RSA NETWITNESS® SUITE

Guide d'utilisation de Reporting

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

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

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

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

février 2018

Sommaire

Présentation du Reporting

Le reporting est une collecte de données résultant de la surveillance du trafic réseau, qui peut être utilisée pour une analyse approfondie. Dans NetWitness Suite, vous pouvez exécuter un rapport pour les services de base des bases de données de NetWitness Suite afin d'identifier les activités réseau. Par exemple, si vous voulez identifier les meilleurs pays source et les meilleurs pays de destination, ou les principales tendances de risques et de menaces qui aident à surveiller les modifications apportées aux catégories normales ou contrôler les utilisateurs et les services qui peuvent potentiellement avoir des activités malveillantes, etc..

Les fonctions de reporting sont généralement constituées de : rapports et graphiques. Vous pouvez générer un rapport lié aux données du log et des paquets collectées et personnaliser les rapports et les graphiques pour améliorer l'aspect visuel. Vous pouvez créer des rapports en temps réel pour l'historique des données. Vous pouvez créer des graphiques et des dashlets, qui peuvent également être ajoutés en temps réel aux dashlets graphiques.

Reporting Engine

Le module Reporting repose sur le Reporting Engine pour fournir des données aux rapports, alertes et graphiques. Par conséquent, vous devez configurer le Reporting Engine en tant que service pour NetWitness Suite avant de pouvoir générer les rapports. Vous devez également spécifier la source de données dans le Reporting Engine à partir de laquelle les données sont extraites.

Les données pour lesquelles vous pouvez générer un rapport ou une alerte dépendent de la configuration de Reporting Engine et des sources de données que vous spécifiez dans le cadre de la définition de la règle.

Remarque : Vérifiez que vous avez accès aux composants du Reporting.

Remarque : Vérifiez que vous avez accès aux sources de données requises. Seuls les utilisateurs privilégiés ayant accès aux informations sensibles sont autorisés à exploiter certaines sources de données. Pour gérer le contrôle d'accès aux sources de données, consultez la rubrique « Ajouter un rôle et attribuer des autorisations pour Warehouse Analytics » dans le *Guide Warehouse Analytics*. Cependant, pour les rapports, les alertes et les graphiques existants, si le rôle de l'utilisateur ou les autorisations sont modifiés pour les sources de données, alors ils ne seront pas applicables, sauf si vous mettez à jour les autorisations manuellement.

Remarque : Reporting est accessible en fonction de l'accès basé sur les rôles, défini pour l'utilisateur.

Rapport

Un rapport est une combinaison de règles et d'autres objets de formatage, par exemple des en-têtes, des remarques au format HTML, qui décrivent et identifient des données concernant un domaine d'intérêt spécifique. Les rapports sont définis et gérés dans la page Élaborer le rapport et leur exécution peut être planifiée ponctuellement ou en temps voulu. Lorsqu'un rapport est exécuté, les résultats sont stockés de manière centralisée et peuvent être envoyés automatiquement par e-mail, SFTP, URL et NFS aux utilisateurs, consultés via l'interface Web NetWitness Suite et téléchargés sous forme de fichiers PDF et CSV.

Un rapport se compose des éléments suivants :

Property	Description	Exemple
Nom du rapport **Remarque :** Pour le champ **Nom**, l'icône permettant d'étendre la taille de la colonne ne s'affiche pas à la fin du champ de colonne. Vous devez placer le pointeur de la souris un peu à gauche pour voir apparaître l'icône qui permet d'étendre la colonne.	Sert à identifier le rapport en vue de le planifier à une date ultérieure.	Rapport1
Text	Champs de texte prédéfinis utilisés dans un rapport pour rendre le rapport plus explicite pour l'utilisateur.	En-tête1, Commentaire
d'association	Règles (requêtes) utilisées pour créer un rapport.	select user.dst where ip.src = 10.10.10.1

Remarque : Dans l'interface utilisateur Reporting, la date ou l'heure affichée correspond toujours au profil de fuseau horaire sélectionné par l'utilisateur.

Règle

Une règle est le membre basique et essentiel du bloc de construction Reporting. Vous devez créer une règle qui peut être utilisée dans un Rapport, un Graphique ou une Alerte.

Une règle représente une requête unique qui détecte et récapitule les informations requises dans une collecte de données réseau.

