



Guide de configuration de NetWitness Respond

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

À propos de ce document	5
Présentation de la configuration de NetWitness Respond	5
Configuration de NetWitness Respond	7
Étape 1. Configurer les sources d’alertes pour afficher les alertes dans la vue Répondre	8
Conditions préalables	8
Configurer Reporting Engine pour qu’il affiche les alertes déclenchées par Reporting Engine dans la vue Répondre.	8
Configurer Malware Analytics pour afficher les alertes déclenchées par Malware Analytics dans la vue Respond	9
Configurer NetWitness Endpoint pour afficher les alertes déclenchées par NetWitness Endpoint dans la vue Répondre	9
Configurer NetWitness Endpoint pour afficher les alertes NetWitness Endpoint	10
Étape 2. Attribuer des autorisations sur la vue Répondre	12
Serveur de réponse	13
Incidents	15
Étape 3. Créer une règle d’agrégation pour les alertes	17
Procédures supplémentaires pour la configuration de Respond	19
Définir une période de rétention pour les alertes et les incidents	19
Conditions préalables	20
Procédure	20
Résultat	21
Obfusquer les données privées	22
Conditions préalables	22
Procédure	23
Gérer des incidents dans le gestionnaire NetWitness SecOps	24
Conditions préalables	24
Procédure	24
Définir le compteur des alertes et incidents rencontrés	26
Configurer une base de données pour le service du serveur de réponse	28
Conditions préalables	28
Procédure	28

Référence de configuration pour NetWitness Respond	31
Vue Configurer	31
Onglet Règles d'agrégation	32
Que voulez-vous faire ?	32
Rubriques connexes	32
Règles d'agrégation	32
Onglet Nouvelle règle	35
Que voulez-vous faire ?	35
Rubriques connexes	35
Nouvelle règle	35

À propos de ce document

Ce guide présente NetWitness Respond, fournit des instructions précises sur la configuration de NetWitness Respond au sein de votre réseau, indique des procédures supplémentaires utilisées à d'autres périodes et propose des supports de référence décrivant l'interface utilisateur de configuration de NetWitness Respond dans votre réseau.

Rubriques

- [Présentation de la configuration de NetWitness Respond](#)
- [Configuration de NetWitness Respond](#)
- [Procédures supplémentaires pour la configuration de Respond](#)
- [Référence de configuration pour NetWitness Respond](#)

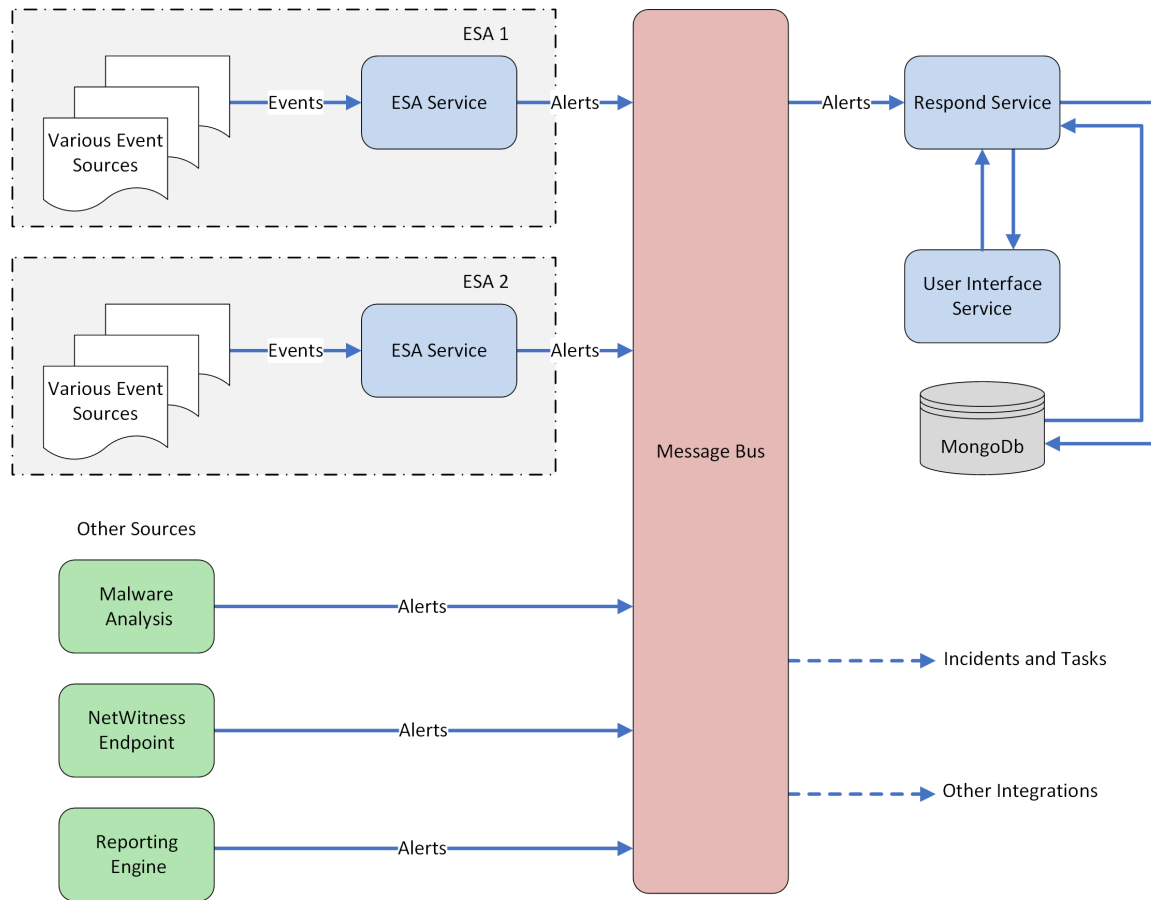
Présentation de la configuration de NetWitness Respond

RSA NetWitness® Suite NetWitness Respond utilise les données d'alerte issues de diverses sources via le bus de messages et affiche ces alertes dans l'interface utilisateur NetWitness Suite. Le service Service du serveur Respond vous permet de grouper les alertes de manière logique et de lancer un workflow NetWitness Respond pour rechercher les problèmes de sécurité qui se sont produits et y remédier.

Le service Service du serveur Respond utilise les alertes provenant du bus de messages et standardise les données en un format commun (tout en conservant les données initiales) afin de simplifier l'exécution des règles. Il exécute périodiquement des règles pour agréger plusieurs alertes en un incident et définir certains attributs de l'incident (par exemple gravité, catégorie, etc.). Les incidents sont conservés dans MongoDB par le service Service du serveur Respond. Les incidents sont aussi publiés sur le bus de messages pour être utilisés par d'autres systèmes (par exemple l'intégration Archer).

Remarque : NetWitness Respond nécessite un serveur primaire ESA qui contient l'instance MongoDB. Les enregistrements d'alertes, d'incidents et de tâches sont conservés dans cette instance MongoDB par le serveur de réponse.

Le schéma suivant illustre le flux général des alertes.



Vous devez configurer différentes sources depuis lesquelles les alertes sont collectées et agrégées par le service Service du serveur Respond.

Configuration de NetWitness Respond

Cette rubrique décrit les tâches générales nécessaires à la configuration du service Service du serveur Respond. L'administrateur doit réaliser les étapes dans l'ordre indiqué.

Rubriques

- [Étape 1. Configurer les sources d'alertes pour afficher les alertes dans la vue Répondre](#)
- [Étape 2. Attribuer des autorisations sur la vue Répondre](#)
- [Étape 3. Créer une règle d'agrégation pour les alertes](#)

Étape 1. Configurer les sources d'alertes pour afficher les alertes dans la vue Répondre

Cette procédure est requise pour que les alertes provenant des sources d'alerte soient affichées dans NetWitness Respond. Une option vous permet d'activer ou de désactiver les alertes renseignées dans la vue Répondre. Par défaut, cette option est désactivée dans Reporting Engine, Malware Analytics et NetWitness Endpoint et activée uniquement dans Event Stream Analysis. Ainsi, lorsque vous installez le service Service du serveur Respond, vous devez activer cette option dans Reporting Engine, Malware Analytics et NetWitness Endpoint pour renseigner les alertes correspondantes dans la vue Répondre.

