESM mappe plusieurs clés sur une valeur unique. Il mappe les attributs DeviceAddress, Forwarder et DeviceType à groupName.

Le but du feed ESM est d'enrichir la méta de l'événement source avec le groupName collecté sur Log Decoder.

Fonctionnement

Le générateur de feed est prévu pour se mettre à jour chaque minute. Cependant, il ne se déclenche qu'en cas de changements (créer, mettre à jour ou supprimer) dans les sources ou les groupes d'événements.

Il génère un fichier de feed unique avec une source d'événement au mappage de groupe, et envoie le même feed sur tous les Log Decoder qui sont connectés à NetWitness Suite.

Une fois le fichier de feed chargé sur les Log Decoder, pour tous les nouveaux événements, il enrichit les métadonnées des événements avec groupName, et ajoute ce groupName à logstats.

Une fois que groupName se trouve dans logstats, ESM Aggregator groupe les informations et les envoie à ESM. À ce stade, vous devriez voir la colonne **Nom du groupe** sous l'onglet **Surveillance des sources d'événements**.

L'ensemble du processus peut prendre un certain temps. Par conséquent, vous devrez peut-être attendre plusieurs secondes après avoir ajouté une nouvelle source de groupe ou d'événement, avant que le nom du groupe ne s'affiche.

Remarque : Si l'attribut du type de source de l'événement change lorsque le feed est mis à jour, NetWitness Suite ajoute une nouvelle entrée logstats, plutôt que de mettre à jour l'entrée existante. Ainsi, il y a deux entrées de logstats différentes dans logdecoder. Auparavant, les messages existants auraient été répertoriés dans le type précédent. Tous les nouveaux messages sont enregistrés pour le nouveau type de source d'événement.

Fichier de feed

Le format du fichier de feed est le suivant :

`DeviceAddress, Forwarder, DeviceType, GroupName`

`DeviceAddress` est soit `ipv4, ipv6`, soit `hostname`, selon ce qui a été défini pour la source d'événement.

Voici un exemple de fichier de feed :

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apachegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"

"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","Apache
grp"
```

Résolution des problèmes

Vous pouvez vérifier les éléments suivants pour vérifier où le problème se produit.

Existence des fichiers de feed

Vérifiez que l'archive ZIP contenant les feeds existe à l'emplacement suivant :

`/opt/rsa/sms/esmfeed.zip`

Ne modifiez pas ce fichier.

Groupe méta rempli sur LD

Vérifiez que le groupe méta est rempli sur Log Decoder. Naviguez vers le REST de Log Decoder et vérifiez logstats :

```
http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain
```

Voici un exemple de fichier logstats avec des informations de groupe :

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4 count=338 lastSeenTime=2015-Feb-04 22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19 groups=IP1234Group,apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304 source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04 22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19 groups=AllOtherGroup,ApacheTomcatGroup
```

Dans le texte ci-dessus, les informations du groupe sont en **gras**.

Méta du groupe de périphériques sur Concentrator

Vérifiez que la méta du **Groupe de périphériques** existe sur le Concentrator et que les événements comportent des valeurs dans le champ `device.group`.

Fichier log SMS

Vérifiez le fichier log SMS à l'emplacement suivant pour afficher les messages d'information et d'erreur : `/opt/rsa/sms/logs/sms.log`

Voici des exemples de messages d'information :

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

Voici des exemples de messages d'erreur :

```
Error creating CSV File : <reason>Unable to push the ESM Feed: Unable to
create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> : Error: <error>
Unable to push the ESM Feed: CSV file is empty, make sure you have al-
least on group with al-least one eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on LogDecoder-
<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error: The zip
archive "/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not be
opened
Unable to push the ESM Feed: <reason>
```

Vérifiez que les données Logstats sont lues et publiées par ESMReader et ESMAggregator

Voici les étapes de vérification de collecte des logstats par **collectd** et de leur publication dans la gestion de source d'événements.

ESMReader

1. Sur LogDecoders, ajoutez la balise **debug "true"** dans **/etc/collectd.d/NwLogDecoder_ESM.conf** :

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>        </stats>    </Module>    <Module
```

```
"NgEsmReader" "update">        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>        </stats>    </Module></Plugin>
```

2. Exécutez la commande `collectd service restart` :
3. Exécutez la commande suivante :
   `tail –f /var/log/messages | grep collectd`
   Vérifiez que ESMReader lit logstats et qu'il n'y a pas d'erreur. S'il existe des problèmes de lecture, vous verrez des erreurs similaires à ce qui suit :

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. Dans NetWitness Suite, supprimez les commentaires de la balise verbose dans **/etc/collectd.d/ESMAggregator.conf** :

```
# ESMAggregator module collectd.conf configuration file
#
# Copyright (c) 2014 RSA The Security Divsion of EMC
#

<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"

<Module "ESMAggregator">
        verbose 1
```

```
                interval "60"
                cache_save_interval "600"
                persistence_dir "/var/lib/netwitness/collectd"
        </Module>    </Plugin>
```

2. Exécutez ce qui suit :
   `collectd service restart.`
3. Exécutez la commande suivante :
   `run "tail -f /var/log/messages | grep ESMA`
   Recherchez les données ESMAggregator et assurez-vous que votre entrée logstat est disponible dans les logs.

Exemple de sortie :

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
```

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Configurer l'intervalle de tâche du générateur de feed JMX

Bien que la tâche de génération de feed est prévue pour s'exécuter chaque minute par défaut, vous pouvez la modifier avec `jconsole`, le cas échéant.

Pour modifier l'intervalle de tâche du générateur de flux :

1. Ouvrez **jconsole** pour le service SMS.
2. Sous l'onglet MBeans, accédez à **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributs**.
3. Modifiez la valeur de la propriété **FeedGeneratorJobIntervalInMinutes**.
4. Accédez à **Opérations** sous la même arborescence de navigation, puis cliquez sur **commit ()**. Cette opération enregistre la nouvelle valeur dans le fichier JSON correspondant sous **/opt/rsa/sms/conf** et utilise la valeur si SMS est redémarré.

La définition d'une nouvelle valeur replanifie la tâche du générateur de flux pour le nouvel intervalle.

Références

Cette section décrit les vues de l'interface utilisateur de NetWitness Suite dans laquelle vous pouvez effectuer les tâches de maintenance du système. Cette interface vous permet de :

- Assurer la surveillance et le maintien en conditions opérationnelles des services (paramètres, statistiques, syntaxe des commandes et messages, API REST, utilitaire de la console RSA et protocoles pris en charge dans NetWitness Suite).
- Afficher la version actuelle de NetWitness Suite et l'état de la licence.
- Gérer le référentiel local des mises à jour à partir duquel vous appliquez les mises à jour de version logicielle aux hôtes.

Les sections suivantes décrivent chaque interface en détail :

- Vue Intégrité
- Vue système - Panneau informations du système

Vue Intégrité

Les paramètres Intégrité vous permettent de définir et d'afficher les alarmes, de surveiller les événements et d'afficher les règles et statistiques du système. Pour plus d'informations sur chacun de ces éléments, consultez les rubriques suivantes :

- Vue Intégrité - Vue Alarmes
- Vue Contrôle des sources d'événements
- Graphiques de l'historique d'intégrité
- Vue Paramètres d'intégrité - Archiver
- Vue Paramètres d'intégrité - Sources d'événements
- Vue Paramètres d'intégrité - Warehouse Connector
- Vue Surveillance
- Vue Règles
- Vue Navigateur Stat. système

Vue Intégrité - Vue Alarmes

Vous pouvez surveiller les hôtes et les services pour déterminer quand les limites définies par l'utilisateur ont été atteintes en affichant toutes les alarmes actives. Les règles de stratégie, que vous définissez ou associez aux hôtes et services dans l'**onglet Règles**, déclenchent ces alarmes. Vous pouvez :

- Afficher toutes les alarmes qui sont actuellement actives pour tous vos systèmes et services
- Sélectionner une alarme et afficher ses détails

Que voulez-vous faire ?

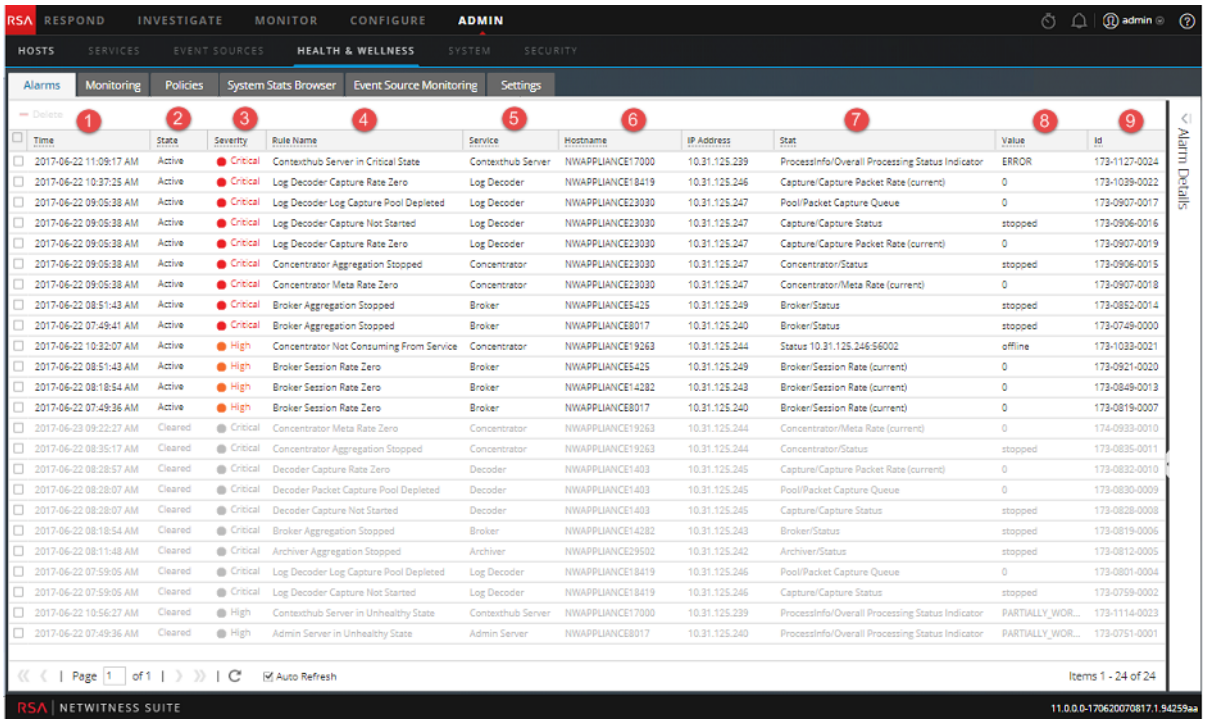
Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher l'état des alarmes des Serveur NetWitness et services.	Surveiller les alarmes
Administrateur	Affichez les informations détaillées sur une alarme spécifique.	Surveiller les alarmes

Rubriques connexes

Gérer les règles

Aperçu rapide

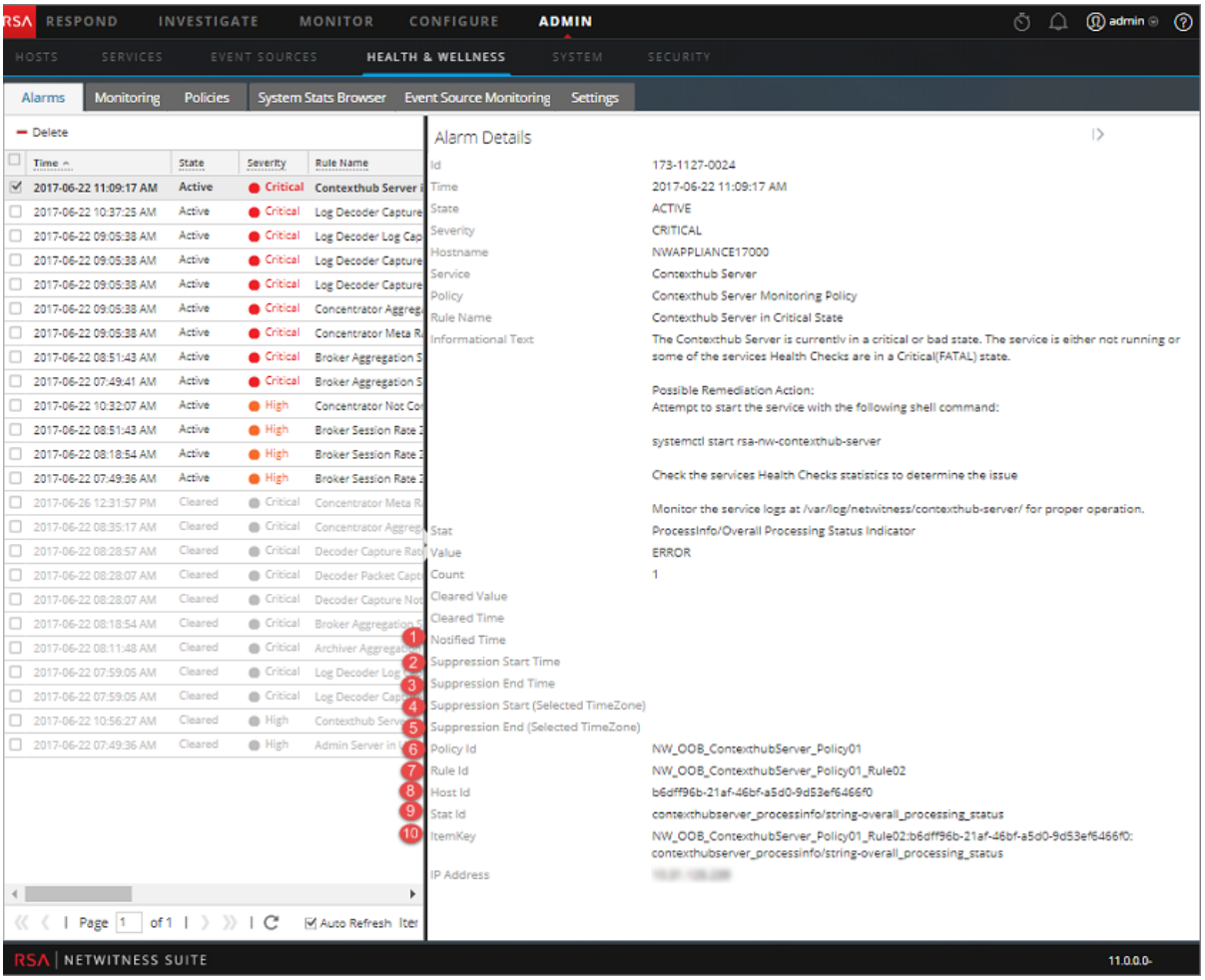
L'autorisation requise pour accéder à cette vue est **Gérer les services**. Pour accéder à la vue Alarmes, accédez à **Admin** > **Intégrité**. L'interface Intégrité s'ouvre avec la vue Alarmes. L'onglet Alarmes contient la liste des alarmes et un panneau Détails de l'alarme.



1	Heure à laquelle l'alarme a été déclenchée.
2	État de l'alarme : • **Actif** - le seuil statistique a été atteint déclenchant ainsi l'alarme. • **Effacé** - le seuil d'effacement a été atteint et l'alarme n'est plus active.
3	Gravité affectée à l'alarme : • **Critique** • **Élevée** • **Medium** • **Faible**
4	Nom de la règle qui déclenche l'alarme.
5	Service défini dans la règle.
6	Hôte sur lequel l'alarme est déclenchée.
7	Statistique sélectionnée dans la règle qui déclenche l'alarme.
8	Valeur de la statistique qui a déclenché l'alarme.
9	Numéro d'identification de l'alarme.

Remarque : NetWitness Suite trie les alarmes par date. Vous pouvez trier les paramètres pertinents dans l'ordre croissant ou décroissant.

La figure suivante illustre l'onglet Alarmes dans lequel le panneau Détails de l'alarme est développé.



Panneau Détails de l'alarme

Le panneau Détails de l'alarme affiche des informations pour l'alarme sélectionnée dans la liste des alarmes. Il contient toutes les informations indiquées dans la liste des alarmes plus les champs suivants.

1	Heure de notification de l'alarme
2	Heure de début de suppression
3	Heure de fin de suppression
4	Début de la suppression (fuseau horaire sélectionné)
5	Fin de la suppression (fuseau horaire sélectionné)

6	ID de règle
7	ID de règle
8	ID de l'hôte
9	ID des statistiques
10	Clé d'élément

Vue Contrôle des sources d'événements

Remarque : Pour gérer les sources d'événements, reportez-vous à la section « À propos de la gestion de la source d'événements » dans le *Guide de gestion de la source d'événements RSA NetWitness Suite*.

NetWitness Suite fournit un moyen de surveiller les statistiques des différentes sources d'événements dans l'interface utilisateur. Les informations affichées correspondent à l'historique et proviennent du Log Decoder. Vous pouvez personnaliser la vue selon le paramètre que vous sélectionnez pour filtrer les données.

Pour accéder à la vue Surveillance des sources d'événements :

1. Accédez à **ADMIN > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

2. Cliquez sur **Contrôle des sources d'événements**.

Que voulez-vous faire ?

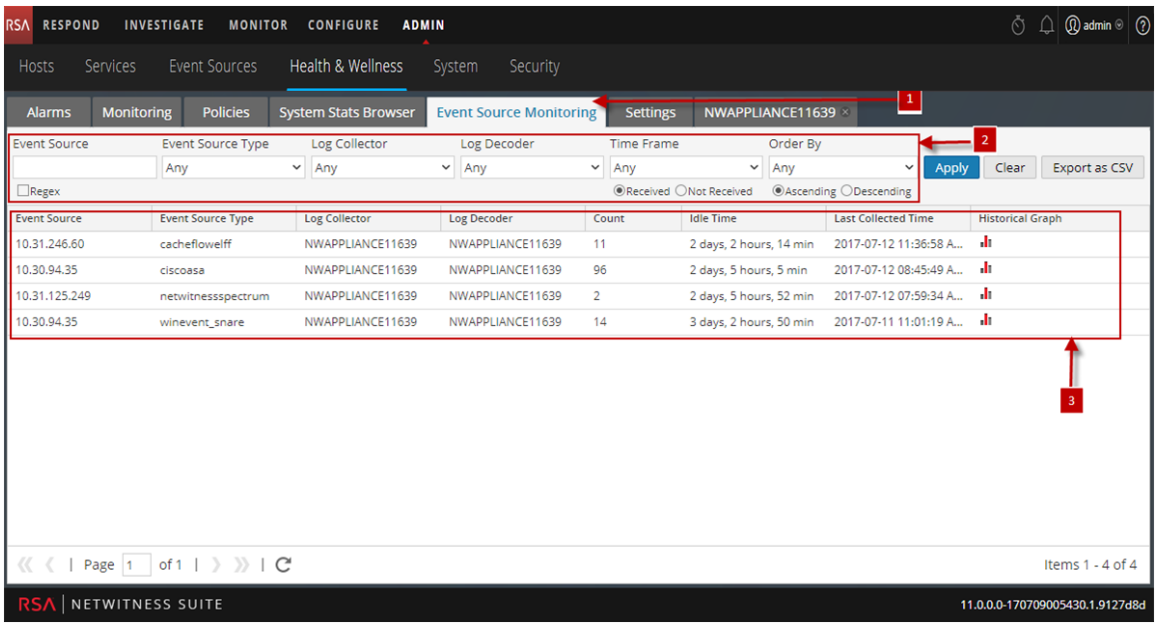
Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher les événements collectés à partir d'une source d'événements	Vue Graphique de l'historique des événements collectés à partir d'une source d'événements

Rubriques connexes

- Surveiller des sources d'événements
- Filtrer des sources d'événements
- Afficher le graphique de l'historique des événements collectés pour une source d'événement

Aperçu rapide

La vue Contrôle des sources d'événements s'affiche.



1	Affiche l'onglet Surveillance des sources d'événements.
2	Barre d'outils utilisé pour filtrer et personnaliser l'onglet Surveillance des sources d'événements.
3	Affiche le panneau Statistiques des sources d'événements.

Filtres

Ce tableau récapitule les différents paramètres que vous pouvez utiliser pour filtrer et personnaliser la vue de surveillance de source d'événement.

Paramètre	Description
Source d'événement	Saisissez le nom d'une source d'événement que vous souhaitez surveiller. Sélectionnez Regex pour activer ce filtre. Il effectue une recherche des expressions régulières dans du texte et répertorie la catégorie spécifiée. Si Regex n'est pas sélectionné, il prend en charge la mise en correspondance des schémas de globbing.
Type de source d'événement	Sélectionnez un type de source d'événement pour la source d'événement sélectionnée.
Log Collector	Sélectionnez le Log Collector pour afficher les données collectées par le Log Collector spécifié.

Paramètre	Description
Log Decoder	Sélectionnez un Log Decoder pour afficher les données collectées par le Log Decoder spécifié.
Période	Sélectionnez le délai pour lequel vous souhaitez afficher les statistiques. Sélectionnez **Reçu** si vous souhaitez que les résultats de la requête ne contiennent que les sources d'événements dont les logs ont été reçus dans le délai sélectionné ou sélectionnez **Non reçu(e)** si vous souhaitez que les résultats de la requête contiennent uniquement les sources d'événements dont les logs n'ont pas été reçus dans le délai sélectionné
Réorganiser par	Sélectionnez l'ordre dans lequel la liste doit être filtrée. Sélectionnez Croissant pour la filtrer dans l'ordre croissant.
Appliquer	Cliquez pour appliquer les filtres choisis et afficher la liste correspondante.
Clear	Cliquez sur cette option pour effacer les filtres choisis.
Exporter au format CSV	Cliquez pour exporter les informations sous forme de fichier CSV.

Affichage Statistiques de la source d'événement

Paramètre	Description
Source d'événement	Affiche le nom de la source d'événement.
Type de source d'événement	Affiche le type de source d'événement.
Log Collector	Affiche le Log Collector à partir duquel les événements ont été initialement capturés.
Log Decoder	Affiche le Log Decoder où les événements sont traités.

Paramètre	Description
Count	Affiche le nombre d'événements reçus par le décodeur de log depuis la dernière réinitialisation de la valeur de décompte.
Temps d'inactivité	Affiche la durée écoulée après la dernière collecte de statistiques.
Dernière heure de collecte	Affiche la dernière heure à laquelle le Log Decoder a traité un événement pour la source d'événement.
Graphique de l'historique	Cliquez sur pour afficher le graphique historique des statistiques collectées pour la source d'événement.