La syntaxe de règle est fortement similaire à celle du Standard Query Language (SQL) où vous pouvez utiliser la clause select, la clause where, les options de tri et de groupe et les limites pour l'ensemble de résultats. Une règle se compose des éléments suivants :

Property	Description	Exemple
Name	Nom de la règle.	Activité de compte du système Windows
Sélectionner	Liste de types de métadonnées renvoyés dans l'ensemble de résultats. La liste de types de métadonnées est fournie dans la bibliothèque de métadonnées. La bibliothèque de métadonnées dans le Générateur de règles est continuellement synchronisée avec la configuration d'index de l'hôte NetWitness Suite auquel NetWitness Suite est connecté. Le nombre de types de métadonnées que cette propriété peut représenter dépend de la façon dont la règle doit être triée. Si la propriété Trier par est « Aucun » ou non agrégée, une règle peut avoir plusieurs champs de sélection et, par exemple, inclure les paramètres ip.src, ip.dst, taille et heure dans le résultat de la règle pour chaque correspondance. Si une règle doit être triée, par nombre de sessions, taille de session ou taille de paquet, il ne peut y avoir qu'un seul champ sur lequel effectuer la sélection.	
Où	Clause qui fournit la requête de base pour la règle.	`alert='cleartext_ftp_passwords'`

Property	Description	Exemple
Then (actions de règle)	Série de fonctions qui manipule l'ensemble de résultats original afin de rendre le résultat d'un rapport plus explicite ou d'ajouter de nouvelles fonctionnalités autres que l'interrogation et l'affichage des données.	`lookup_and_add ('username','ip.src',10);`
Trier par	Détermine la façon dont les données sont triées dans l'ensemble de résultats. Les différentes possibilités sont : • Total • Valeur • Nom de colonne	Total
Limite	Désigne la taille maximale d'un ensemble de résultats pour la règle donnée. Les utilisateurs doivent noter que si un ensemble de résultats est trié par nombre ou taille, la limite représente les N valeurs supérieures (ou inférieures) à renvoyer. Si l'ensemble de résultats n'est pas trié, les premières valeurs N sont renvoyées.	20

Remarque : Dans l'interface utilisateur, la date ou l'heure qui s'affiche dépend du fuseau horaire sélectionné par l'utilisateur.

Types de règles

Il existe différents types de règles dans Reporting. Les types de règles correspondent à la source des données d'une règle de rapport. Les types de règles sont les suivants :

Type de règle	Description
Base de données NetWitness Database (**Base de données NetWitness**)	La base de données NetWitness extrait les métadonnées d'un Reporting Engine configuré pour utiliser un Concentrator, un Broker et un Archiver comme sources de données et fournit les métadonnées pour les règles.
Base de données Warehouse (**Warehouse DB**)	La base de données Warehouse, appelée aussi RSA NetWitness Warehouse, stocke de gros volumes de données. La base de données Warehouse est conçue de façon à pouvoir récupérer de gros volumes de données facilement et efficacement. La base de données Warehouse extrait aussi les métadonnées du Reporting Engine.
Base de données Répondre (**Respond DB**)	La base de données Répondre génère des rapports sur les alertes et les incidents. La base de données Répondre contient des alertes et des incidents générés à partir de différents services et vous pouvez créer un rapport sur les incidents et les alertes.

Remarque : Dans l'interface utilisateur, la date ou l'heure qui s'affiche dépend du fuseau horaire sélectionné par l'utilisateur.

Liste

Une liste est une variable qui se réfère à une série de valeurs séparées par une virgule (CSV). Vous pouvez insérer une liste dans une règle ou l'utiliser comme argument pour une action de règle. Les listes peuvent servir d'espaces réservés pour d'autres valeurs, que vous pouvez indiquer et mettre à jour si nécessaire.

Vous pouvez créer, gérer et afficher des listes qui peuvent servir à définir des règles pour le Reporting et l'Alerting.

Les listes ne peuvent pas être vides et contenir des valeurs en double ou vides.

Remarque : Si vous définissez un rapport avec une règle qui contient lookup_and_add dans la clause **Then** et que vous dirigez le résultat du rapport dans une liste, le résultat n'est pas intégré dans la liste.
Par exemple, si vous créez une règle avec ip.src dans la clause **select** et lookup_and_add ('ip.dst','ip.src', 10) dans la clause **Then**, le rapport affiche le résultat, mais si vous avez redirigé le résultat dans une liste, cette liste est vide.

Graphique

Un graphique est une représentation sous forme de tableau ou une grille de données. Il comprend les éléments suivants :

Propriété	Description	Exemple
Nom du graphique	Identifie le graphique.	Graphique1
Base de règle	Identifie le chemin d'accès de la règle choisi dans la hiérarchie des dossiers.	

Toute règle de base de données NetWitness Suite dans le système Reporting Engine qui n'est pas triée par Aucun peut être utilisée pour créer instantanément un graphique. Dans NetWitness Suite, le début du graphique peut être ajusté dans le panneau même de définition du graphique. Chaque fois qu'un graphique est exécuté, il stocke ses résultats de données localement dans le Reporting Engine afin d'être consulté dans la vue Tableau de bord ou Graphique sans impact sur les performances.

Remarque : Dans l'interface utilisateur de Reporting, le résultat du champ où la date et l'heure sont affichées dépend toujours du profil de fuseau horaire sélectionné par l'utilisateur.