Conditions préalables

Assurez-vous que :

- le Service du serveur Respond est installé et fonctionne sur NetWitness Suite.
- une base de données est configurée pour le Service du serveur Respond.
- NetWitness Endpoint est installé et fonctionne.

Configurer Reporting Engine pour qu'il affiche les alertes déclenchées par Reporting Engine dans la vue Répondre.

Par défaut, les alertes Reporting Engine ne s'affichent pas dans la vue Répondre. Pour afficher et visualiser les alertes Reporting Engine, vous devez activer les alertes NetWitness Respond dans la vue Configuration des services > onglet Général de Reporting Engine.

1. Accédez à **ADMIN > Services**, sélectionnez un service Reporting Engine et cliquez sur  > **Vue > Config.**

La vue Configuration des services s'ouvre sur l'onglet Général du Reporting Engine.

2. Sélectionnez **Configuration système**.
3. Activez la case à cocher **Transférer des alertes vers Respond**.

Reporting Engine transfère immédiatement les alertes vers NetWitness Respond.

Pour plus d'informations sur les paramètres de l'onglet Général, consultez la rubrique « Onglet Général du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.

Configurer Malware Analytics pour afficher les alertes déclenchées par Malware Analytics dans la vue Respond

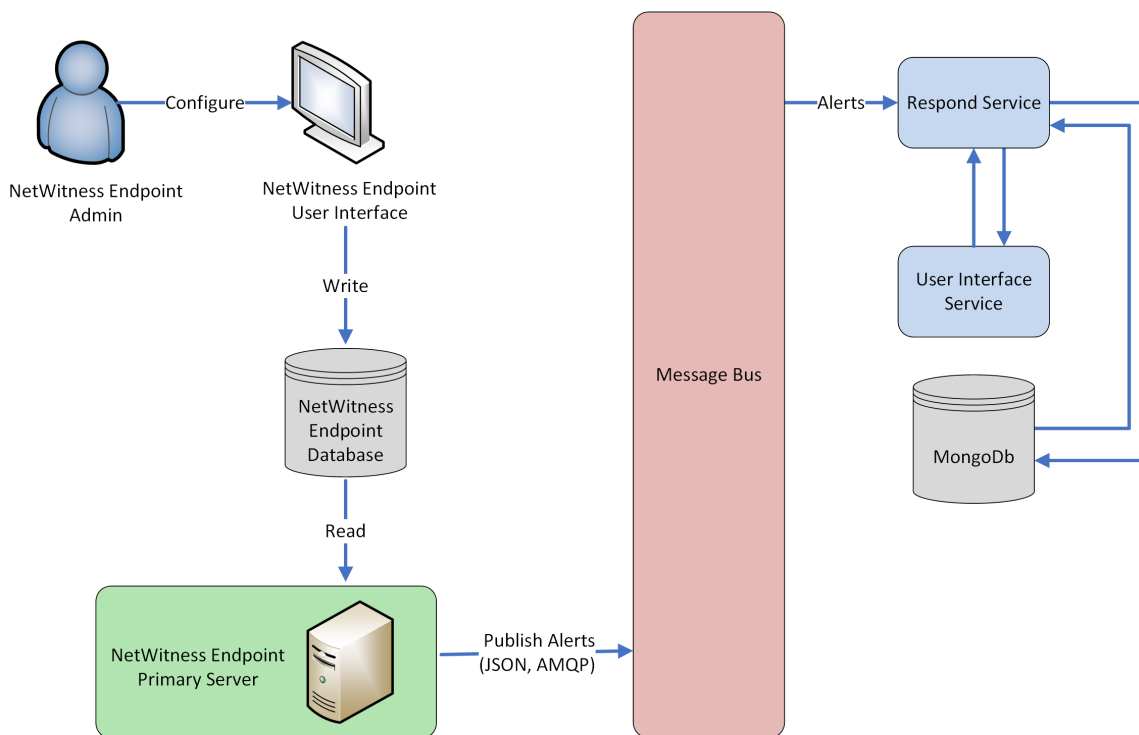
L'affichage des alertes NetWitness Respond est une fonction d'audit de Malware Analysis. La procédure d'activation des alertes NetWitness Respond est décrite dans la rubrique « (Facultatif) Configurer l'auditing sur l'hôte Malware Analysis » du *Guide de configuration de Malware Analysis*.

Configurer NetWitness Endpoint pour afficher les alertes déclenchées par NetWitness Endpoint dans la vue Répondre

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

Remarque : RSA prend en charge NetWitness Endpoint 4.3.0.4, 4.3.0.5 ou une version ultérieure pour l'intégration de NetWitness Respond. Pour plus d'informations, reportez-vous à la rubrique « Intégration de RSA NetWitness Suite » dans *NetWitness Endpoint Guide d'utilisation*.

Le schéma ci-dessous représente le flux d'alertes NetWitness Endpoint vers le NetWitness Suite Service du serveur Respond et son affichage dans la vue **RÉPONDRE > Alertes**.

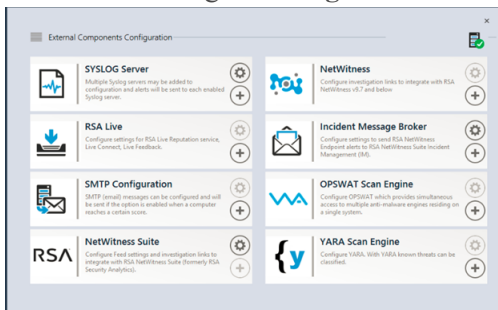


Configurer NetWitness Endpoint pour afficher les alertes NetWitness Endpoint

Pour configurer NetWitness Endpoint pour qu'il affiche les alertes NetWitness Endpoint dans l'interface utilisateur NetWitness Suite :

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

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



2. Dans les composants répertoriés, sélectionnez **Incident Message Broker**, puis cliquez sur + pour ajouter un nouveau composant IM Broker.
3. Renseignez les champs suivants :
 - a. **Nom de l'instance** : Indiquez un nom spécifique pour identifier le composant IM Broker.
 - b. **Nom d'hôte ou adresse IP du serveur** : Saisissez le DNS de l'hôte ou l'adresse IP du composant IM Broker (Serveur NetWitness).
 - c. **Numéro de port** : Le port par défaut est le port 5671.
4. Cliquez sur **Enregistrer**.
5. Accédez au fichier **ConsoleServer.exe.Config** dans **C:\Program Files\RSA\ECAT\Server**.
6. Modifiez les configurations d'hôte virtuel dans le fichier comme suit :


```
<add key="IMVirtualHost" value="/rsa/system" />
```

Remarque : dans NetWitness Suite 11.0, l'hôte virtuel est « /rsa/system ». Pour la version 10.6.x et les versions antérieures, l'hôte virtuel est « /rsa/sa ».

7. Redémarrez le serveur API et le serveur de console.
8. Pour configurer SSL pour les alertes Respond, suivez la procédure ci-dessous sur le serveur de console primaire NetWitness Endpoint pour définir les communications SSL :

- a. Exportez le certificat de l'autorité de certification NetWitness Endpoint au format .cer (chaîne codée X.509 Base 64) du magasin de certificats personnel de l'ordinateur local (sans sélectionner la clé privée).
- b. Générez un certificat client pour NetWitness Endpoint à l'aide du certificat de l'autorité de certification NetWitness Endpoint. (Vous DEVEZ définir le nom CN sur ecat).

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

Remarque : Dans l'exemple de code ci-dessus, si vous avez mis à niveau vers Endpoint version 4.3 à partir d'une version précédente et que nous n'avez pas généré de nouveaux certificats, vous devez remplacer par « NWECA » par « EcatCA ».