Graphiques de l'historique d'intégrité

La configuration de la surveillance d'Archiver vous permet de générer automatiquement des notifications lorsque des seuils critiques concernant l'agrégation et le stockage Archiver ont été atteints. La vue Graphique de l'historique fournit une représentation visuelle des données historiques,

Consultez les rubriques suivantes pour plus d'informations :

- Vue Graphique de l'historique des événements collectés à partir d'une source d'événements
- Graphique de l'historique relatif aux statistiques du système

Vue Graphique de l'historique des événements collectés à partir d'une source d'événements

La vue Graphique de l'historique des événements collectés dans une source d'événements fournit une représentation visuelle des données historiques. Pour accéder à cette vue :

1. Accédez à **Administrateur > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Contrôle ouvert.

2. Cliquez sur **Contrôle des sources d'événements**.

   La vue Contrôle des sources d'événements s'affiche.

3. Dans la colonne **Graphique de l'historique**, sélectionnez .

   Le graphique de l'historique du type de source d'événements sélectionné s'affiche dans une fenêtre contextuelle.

   La figure affiche les éléments collectés dans le type de source d'événements **winevent_**

snare.

Vous pouvez utiliser la vue du graphique si nécessaire. Le tableau répertorie les différents paramètres utilisés pour personnaliser le graphique de l'historique.

Paramètre	Description
Période	Sélectionnez la période pour laquelle vous souhaitez afficher l'historique des données. Les options disponibles sont les suivantes : Jour en cours, Semaine en cours, Mois en cours.
Du <date> au <date>	Sélectionnez la période pour laquelle vous souhaitez afficher l'historique des données.

Vous pouvez effectuer une analyse détaillée des données dans la vue Graphique de l'historique.

Fonction de zoom 1 et 2

Vous pouvez sélectionner une des valeurs pour afficher l'historique des données de la valeur sélectionnée. La figure ci-dessous affiche un exemple de la période de 6 heures sélectionnée pour le zoom avant. Le curseur dans le coin inférieur droit est également remplacé par une fenêtre de 6 heures.

Autrement, vous pouvez faire glisser la barre située dans le coin droit pour analyser une période donnée.

Fonction de zoom 3

Vous pouvez effectuer un cliquer–déplacer dans la zone de tracé pour effectuer un zoom sur la période voulue.

Graphique de l'historique relatif aux statistiques du système

Pour accéder au graphique de l'historique relative aux statistiques système :

1. Accédez à **Administrateur > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

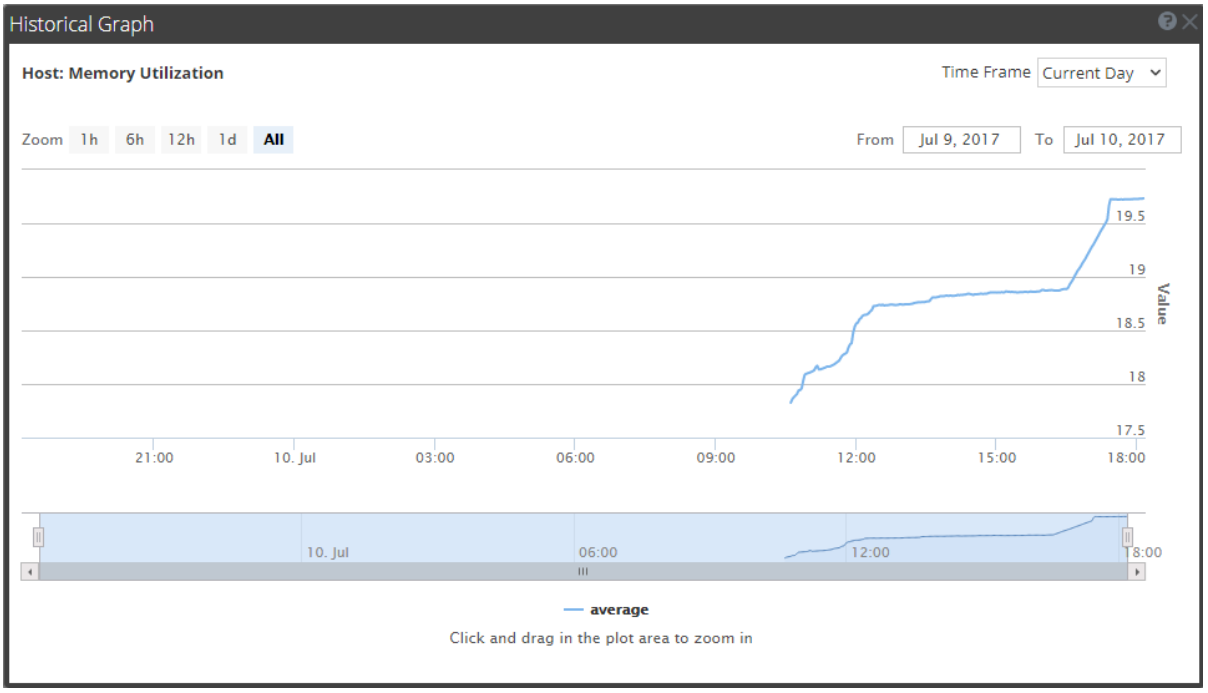
2. Cliquez sur l'onglet **Navigateur Stat. système**.

   L'onglet Navigateur Stat. système s'affiche.

3. Dans la colonne **Graphique de l'historique**, sélectionnez .

   Le graphique historique de la statistique sélectionnée pour un hôte s'affiche.

   Cette figure affiche la vue Statistique système de la statistique Utilisation de mémoire.



Paramètres

Vous pouvez utiliser la vue du graphique si nécessaire. Le tableau répertorie les différents paramètres utilisés pour personnaliser la vue Graphique de l'historique.

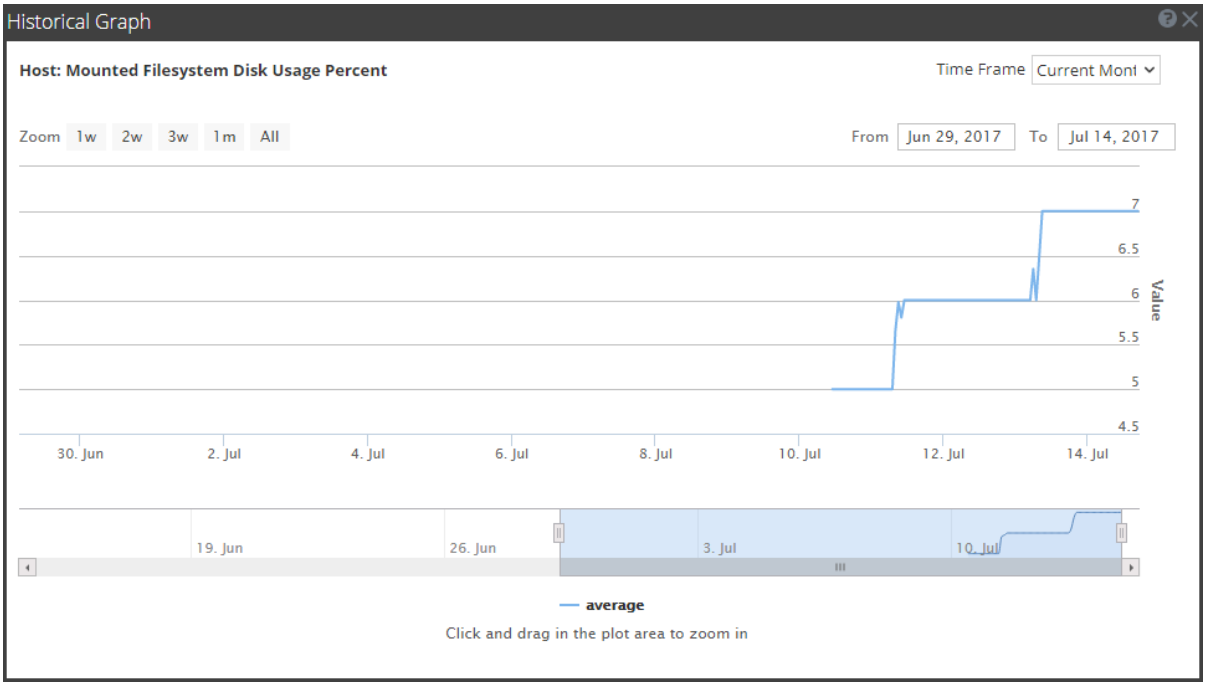
Paramètre	Description
Période	Sélectionnez la période pour laquelle vous souhaitez afficher l'historique des données. Les options disponibles sont les suivantes : **Jour en cours, Semaine en cours**, **Mois en cours** et **Année en cours**.
Du <date> au <date>	Sélectionnez la période pour laquelle vous souhaitez afficher l'historique des données :

Vous pouvez effectuer une analyse détaillée des données dans la vue Graphique de l'historique.

Fonction de zoom 1 et 2 :

Vous pouvez sélectionner une des valeurs pour afficher l'historique des données de la valeur sélectionnée. La figure ci-dessous affiche un exemple de la période de 6 heures sélectionnée pour le zoom avant. Le curseur dans le coin inférieur droit est également remplacé par une fenêtre de 6 heures.

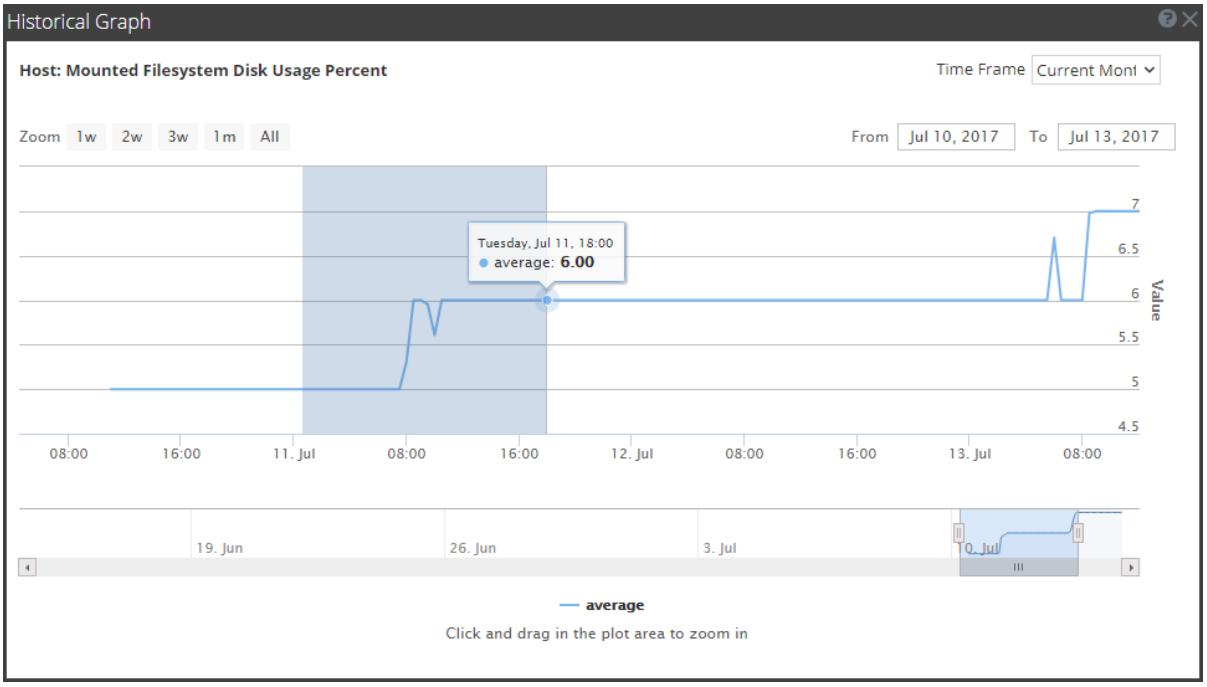
Autrement, vous pouvez faire glisser la barre située dans le coin droit pour analyser une période donnée.



Fonction de zoom 3 :

Vous pouvez effectuer un cliquer–déplacer dans la zone de tracé pour effectuer un zoom sur la période voulue.

La figure ci-dessous montre un exemple de la façon dont le graphique apparaît lorsque vous cliquez dessus pour le faire glisser.



Vue Paramètres d'intégrité - Archiver

Remarque : Pour surveiller les services Archiver and Warehouse Connector, voir Politique d'intégrité.

Pour accéder à la vue Surveillance d'Archiver :

1. Accédez à **Administration > Intégrité**.
2. Sélectionnez **Paramètres > Archiver**.

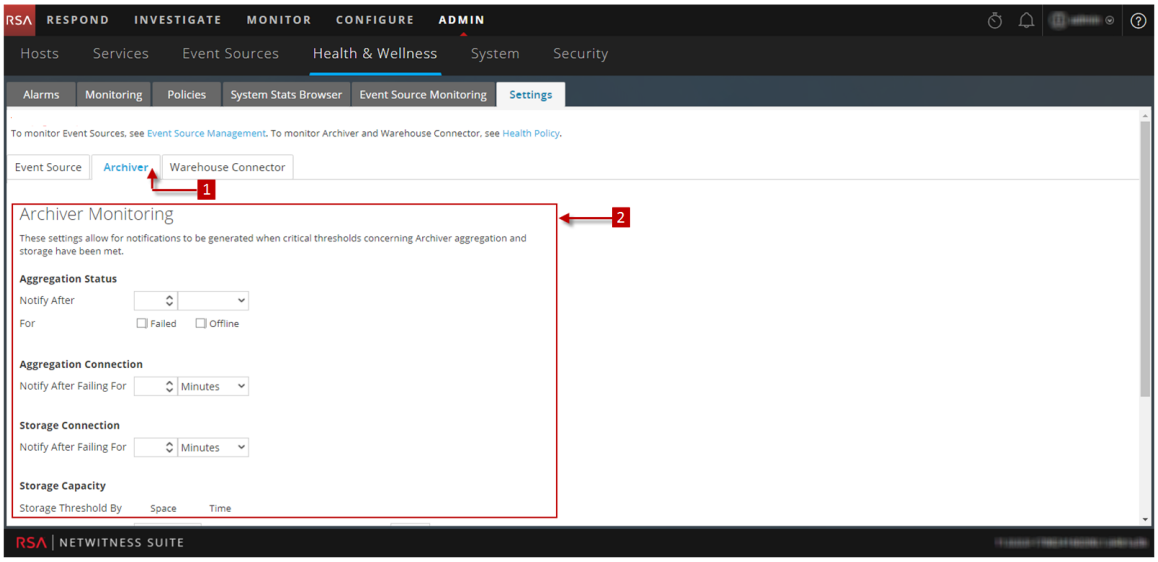
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Contrôler les détails du service Archiver	Surveiller les détails d'un service

Rubriques connexes

Surveiller les détails d'un service

Aperçu rapide



1	Affiche le panneau Surveillance d'Archiver
2	Configurer le panneau Surveillance d'Archiver pour recevoir automatiquement une notification

Fonctionnalités

Le tableau suivant répertorie les paramètres requis pour configurer Archiver afin qu'il génère automatiquement une notification lorsque les seuils critiques sont atteints.

Paramètre	Valeur	Description
État de l'agrégation	Avertir après	Délai (en minutes ou en heures) après lequel vous serez informé de l'état de l'agrégation.
	Pour	En échec - En cas d'activation, vous recevez une notification lorsque l'état d'agrégation de Archiver est en échec pour le délai (en minutes ou en heures) défini. Offline - En cas d'activation, vous recevez une notification lorsque l'état d'agrégation de Archiver est hors ligne pour le nombre défini de minutes ou heures

Paramètre	Valeur	Description
Connexion de l'agrégation	Avertir après une durée d'échec de	Nombre de minutes ou d'heures après lesquelles vous recevez une notification si la connexion à l'agrégation de Archiver échoue.
Connexion du stockage	Avertir après une durée d'échec de	Délai (en minutes ou en heures) après lequel vous recevez une notification si la connexion au stockage de Archiver échoue.
Capacité de stockage	Seuil de stockage	Sélectionnez **Espace** si vous souhaitez recevoir une notification lorsque la capacité de stockage d'Archiver dépasse le pourcentage défini dans le champ **Lorsque la taille du stockage est**. Sélectionnez **Durée** si vous souhaitez recevoir une notification lorsque les fichiers stockés dans Archiver dépasse le nombre défini de jours dans le champ **Lorsque le fichier de stockage le plus ancien est**
	Lorsque la taille du stockage est	Saisissez le pourcentage de saturation du stockage à partir duquel vous souhaitez recevoir une notification.
	Lorsque la taille du stockage à chaud est	Saisissez le pourcentage de saturation du stockage à chaud partir duquel vous souhaitez recevoir une notification.

Paramètre	Valeur	Description
Type de notification	Configurer l'e-mail ou la liste de distribution	Cliquez pour configurer la messagerie électronique afin de recevoir des notifications dans NetWitness Suite.
	Configurer les serveurs de traps Syslog et SNMP	Cliquez pour configurer des logs d'audit.
	Console NW, E-mail, Notification Syslog, Notification des traps SNMP	Activez la Console NW pour recevoir des notifications dans la barre d'outils de notification de l'interface utilisateur NetWitness Suite. Activez la messagerie pour recevoir des notifications par e-mail Activez la notification Syslog pour générer des événements Syslog. Activez Notification des traps SNMP pour recevoir des événements d'audit sous la forme de traps SNMP.

Vue Paramètres d'intégrité - Sources d'événements

Remarque : Pour gérer les sources d'événements, reportez-vous à la section **À propos de la gestion de la source d'événements** dans le *Guide de gestion de la source d'événements RSA NetWitness Suite*.

La vue Contrôle des sources d'événements comprend le panneau Source d'événement, la boîte de dialogue Ajouter/Modifier la surveillance des sources, le panneau Décommissionner et la boîte de dialogue Décommissionner. Vous utilisez la vue pour configurer :

- à quel moment générer des notifications pour les sources d'événements à partir desquelles le Log Collector ne reçoit plus de logs ;
- où envoyer ces notifications ;
- à quel moment décommissionner un Log Collector lorsqu'un collecteur distant et le collecteur local basculent vers un Log Decoder en veille.

Le rôle requis pour accéder à cette vue est **Gérer les audits NW**. Pour accéder à cette vue :

1. Accédez à **Administration > Intégrité**.
2. Sélectionnez **Paramètres > Source d'événements**.

Que voulez-vous faire ?

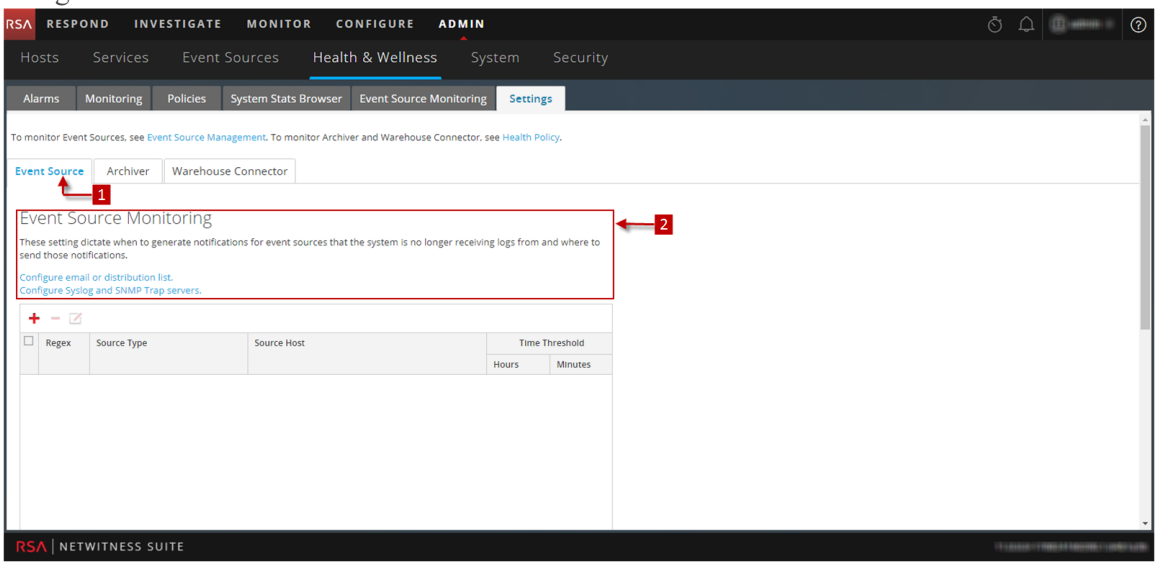
Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher les fonctionnalités de surveillance des sources d'événements	Surveiller des sources d'événements

Rubriques connexes

Configurer la surveillance des sources d'événements

Aperçu rapide

L'onglet Source d'événement s'affiche.



1	Panneau Contrôle des sources d'événements
2	Configurer le panneau Contrôle des sources d'événements pour recevoir une notification

Panneau Contrôle des sources d'événements

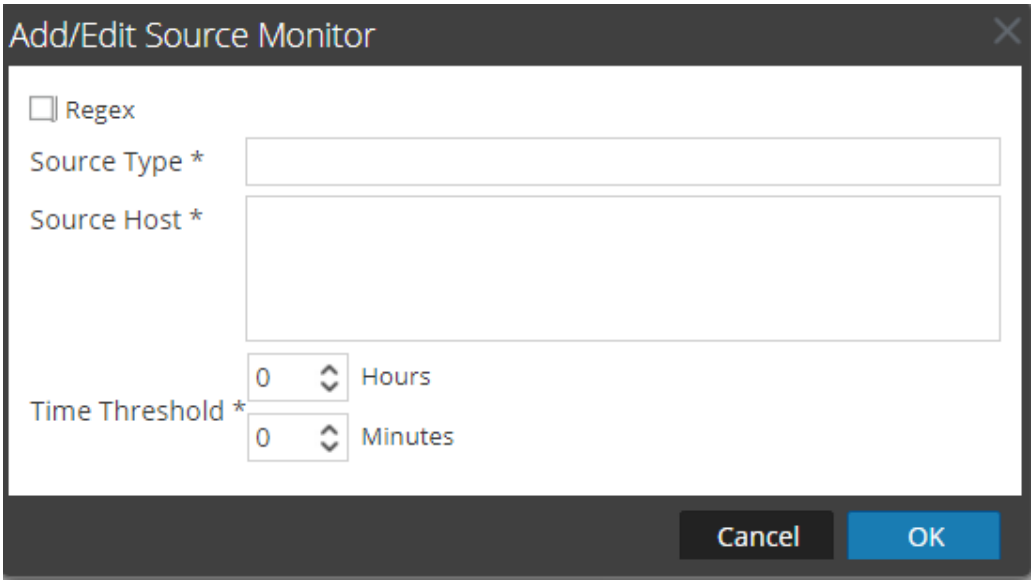
Fonctionnalité	Description
Configurer l'e-mail ou la liste de distribution.	Ouvre la vue **Administration** > **Système** > E-mail pour que vous puissiez régler la distribution par e-mail pour la sortie de la surveillance des sources d'événements, si nécessaire.
Configurer les serveurs de traps SNMP et Syslog.	Ouvre la vue **Administration** > **Système** > Audits pour que vous puissiez régler la distribution de traps Syslog et SNMP pour la sortie de la surveillance des sources d'événements, si nécessaire.
	Affiche la boîte de dialogue Ajouter/Modifier la surveillance des sources dans laquelle vous pouvez ajouter ou modifier des sources d'événements à contrôler.
	Supprime les sources d'événements sélectionnées du contrôle.
	Sélectionne une source d'événement.
Type de source	Affiche le type de source de la source d'événement.
Hôte source	Affiche l'hôte source de la source d'événement.
Seuil de délai d'attente	Affiche la période après laquelle NetWitness Suite arrête d'envoyer des notifications.
Appliquer	Applique tous les ajouts, toutes les suppressions ou toutes les modifications, qui entrent en vigueur immédiatement.
Annuler	Annule tous les ajouts, toutes les suppressions ou toutes les modifications.