- c. Notez l'empreinte du certificat client généré à l'étape b. Saisissez la valeur d'empreinte du certificat client dans la section IMBrokerClientCertificateThumbprint du fichier ConsoleServer.Exe.Config comme indiqué.

```
<add key="IMBrokerClientCertificateThumbprint"  
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```
9. Sur Serveur NetWitness, copiez le fichier de certificat d'autorité de certification NetWitness Endpoint au format .cer dans le dossier de l'importation :
`/etc/pki/nw/trust/import`
10. Exécutez la commande suivante pour démarrer l'exécution de Chef nécessaire :
`orchestration-cli-client --update-admin-node`
Cette opération ajoute tous ces certificats au magasin d'approbations.
11. Redémarrez le serveur RabbitMQ :
`systemctl restart rabbitmq-server`
Le compte NetWitness Endpoint doit être automatiquement disponible sur RabbitMQ.
12. Importez les fichiers `/etc/pki/nw/ca/nwca-cert.pem` et `/etc/pki/nw/ca/ssca-cert.pem` à partir de Serveur NetWitness et ajoutez-les aux magasins de certification racines de confiance sur le serveur Endpoint.

Étape 2. Attribuer des autorisations sur la vue Répondre

Ajouter des utilisateurs disposant des autorisations requises pour analyser les incidents et les alertes dans NetWitness Respond. Les utilisateurs ayant accès à la vue Répondre ont besoin des autorisations sur les incidents et le serveur de réponse.

Les rôles préconfigurés suivants disposent d'autorisations dans la vue Répondre :

- **Analystes** : Les analystes du centre des opérations de sécurité (SOC) ont accès à la gestion des alertes, à NetWitness Respond, Procédure d'enquête et Reporting, mais pas aux configurations système.
- **Analystes du malware** : Les analystes du malware ont accès aux procédures d'enquête et aux événements de malware.
- **Opérateurs** : Les opérateurs ont accès aux configurations, mais n'ont pas accès aux procédures d'enquête, à ESA, à la gestion des alertes, aux rapports et à NetWitness Respond.
- **SOC_Managers (Responsables de SOC)**: Les Responsables de SOC ont le même accès que les analystes et disposent aussi d'autorisations pour gérer les incidents et configurer NetWitness Respond.
- **Data_Privacy_Officers** (Responsables de la confidentialité des données) : Les Responsables de la confidentialité des données ont le même accès que les administrateurs, mais s'occupe aussi des options de configuration qui gèrent l'obscurcissement et l'affichage des données sensibles dans le système. Pour plus d'informations, reportez-vous à la rubrique *Gestion de la confidentialité des données*.
- **Administrateur de réponse** : L'administrateur de réponse a un accès complet à NetWitness Respond.
- **Administrateurs** : l'administrateur a un accès système complet à NetWitness Suite et dispose de toutes les autorisations par défaut.

Les autorisations par défaut NetWitness Respond sont indiquées dans les tableaux ci-dessous. Vous devez attribuer des autorisations d'utilisateur dans les onglets **Incidents** et **Serveur de réponse**, qui sont les noms des onglets Autorisations dans les boîtes de dialogue Ajouter ou Modifier les rôles de la vue ADMIN > Sécurité. Vous souhaitez peut-être ajouter des autorisations d'utilisateur supplémentaires pour la gestion des alertes, Context Hub, Enquêteur, le serveur de procédure d'enquête et les rapports.

Serveur de réponse

Autorisations	Analystes	Responsables de SOC	DP O	Administrateur de réponse	Opérateurs	M A
respond-server.alert.delete			Ou i*	Oui*		
respond-server.alert.manage	Oui	Oui	Ou i*	Oui*		O ui
respond-server.alert.read	Oui	Oui	Ou i*	Oui*		O ui
respond-server.alertrule.manage		Oui	Ou i*	Oui*		
respond-server.alertrule.read		Oui	Ou i*	Oui*		
respond-server.configuration.manage			Ou i*	Oui*		
respond-server.health.read			Ou i*	Oui*		
respond-server.incident.delete			Ou i*	Oui*		
respond-server.incident.manage	Oui	Oui	Ou i*	Oui*		O ui
respond-server.incident.read	Oui	Oui	Ou i*	Oui*		O ui
respond-server.journal.manage	Oui	Oui	Ou i*	Oui*		O ui

Autorisations	Analystes	Responsables de SOC	DP O	Administrateur de réponse	Opérateurs	M A
respond-server.journal.read	Oui	Oui	Oui*	Oui*		Oui
respond-server.logs.manage			Oui*	Oui*		
respond-server.metrics.read			Oui*	Oui*		
respond-server.process.manage			Oui*	Oui*		
respond-server.remediation.manage	Oui	Oui	Oui*	Oui*		Oui
respond-server.remediation.read	Oui	Oui	Oui*	Oui*		Oui
respond-server.security.manage			Oui*	Oui*		
respond-server.security.read			Oui*	Oui*		

*Les responsables de la confidentialité des données et les administrateurs de réponse ont l'autorisation **respond-server**.*Elle leur accorde toutes les autorisations sur le serveur de réponse.

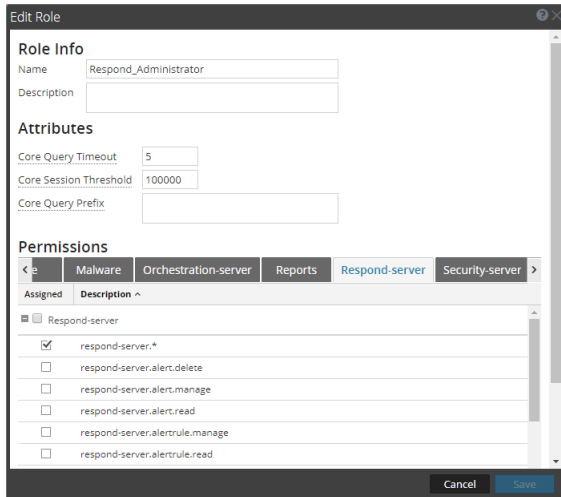
Incidents

Autorisations	Analystes	Responsables de SOC	DP O	Administrateur de réponse	Opérateurs	M A
Accéder au module Incident	Oui	Oui	Oui	Oui		Oui
Configurer l'intégration Incident Management		Oui	Oui	Oui		
Supprimer les alertes et incidents			Oui	Oui		
Gérer les règles de gestion des alertes		Oui	Oui	Oui		
Afficher et gérer les incidents	Oui	Oui	Oui	Oui		Oui

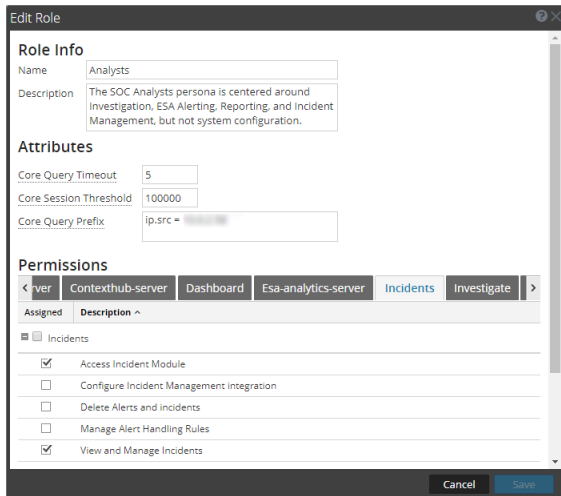
L'administrateur de réponse dispose de toutes les autorisations sur le serveur de réponse et les incidents.

Attention : Il importe que vous attribuez des autorisations utilisateur équivalentes À LA FOIS dans l'onglet Serveur de réponse et dans l'onglet Incidents.

La figure suivante présente les autorisations sur le serveur de réponse pour le rôle Administrateur de réponse. Le rôle Administrateur de réponse contient toutes les autorisations NetWitness Respond.



La figure suivante présente les autorisations Incidents pour le rôle Analystes par défaut :



Pour plus d'informations, reportez-vous à la rubrique Autorisations du rôle et Gérer les utilisateurs à l'aide de rôles et d'autorisations dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Étape 3. Créer une règle d'agrégation pour les alertes

Vous pouvez créer des règles d'agrégation avec plusieurs critères pour automatiser le processus de création d'incidents. Les alertes qui répondent aux critères de la règle sont regroupées pour former un incident. Cette procédure est utile lorsqu'un ensemble d'alertes spécifique peut être regroupé en incident et que vous pouvez définir une règle d'agrégation qui regroupe les alertes au lieu de créer manuellement un incident et d'ajouter chaque alerte à cet incident. Pour créer automatiquement des incidents, vous devez créer une règle d'agrégation.

Pour créer une règle d'agrégation :

1. Accédez à **CONFIGURER > Règles de l'incident**.

L'onglet **Règles d'agrégation** s'affiche.

	Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
<input type="checkbox"/>	1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
<input type="checkbox"/>	2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
<input type="checkbox"/>	3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
<input type="checkbox"/>	4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
<input type="checkbox"/>	5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
<input type="checkbox"/>	6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addre...		0	0
<input type="checkbox"/>	7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
<input type="checkbox"/>	8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
<input type="checkbox"/>	9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
<input type="checkbox"/>	10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
<input type="checkbox"/>	11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0

La liste des 11 règles prédéfinies s'affiche. Exécutez l'une des opérations suivantes :

- ajouter une nouvelle règle
 - modifier une règle existante
 - cloner une règle
2. Pour ajouter une nouvelle règle, sélectionnez **+**.

L'onglet **Nouvelle règle** s'affiche.

L'exemple ci-dessous illustre le regroupement des alertes en incident en fonction du score de risque.

The screenshot displays the configuration page for a new aggregation rule in NetWitness Respond. The rule is titled "Risk based" and is currently enabled. Its description is "Alerts grouped by risk score". Under "Match Conditions*", the "Query Builder" option is selected, and a single condition is defined: "Risk Score" is "greater than" 40. The "Action" is set to "Group into an Incident". In the "Grouping Options*" section, the rule is configured to "Group By" "Alert Type" within a "1" hour "Time Window". The "Incident Options" section shows the "Title" as a template string "\${ruleName} for \${groupByValue1}", a blank "Summary" field, and "Categories" set to "Hacking: Abuse of functionality". The "Priority" section indicates the rule uses the "Average of Risk Score across all of the Alerts" to determine incident priority. A visual scale for this priority is shown, ranging from 1 (Low) to 100 (Critical), with the current value set at 90. The interface includes "Save" and "Close" buttons at the bottom left and the RSA NetWitness Suite logo and version (11.0.0.0) at the bottom.

3. Cliquez sur **Enregistrer**.

La règle s'affiche dans l'onglet **Règles d'agrégation**. La règle est activée et commence à créer des incidents en fonction des alertes entrantes qui répondent aux critères sélectionnés.

Voir aussi :

- Pour des détails sur les différents paramètres pouvant être définis comme critères pour une règle d'agrégation, reportez-vous à la rubrique [Onglet Nouvelle règle](#).
- Pour des détails sur les descriptions des paramètres et des champs de l'onglet Règles d'agrégation, reportez-vous à la rubrique [Onglet Règles d'agrégation](#).

Procédures supplémentaires pour la configuration de Respond

Utilisez cette section si vous recherchez des instructions pour effectuer une tâche spécifique après la configuration initiale de NetWitness Respond.

- [Définir une période de rétention pour les alertes et les incidents](#)
- [Obfusquer les données privées](#)
- [Gérer des incidents dans le gestionnaire NetWitness SecOps](#)
- [Définir le compteur des alertes et incidents rencontrés](#)
- [Configurer une base de données pour le service du serveur de réponse](#)

Définir une période de rétention pour les alertes et les incidents

Parfois, les responsables de la confidentialité des données souhaitent conserver les données sur une période donnée, puis les supprimer. Une période de rétention réduite libère plus rapidement de l'espace sur le disque. Parfois, la période de rétention doit être courte. Par exemple, la législation européenne précise que les données confidentielles ne doivent pas être conservées plus de 30 jours. Au-delà de ce délai, les données doivent être occultées ou supprimées.

La définition d'une période de rétention de données est facultative. L'heure à laquelle NetWitness Respond reçoit des alertes et crée un incident détermine le début de la rétention. Les périodes de rétention sont comprises entre 30 et 365 jours. Si vous définissez une telle période, les données sont supprimées définitivement un jour après la fin de la période.

La rétention dépend de l'heure à laquelle NetWitness Respond reçoit les alertes et de l'heure de création de l'incident.

Attention : Les données supprimées après la période de rétention ne peuvent pas être récupérées.

Au terme de cette période, les données suivantes sont **supprimées définitivement** :

- Alertes
- Incidents
- Tâches
- Entrées du journal

Les logs analysent la rétention et les suppressions manuelles. Ainsi, vous pouvez voir ce qui a été supprimé. Vous pouvez visualiser les logs Serveur Respond dans les emplacements suivants :


- **Serveur Respond Log des services** : /var/log/netwitness/respond-server/respond-server.log
- **Serveur Respond Log des services** : /var/log/netwitness/respond-server/respond-server.log

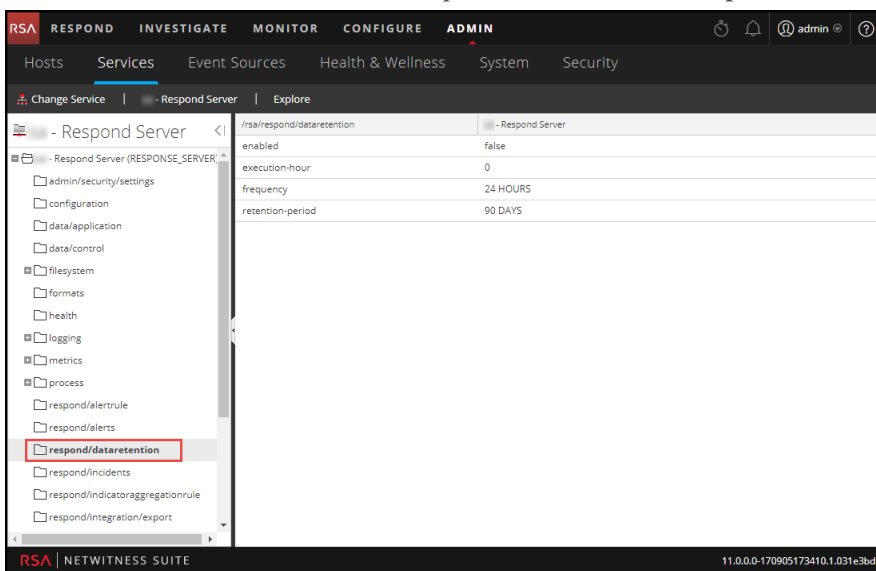
La période de rétention des données que vous définissez ici ne s'applique pas aux outils SOC Archer ou tiers. Les alertes et incidents provenant d'autres systèmes doivent être supprimés séparément.

Conditions préalables

Le rôle Administrateur doit vous être attribué.

Procédure

1. Accédez à **ADMIN > Services**, sélectionnez le service Service du serveur Respond et cliquez sur  > **Vue > Explorer**.
2. Dans la liste des nœuds de la vue Explorer, sélectionnez **respond/dataretention**.



3. Dans le champ **activé**, sélectionnez **true** pour supprimer les incidents et les alertes dont l'ancienneté est supérieure à la période de rétention.
Le planificateur est exécuté tous les jours à 23 h 00.
Un avis s'affiche indiquant que la configuration a été mise à jour correctement.
4. Dans le champ **période de rétention**, indiquez le nombre de jours de conservation des incidents et alertes. Par exemple, saisissez 30 JOURS, 60 JOURS, 90 JOURS, 120 JOURS,

365 JOURS ou un autre nombre de jours.

Un avis s'affiche indiquant que la configuration a été mise à jour correctement.

Résultat

Dans les 24 heures suivant la fin de la période de rétention, le planificateur supprime définitivement les alertes et les incidents antérieurs à la période spécifiée dans NetWitness Respond. Les entrées des journaux et les tâches associées aux incidents supprimés sont également supprimées.

Obfusquer les données privées

Le rôle du responsable de la confidentialité des données peut identifier les clés méta qui contiennent des données sensibles et doivent afficher des données obfusquées. Cette rubrique explique comment l'administrateur mappe ces clés méta pour afficher une valeur hachée au lieu de la valeur réelle.

Les restrictions suivantes s'appliquent aux valeurs de métadonnées hachées :

- NetWitness Suite prend en charge deux méthodes de stockage pour les valeurs de métadonnées hachées, HEX (par défaut) et chaîne.
- Lorsqu'une clé méta est configurée de façon à afficher une valeur hachée, tous les rôles de sécurité voient uniquement la valeur hachée dans le module Incidents.
- Vous pouvez utiliser des valeurs hachées de la même façon que vous utilisez des valeurs réelles. Par exemple, lorsque vous utilisez une valeur hachée dans les critères de règle, les résultats sont les mêmes que si vous aviez utilisé la valeur réelle.

Cette rubrique explique comment obfusquer des données privées dans NetWitness Respond. Reportez-vous à la rubrique **Présentation de la gestion de la confidentialité des données** dans le *Guide de gestion de la confidentialité des données* pour plus d'informations sur la confidentialité des données.

Mappage du fichier vers des clés méta obfusquées

Dans NetWitness Respond, le fichier de mappage pour l'obfuscation des données est `data_privacy_map.js`. Vous pouvez y saisir le nom de clé méta obfusqué et le mapper vers le nom de clé méta réel.

L'exemple suivant présente les mappages pour obfusquer les données pour deux clés méta, `ip.src` et `user.dst` :