Panneau Décommissionner

Fonctionnalité	Description
	Affiche la boîte de dialogue Décommissionner dans laquelle vous pouvez ajouter ou modifier des sources d'événements à décommissionner.

Fonctionnalité	Description
	Supprime les sources d'événements sélectionnées de la décommission.
	Sélectionne une source d'événement.
Regex	Indique si vous choisissez d'utiliser des expressions régulières.
Type de source	Affiche le type de source de la source d'événement décommissionnée.
Hôte source	Affiche l'hôte source de la source d'événement décommissionnée.
Appliquer	Applique tous les ajouts, toutes les suppressions ou toutes les modifications, qui entrent en vigueur immédiatement.
Annuler	Annule tous les ajouts, toutes les suppressions ou toutes les modifications.

Boîte de dialogue Ajouter/Modifier la surveillance des sources



Dans la boîte de dialogue **Ajouter/Modifier la surveillance des sources**, vous ajoutez ou modifiez les sources d'événements que vous souhaitez contrôler. Les deux paramètres qui identifient une source d'événement sont **Type de source** et **Hôte source**. Vous pouvez utiliser le « **globbing** » (englobement, c'est-à-dire la mise en correspondance de schémas et les caractères génériques) pour indiquer le type de source et l'hôte source des sources d'événements, comme illustré dans l'exemple suivant :

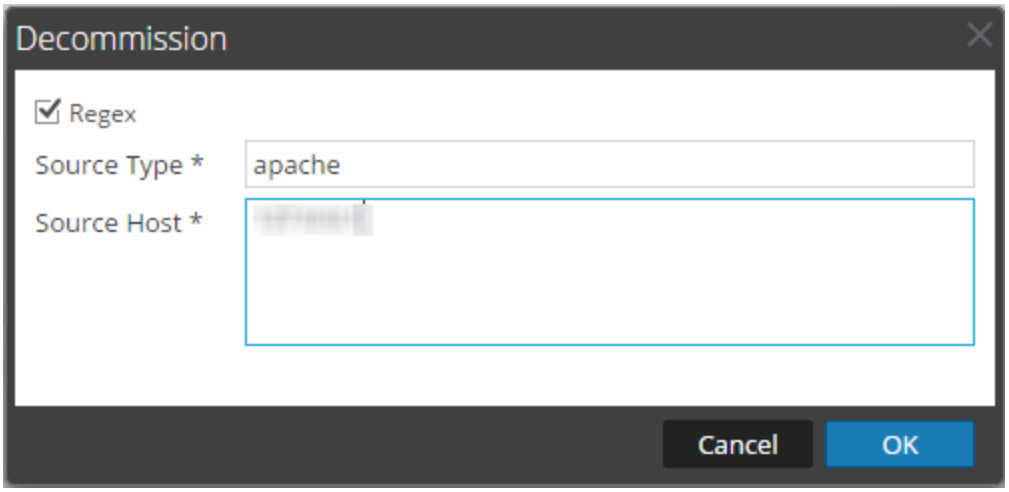
Type de source	Hôte source
ciscopix	**1.1.1.1**
*	**1.1.1.1**
*	*
*	**1.1.1.1|1.1.1.2**
*	**1.1.1.[1|2]**
*	**1.1.1.[123]**
*	**1.1.1.[0-9]**
*	**1.1.1.11[0-5]**
*	**1.1.1.1,1.1.1.2**
*	**1.1.1.[0-9]|1.1.1.11[0-5]**
*	**1.1.1.[0-9]|1.1.1.11[0-5],10.31.204.20**
*	**1.1.1.***
*	**1.1.1.[0-9]{1,3}**

Fonctionnalités

Fonctionnalité	Description
Regex	Activez la case à cocher si vous souhaitez utiliser des expressions régulières
Type de source	Type de la source de l'événement source. Vous devez utiliser la valeur que vous avez configurée pour la source d'événement sous l'onglet **Sources d'événements** de la vue **Administration** >**Services** > service Log Collector > **Afficher** > vue **Config** .

Fonctionnalité	Description
Hôte source	Nom d'hôte ou adresse IP de la source d'événement. Vous devez utiliser la valeur que vous avez configurée pour la source d'événement sous l'onglet **Sources d'événements** de la vue **Administration** > **Services** > Périphérique Log Collector > **Afficher** > vue **Config**.
Seuil de délai d'attente	La période après laquelle NetWitness Suite commence à envoyer des notifications.
Annuler	Ferme la boîte de dialogue sans ajouter la source d'événement ou passe à la source d'événement, sur le panneau Contrôle des sources d'événements.
OK	Ajoute la source d'événement au panneau Contrôle des sources d'événements.

Boîte de dialogue Décommissionner



Fonctionnalité	Description
Type de source	Type de la source de l'événement source. Vous devez utiliser la valeur que vous avez configurée pour la source d'événement sous l'onglet **Sources d'événements** de la vue **Administration** > **Services** > Périphérique Log Collector > **Afficher** > vue **Config**.

Fonctionnalité	Description
Hôte source	Nom d'hôte ou adresse IP de la source d'événement. Vous devez utiliser la valeur que vous avez configurée pour la source d'événement sous l'onglet **Sources d'événements** de la vue **Administration** >**Services** > service Log Collector > **Afficher** > vue **Config** .
Annuler	Ferme la boîte de dialogue sans appliquer les éventuels ajouts, suppressions et modifications apportés au panneau Décommissionner.
OK	Applique les ajouts, suppressions ou modifications apportés au panneau Décommissionner.

Vue Paramètres d'intégrité - Warehouse Connector

Remarque : Pour surveiller les services Archiver and Warehouse Connector, voir Politique d'intégrité.

La configuration de la surveillance de Warehouse Connector vous permet de générer automatiquement une notification lorsque des seuils critiques concernant Warehouse Connector et le stockage ont été atteints.

Accéder à la vue Surveillance de Warehouse Connector

1. Accédez à **Admin > Intégrité**.
2. Sélectionnez **Paramètres > Warehouse Connector**.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Vue Détails du service Warehouse Connector	Vue Détails du service Warehouse Connector

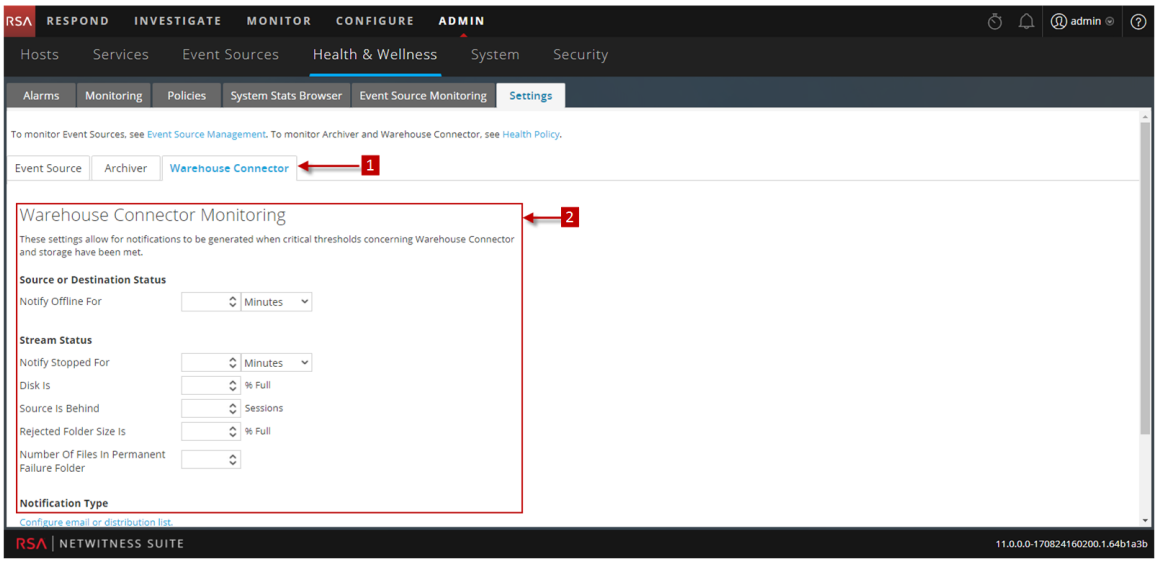
Rubriques connexes

Vue Détails du service Warehouse Connector

Surveiller les détails d'un service

Aperçu rapide

La vue Surveillance de Warehouse Connector s'affiche.



1 Affiche le panneau Vue Surveillance de Warehouse Connector.

2 Permet de configurer les paramètres de surveillance de Warehouse Connector

Paramètres de surveillance de Warehouse Connector

Le tableau suivant répertorie les paramètres requis pour configurer le Warehouse Connector afin qu'il génère automatiquement une notification lorsque les seuils critiques sont atteints.

Paramètre	Valeur	Description
État de la source ou destination	Avertir de la mise hors ligne pour	Nombre de minutes ou d'heures après lesquelles vous recevez une notification si la connexion à la source ou la destination échoue.
État des flux	Avertir de l'arrêt pour	Nombre de minutes ou d'heures après lesquelles vous souhaitez recevoir une notification lorsque le flux est hors ligne.
	Le disque est	Limite du pourcentage d'utilisation du disque après laquelle vous souhaiteriez recevoir une notification.
	La source est derrière	Nombre de sessions après lesquelles une notification est émise si la source est inférieure au nombre de sessions défini.

Paramètre	Valeur	Description
	La taille du dossier rejeté est	Limite du pourcentage d'utilisation du dossier après laquelle vous souhaiteriez recevoir une notification.
	Nombre de fichiers contenus dans le dossier des défaillances permanentes	Limite du nombre de fichiers dans le dossier d'échec permanent après laquelle vous souhaiteriez recevoir une notification.
Type de notification	Configurer l'e-mail ou la liste de distribution	Cliquez pour configurer la messagerie électronique afin de recevoir des notifications dans NetWitness Suite.
	Configurer les serveurs de traps Syslog et SNMP	Cliquez pour configurer des logs d'audit.
	Console NW, E-mail, Notification Syslog, Notification des traps SNMP	Activez la Console NW pour recevoir des notifications dans la barre d'outils de notification de l'interface utilisateur NetWitness Suite. Activez la messagerie pour recevoir des notifications par e-mail. Activez la notification Syslog pour générer des événements Syslog. Activez Notification des traps SNMP pour recevoir des événements d'audit sous la forme de traps SNMP.

Vue Surveillance

NetWitness Suite fournit des statistiques précises et d'autres informations sur l'hôte et les différents services de NetWitness Suite dans les vues Détails. La vue Surveillance vous permet d'afficher l'intégrité actuelle de tous les hôtes, de tous les services exécutés sur les hôtes, les différents aspects de l'intégrité des hôtes, ainsi que les détails relatifs aux hôtes et services.

Pour accéder à cette vue :

1. Accédez à **ADMIN > Intégrité**.
2. Cliquez sur l'onglet **Surveillance**.

Que voulez-vous faire ?

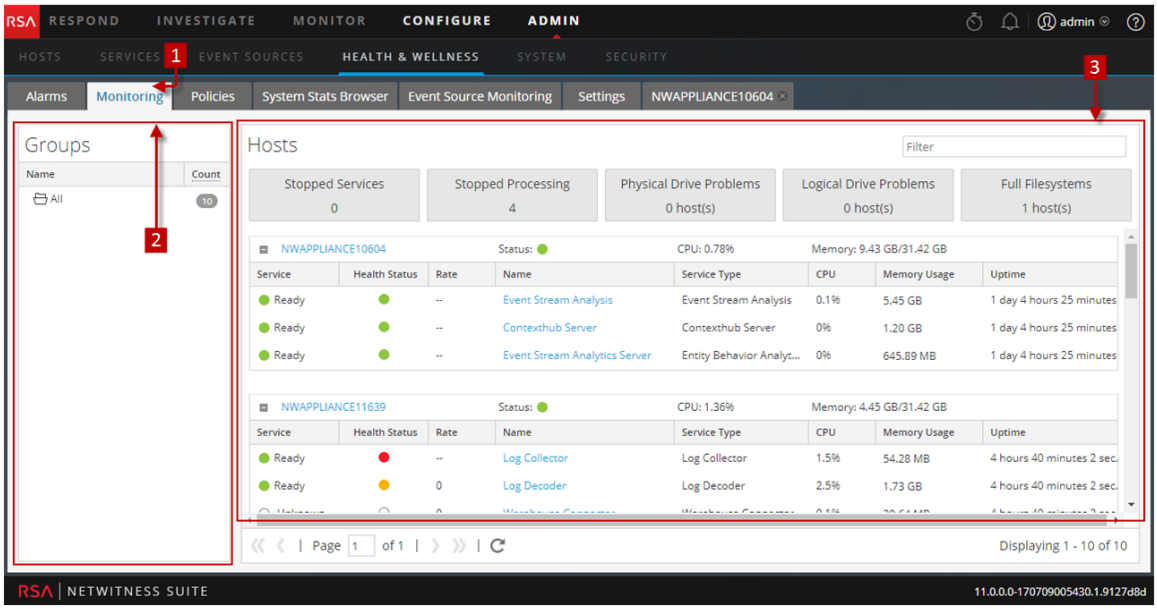
Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher et exécuter des procédures	Surveiller les hôtes et les services

Rubriques connexes

- Surveiller les hôtes et les services

Aperçu rapide

La vue Surveillance s'affiche.



1	Affiche l'onglet Surveillance.
2	Panneau Groupes permettant de sélectionner un groupe.
3	Panneau Hôtes affichant les statistiques de fonctionnement.

Panneau Groupes

Le panneau Groupes affiche tous les groupes d'hôtes disponibles. Lorsque vous sélectionnez un groupe, le contenu associé s'affiche dans le panneau Hôtes.

Remarque : Si le **nombre** d'hôtes total dans le panneau **Groupes** est inférieur au nombre réel d'hôtes affichés dans le panneau **Hôtes**, veuillez vous reporter à la section Résolution des problèmes liés à l'intégrité pour identifier les causes probables et les solutions recommandées.

Panneau Hôtes

Le panneau Hôtes affiche les statistiques de fonctionnement des hôtes et des services exécutés sur chaque hôte.

Paramètre	Description
Filter	Saisissez un nom d'hôte ou un nom de service dans le champ Filtre pour afficher les hôtes et les services correspondants dans le panneau Hôte.
Services arrêtés	Cliquez sur **Services arrêtés** pour afficher la liste de tous les services arrêtés. Est également affiché l'hôte sur lequel le service est installé.
Traitement arrêté	Cliquez sur **Traitement arrêté** pour afficher la liste de tous les hôtes dotés des services à l'état de traitement arrêté.
Problèmes de lecteur physique <#> hôte(s)	Cliquez pour afficher les hôtes rencontrant des problèmes de lecteur physique.
Problèmes de disque logique <#> hôte(s)	Cliquez pour afficher les hôtes rencontrant des problèmes de disque logique.
Systèmes de fichiers complets <#> hôte(s)	Cliquez pour afficher les hôtes rencontrant des problèmes de systèmes de fichiers complets.

Remarque : Les informations récapitulatives figurant dans les zones du haut fournissent les statistiques du système pour tous les hôtes configurés dans NetWitness Suite et ne changent pas en fonction des filtres appliqués aux groupes.

Le panneau du haut est suivi d'une liste d'hôtes, des services qui y sont installés, ainsi que des informations relatives aux hôtes et services.

Paramètre	Description
Nom d'hôte	Affiche le nom de l'hôte. Si un hôte est doté de services, vous verrez ⊞ en préfixe du nom de l'hôte. Cliquez sur ⊞ pour afficher tous les services installés sur l'hôte.
État	Affiche l'état de l'hôte. ● - indique que l'hôte est actif et en cours d'exécution. ● - indique que l'hôte est arrêté ou encore en début de traitement.
CPU	Affiche l'utilisation du CPU de l'hôte.
Mémoire	Affiche la mémoire utilisée par l'hôte.

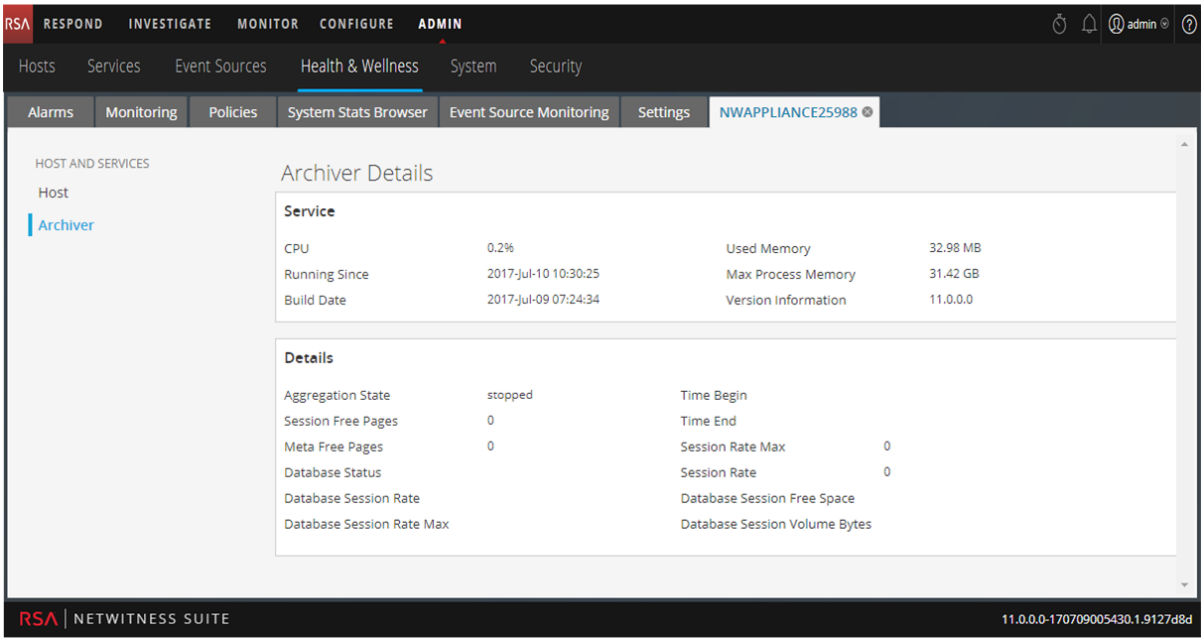
Lorsque vous cliquez sur ⊞ en préfixe du nom d'hôte, la liste de tous les services installés sur l'hôte s'affiche. Le tableau ci-dessous décrit les différents paramètres affichés pour un service et leur description.

Paramètre	Description
Service	Affiche l'état actuel du service. ● Prêt - indique que le service est actif et en cours d'exécution. ● Arrêté - indique que le service est arrêté ou encore en début de traitement.
État de santé	Affiche l'état de traitement du service. ● - indique que le processus est en cours et que les données sont traitées à une vitesse supérieure à zéro. ● - indique que le processus est arrêté. ● - indique que le processus est activé mais que les données ne sont pas en cours de traitement.
Débit	Indique la vitesse à laquelle les données sont traitées.
Nom	Nom du service.
Type de service	Nom du type de service.

Paramètre	Description
CPU	Affiche l'utilisation CPU actuelle du service.
Memory Usage	Affiche la mémoire utilisée par le service.
Uptime	Affiche la durée d'exécution du service.

Vue Détails d'Archiver

La vue Détails d'Archiver fournit des informations relatives au service Archiver. La figure ci-dessous décrit la vue Détails d'Archiver.



Pour la procédure associée, reportez-vous à la rubrique Surveiller les détails d'un service

Cette section affiche les statistiques génériques du service.

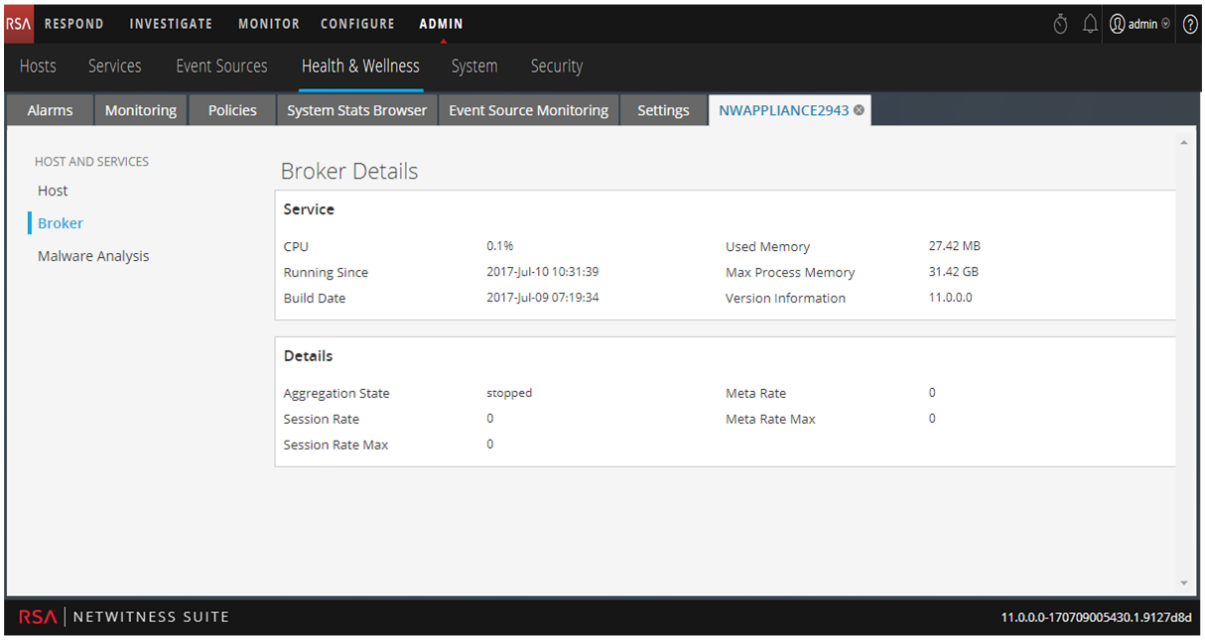
Statistiques	Description
État d'agrégation	État d'agrégation des données
Heure de début	Heure (UTC) du suivi de la première session en fonction de l'index.
Pages libres de session	Pages de session disponibles pour l'agrégation.
Heure de fin	Heure (UTC) du suivi de la dernière session en fonction de l'index.
Pages libres méta	Pages disponibles pour l'agrégation.

Statistiques	Description
Débit de session max.	Taux maximal de sessions par seconde.
Database Status	État des bases de données. Les valeurs autorisées sont les suivantes : • **fermé** - non disponible pour les fonctions QUERY et UPDATE (les bases de données sont en cours d'initialisation). Cette valeur est rarement vue. • **ouvert** - disponible pour les fonctions QUERY et UPDATE. • **échec** - échec d'ouverture. Cela peut se produire pour un nombre de raisons. Vous pouvez vérifier ce point si la CAPTURE échoue à démarrer ou si les requêtes échouent à renvoyer les données. Cela est normalement causé par la corruption de base de données.
Débit de session	Sessions per second rate
Taux de session de la base de données	Taux de session max. de la base de données
Espace libre de session de la base de données	Quantité d'espace libre de session disponible pour l'agrégation.
Débit de session max. de la base de données	Taux maximal par seconde auquel le service écrit des sessions dans la base de données.

Statistiques	Description
Octets de volume de session de la base de données	Nombre d'octets de session dans la base de données.

Vue Détails du courtier

La vue Détails du courtier fournit des informations pour le Broker. La figure suivante illustre les détails du Broker.



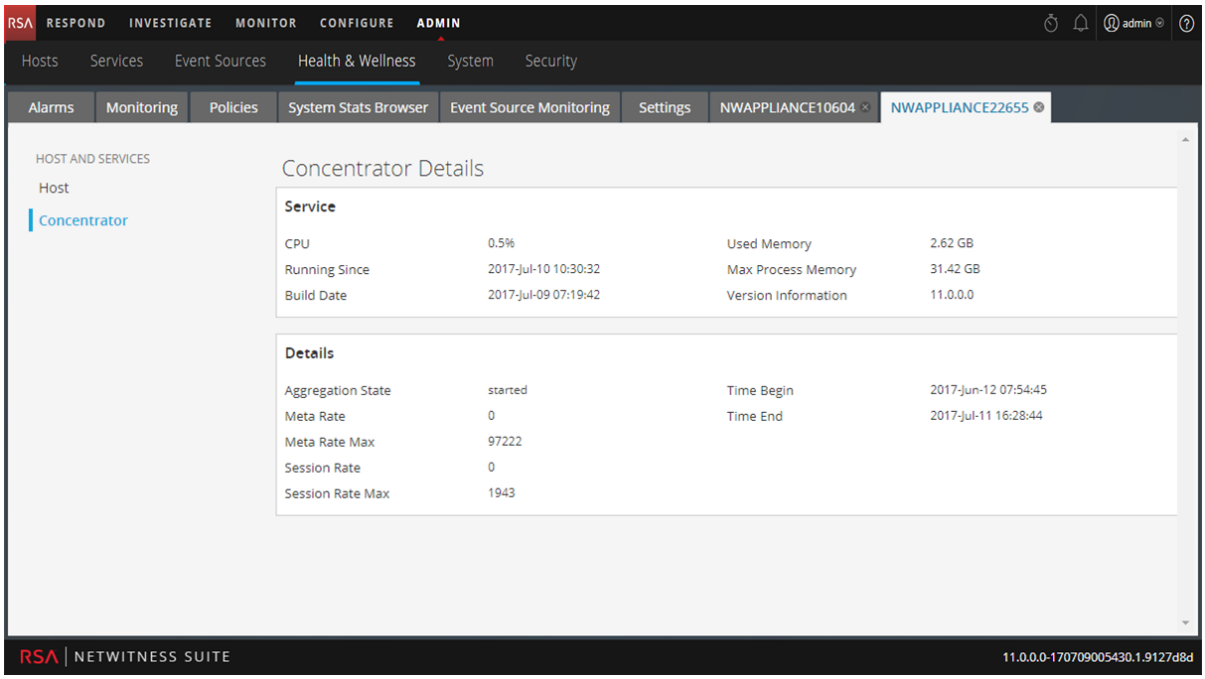
Pour la procédure associée, reportez-vous à la rubrique Surveiller les détails d'un service.

Cette section affiche les statistiques génériques du service.

Statistiques	Description
État d'agrégation	État d'agrégation des données
Débit méta	Objets de métadonnées en taux par seconde.
Débit de session	Sessions per second rate
Débit méta max.	Nombre maximal d'objets de métadonnées en taux par seconde.
Débit de session max.	Taux maximal de sessions par seconde.

Vue Détails du Concentrator

La vue Détails du Concentrator fournit des informations pour le Concentrator. La figure suivante illustre les détails du Concentrator.



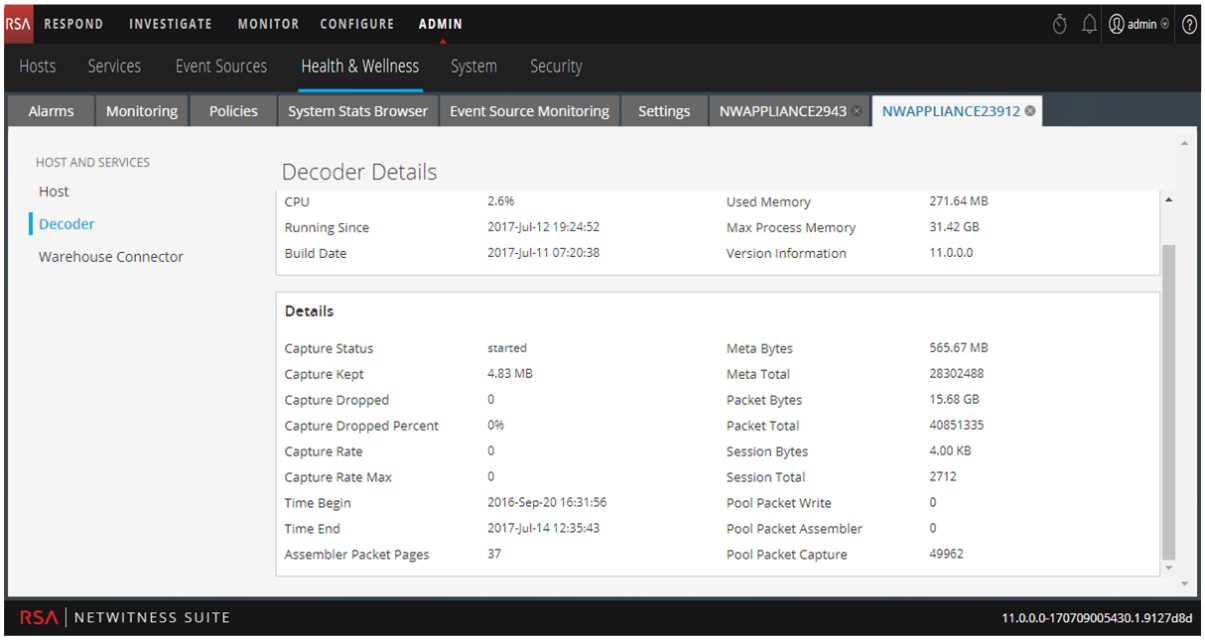
Pour la procédure associée, reportez-vous à la rubrique Surveiller les détails d'un service

Cette section affiche les statistiques génériques actuelles du service.

Statistiques	Description
État d'agrégation	État d'agrégation des données
Heure de début	Heure (UTC) du suivi de la première session en fonction de l'index.
Débit méta	Objets de métadonnées en taux par seconde.
Heure de fin	Heure (UTC) du suivi de la dernière session en fonction de l'index.
Débit méta max.	Nombre maximal d'objets de métadonnées en taux par seconde.
Débit de session	Sessions per second rate
Débit de session max.	Taux maximal de sessions par seconde.

Vue Détails du service Decoder

La vue Détails du service Decoder fournit des informations pour le Decoder. La figure suivante décrit la vue Détails du service Decoder.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Cette section affiche les statistiques génériques du service.

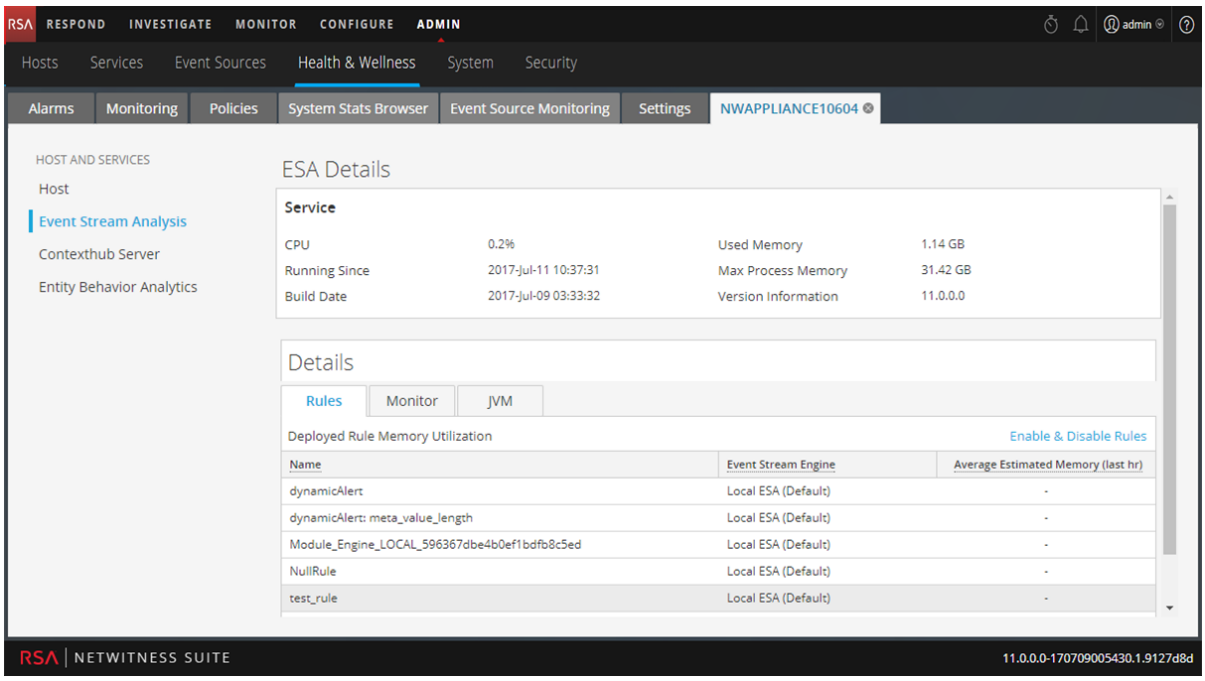
Statistiques	Description
État de la capture	État de la capture de données. Les valeurs autorisées sont les suivantes : • **démarrage** - Démarrage de la capture de données (pas encore de capture de données). • **démarrée**- Capture de données. • **arrêt**- Arrêt de la capture de données (réception de la demande d'arrêt de la capture des données, mais l'arrêt n'est pas encore effectif). • **arrêtée** - Aucune capture de données. • **désactivée** - Fonctionnalité non configurée en tant que service Decoder.
Octets méta	Nombre d'octets de métadonnées dans la base de données.
Capture conservée	Nombre de paquets conservés pendant la capture.

Statistiques	Description
Total méta	Nombre de métadonnées dans la base de données.
Capture interrompue	Nombre de paquets signalés par la carte réseau lors de la suppression. Après l'arrêt de la capture des données, le taux est réinitialisé à zéro.
Octets de paquet	Nombre d'octets de paquet dans la base de données.
Pourcentage de capture interrompue	Les paquets signalés par la carte réseau tels que supprimés en tant que pourcentage.
Total de paquet	Nombre actuel d'objets de paquets contenus dans la base de données des paquets. Le total diminue lorsque la base de données sort les fichiers pour cause de contraintes de taille. Lorsque le service cesse de capturer des données, le nombre n'est pas réinitialisé.
Taux de capture	Taux en mégaoctets par seconde auquel le service capture des données. Le taux est un exemple moyen répété sur une courte période de temps (10 secondes). Après l'arrêt de la capture des données, le taux est réinitialisé à zéro.
Octets de session	Nombre d'octets de session dans la base de données.
Taux de capture max.	Taux en mégaoctets maximum par seconde auquel le service capture des données. Le taux est un exemple moyen répété sur une courte période de temps (10 secondes). Une fois que le service arrête la capture des données, affiche le taux maximal lors de la capture de données.
Total de session	Nombre de sessions contenu dans la base de données de session. Cette valeur se réduit lorsque la base de données lance les fichiers pour cause de contraintes de taille. Lorsque le service cesse de capturer des données, le nombre n'est pas réinitialisé.

Statistiques	Description
Heure de début	Heure de capture du premier paquet (heure à laquelle le premier paquet a été stocké dans la base de données de paquets). Ce temps augmente au fur et à mesure que les paquets sortent de la base de données des paquets.
Écriture de paquet de pool	Nombre de pages de paquet actuellement dans le pipeline PCS qui sont écrites dans la base de données.
Heure de fin	Heure de capture du dernier paquet (heure à laquelle le paquet a été écrit dans la base de données). Le temps augmente au fur et à mesure que les nouveaux paquets sont capturés.
Assembleur de paquet de pool	Nombre de pages de paquets en attente d'assemblage.
Pages des paquets d'assembleur	Nombre de pages de paquets en attente d'assemblage.
Capture de paquet de pool	Nombre de pages de paquets disponibles pour la capture.

Vue Détails Event Stream Analysis (ESA)

La vue Détails Event Stream Analysis (ESA) fournit des informations pour ESA. La figure suivante illustre les Détails du service Event Stream Analysis (ESA).



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Cette section affiche les statistiques génériques actuelles et les informations de règle du service. Elles sont regroupées sous les onglets **Règles**, **Surveillance** et Java Virtual Machine (**JVM**) qui affichent les règles Event Stream Analysis et d'autres statistiques.

Onglet Surveillance

Affiche les informations statistiques génériques suivantes pour le Event Stream Analysis :

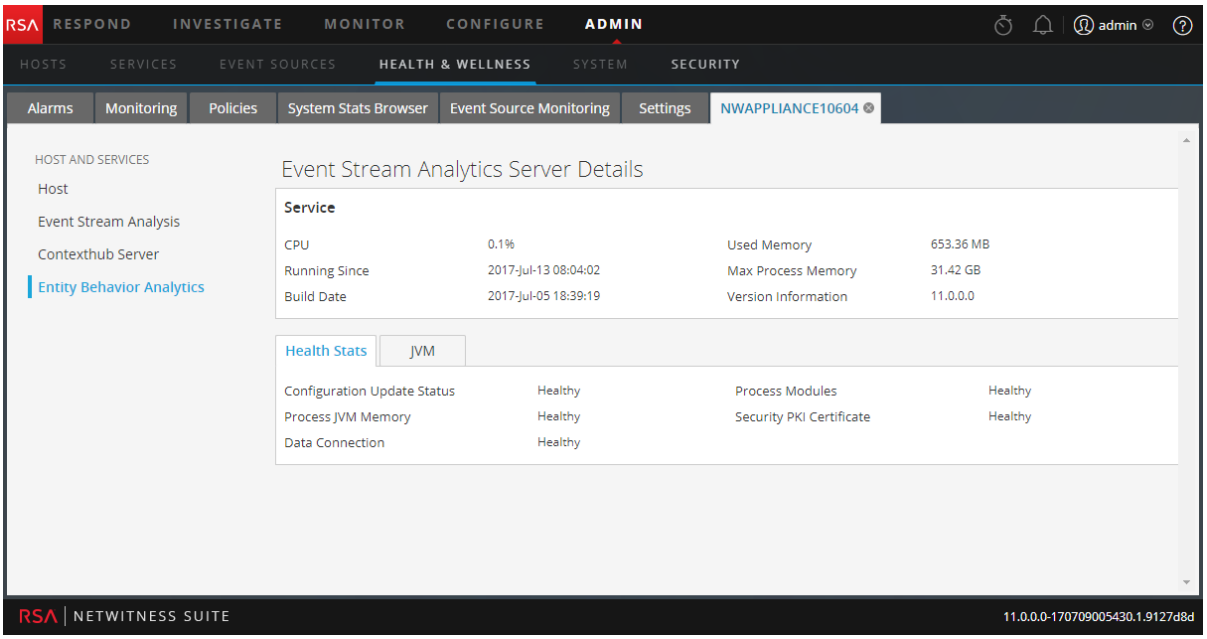
- Champ Nombre moyen d'octets reçus par message d'événement.
- Nombre moyen d'octets reçus par message d'événement.
- Nombre total d'octets reçus.
- Nombre total de champs reçus.
- Nombre de règles déployées sur le service ESA. La somme des règles Activé et Désactivé doit être égale au nombre de règles Déployé.
- Nombre total d'événements correspondant à toutes les règles sur le service ESA.
- Nombre total d'événements analysés par le service ESA depuis son dernier démarrage.
- Nombre total d'alertes déclenchées sur la base de toutes les règles du service ESA.
- Total interrompu en retard
- Total alimenté à temps

- Total sortie précoce
- Secondes entre les feeds
- Délai dans la fenêtre
- Total d'événements dans la fenêtre
- Pourcentage de fenêtre consommé
- Total d'unités de travail source
- Total de bus interrompus par charge utile
- Total de bus interrompus par événements
- Total de bus interrompus par champs
- Nombre total d'alertes envoyées au bus de messages
- Nombre total d'événements de bus
- Nombre total d'unités de travail de bus
- Total de points de terminaison détectés
- Total de points de terminaison perdus
- Nombre total de clients en échec
- Nombre total de clients réussis
- Nombre total de serveurs réussis
- Minutes écoulées depuis la dernière réussite
- Nombre de fois que le proxy a été demandé et accordé.
- Total de requêtes réussies
- Nombre de fois que le proxy a été demandé et non accordé.
- Total de requêtes non réussies

Vue Détails du service ESA Analytics

La vue Détails du service ESA Analytics fournit des informations sur l'état d'intégrité du service ESA Analytics sélectionné. Les services ESA Analytics traitent les données de détection automatisée des menaces. Il est important que vous abordiez tout élément coché affichant un état autre que vert (sain), afin que le traitement des données ne soit pas interrompu et que les événements critiques ne soient pas ignorés.

La figure suivante illustre la vue Détails du service ESA Analytics.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Détails ESA Analytics

Cette section affiche les statistiques génériques du service ESA Analytics sélectionné.

État de santé

La section État d'intégrité affiche l'intégrité des éléments suivants pour le service ESA Analytics sélectionné :

- Mongo
- JVM (Machine virtuelle Java)
- Espace disque
- Module Domaines suspects
- Module Analytique comportementale de l'utilisateur

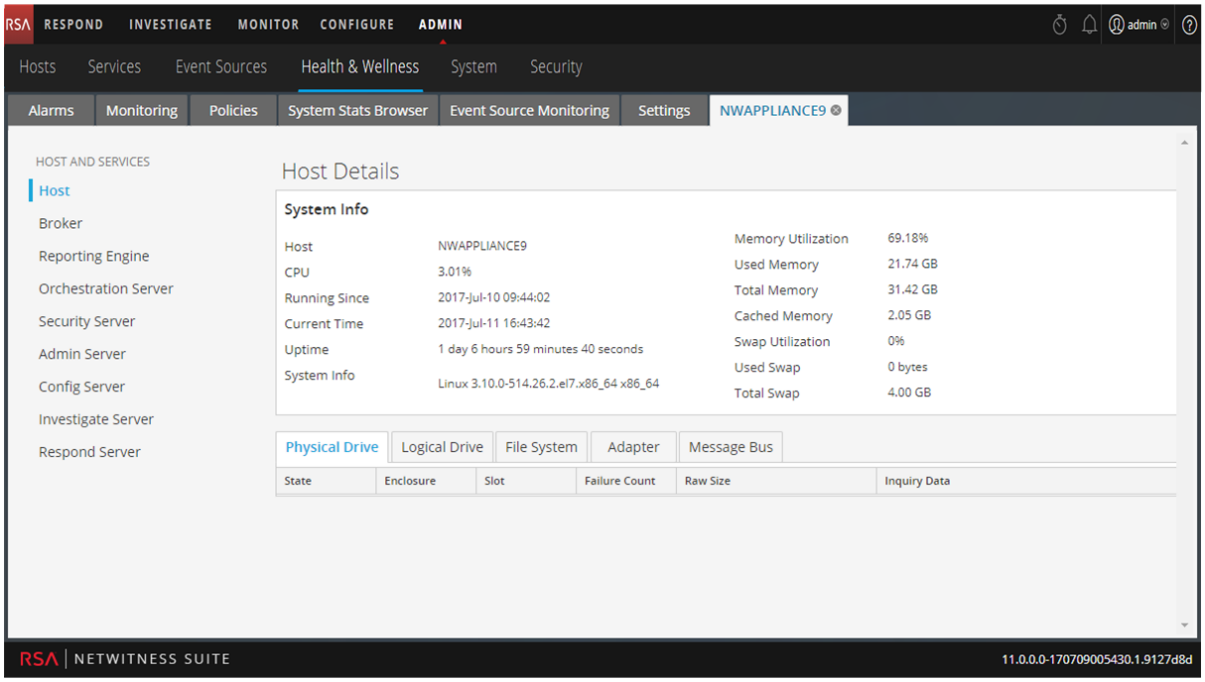
Le tableau suivant décrit la signification de chaque état d'intégrité.

État de santé	Description
Vert	Sain
Jaune	Défectueux
Rouge	Critique et il a besoin d'une attention immédiate.

État de santé	Description
- -	Inapplicable

Vue Détails de l'hôte

La vue Détails de l'hôte fournit des informations sur un hôte. La figure suivante décrit les Détails de l'hôte.



Le panneau Options sur la gauche affiche l'hôte et les services installé sur l'hôte. Vous pouvez cliquer sur Héberger un service pour afficher les statistiques et d'autres informations pertinentes pour cet hôte ou service.