```
'ip.src.hash' : 'ip.src',  
'user.dst.hash' : 'user.dst'
```

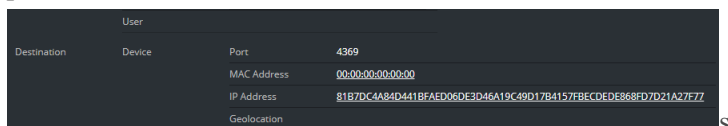
Vous déterminez la convention de dénomination pour les noms de clé méta obfusquées. Par exemple, `ip.src.hash` peut être `ip.src.private` ou `ip.src.bin`. Vous devez choisir une convention de dénomination et l'utiliser de façon cohérente sur tous les hôtes.

Conditions préalables

- Le rôle du responsable de la confidentialité des données doit préciser quelles clés méta requièrent une obfuscation des données.
- Le rôle d'administrateur doit mapper des clés méta pour l'obfuscation des données.

Procédure

1. Ouvrez le fichier de mappage de confidentialité des données :
`/var/lib/netwitness/respond-server/scripts/data_privacy_map.js`
2. Dans la variable `obfuscated_attribute_map`, saisissez le nom d'une clé méta devant contenir les données obfusquées. Puis, mappez-le sur la clé méta qui ne contient pas de données obfusquées en respectant le format suivant :
`'ip.src.hash' : 'ip.src'`
3. Répétez l'étape 2 pour chaque clé méta devant afficher une valeur hachée.
4. Utilisez la même convention de dénomination que dans l'étape 2 et utilisez-la de manière cohérente sur tous les hôtes.
5. Enregistrez le fichier.
Toutes les clés méta mappées afficheront des valeurs hachées au lieu des valeurs réelles. Dans la figure suivante, une valeur hachée s'affiche pour l'adresse IP de destination dans le panneau Détails de l'événement :



The screenshot shows a dark-themed interface with a table of event details. The table has columns for Destination, Device, Port, MAC Address, IP Address, and Geolocation. The IP Address field contains a long alphanumeric hash instead of a standard IP address.

User					
Destination	Device	Port	4369		
		MAC Address	00:00:00:00:00		
		IP Address	81B7DC6A84D441BFAED06DE3D46A19C49D17B4157FBECDDED868FD7D21A27E77		
		Geolocation			

De nouvelles alertes afficheront les données obfusquées.

Remarque : Les alertes existantes affichent toujours des données sensibles. Cette procédure n'est pas rétroactive.

Gérer des incidents dans le gestionnaire NetWitness SecOps

Si vous souhaitez gérer des incidents dans RSA NetWitness® SecOps Manager au lieu de NetWitness Respond, vous devez configurer les paramètres d'intégration système dans la vue Explorer de Service du serveur Respond. Une fois que vous avez configuré les paramètres d'intégration système, tous les incidents sont gérés dans NetWitness SecOps Manager. Les incidents créés avant l'intégration ne seront pas gérés dans NetWitness SecOps Manager.


Attention : Si vous gérez des incidents dans NetWitness SecOps Manager au lieu de NetWitness Respond, n'utilisez pas les éléments suivants dans la vue Répondre : Vue Liste des incidents, vue Détails de l'incident et vue Liste des tâches. Ne créez pas d'incidents dans la vue Liste des alertes de la vue Répondre ou dans Enquêter.

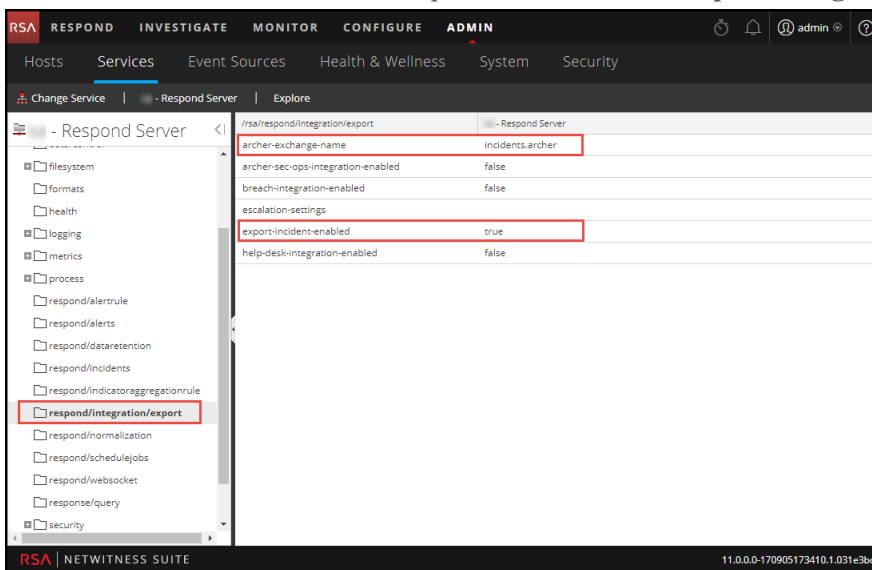
Conditions préalables

- NetWitness SecOps Manager 1.3.1.2 (NetWitness Suite 11.0 ne fonctionne qu'avec NetWitness SecOps Manager 1.3.1.2.)

Procédure

Suivez cette procédure pour configurer les paramètres du service du serveur de réponse pour gérer les incidents dans NetWitness SecOps Manager.

1. Accédez à **ADMIN > Services**, sélectionnez le service Service du serveur Respond, puis cliquez sur  > **Config > Explorer**.
2. Dans la liste de nœuds de la vue Explorer, sélectionnez **respond/integration/export**.



3. Dans le champ **archer-exchange-name**, saisissez le nom d'échange de NetWitness SecOps Manager.
Un avis s'affiche indiquant que la configuration a été mise à jour correctement.
4. Dans le champ **archer-sec-ops-integration-enabled**, sélectionnez **true**.
Un avis s'affiche indiquant que la configuration a été mise à jour correctement.
Les incidents seront gérés exclusivement dans NetWitness SecOps Manager.

Définir le compteur des alertes et incidents rencontrés

Cette procédure est facultative. Les administrateurs peuvent l'utiliser pour effectuer un changement lorsque le nombre des alertes mises en correspondance est remis à 0. L'onglet Règles d'agrégation affiche ces nombres dans les colonnes à droite.

Order	Enabled	Name	Description	Last Matched	Matched Alerts	Incidents
1	●	Suspected Command & Control Communication By Domain	This incident rule captures suspected communication wi...		0	0
2	●	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA ...		0	0
3	●	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA ...		0	0
4	●	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA ...	2017-08-11 18:2...	2510	62
5	●	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ...	2017-08-12 20:0...	105464	1236