Le panneau Détails affiche des informations spécifiques à l'hôte et fournit des informations supplémentaires concernant le matériel de l'hôte.

Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Cette section affiche les performances, la capacité et les statistiques historiques actuelles pour l'hôte.

Paramètre	Description
Hôte	Nom d'hôte.
CPU	Utilisation de CPU actuelle de l'hôte.
Exécution depuis	Date et heure de début de l'hôte.

Paramètre	Description
Heure actuelle	Heure actuelle sur l'hôte.
Temps de disponibilité	Durée pendant laquelle l'hôte est resté actif.
Informations sur le système	Version du système d'exploitation installée sur l'hôte.
Utilisation de la mémoire	Pourcentage de mémoire utilisé par l'hôte.
Mémoire utilisée	Mémoire utilisée en Go.
Mémoire totale	Capacité de la mémoire installée sur le système.
Mémoire mise en cache	Mémoire mise en cache sur disque, en Go.
Utilisation de la permutation	Pourcentage d'utilisation de la permutation.
Permutation utilisée	Permutation utilisée en Go.
Permutation totale	Capacité de la permutation installée sur le système.

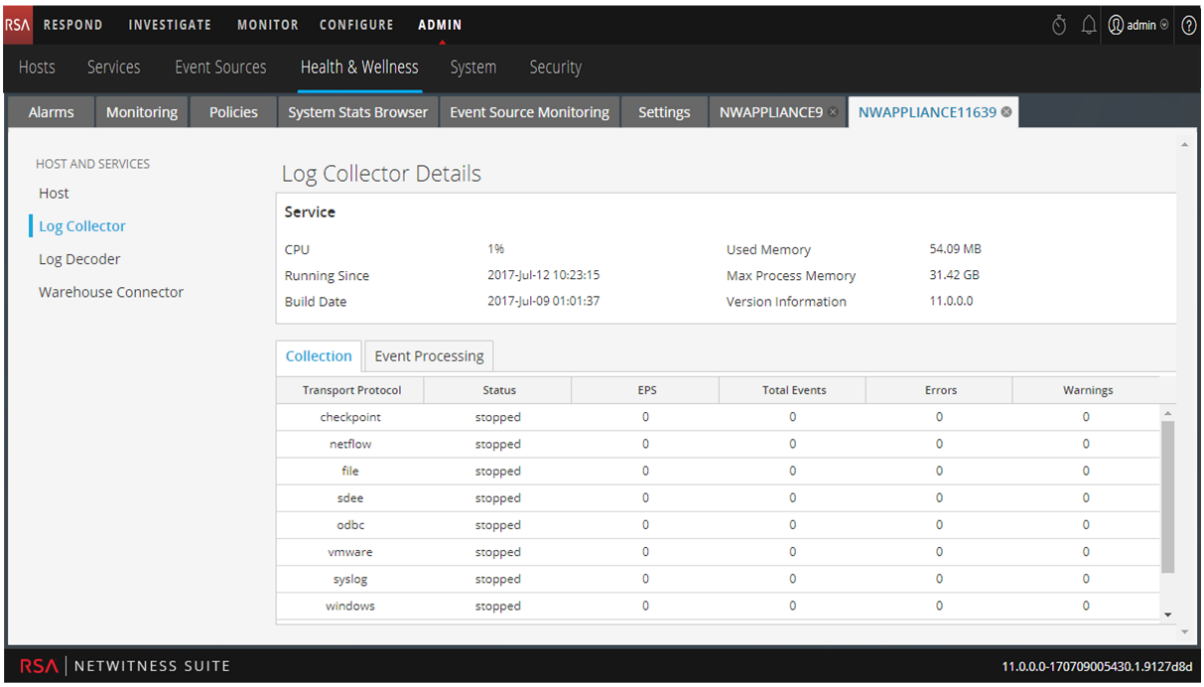
La section inférieure affiche les statistiques génériques en cours pour l'hôte sous les onglets décrits dans le tableau ci-dessous.

Onglet	Description
Lecteur physique	Type de lecteur physique, son utilisation et informations supplémentaires de l'unité physique sur l'hôte.
Lecteur logique	Lecteur logique sur l'hôte.
Système de fichiers	Informations sur le système de fichiers, taille, utilisation actuelle et capacité disponible sur l'hôte.
Adaptateur	Adaptateur utilisé sur l'hôte.

Onglet	Description
Bus de messages	**Publier dans le taux** - taux auquel les messages entrants sont publiés dans la file d'attente du bus de messages. **Nbre total de messages en attente** - nombre de messages contenus dans la file d'attente des messages. **Mémoire utilisée** - quantité de mémoire utilisée par le bus de messages (en octets). **Disque libre** - espace disque libre disponible pour le bus de messages (en octets). **Limite de mémoire** - limite de la mémoire système. Si l'utilisation de mémoire dépasse cette valeur, cela déclenche l'**Alarme de mémoire** et Security Analytics cesse d'accepter des messages. **Limite d'espace libre sur le disque** - espace disque libre disponible pour le bus de messages. Si l'espace disque disponible est inférieur à cette valeur, cela déclenche l'**Alarme disque libre** et Security Analytics arrête d'accepter des messages. **Limite de mémoire disponible** - quantité de mémoire disponible dans ce courtier de messages (en octets) avant que l'**alarme Mémoire utilisée** soit déclenchée. **Limite d'espace libre sur le disque** - quantité d'espace disque libre disponible pour ce courtier de messages (en octets) avant que l'alarme **Limite d'espace libre** sur le disque soit déclenchée. **Alarme d'espace libre sur le disque** - **True** ou **False**. **True** indique que l'espace disque disponible est inférieur à la valeur définie sous **Limite d'espace libre** sur le disque et Security Analytics a arrêté l'acceptation des messages. **Alarme de mémoire** - **True** ou **False**. **True** indique que la mémoire disponible est inférieure à la valeur définie sous **Limite Mémoire** et Security Analytics a arrêté l'acceptation des messages.

Vue Détails du service Log Collector

La vue Détails du service Log Collector fournit des informations pour le Log Collector. La figure ci-dessous décrit les Détails du service Log Collector.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

La section inférieure comprend les onglets **Collecte** et **Traitement des événements**qui affichent des statistiques génériques pour le service.

Onglet Collecte

Affiche les statistiques de collecte des événements pour chaque protocole Log Collection implémenté dans NetWitness Suite (reportez-vous au ***Guide de mise en route de Log Collection*** dans les ***Guides de Log Collection***).

Onglet Traitement des événements

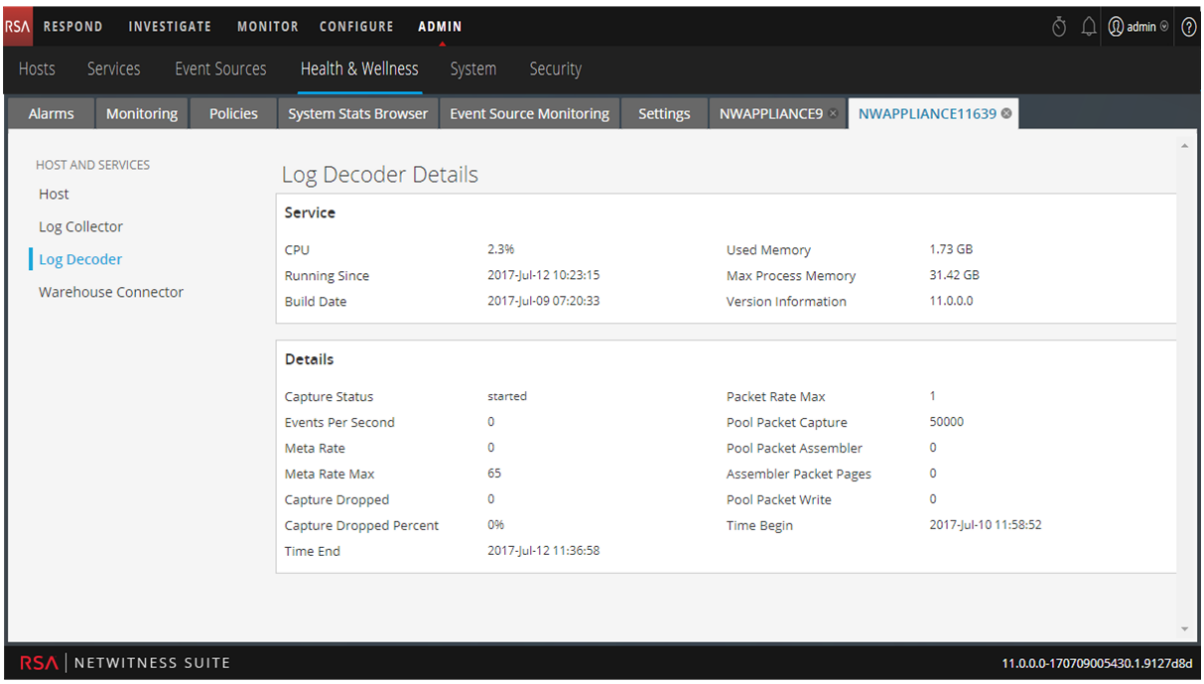
Affiche les statistiques pour le protocole de traitement d'événements interne NetWitness Suite (c'est-à-dire, le Log Decoder) pour Log Collection.

Paramètre	Description
Protocole de transport	NetWitness Suite Utilisation du protocole pour les Log Collection (c'est-à-dire, le Log Decoder).

Paramètre	Description
État	État du Log Decoder. Les valeurs autorisées sont les suivantes : • **démarrage** - Démarrage de la capture de données (pas encore de capture de données). • **démarrée**- Capture de données. • **arrêt**- Arrêt de la capture de données (réception de la demande d'arrêt de la capture des données, mais l'arrêt n'est pas encore effectif). • **arrêtée** - Aucune capture de données. • **désactivée** - Fonctionnalité non configurée en tant que service Decoder.
EPS	Taux (événements par seconde) auquel le Log Decoder traite des événements du Log Collector.
Nombre total d'événements	Nombre total d'événements traités par le Log Decoder.
Erreurs	Nombre d'erreurs rencontrées.
Avertissements	Nombre d'avertissements rencontrés.
Débit en octets	Débit actuel en octets par seconde.

Vue Détails du service Log Decoder

La vue Détails du service Log Decoder fournit des informations sur le service Log Decoder. La figure suivante illustre la vue Détails du service Log Decoder.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Cette section affiche les statistiques génériques du service.

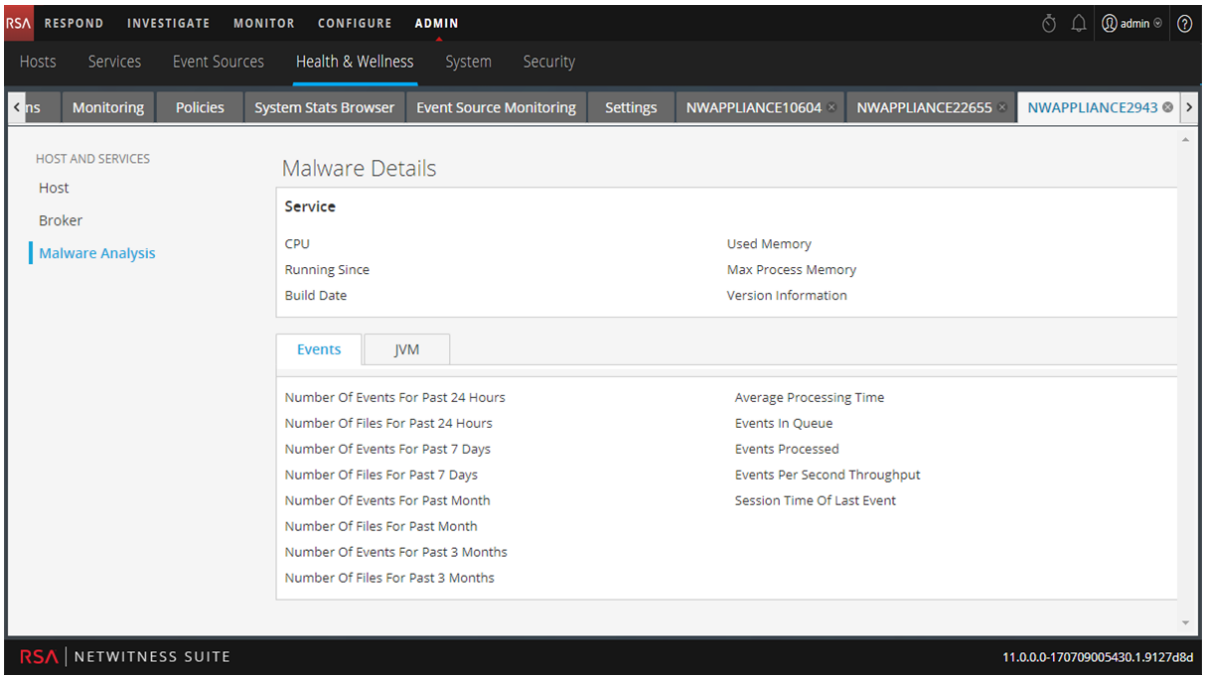
Statistiques	Description
État de la capture	État de la capture de données. Les valeurs autorisées sont les suivantes : • **démarrage** - Démarrage de la capture de données (pas encore de capture de données). • **démarré** - Capture de données. • **arrêt** - Arrêt de la capture de données (réception de la demande d'arrêt de la capture des données, mais l'arrêt n'est pas encore effectif). • **arrêté** - Aucune capture de données. • **désactivé** - Fonctionnalité non configurée en tant que service Log Decoder.
Taux de paquet max.	Taux maximal par seconde auquel le service écrit des paquets dans la base de données. Le taux est un exemple moyen répété sur une courte période de temps (10 secondes). Une fois que le service arrête la capture des données, affiche le taux maximal lors de la capture de données.

Statistiques	Description
Événements par seconde	Taux (événements par seconde) auquel le Log Decoder traite des événements du Log Collector.
Capture de paquet de pool	Nombre de pages de paquets disponibles pour la capture.
Débit méta	Taux par seconde auquel le service écrit des objets de métadonnées dans la base de données. Le taux est un exemple moyen répété sur une courte période de temps (10 secondes). Après l'arrêt de la capture des données, le taux est réinitialisé à zéro.
Assembleur de paquet de pool	Nombre de pages de paquets en attente d'assemblage.
Débit méta max.	Taux maximal par seconde auquel le service écrit des objets de métadonnées dans la base de données. Le taux est un exemple moyen répété sur une courte période de temps (10 secondes). Une fois que le service arrête la capture des données, affiche le taux maximal atteint lors de la capture de données.
Pages des paquets d'assembleur	Nombre de pages de paquets en attente d'assemblage.
Capture interrompue	Nombre de paquets signalés par la carte réseau lors de la suppression. Après l'arrêt de la capture des données, le taux est réinitialisé à zéro.
Écriture de paquet de pool	Nombre de pages de paquet dans le pipeline PCS qui sont écrites dans la base de données.
Pourcentage de capture interrompue	Les paquets signalés par la carte réseau tels que supprimés en tant que pourcentage.

Statistiques	Description
Heure de début	Heure de capture du premier paquet (heure à laquelle le premier paquet a été stocké dans la base de données de paquets). Ce temps augmente au fur et à mesure que les paquets sortent de la base de données des paquets.
Heure de fin	Heure de capture du dernier paquet (heure à laquelle le paquet a été écrit dans la base de données). Le temps augmente au fur et à mesure que les nouveaux paquets sont capturés.

Vue Détails du service Malware

La vue Détails du service Malware fournit des informations pour le service Malware Analysis. La figure suivante illustre les Détails du service Malware.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

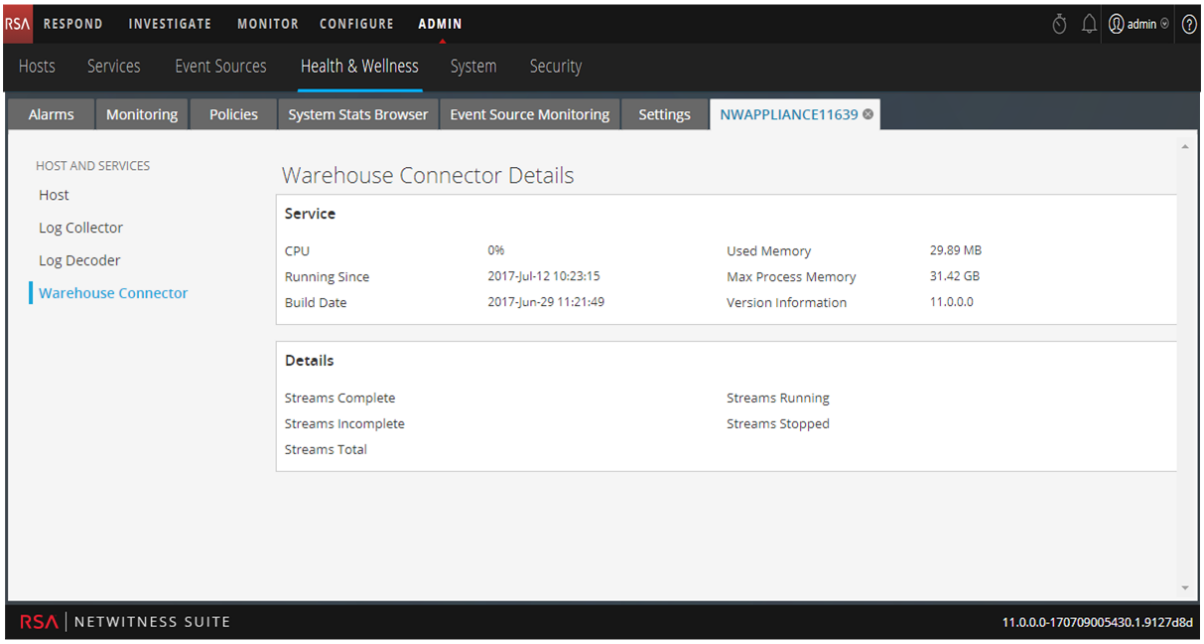
Affiche les informations statistiques suivantes liées aux événements pour le service Malware Analysis.

- Nombre d'événements durant les 24 dernières heures
- Temps moyen de traitement
- Nombre de fichiers durant les 24 dernières heures
- Événements dans la file d'attente

- Nombre d'événements durant les 7 derniers jours
- Événements traités
- Nombre d'événements durant les 7 derniers jours
- Débit d'événements par seconde
- Nombre d'événements durant le mois dernier
- Heure de session du dernier événement
- Nombre de fichiers durant le mois dernier
- Nombre d'événements durant les 3 derniers mois
- Nombre de fichiers durant les 3 derniers mois

Vue Détails du service Warehouse Connector

L'onglet Détails du service Warehouse Connector fournit des informations pour le service Warehouse Connector, telles que sa date d'intégration, le CPU et des informations de version. La figure suivante illustre les Détails du service Warehouse Connector.



Pour la procédure associée, reportez-vous à la section Surveiller les détails d'un service.

Vue Règles

L'autorisation requise pour accéder à cette vue est **Gérer les services**.

Que voulez-vous faire ?

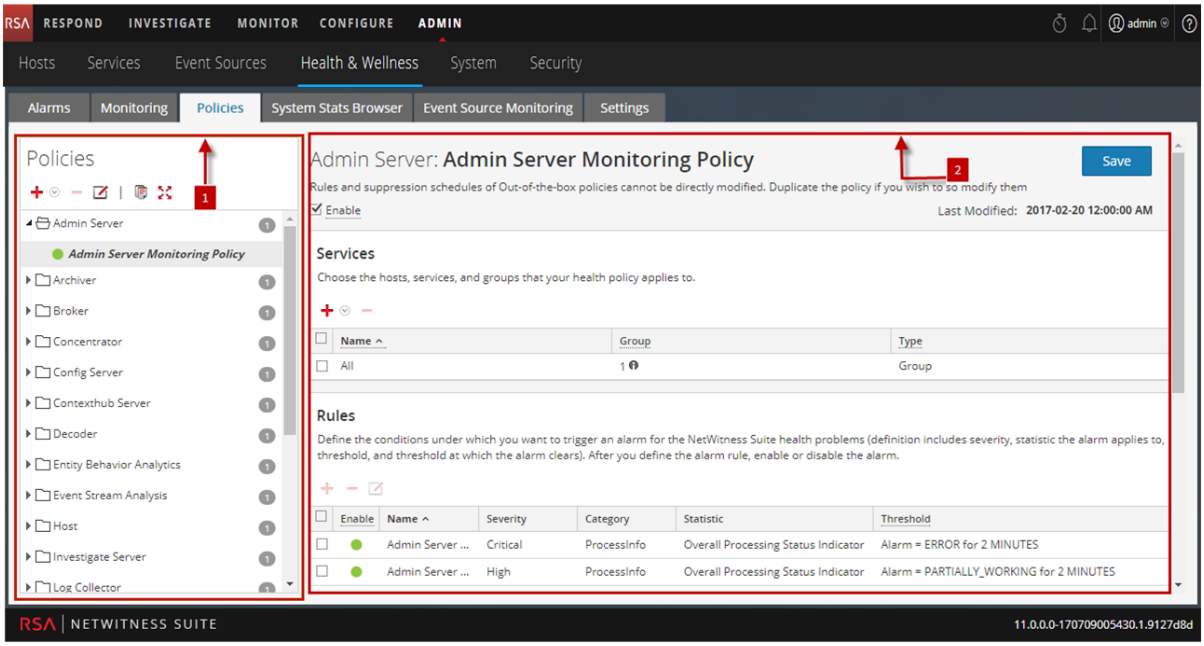
Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher les règles Serveur NetWitness et services	Gérer les règles
Administrateur	Ajouter, modifier, dupliquer et supprimer des règles	Gérer les règles

Rubriques connexes

Gérer les règles

Aperçu rapide

Cette figure illustre la vue Règles.



1	Panneau Règles
2	Panneau Détails des règles

1. Accédez à **ADMIN > Intégrité**.
2. Cliquez sur l'onglet **Stratégies**.

Panneau Stratégies

Le panneau Stratégies vous permet d'ajouter ou de supprimer des stratégies pour les hôtes et les services.

Fonctionnalité	Description
	Affiche les types de services disponibles pour créer une nouvelle stratégie. Sélectionnez-en un pour être en mesure de lui définir une ou des stratégies.
	Supprime la stratégie sélectionnée du panneau Stratégies. Vous ne pouvez supprimer qu'une stratégie à la fois.
	Permet de modifier le nom de la stratégie.
	Crée une copie de la stratégie sélectionnée. Par exemple, si vous sélectionnez **Première stratégie**, puis que vous cliquez sur  , NetWitness Suite crée une copie de cette stratégie et la nomme Première stratégie (1).
	Développe la liste des stratégies sous les services et les hôtes du panneau **Stratégies**.
	Réduit la liste des stratégies sous les services et les hôtes du panneau **Stratégies**.
	Liste des : • services et hôtes pour lesquels vous avez défini des stratégies. • stratégies RSA standard que vous pouvez appliquer aux hôtes et aux services.

Panneau Détails de la stratégie

Le panneau **Détails de la stratégie** affiche la stratégie sélectionnée dans le panneau Stratégies.

Fonctionnalité	Description
Enregistrer	Enregistre les modifications que vous avez effectuées dans ce panneau.

Fonctionnalité	Description
Type de politique	Affiche le type de politique que vous avez sélectionnée.
Date de modification	Affiche la date de dernière modification de cette stratégie.
☐ Activer	Cochez ou décochez cette case pour activer ou désactiver la stratégie.
Services	
	Affiche un menu dans lequel vous sélectionnez : • **Groupes** pour afficher la boîte de dialogue **Groupes** à partir de laquelle vous sélectionnez les groupes de services pour cette stratégie. • **Service/Hôte** pour afficher la boîte de dialogue **Service/Hôte** à partir de laquelle vous sélectionnez les groupes de services pour cette stratégie. Si la stratégie est de type **Hôte**, le menu affichera **Hôte** et non **Service**. Vous pouvez sélectionner des services en fonction du type de stratégie.
	Supprime le service ou le groupe sélectionné de la stratégie.
Règles	
	Affiche la boîte de dialogue Ajouter une règle qui vous permet de définir une règle pour la stratégie.
	Supprime la règle sélectionnée de la politique.
	Affiche la boîte de dialogue Modifier une règle pour la règle sélectionnée.
Suppression de politique	
	Ajoute une ligne relative à la période de suppression d'une politique.
	Supprime la ligne relative à la période de suppression de la politique sélectionnée.

Fonctionnalité	Description
Fuseau horaire	Sélectionne un fuseau horaire pour la politique dans la liste déroulante. Cette période s'appliquera à la fois aux zones Fuseau horaire et Suppression de politique.
☐	Permet d'activer la case à cocher pour sélectionner la ligne relative à la période de suppression d'une politique.
Jours	Jours de la semaine où vous souhaitez supprimer la stratégie en fonction de l'intervalle de temps spécifié. Cliquez sur le jour de la semaine auquel supprimer la stratégie. Vous pouvez sélectionner une combinaison de jours incluant tous les jours.
Période	Période durant laquelle la stratégie est supprimée pour les jours sélectionnés.
Notifications	
+	Ajoute une ligne de notification EMAIL.
−	Supprime la ligne relative à la période de suppression de la politique sélectionnée.
Paramètres de notification	Ouvre la vue Serveurs de notification dans laquelle vous pouvez définir les paramètres de notification par e-mail.
☐	L'activation de la case à cocher permet de sélectionner la ligne relative à la période de suppression d'une politique.
Résultat	Type de notification défini sur la page Notifications globales. Peut être effectué par e-mail, SNMP, Syslog ou Script.
Destinataire	Nom de la personne qui reçoit la notification.
Serveur de notification	Sélectionnez le serveur de notification par E-MAIL Consultez la section Configurer les serveurs de notification dans le *Guide de configuration système* pour obtenir la source des valeurs indiquées dans cette liste déroulante.

Fonctionnalité	Description
Modèle	Sélectionnez un modèle pour cette notification par E-MAIL. RSA fournit le modèle SMTP par défaut de type Intégrité et le modèle d'alarmes. Consultez la section **Configurer des modèles pour les notifications** dans le *Guide de configuration système* pour obtenir la source des valeurs indiquées dans cette liste déroulante. **Remarque :** Reportez-vous à Inclure la ligne d'objet de l'e-mail par défaut si vous souhaitez inclure la ligne d'objet de l'e-mail par défaut du modèle de type Intégrité dans vos notifications par e-mail Intégrité pour des destinataires spécifiés.

Boîte de dialogue Groupes

Fonctionnalité	Description
Panneau **Groupes**	
Nom	Affiche les groupes de services que vous avez définis. Vous pouvez sélectionner : • **Tout** pour afficher tous vos services dans le panneau **Service**s. • Groupe affichant les services qu'il contient dans le panneau **Services**.
Panneau **Services**	
Name	Affiche l'état du service.
Hôte	Affiche l'hôte sur lequel le service est exécuté.
Type	Affiche le type de service.

Boîte de dialogue Règles

Fonctionnalité	Description
☐ Activer	Cochez ou décochez cette case pour activer ou désactiver la règle de cette stratégie.
Name	Affiche le nom de la règle.

Fonctionnalité	Description
Description	Indiquez la description de la règle. RSA vous suggère d'inclure les informations suivantes dans ce champ. • Description des informations - objectif de la règle et les problèmes qu'elle surveille. • Correction - procédures à suivre pour résoudre la condition qui déclenche l'alarme pour cette règle.
Gravité	Sélectionnez la gravité de la règle. Les valeurs autorisées sont les suivantes : • Critique • Élevée • Medium • Faible
Statistiques	Sélectionnez les statistiques que vous souhaitez vérifier avec cette règle. Vous pouvez sélectionner : • une catégorie statistique dans la liste déroulante de gauche. • des statistiques dans la liste déroulante de droite. **Remarque :** Pour la politique d'infrastructure à clé publique (PKI), sélectionnez PKI dans la catégorie et les statistiques comme l'une des opérations suivantes : - Serveur NetWitness Expiration du certificat PKI : affiche le temps restant avant l'expiration du certificat. - Serveur NetWitness Expiration du certificat PKI CRL : affiche le temps restant avant la révocation des certificats (CRL). - Serveur NetWitness État CRL de l'infrastructure PKI : affiche l'état actuel de la liste CRL. Reportez-vous à la Vue Navigateur Stat. système pour obtenir des exemples de statistiques que vous souhaitez vérifier avec une règle.

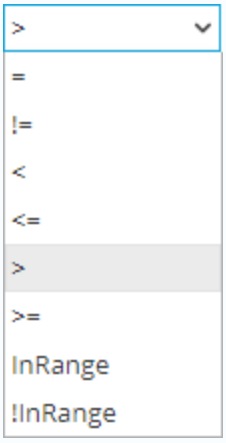
Fonctionnalité	Description
Seuil d'alarme	Définissez le seuil d'alarme de la règle qui déclenchera l'alarme de la stratégie : • Quantité **Remarque :** Pour l'expiration de la liste de révocation des certificats, le format pris en charge est jjjjhhmm, par exemple : - 10 000 représente 1 jour - 2 359 représente 23 heures et 59 minutes - 10 023 représente 1 jour et 23 minutes - 3 650 100 représente 365 jours et 1 heure • Durée en minutes
Restauration	Définissez à quel moment effacer le seuil de la règle : • Opérateur : • Pour NetWitness Suite 10.5 (=, !=, <, <=, > ou >=) • Pour NetWitness Suite 10.5.0.1 et toute version ultérieure (Voir Opérateurs de seuil ci-dessous) • Quantité • Durée en minutes
Suppression de règle	
+	Cette option vous permet d'ajouter une ligne de période de suppression de règle.
−	Cette option vous permet de supprimer la ligne de période de suppression de règle sélectionnée.
☐	Activez la case à cocher pour sélectionner la ligne relative à la période de suppression d'une règle.
Fuseau horaire : *time-zone*	Affiche le fuseau horaire de la stratégie. Sélectionnez le fuseau horaire d'une stratégie dans le panneau Suppression de politique.

Fonctionnalité	Description
Jours	Jours de la semaine où vous souhaitez supprimer la règle en fonction de l'intervalle de temps spécifié. Cliquez sur le jour de la semaine auquel supprimer la règle. Vous pouvez sélectionner une combinaison de jours incluant tous les jours.
Période	Période durant laquelle la règle est supprimée pour les jours sélectionnés.

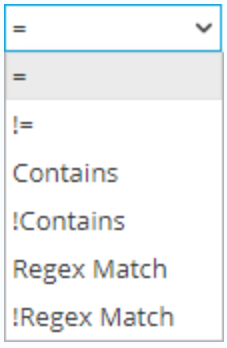
Opérateurs de seuil

Les champs **Seuil d'alarme** et **Seuil de restauration** de la boîte de dialogue **Règles** vous invitent à saisir des opérateurs numériques ou des opérateurs de chaîne en fonction des critères statistiques que vous avez spécifiés.

Menu déroulant des opérateurs numériques :



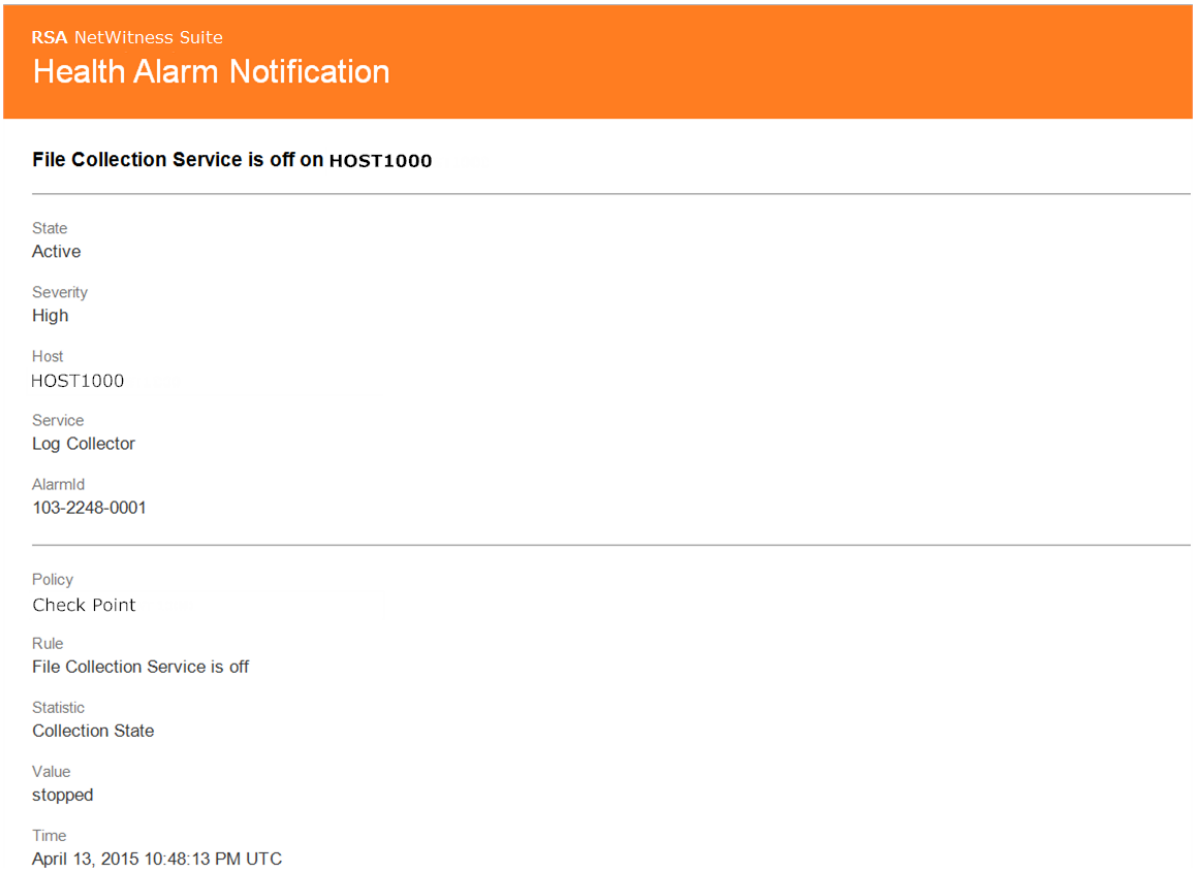
Menu déroulant des opérateurs de chaîne :



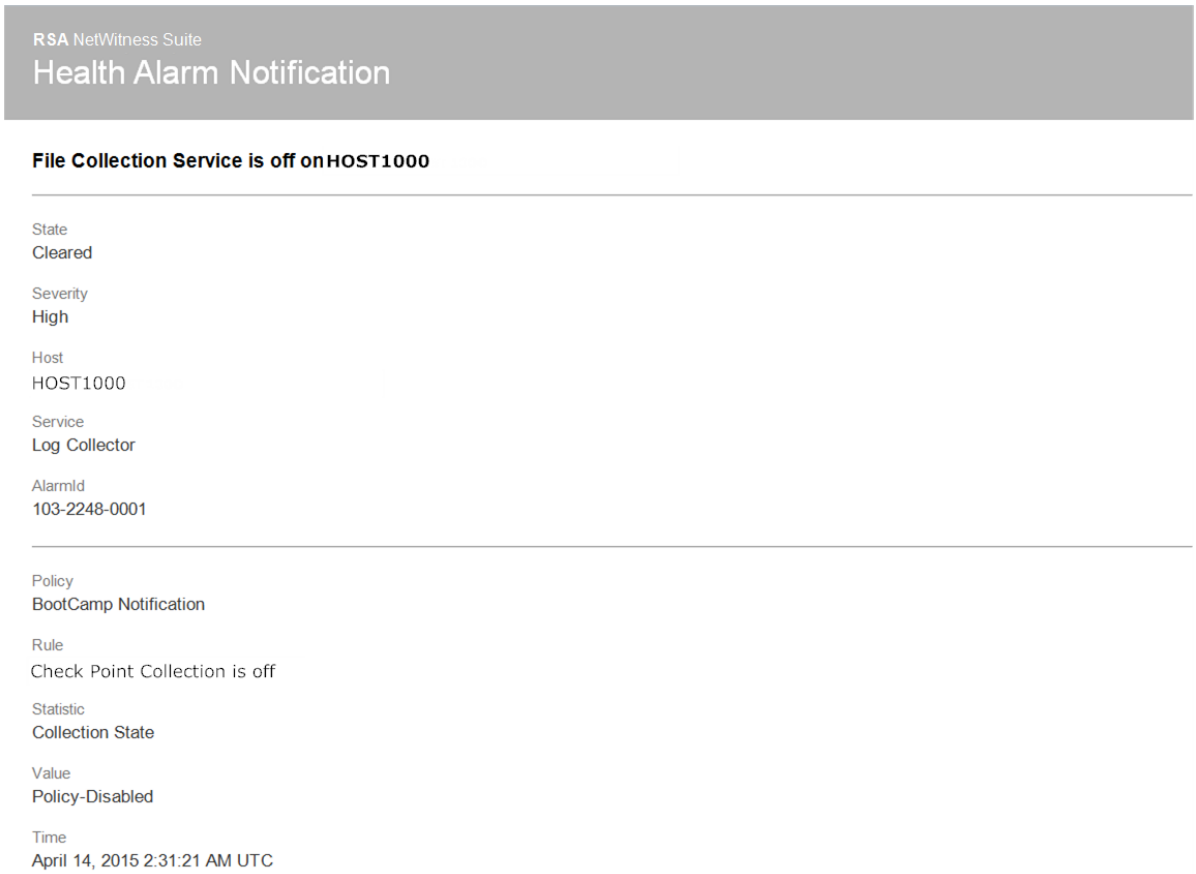
Modèles d'e-mail de type Intégrité RSA

Remarque : Reportez-vous à Inclure la ligne d'objet de l'e-mail par défaut si vous souhaitez inclure la ligne d'objet de l'e-mail par défaut du modèle de type Intégrité dans vos notifications par e-mail Intégrité pour des destinataires spécifiés.

Modèle SMTP par défaut de type Intégrité



Modèle d'alarmes


RSA NetWitness Suite

Health Alarm Notification

File Collection Service is off on HOST1000

State
Cleared

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
BootCamp Notification

Rule
Check Point Collection is off

Statistic
Collection State

Value
Policy-Disabled

Time
April 14, 2015 2:31:21 AM UTC

Règles prédéfinies NetWitness

Le tableau suivant répertorie les stratégies prédéfinies NetWitness Suite avec les règles définies pour chaque stratégie.

Cet onglet vous permet d'effectuer les tâches suivantes sur ces stratégies :

- Modifier les attributions de services/groupes.
- Les désactiver/activer.

Vous ne pouvez effectuer aucune des tâches suivantes sur ces stratégies :

- Les supprimer.
- Modifier les noms des stratégies.

Remarque : Des informations supplémentaires sur les règles prêtes à l'emploi figurent dans l'interface utilisateur sous
Intégrité – Règles.

Nom de la règle	Nom de la règle	Alarme déclenchée
	Échec de la communication entre l'hôte Security Analytics maître et un hôte distant.	L'hôte est arrêté, le réseau est arrêté, le Message Broker est arrêté, ou bien des certificats de sécurité ont été non valides ou manquants pendant 10 minutes ou plus.

Nom de la règle	Nom de la règle	Alarme déclenchée
Serveur NetWitness Règle de surveillance	Utilisation critique sur le système de fichiers du Broker de messages Rabbitmq	Pour `var/lib/rabbitmq`, l'utilisation totale du disque du système de fichiers monté dépasse 75 %.
	Le système de fichiers est plein.	L'utilisation totale du disque du système de fichiers monté atteint 100 %.
	Utilisation élevée du système de fichiers	L'utilisation totale du disque du système de fichiers monté dépasse 95 %.
	Utilisation élevée de la permutation système	L'utilisation de la permutation passe sous la barre des 5 % pendant 5 minutes ou plus.
	Utilisation élevée sur le système de fichiers du Broker de messages Rabbitmq	L'utilisation totale du disque du système de fichiers pour `var/lib/rabbitmq` dépasse 60 %.
	L'hôte n'est pas accessible	L'hôte est en panne.
	État Liaisons d'échange de processeur d'événements LogCollector	Problème avec les files d'attente de Broker de message de collecte de logs pendant 10 minutes ou plus.
	File d'attente de processeur d'événements LogCollector sans liaison	Problème avec les files d'attente de Broker de message de collecte de logs pendant 10 minutes ou plus.

Nom de la règle	Nom de la règle	Alarme déclenchée
	File d'attente de processeur d'événements LogCollector sans utilisateur	Problème avec les files d'attente de Broker de message de collecte de logs pendant 10 minutes ou plus.
	Power Supply Failure	L'hôte n'est pas alimenté
	Le disque logique RAID est dégradé	Pour le disque logique RAID, l'état du disque logique est Dégradé ou Partiellement dégradé.
	Défaillance du disque logique RAID	Pour le disque logique Raid, l'état du lecteur est Hors ligne, En échec ou Inconnu.
	Reconstruction du disque logique RAID	Pour le disque logique RAID, le disque logique est en Reconstruction.
	Défaillance du disque physique RAID	Pour le disque physique RAID, l'état du disque physique n'est pas En ligne, Étendu en ligne ou Disque de secours.
	Défaillance prévue du disque physique RAID	Pour le disque physique RAID, le nombre de défaillances prévues pour le disque physique est supérieur à 1.
	Reconstruction du disque physique RAID	Pour le disque physique RAID, le disque physique est en Reconstruction.
	Disque physique RAID non configuré	Pour le disque physique RAID, le disque physique comprend Unconfigured (good).
	Défaillance de la carte SD	L'état de la carte SD n'est pas OK.

Nom de la règle	Nom de la règle	Alarme déclenchée
Règle de surveillance NetWitness Suite Archiver	Arrêt de l'agrégation Archiver	Archiver n'est pas à l'état de démarrage.
	La ou les bases de données Archiver ne sont pas ouvertes	La base de données n'est pas à l'état d'ouverture.
	Archiver ne consomme pas de données du service	Les périphériques ne sont pas à l'état d'utilisation.
	Le service Archiver est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Arrêt du service Archiver	Le serveur n'est pas à l'état de démarrage.
NetWitness Suite Stratégie de surveillance Broker	Broker >5 requêtes en attente	Requêtes en attente supérieures ou égales à 5 pendant au moins 10 minutes.
	Arrêt de l'agrégation Broker	Le Broker n'est pas à l'état de démarrage.
	Broker ne consomme pas de données du service	Les périphériques ne sont pas à l'état d'utilisation.
	Le service Broker est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Arrêt du service Broker	Le serveur n'est pas à l'état de démarrage.
	Débit de session Broker équivalent à zéro	Le taux de session (actuel) est de 0 pendant au moins 2 minutes.

Nom de la règle	Nom de la règle	Alarme déclenchée
NetWitness Suite Stratégie de surveillance Concentrator	Concentrator >5 requêtes en attente	Requêtes en attente supérieures ou égales à 5 pendant au moins 10 minutes.
	Valeur Behind d'agrégation Concentrator >100 000 sessions	Requêtes en attente supérieures ou égales à 100 000 pendant au moins 1 minute ou plus.
	Valeur Behind d'agrégation Concentrator >1 000 000 sessions	Requêtes en attente supérieures ou égales à 1 000 000 pendant au moins 1 minute.
	Valeur Behind d'agrégation Concentrator >50 000 000 sessions	Requêtes en attente supérieures ou égales à 50 000 000 pendant au moins 1 minute.
	Arrêt de l'agrégation Concentrator	Le Broker n'est pas à l'état de démarrage.
	La ou les bases de données Concentrator ne sont pas ouvertes	La base de données n'est pas à l'état d'ouverture.
	Taux méta du Concentrator équivalent à zéro	Taux méta du Concentrator (actuel) est de 0 pendant au moins 2 minutes.
	Concentrator ne consomme pas de données du service	Les périphériques ne sont pas à l'état d'utilisation.

Nom de la règle	Nom de la règle	Alarme déclenchée
	Le service Concentrator est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Arrêt du service Concentrator	Le serveur n'est pas à l'état de démarrage.
Stratégie de surveillance NetWitness Suite Decoder	La capture de Decoder n'a pas commencé	La capture n'est pas à l'état de démarrage.
	Taux de capture du Decoder équivalent à zéro	Le taux de capture (actuel) est de 0 pendant au moins 2 minutes.
	Base de données Decoder non ouverte	La base de données n'est pas à l'état d'ouverture.
	Interruption Decoder >1 % de paquets	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 1 %.
	Interruption Decoder >10 % de paquets	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 10 %.
	Interruption Decoder >5 % de paquets	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 5 %.
	Pool de capture de paquets Decoder épuisé	La file d'attente des captures de paquets est égale à 0 pendant au moins 2 minutes.
	Le service Decoder est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Service Decoder arrêté	Le serveur n'est pas à l'état de démarrage.