6	●	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addre...		0	0
7	●	User Watch List: Activity Detected	This incident rule captures alerts generated by network ...		0	0
8	●	Suspicious Activity Detected: Windows Worm Propagation	This incident rule captures alerts that are indicative of w...		0	0
9	●	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common l...		0	0
10	●	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert desig...		0	0
11	●	Web Threat Detection	This incident rule captures alerts generated by the RSA ...		0	0


Ces colonnes fournissent les informations suivantes pour une règle :

- La colonne **Dernière correspondance** affiche l'heure à laquelle la règle a correspondu pour la dernière fois avec les alertes.
- La colonne **Alertes mises en correspondance** affiche le nombre d'alertes rencontrées qui correspondaient à la règle.
- La colonne **Incidents** affiche le nombre d'incidents créés par la règle.

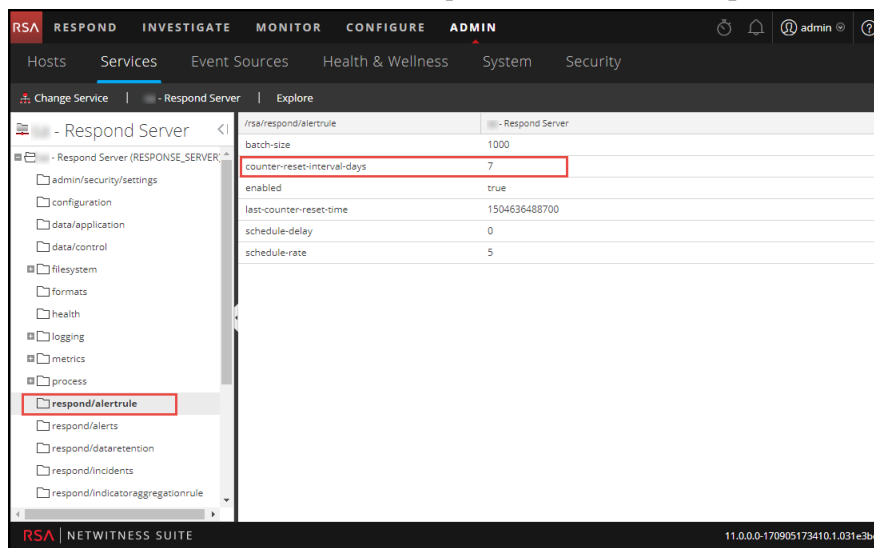
Par défaut, ces valeurs se remettent à zéro tous les 7 jours. Selon la durée que vous choisissez, vous pouvez modifier le nombre de jours par défaut.


Remarque : Lorsque le compteur est remis à zéro, seuls les nombres dans les trois colonnes passent à zéro. Aucune alerte ou incident n'est supprimé.

Pour définir un compteur des alertes et incidents rencontrés :

1. Accédez à **ADMIN > Services**, sélectionnez le service Service du serveur Respond et cliquez sur  > **Vue > Explorer**.

2. Dans la liste des nœuds de la vue Explorer, sélectionnez **respond/alertrule**.



3. Dans le panneau de droite, saisissez le nombre de jours dans le champ **counter-reset-interval-days**.
4. Redémarrez le service Service du serveur Respond pour valider le nouveau paramètre. Pour cela, accédez à **ADMIN > Services**, sélectionnez le service Service du serveur Respond, puis  > **Redémarrer**.

Configurer une base de données pour le service du serveur de réponse



Cette procédure est requise uniquement si vous avez besoin de modifier la configuration de base de données pour le serveur de réponse après le déploiement des hôtes primaires NetWitness ou ESA et de leurs services correspondants. Vous devez sélectionner le serveur principal ESA qui agira comme hôte de base de données pour les données d'application NetWitness Respond, telles que les alertes, les incidents et les tâches. Vous devez également choisir que le serveur NetWitness agisse comme hôte de base de données pour les données de contrôle NetWitness Respond telles que les catégories et règles d'agrégation.

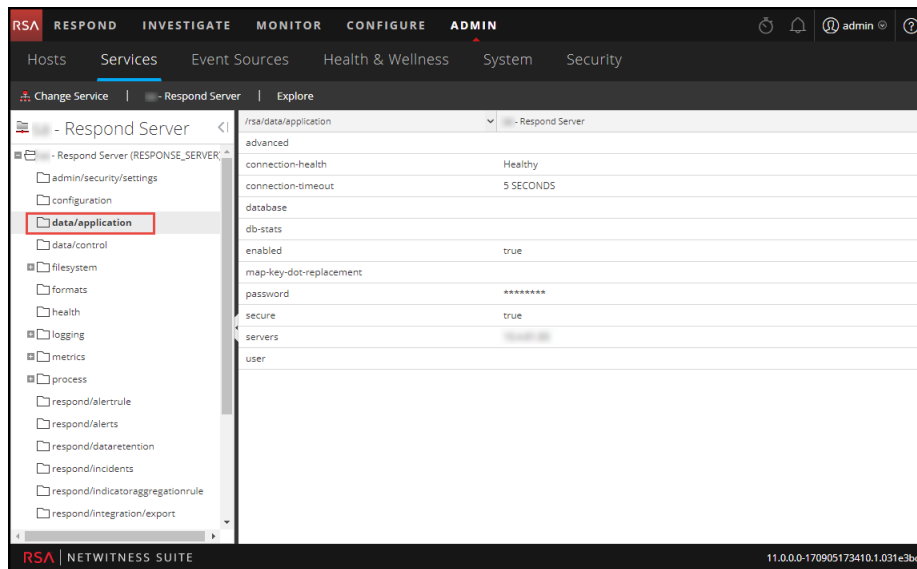
Conditions préalables

Assurez-vous que :

- vous avez installé un hôte sur lequel exécuter le service Service du serveur Respond. Reportez-vous à Étape 1 : Déployer un hôte dans le *Guide de mise en route de l'hôte et des services* pour consulter la procédure d'ajout d'un hôte.
- le Service du serveur Respond est installé et fonctionne sur NetWitness Suite.
- un hôte ESA a été installé et configuré.

Procédure

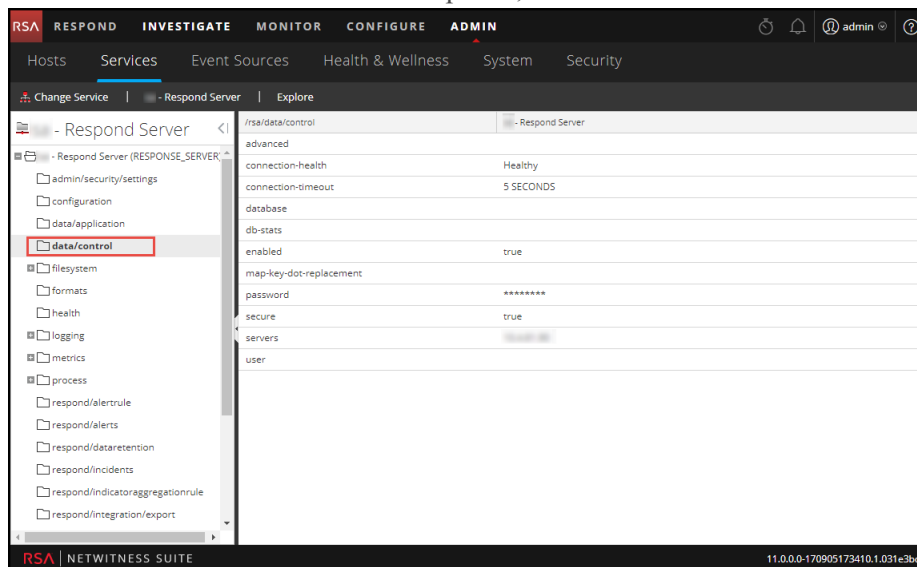
1. Accédez à **ADMIN > Services**.
La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service **Serveur Respond**, puis cliquez sur  
> **Vue > Explorer**.
3. Dans la liste des nœuds de la vue Explorer, sélectionnez **data/application**.





4. Fournissez les informations suivantes :

- **base de données** : La base de données. La valeur par défaut est respond-server.
- **mot de passe** : Le mot de passe utilisé pour le déploiement du serveur principal ESA (mot de passe de l'utilisateur deploy_admin).
- **serveurs** : Le nom d'hôte ou l'adresse IP du **serveur principal ESA** qui sert d'hôte de base de données pour les données d'application NetWitness Respond telles que les alertes, les incidents et les tâches.
- **utilisateur** : Indiquez **deploy_admin**.

5. Dans la liste des nœuds de la vue Explorer, sélectionnez **data/control**.



6. Fournissez les informations suivantes :

- **base de données** : La base de données. La valeur par défaut est respond-server.
 - **mot de passe** : Le mot de passe utilisé pour le déploiement du Serveur NetWitness (mot de passe de l'utilisateur deploy_admin).
 - **serveurs** : Le nom d'hôte ou l'adresse IP du **Serveur NetWitness** qui sert d'hôte de base de données pour les données de contrôle NetWitness Respond, telles que les catégories et règles d'agrégation.
 - **utilisateur** : Indiquez **deploy_admin**.
7. Redémarrez le Service du serveur Respond. Pour cela, accédez à **ADMIN > Services**, sélectionnez le service Service du serveur Respond, puis sélectionnez   > **Redémarrer**.

Remarque : Il est important de redémarrer le service Service du serveur Respond pour terminer la configuration de la base de données.

Référence de configuration pour NetWitness Respond

Cette section contient des informations de référence pour la configuration de NetWitness Respond.

Vue Configurer

La vue Configurer vous permet de configurer la fonctionnalité Répondre de NetWitness.

Vous pouvez configurer des règles d'agrégation pour automatiser le workflow Répondre afin de créer automatiquement des incidents.

Onglet Règles d'agrégation

L'onglet Règles d'agrégation permet de créer et de gérer des règles d'agrégation pour automatiser le processus de création d'incidents. NetWitness Suite fournit 11 règles préconfigurées. Vous pouvez ajouter ces règles et les ajuster à votre propre environnement.

Que voulez-vous faire ?

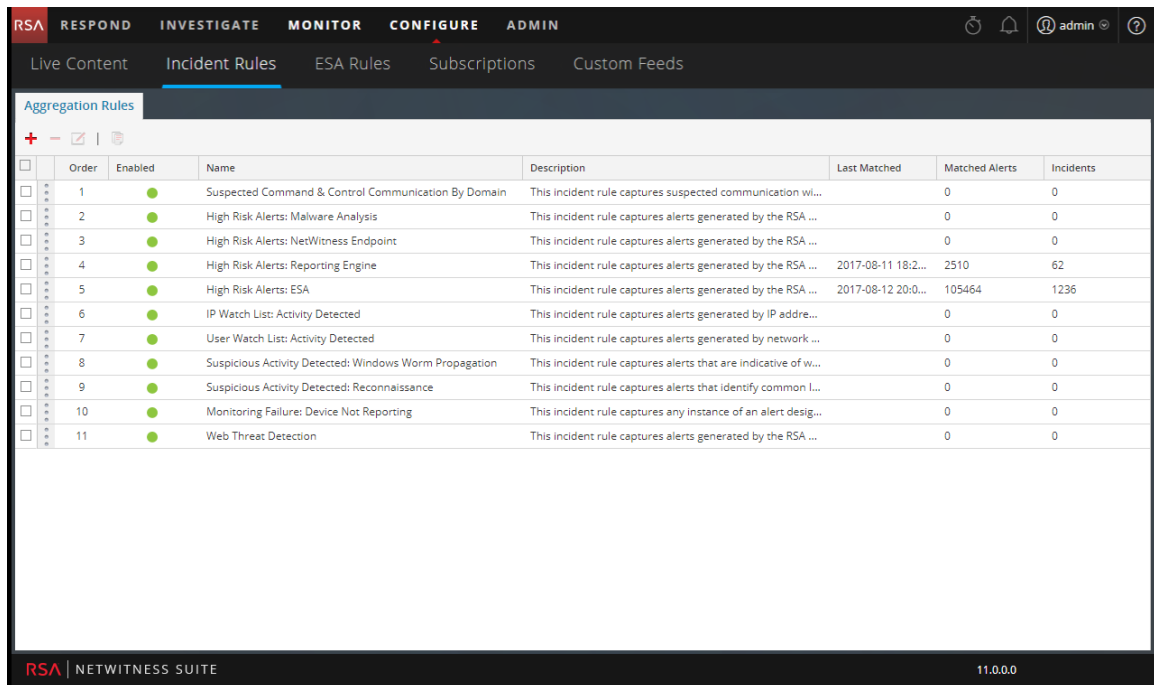
Rôle	Je souhaite...	Me montrer comment
Analyste, expert du contenu, responsable du SOC	Créer une règle d'agrégation.	Étape 3. Créer une règle d'agrégation pour les alertes
Responsables de la réponse aux incidents, analystes, experts du contenu, responsable du SOC	Afficher les résultats de ma règle d'agrégation (vue Menaces détectées).	Reportez-vous à la rubrique « Réponse aux incidents » dans le <i>NetWitness Respond Guide d'utilisation</i> .

Rubriques connexes

- [Onglet Nouvelle règle](#)

Règles d'agrégation

Pour accéder à l'onglet Règles d'agrégation, accédez à **CONFIGURER > Règles d'incidents > Règles d'agrégation**.



L'onglet Règles d'agrégation contient une liste et une barre d'outils.

Liste Règles d'agrégation





Le tableau suivant décrit les colonnes de la liste Règles d'agrégation.

Colonne	Description
Sélectionner	Vous permet de sélectionner une règle pour effectuer une action, par exemple un clonage ou une suppression.
Ordre	Indique l'ordre de placement de la règle. L'ordre des règles détermine la règle appliquée si les critères de plusieurs règles correspondent à la même alerte. Si deux règles correspondent à une alerte, seule la règle ayant la priorité la plus élevée est évaluée.
Nom	Affiche le nom de la règle.
Activée	Indique si la règle est activée ou non. ● indique que la règle est activée.
Description	Affiche la description de la règle.

Colonne	Description
Dernière correspondance	Affiche l'heure à laquelle l'alerte a été correctement mise en correspondance avec la règle. Cette valeur est réinitialisée une fois par semaine.
Alertes mises en correspondance	Affiche le nombre d'alertes mises en correspondance. Cette valeur est réinitialisée une fois par semaine. Pour modifier le paramètre, reportez-vous à la rubrique Définir le compteur des alertes et incidents rencontrés .
Incidents	Affiche le nombre d'incidents créés par la règle. Cette valeur est réinitialisée une fois par semaine. Pour modifier le paramètre, reportez-vous à la rubrique Définir le compteur des alertes et incidents rencontrés .

Barre d'outils Règles d'agrégation

Le tableau ci-dessous répertorie les opérations qui peuvent être effectuées dans la vue Règles d'agrégation.

Option	Description
	Permet d'ajouter une nouvelle règle.
	Permet de modifier une règle.
	Permet de supprimer une règle.
	Permet de dupliquer une règle.

Onglet Nouvelle règle

L'onglet Nouvelles règles vous permet de créer des règles d'agrégation personnalisées pour automatiser le processus de création d'incident. Cette rubrique décrit les informations requises lors de la création d'une nouvelle règle.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Analyste, expert du contenu, responsable du SOC	Créer une règle d'agrégation.	Étape 3. Créer une règle d'agrégation pour les alertes
ID d'incident, analystes, experts du contenu, responsables du SOC	Afficher les résultats de ma règle d'agrégation (vue Menaces détectées).	Reportez-vous à la section « Réponse aux incidents » dans le <i>NetWitness Respond Guide d'utilisation</i> .

Rubriques connexes

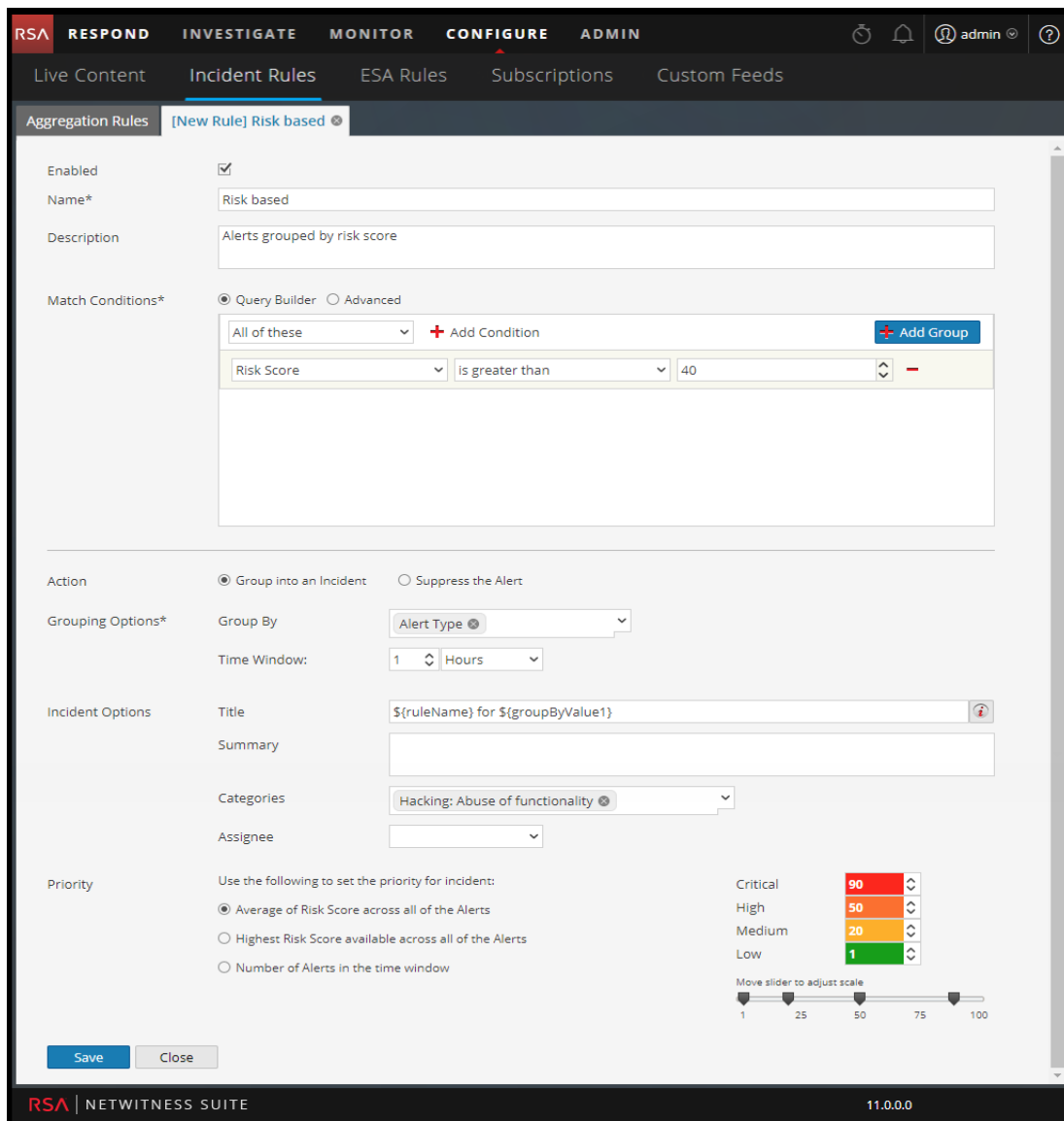
- [Onglet Règles d'agrégation](#)

Nouvelle règle

Pour accéder à la vue de l'onglet Nouvelle règle :

1. Accédez à **CONFIGURER > Règles de l'incident > onglet Règles d'agrégation**.
2. Cliquez sur **+**.

L'onglet **Nouvelle règle** s'affiche.



Le tableau suivant décrit les options disponibles lors de la création de règles d'agrégation personnalisées.

Champ	Description
Activé	Sélectionnez la règle pour l'activer.
Nom*	Nom de la règle. Il s'agit d'un champ obligatoire.
Description	Une description de la règle pour donner une idée des alertes qui sont agrégées.

Champ	Description