Nom de la règle	Nom de la règle	Alarme déclenchée
NetWitness SuiteStratégie de surveillance Event Steam Analysis	Utilisation de la mémoire totale par ESA > 85 %	Le pourcentage d'utilisation de la mémoire totale par ESA est supérieur ou égal à 85 %.
	Utilisation de la mémoire totale par ESA > 95 %	Le pourcentage d'utilisation de la mémoire totale par ESA est supérieur ou égal à 95 %.
	Service ESA arrêté	Le serveur n'est pas à l'état de démarrage.
	Règles d'évaluation ESA désactivées	L'état des règles d'évaluation n'est pas activé.
Stratégie de surveillance NetWitness Suite IPDB Extractor	Le service IPDB Extractor est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Service IPDB Extractor arrêté	Le serveur n'est pas à l'état de démarrage.
Stratégie de surveillance NetWitness Suite Incident Management	Service Incident Management arrêté	Le serveur n'est pas à l'état de démarrage.

Nom de la règle	Nom de la règle	Alarme déclenchée
Stratégie de surveillance NetWitness Suite Log Collector	Arrêt du service Log Collector	Le serveur n'est pas à l'état de démarrage.
	File d'attente d'événements Log Decoder > Saturée à 50%	Le nombre d'événements actuellement dans la file d'attente utilise 50 % ou plus de la file d'attente.
	File d'attente d'événements Log Decoder > Saturée à 80%	Le nombre d'événements actuellement dans la file d'attente utilise 80 % ou plus de la file d'attente.
	Service Log Collector en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.

Nom de la règle	Nom de la règle	Alarme déclenchée
Stratégie de surveillance NetWitness Suite Log Decoder	Interruption Decoder >10 % de paquets	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 10 %
	La capture de Logs n'a pas commencé	La capture n'est pas à l'état de démarrage.
	Taux de capture du Log Decoder équivalent à zéro	Le taux de capture (actuel) est de 0 pendant au moins 2 minutes.
	Base de données Log Decoder non ouverte	La base de données n'est pas à l'état d'ouverture.
	Suppression Log Decoder >1 % des logs	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 1 %.
	Suppression Log Decoder >5 % des logs	Le pourcentage de paquets capturés interrompus (actuel) est supérieur ou égal à 5 %.
	Pool de capture de paquets Log Decoder épuisé	La file d'attente des captures de paquets est égale à 0 pendant au moins 2 minutes.
	Arrêt du service Log Decoder	Le serveur n'est pas à l'état de démarrage.
	Service Log Decoder en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.

Nom de la règle	Nom de la règle	Alarme déclenchée
NetWitness Suite Stratégie de surveillance Malware Analysis	Arrêt du service Malware Analysis	Le serveur n'est pas à l'état de démarrage.
NetWitness Suite Stratégie de surveillance Reporting Engine	Utilisation critique des alertes Reporting Engine	Utilisation des alertes supérieure ou égale à 10 pendant au moins 5 minutes.
	Disque disponible Reporting Engine <10 %	L'espace disque disponible est inférieur à 10 %.
	Disque disponible Reporting Engine <5 %	L'espace disque disponible est inférieur ou égal à 5 %.
	Utilisation critique des graphiques Reporting Engine	Utilisation des graphiques supérieure ou égale à 10 pendant au moins 5 minutes.
	Utilisation critique des règles Reporting Engine	Utilisation des règles supérieure ou égale à 10 pendant au moins 5 minutes.
	Utilisation critique du pool de tâches planifiées Reporting Engine	Utilisation du pool de tâches planifiées supérieure ou égale à 10 pendant au moins 15 minutes.
	Arrêt du service Reporting Engine	Le serveur n'est pas à l'état de démarrage.
	Utilisation critique des tâches partagées Reporting Engine	Utilisation du pool de tâches partagées supérieure ou égale à 10 pendant au moins 5 minutes.

Nom de la règle	Nom de la règle	Alarme déclenchée
NetWitness Suite Stratégie de surveillance Warehouse Connector	Service Warehouse Connector en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Service Warehouse Connector arrêté	Le serveur n'est pas à l'état de démarrage.
	Flux Behind Warehouse Connector	Le flux Behind est supérieur ou égal à 2 000 000.
	Utilisation du disque de flux Warehouse Connector > 75 %	L'utilisation de disque de flux (charge de destination en attente) est supérieure ou égale à 75.
	Flux Warehouse Connector en mauvais état	L'état des flux n'équivaut pas à la valeur Consommation ou En ligne pendant 10 minutes ou plus.
	Le stream Warehouse Connector a rejeté de manière permanente > 300 fichiers	Le nombre de fichiers dans les fichiers rejetés de manière permanente est supérieur ou égal à 300.
	Le flux Warehouse Connector a rejeté le dossier de manière permanente > 75 % complet	L'utilisation de dossier rejeté est supérieure ou égale à 75 %.
NetWitness Suite Stratégie de surveillance Workbench	Le service Workbench est en mauvais état	Le service n'est pas à l'état de démarrage ou Prêt.
	Service Workbench arrêté	Le serveur n'est pas à l'état de démarrage.

Vue Navigateur Stat. système

NetWitness Suite permet de contrôler l'état et le fonctionnement des hôtes et des services installés. L'onglet Navigateur Stat. système affiche les principales informations relatives aux statistiques, au système de service et au système hôte d'un hôte ou d'un service.

Vous pouvez personnaliser la vue des statistiques selon le paramètre que vous sélectionnez pour filtrer les données.

Pour accéder à la vue Navigateur Stat. système :

1. Accédez à **ADMIN > Intégrité**.

   La vue Intégrité s'affiche avec l'onglet Alarmes ouvert.

2. Cliquez sur l'onglet **Navigateur Stat. système**.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Affiche le Graphique de l'historique relatif aux statistiques du système	Graphique de l'historique relatif aux statistiques du système

Rubriques connexes

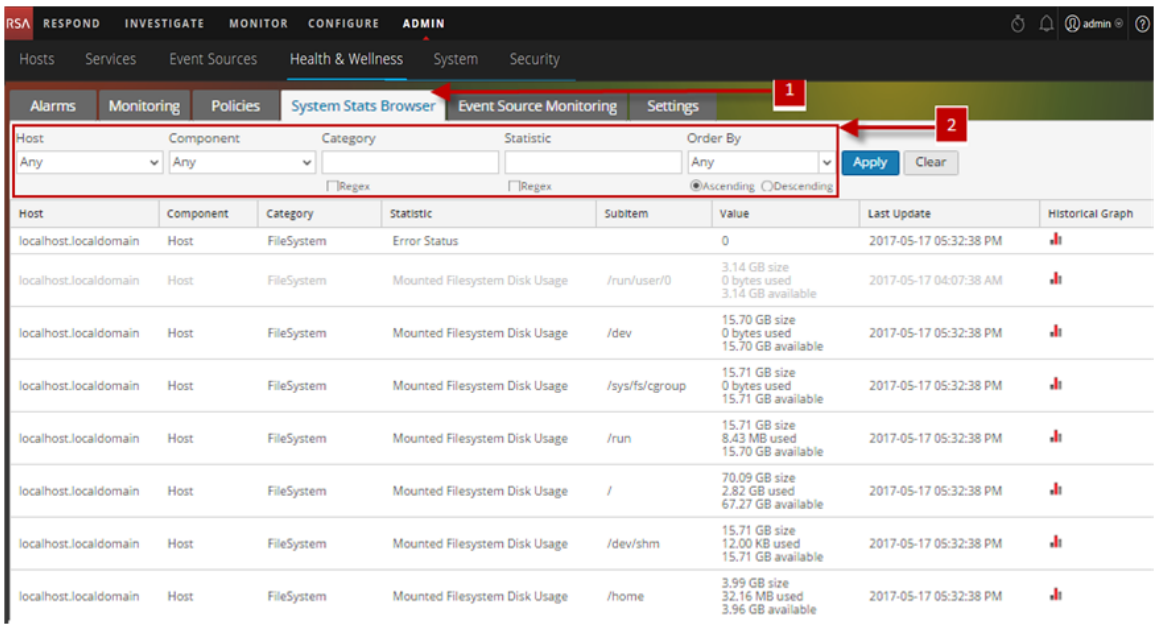
Surveiller les statistiques liées aux services

Filtrer les statistiques du système

Afficher un graphique de l'historique des statistiques du système

Aperçu rapide

La vue Navigateur Stat. système s'affiche.



1 Affiche la vue Navigateur Stat. système

2 Barre d'outils permettant de filtrer et de personnaliser la vue navigateur Stat. système

Filtres

Ce tableau récapitule les différents paramètres que vous pouvez utiliser pour filtrer et personnaliser la vue Statistiques système.

Paramètre	Description
Hôte	Sélectionnez un hôte dans le menu déroulant pour afficher les statistiques correspondantes. Sélectionnez **Tous** pour afficher tous les hôtes disponibles.
Composant	Sélectionnez un composant dans le menu déroulant pour afficher les statistiques correspondantes. Sélectionnez **Tous** pour afficher tous les composants de l'hôte sélectionné.
Catégorie	Saisissez la catégorie pour laquelle afficher des statistiques. Sélectionnez Regex pour activer ce filtre. Une recherche des expressions régulières est effectuée dans du texte et la catégorie spécifiée est répertoriée. Si Regex n'est pas sélectionné, la mise en correspondance des schémas de globbing est prise en charge.

Paramètre	Description
Statistiques	Saisissez la statistique à afficher sur tous les hôtes ou composants. Sélectionnez Regex pour activer ce filtre. Une recherche des expressions régulières est effectuée dans du texte et la catégorie spécifiée est répertoriée. Si Regex n'est pas sélectionné, la mise en correspondance des schémas de globbing est prise en charge.
Réorganiser par	Sélectionnez l'ordre dans lequel la liste doit être filtrée. Sélectionnez Croissant pour la filtrer dans l'ordre croissant.

Commandes

Commande	Action
Appliquer	Cliquez pour appliquer les filtres choisis et afficher la liste correspondante.
Clear	Cliquez sur cette option pour effacer les filtres choisis.

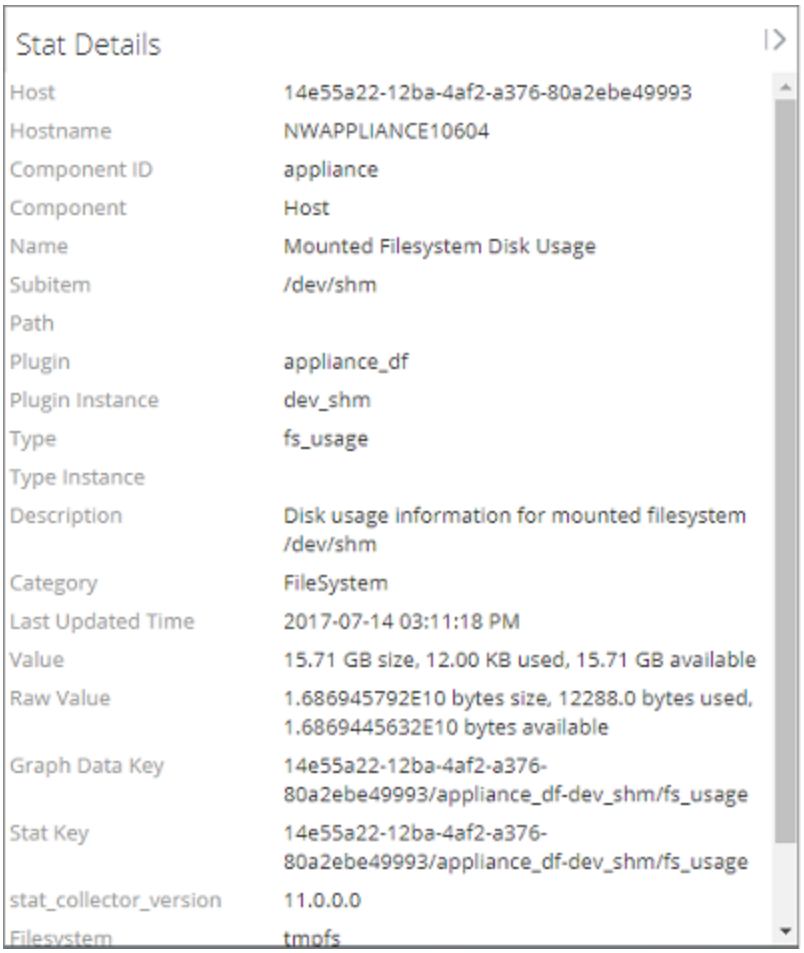
Affichage de la vue Statistiques système

Affiche les informations relatives aux statistiques, au système de services et au système hôte d'un hôte ou d'un service.

Accéder aux détails des statistiques

Sélectionnez une statistique, puis cliquez sur **Détails stat.** sur la droite du panneau.

La section Détails stat. fournit des détails sur les statistiques sélectionnées.



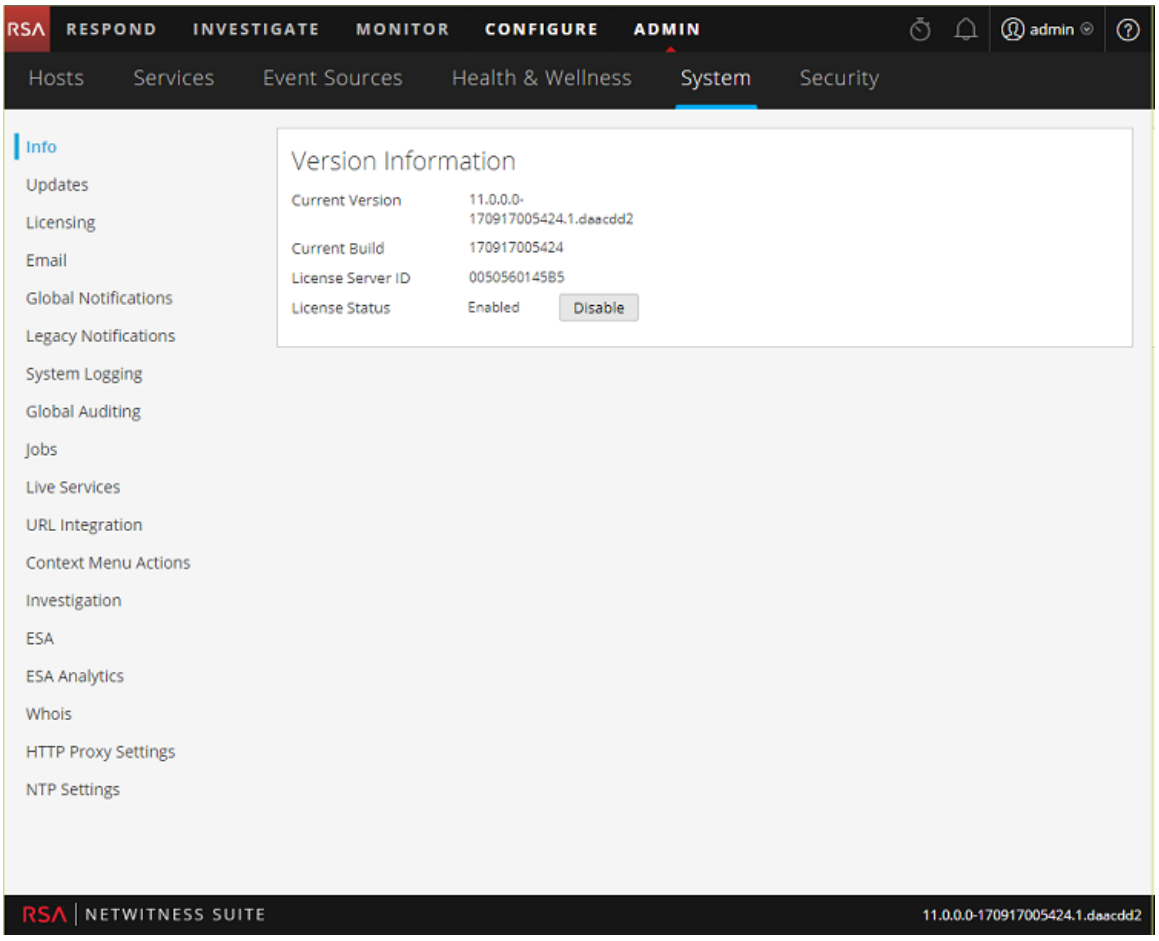
Vue système - Panneau informations du système

Cette section décrit le panneau Informations système qui affiche les informations relatives à la version du système et l'état de la licence.

Le rôle requis pour accéder à cette vue est **Gérer les paramètres du système**.

Pour accéder à cette vue, procédez de l'une des façons suivantes :

- Accédez à **ADMIN > Système**.
  Le panneau Informations système s'affiche par défaut.
- Lorsque vous recevez une notification indiquant qu'une nouvelle version de NetWitness Suite est disponible dans la barre d'état Notifications, cliquez sur **Afficher**.



La section Informations de version affiche des informations relatives à la version de NetWitness Suite actuellement installée. Le tableau ci-dessous décrit les fonctions de la section Informations de version.

Name	Description
Version actuelle	Affiche la version de Security Analytics en cours d'exécution. Le format de la version est *major-relase.minor-release.stability-id.build-number*. Les valeurs possibles pour *stability-id* sont les suivantes : • 1 - Development • 2 - Alpha • 3 - Beta • 4 - RC • 5 - Gold

Name	Description
Build actuel	Identifie la révision de la build actuelle à utiliser lors de la résolution des problèmes.
ID de serveur de licences	Le serveur LLS (Local Licensing Server) est installé sur chaque client hôte pour gérer les licences hôtes. Ce champ indique si le serveur LLS est installé pour cette instance de Security Analytics. • Si le serveur LLS est installé, son ID s'affiche. • **Inconnu** indique que le serveur LLS n'est pas installé.
État des licences	Indique si la licence est activée ou non. Si la licence est : • Activée, ce champ indique **Activé** et un bouton **Désactiver** apparaît à droite pour vous permettre de le désactiver. • Désactivée, ce champ indique **Désactivé** et un bouton **Activer** apparaît à droite pour vous permettre de l'activer.

Panneau Mises à jour système - Onglet Paramètres

Cette section décrit l'interface que vous utilisez pour configurer une connexion au référentiel des mises à jour Live. Ces paramètres permettent à NetWitness Suite d'accéder au référentiel des mises à jour Live et de le synchroniser avec votre référentiel local des mises à jour.

L'autorisation requise pour accéder à cette vue est **Appliquer les mises à jour du système**.

Pour accéder à cette vue :

1. Accédez à **ADMIN > Système**.
2. Sélectionnez **Mises à jour**.

Que voulez-vous faire ?

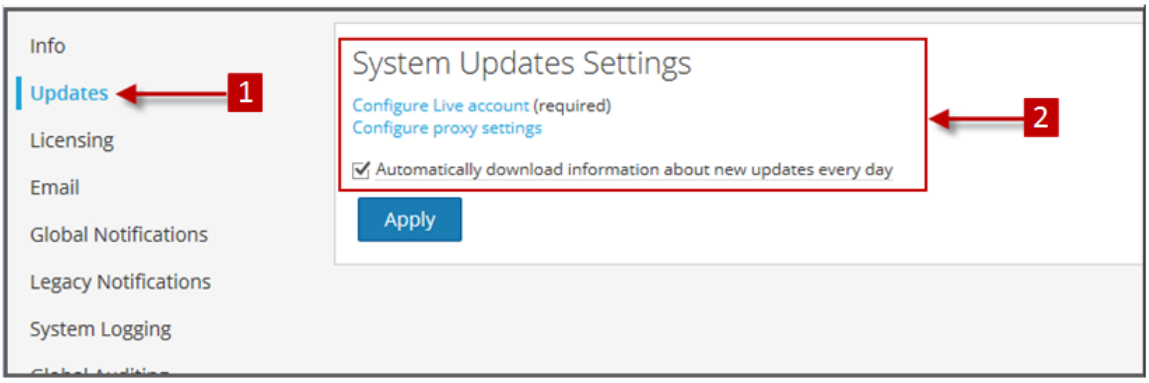
Rôle	Je souhaite...	Me montrer comment
Administrateur	Télécharger automatiquement les mises à jour	Activer la synchronisation automatique avec le référentiel des mises à jour RSA.

Rubriques connexes

Gestion des mises à jour de NetWitness Suite

Aperçu rapide

Le panneau Paramètres des mises à jour système s'affiche.



1	Affiche l'onglet Paramètres des mises à jour système
2	Configure le compte et les paramètres pour les mises à jour automatiques

Fonctionnalités

Ce tableau décrit les fonctions du panneau Paramètres des mises à jour système.

Fonctionnalité	Description
Configurer un compte Live	Affiche le panneau **ADMIN** > **Système** > **Services Live** dans lequel vous pouvez configurer les informations d'identification de votre compte Live si elles ne sont pas déjà configurées.
Configurer les paramètres proxy	Affiche le panneau **ADMIN** > **Système** > **Paramètres Proxy HTTP** dans lequel vous pouvez configurer un proxy HTTP, s'il n'est pas déjà configuré.
Télécharger automatiquement les informations sur les nouvelles mises à jour tous les jours	Permet d'activer la synchronisation automatique avec le référentiel des mises à jour RSA. S'il existe de nouvelles mises à jour disponibles, les informations s'afficheront automatiquement dans le panneau **ADMIN** > **HÔTES**.
Appliquer	Applique les paramètres contenus dans cet onglet.

Consignation du système - vue Paramètres

La vue Paramètres de RSA NetWitness Suite, accessible dans le panneau Consignation système, permet de 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. La section **Configurer les paramètres des fichiers Log** figurant dans le *Guide de configuration système* fournit des procédures détaillées.

Pour accéder à l'onglet Paramètres :

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

Le panneau Consignation système qui s'ouvre affiche par défaut l'onglet En temps réel.

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

Que voulez-vous faire ?

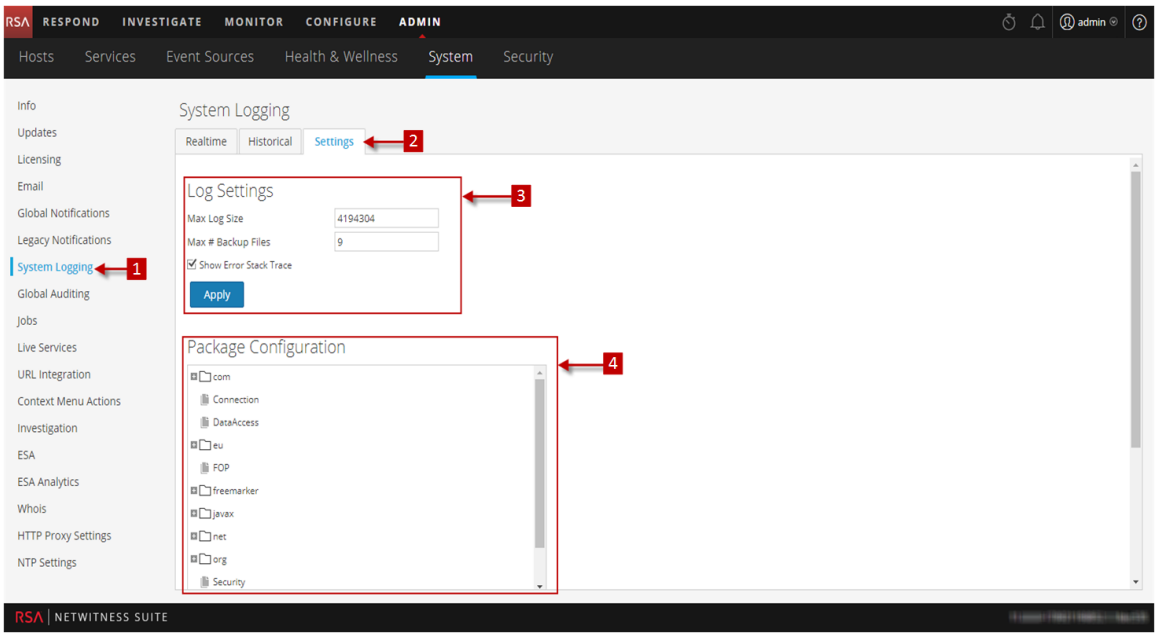
Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer la taille des fichiers Log	Configuration de la barre d'outils Paramètres des logs

Rubriques connexes

Consignation système - onglet Historique

Consignation système - onglet En temps réel

Aperçu rapide



1	Affiche le panneau Consignation système
2	Affiche l'onglet Paramètres
3	La section permet à l'utilisateur de configurer les paramètres des logs
4	La section permet à l'utilisateur de configurer le package

Fonctionnalités

L'onglet **Paramètres** présente deux sections : Paramètres de log et Configuration des packages.

Paramètres de log

La section Paramètres de log permet de configurer la taille des fichiers logs NetWitness Suite et le nombre de logs de sauvegarde gérés par NetWitness Suite.

Fonctionnalité	Description
Taille de log max.	Configure la taille maximale (en octets) de chaque fichier log. La valeur minimale de ce paramètre est **4096**.
Nbre max. de fichiers de sauvegarde	Indique le nombre de fichiers logs de sauvegarde qui sont gérés. 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.
Afficher la trace de pile d'erreurs	Activez la case à cocher pour afficher les messages log ERROR, STACK et TRACE.
Appliquer	Applique immédiatement les paramètres pour tous les futurs logs.

Configuration des packages

La section Configuration des packages affiche les packages NetWitness Suite sous forme d'arborescence.

Fonctionnalité	Description
Arborescence des packages	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 **racine** correspond au niveau de consignation par défaut de tous les packages qui ne sont pas explicitement définis. Le niveau racine est paramétré sur **INFO**

Fonctionnalité	Description
Champ Package	Ce champ contient le nom du package que vous sélectionnez dans l'arborescence **Package**.
Log Level	Si le package sélectionné est associé à un niveau de consignation explicite, sa valeur est affichée dans le champ **Niveau de consignation**.
Réinitialiser de manière récursive	Activez la case à cocher pour réinitialiser le log de manière récursive.
Appliquer	Ce bouton permet d'appliquer immédiatement les paramètres pour tous les futurs logs.
Réinitialiser	Ce bouton permet de réinitialiser le package sélectionné sur le niveau de consignation **racine**.

Consignation système - onglet En temps réel

Cette section décrit les fonctions des onglets En temps réel accessibles dans Consignation système et Logs de services.

L'onglet **En temps réel** affiche une vue du log ou du log des services NetWitness Suite. Lors de son chargement initial, cette vue contient les 10 dernières entrées du log. Lorsque de nouvelles entrées deviennent disponibles, elles sont intégrées à la vue.

Pour accéder à l'onglet En temps réel :

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

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Voir les détails d'une entrée de log	Affichage des logs système et des logs de services

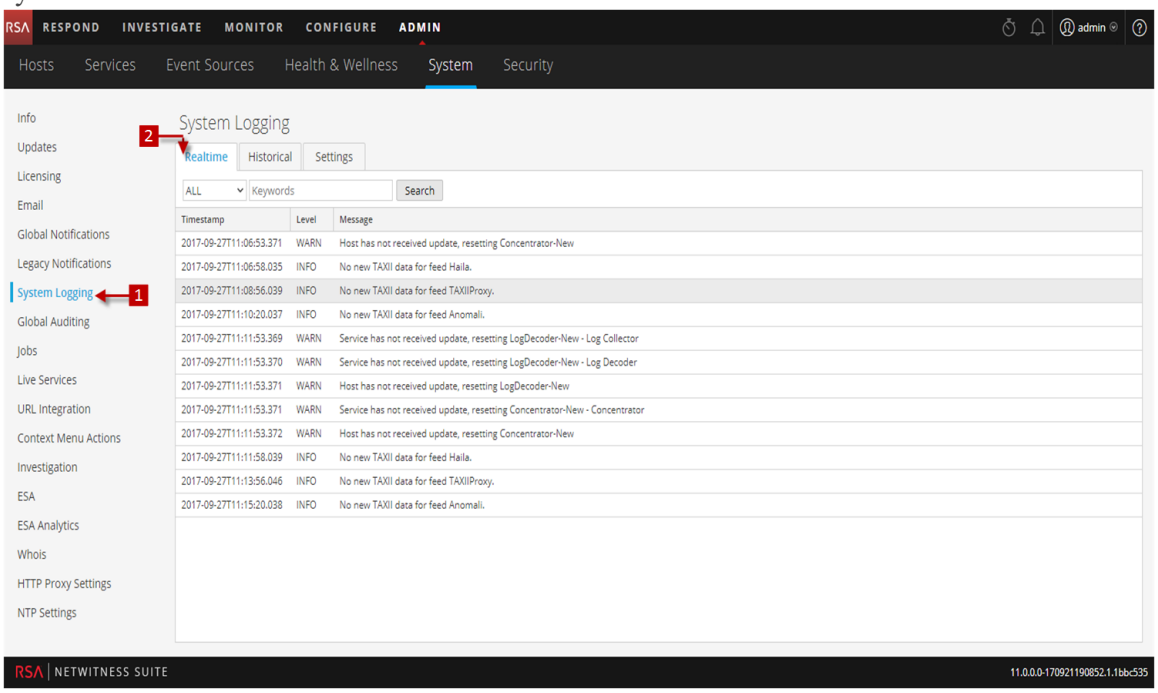
Rubriques connexes

Consignation du système - vue Paramètres

Consignation système - onglet Historique

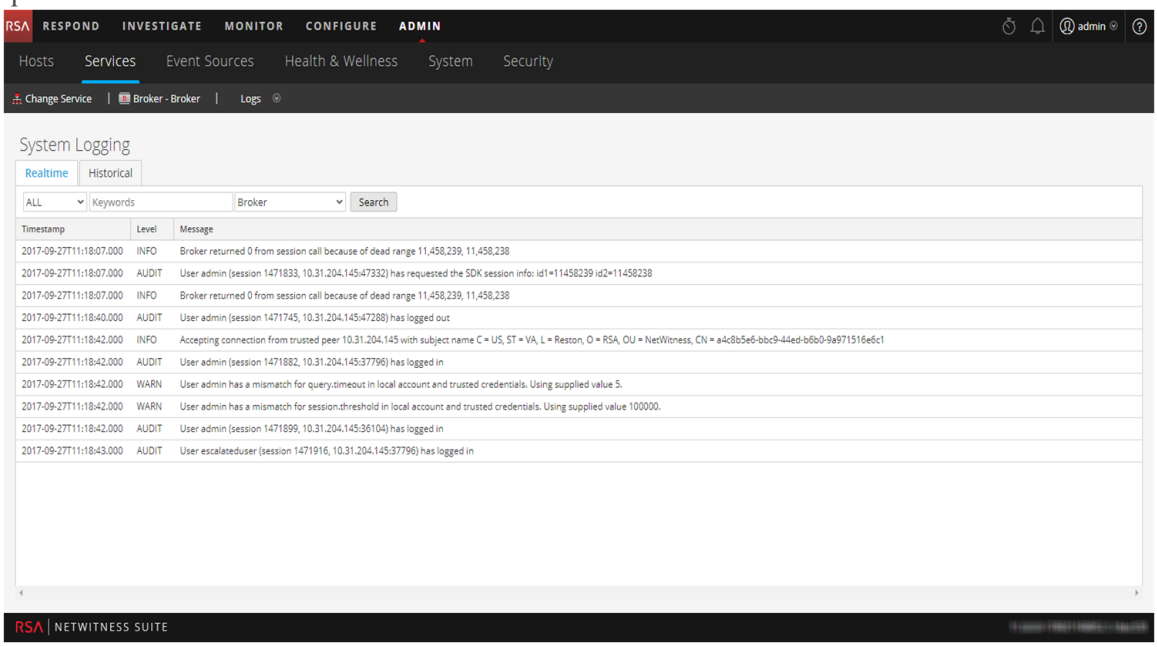
Aperçu rapide

Vous trouverez ci-dessous un exemple de l'onglet **En temps réel** dans le panneau Consignation système.



1	Affiche le panneau Consignation système
2	Affiche l'onglet En temps réel

Vous trouverez ci-dessous un exemple de l'onglet **En temps réel** dans la vue Logs de services, qui est similaire.



Fonctionnalités

L'onglet **En temps réel** comporte une barre d'outils dotée de champs de saisie qui permettent de filtrer les entrées. Sous cette barre d'outils se trouve une grille contenant les entrées du log.

Barre d'outils

Fonctionnalité	Description
Liste déroulante Niveau du log 	Sélectionne le niveau de consignation pour les entrées à afficher dans la grille. La liste déroulante **Niveau du log** affiche les niveaux de consignation disponibles pour le système ou le service. • Les logs système disposent de sept niveaux de consignation. • Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. • La valeur par défaut est **TOUTES** les entrées de log.
Champ Mot clés	Spécifie un mot clé à utiliser lors du filtrage des entrées. Ce champ est le même pour le filtrage des logs de service et de système.

Fonctionnalité	Description
Champ Service (Logs de service uniquement)	Spécifie le type de service à utiliser lors du filtrage des entrées de log de service. Les valeurs possibles sont l'hôte ou le service.
Bouton Filtrer	Cliquez sur ce bouton pour activer le filtre sur la base des niveaux de consignation, mots-clés et services sélectionnés.

Colonnes de la grille des logs

Colonne	Description
Timestamp	Il s'agit de l'horodatage de l'entrée.
Niveau	Il s'agit du niveau de consignation du message.
Message	Il s'agit du texte de l'entrée de log.

Consignation système - onglet Historique

L'onglet Historique fournit une vue du log NetWitness Suite dans laquelle une recherche peut être effectuée, ou le log de service au format page. Lors du chargement initial, la grille affiche la dernière page des entrées de log pour le système ou le service.

Pour accéder à l'onglet Historique :

1. Accédez à **ADMIN > Système**.
2. Dans le panneau des options, cliquez sur **Consignation système**.

   Le panneau Consignation système qui s'ouvre affiche par défaut l'onglet **En temps réel**.
3. Cliquez sur l'onglet **Historique**.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher le graphique de l'historique	Graphique de l'historique relatif aux statistiques du système

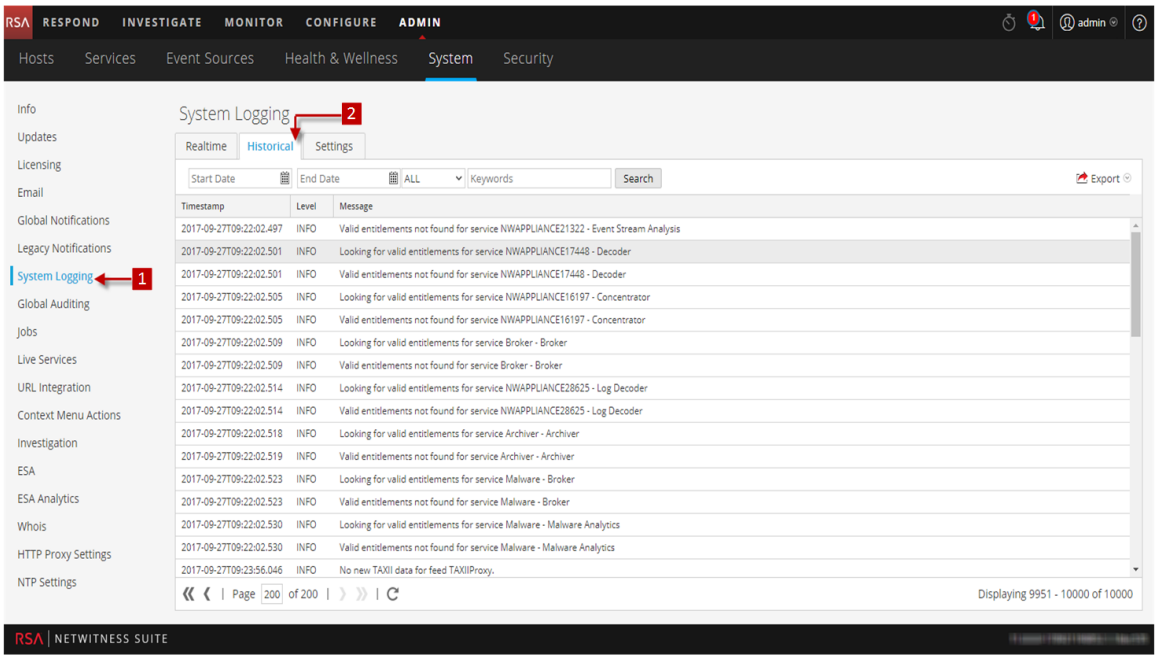
Rubriques connexes

Consignation système - onglet En temps réel

Consignation du système - vue Paramètres

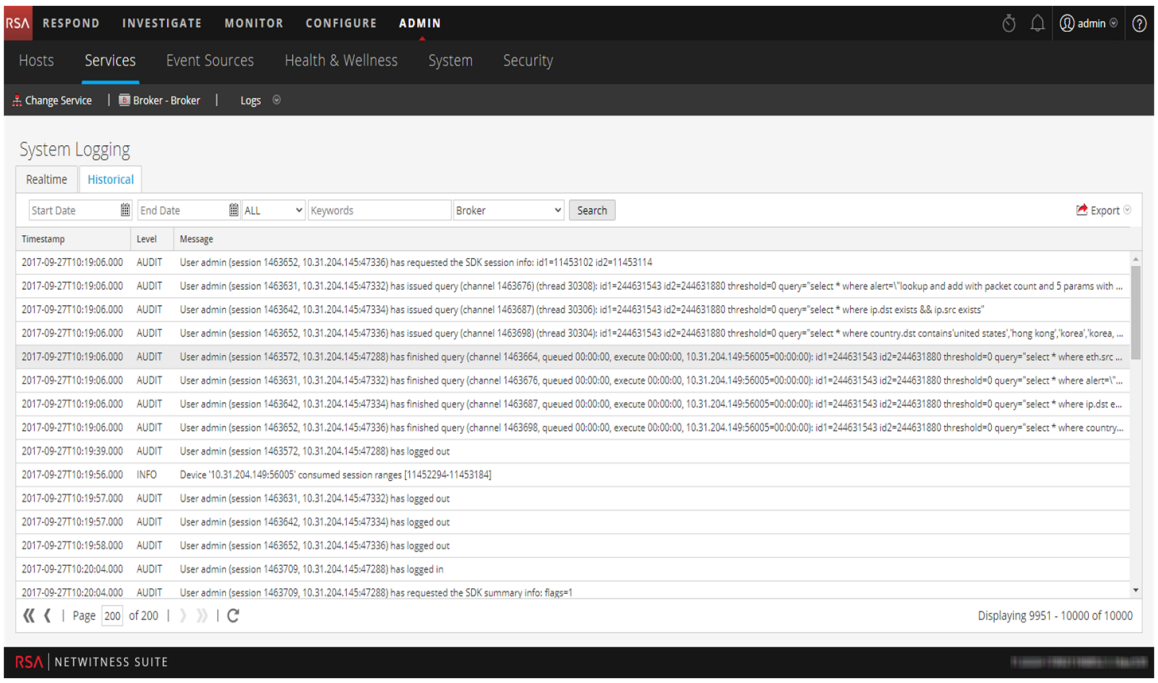
Aperçu rapide

Exemple de l'onglet **Historique** dans le panneau Consignation système. Il affiche les logs NetWitness Suite.



1	Affiche l'onglet Consignation système
2	Affiche l'onglet Historique

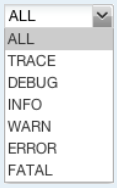
Exemple de l'onglet **Historique** dans le panneau Logs de services. Il affiche les logs de services.



Fonctionnalités

L'onglet **Historique** contient une barre d'outils avec des champs de saisie permettant le filtrage des entrées, ainsi qu'une grille contenant les entrées de log et les outils de pagination.

Fonctionnalité	Description
Date de début et **Date de fin**	Les options de recherche dans la plage **Date de début** et **Date de fin** limitent les entrées de log à un point dans le temps. En cas d'utilisation, vous devez fournir la date de début et la date de fin. Les heures sont facultatives. La période est validée pour vérifier que la date de fin n'est pas antérieure à la date de début.

Fonctionnalité	Description
Liste déroulante Niveau du log 	Sélectionne le niveau de consignation pour les entrées à afficher dans la grille. La liste déroulante **Niveau du log** affiche les niveaux de consignation disponibles pour le système ou le service. • Les logs système disposent de sept niveaux de consignation. • Les logs des services ne comptent que six niveaux de consignation car ils ne comprennent pas le niveau **SUIVRE**. • La valeur par défaut est **TOUTES** les entrées de log.
Champ Mot-clé	Spécifie un mot clé à utiliser lors du filtrage des entrées. Ce champ est le même pour le filtrage des logs de service et de système.
Champ Service (Logs de service uniquement)	Spécifie le type de service à utiliser lors du filtrage des entrées de log de service. Les valeurs possibles sont l'hôte ou le service.
Bouton Rechercher	Cliquez pour activer une recherche basée sur les dates de début et de fin, le niveau de log, les mots-clés et les sélections de service.
Exporter	Cliquez pour exporter les entrées de la grille en cours d'affichage au format de fichier texte. Vous pouvez sélectionner un format texte séparé par des virgules ou des tabulations pour les entrées du fichier.

Colonne	Description
Horodatage	Il s'agit de l'horodatage de l'entrée.
Niveau	Il s'agit du niveau de consignation du message.
Message	Il s'agit du texte de l'entrée de log.

Les outils de pagination figurant sous la grille permettent de parcourir les pages du log.

Rechercher les entrées de log

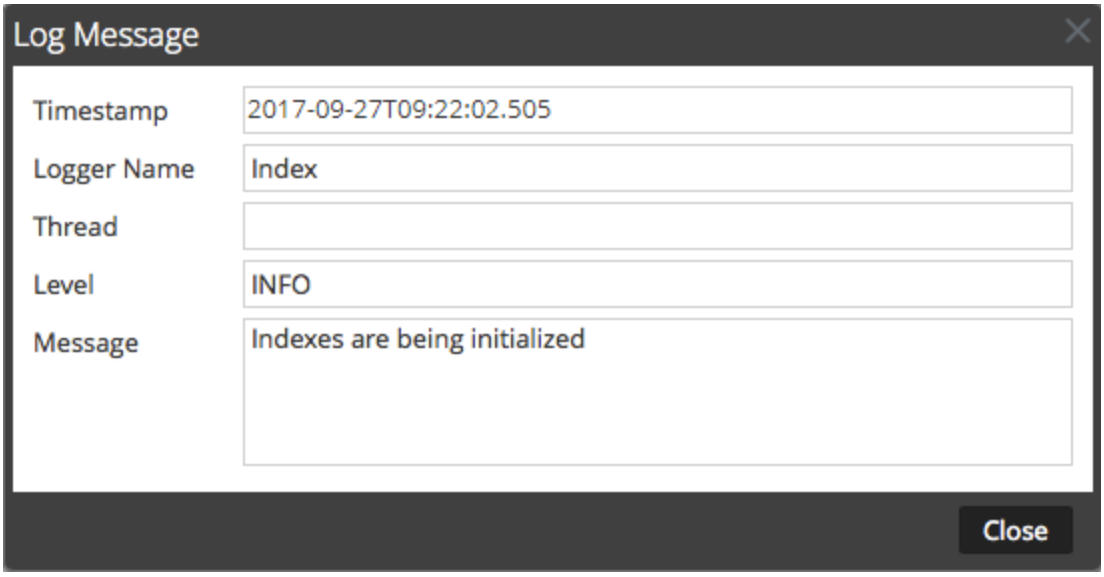
Pour rechercher les résultats affichés sous l'onglet **Historique** :

1. (Facultatif) Sélectionnez une **Date de début** et une **Date de fin**. Éventuellement, sélectionnez une **Heure de début** et une **Heure de fin**.
2. (Facultatif) Pour les logs de système et de service, sélectionnez le **Niveau du log** et un **Mot clé**, ou les deux.
3. (Facultatif) Pour les logs de service, sélectionnez le **Service** : hôte ou service.
4. Cliquez sur **Rechercher**.
   La vue est réinitialisée avec les 10 entrées les plus récentes qui correspondent à votre filtre. Alors que de nouvelles entrées de log correspondantes deviennent disponibles, la vue est mise à jour pour afficher ces entrées.

Afficher les détails d'une entrée de log

Chaque ligne de la grille de log sous l'onglet **Historique** propose des informations de synthèse sur l'entrée de log. Pour afficher les détails complets :

1. Cliquez deux fois sur une entrée de log.
   La boîte de dialogue Message log, qui contient l'horodatage, le nom de l'enregistreur, le thread, le niveau et le message, s'affiche.



2. Lorsque vous avez terminé de la consulter, cliquez sur **Fermer**.

Parcourir les entrées

Pour consulter les différentes pages de la grille, utilisez les commandes de pagination en bas de la grille, comme suit :

- Utilisez les boutons de navigation
- Saisissez manuellement le numéro de la page que vous souhaitez afficher, puis appuyez sur **ENTRÉE**.

Exporter

Pour exporter les logs dans la vue actuelle :

Cliquez sur **Exporter** et sélectionnez l'une des options de la liste déroulante, le **Format CSV** ou **Séparé par des tabulations**.
Le fichier est téléchargé avec un nom de fichier qui identifie le type de log et le séparateur de champ. Par exemple, un log système NetWitness Suite exporté avec des valeurs séparées par des virgules est nommé **UAP_log_export_CSV.txt**, et un log d'appliance exporté avec des valeurs séparées par des tabulations est nommé **APPLIANCE_log_export_TAB.txt**.