Conditions de mise en correspondance*	<p>Générateur de requête - Sélectionnez cette option si vous souhaitez créer une requête avec différentes conditions pouvant être regroupées. Vous pouvez également avoir des groupes imbriqués de conditions.</p> <p>Conditions de mise en correspondance - Vous pouvez définir la valeur sur Tous, N'importe lequel ou Aucun d'entre eux. En fonction de votre sélection, les types de critères spécifiés dans les conditions et le groupe de conditions sont mis en correspondance pour regrouper les alertes.</p> <p>Par exemple, si vous définissez la condition d'association sur Tous, les alertes qui correspondent aux critères mentionnés dans les Conditions et Conditions de groupe sont regroupées en un incident.</p> <ul style="list-style-type: none"> • Ajouter une condition à mettre en correspondance en cliquant sur + Ajouter une condition. • Ajouter un groupe de conditions en cliquant sur + Ajouter un groupe et ajouter des conditions en cliquant sur + Ajouter une condition. <p>Vous pouvez inclure plusieurs conditions et groupes de conditions qui peuvent être mis en correspondance selon les critères définis et regrouper les alertes entrantes en incidents.</p> <p>Avancé - Sélectionnez cette option si vous souhaitez ajouter un générateur de requête avancé. Vous pouvez ajouter une condition spécifique qui peut être mise en correspondance selon l'option correspondante sélectionnée.</p> <p>Par exemple : vous pouvez saisir le format de générateur de critères <code>{"\$and": [{"alert.severity": {"\$gt":4}}]}</code> pour regrouper les alertes qui possèdent une gravité supérieure à 4.</p> <p>Pour la syntaxe avancée, reportez-vous à http://docs.mongodb.org/manual/reference/operator/query/ ou http://docs.mongodb.org/manual/reference/method/db.collection.find/</p>
Action	<p>Regrouper dans un incident - Si cette option est activée, les alertes qui correspondent à l'ensemble de critères sont regroupées en une alerte.</p> <p>Supprimer l'alerte - Si cette option est activée, les alertes qui correspondent aux critères sont supprimées.</p>

Champ	Description
Options de regroupement*	<p>Grouper par : Critères de regroupement des alertes selon la catégorie spécifiée. Vous pouvez utiliser un maximum de deux attributs pour regrouper les alertes. Vous pouvez regrouper les alertes présentant un ou deux attributs. Vous ne pouvez plus regrouper les alertes avec des attributs qui n'ont pas de valeurs (attributs vides). Le regroupement avec un attribut signifie que toutes les alertes correspondantes contenant la même valeur de cet attribut sont regroupées dans le même incident.</p> <p>Période : Plage de temps spécifiée aux alertes de groupe. Par exemple, si la période est définie sur 1 heure, toutes les alertes qui correspondent aux critères définis dans le champ Regrouper par et qui arrivent chaque heure sont regroupés dans un incident.</p>
Options d'incident	<p>Titre :(Facultatif) Titre de l'incident. Vous pouvez fournir des espaces réservés en fonction des attributs groupés. Les espaces réservés sont facultatifs. Si vous n'utilisez pas d'espaces réservés, tous les incidents créés par la règle auront le même titre.</p> <p>Par exemple, si vous les regroupez en fonction de la source, vous pouvez nommer l'incident comme Alertes pour \${groupByValue1} et les incidents de toutes les alertes issues de NetWitness Endpoint sont nommées Alertes pour NetWitness Endpoint .</p> <p>Récapitulatif - (Facultatif) Récapitulatif de l'incident.</p> <p>Catégorie - (Facultatif) Catégorie de l'incident créé. Un incident peut être classé en utilisant plusieurs catégories.</p> <p>Personne affectée - (Facultatif) Nom de la personne affectée à laquelle l'incident est attribué.</p>

Champ	Description
Priorité	<p>Score moyen de risque pour toutes les alertes - Utilise la moyenne des notes de risque sur toutes les alertes pour définir la priorité de l'incident créé.</p> <p>Score de risque le plus élevé pour toutes les alertes - Utilise la note supérieure disponible sur toutes les alertes pour définir la priorité de l'incident créé.</p> <p>Nombre d'alertes dans la période - Utilise la somme du nombre d'alertes dans la période sélectionnée pour définir la priorité de l'incident créé.</p> <p>critique, élevée, moyenne, faible - Spécifie la priorité des incidents mis en correspondance. Par défaut :</p> <ul style="list-style-type: none"> • Critique : 90 • Élevée : 50 • Moyenne : 20 • Faible : 1 <p>Par exemple, avec la priorité Critique définie sur 90, les incidents associés à un score de risque supérieur ou égal à 90 recevront une priorité Critique pour cette règle.</p> <p>Vous pouvez modifier ces paramètres par défaut en modifiant manuellement les priorités ou en déplaçant le curseur sous Déplacez le curseur pour ajuster l'échelle.</p>