Remarque : Le Reporting Engine (RE) vérifie automatiquement l'espace disque disponible avant d'exécuter une règle, un rapport, un graphique et une alerte. Si l'espace de disque RE (en pourcentage) est inférieur au seuil de l'espace disque minimal (la valeur par défaut est 5), le RE arrête l'exécution en cours et un message d'erreur « Espace disque disponible pour la base de Reporting Engine < 5 %, veuillez nettoyer l'espace afin de poursuivre » s'affiche. En outre, vous pouvez également configurer le seuil d'espace disque minimal en utilisant le chemin d'accès suivant :
RE>Explore>com.rsa.soc.re>Configuration>CommonConfig>minDiskSpaceThreshold.

Directives de reporting

Cette rubrique affiche les instructions recommandées par RSA pour améliorer la durée d'exécution de vos entités de reporting telles que les règles, les rapports, les alertes, les graphiques et les listes. Des instructions sont fournies pour les rubriques suivantes :

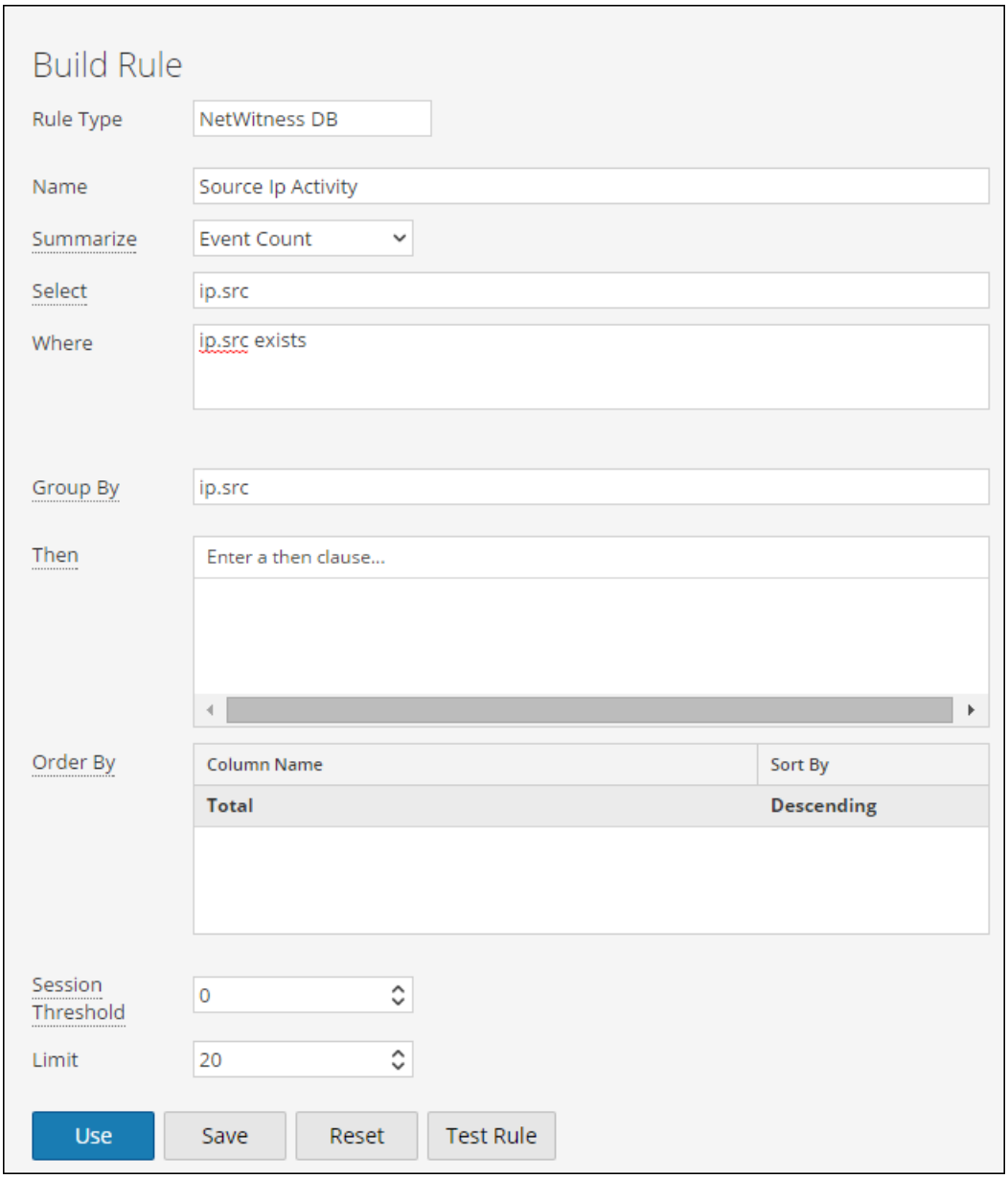
- Règles NWDB
- Configuration du délai d'expiration des règles NWDB
- Action de la règle LookupAndAdd
- Rapports de valeur de liste

Règles NWDB

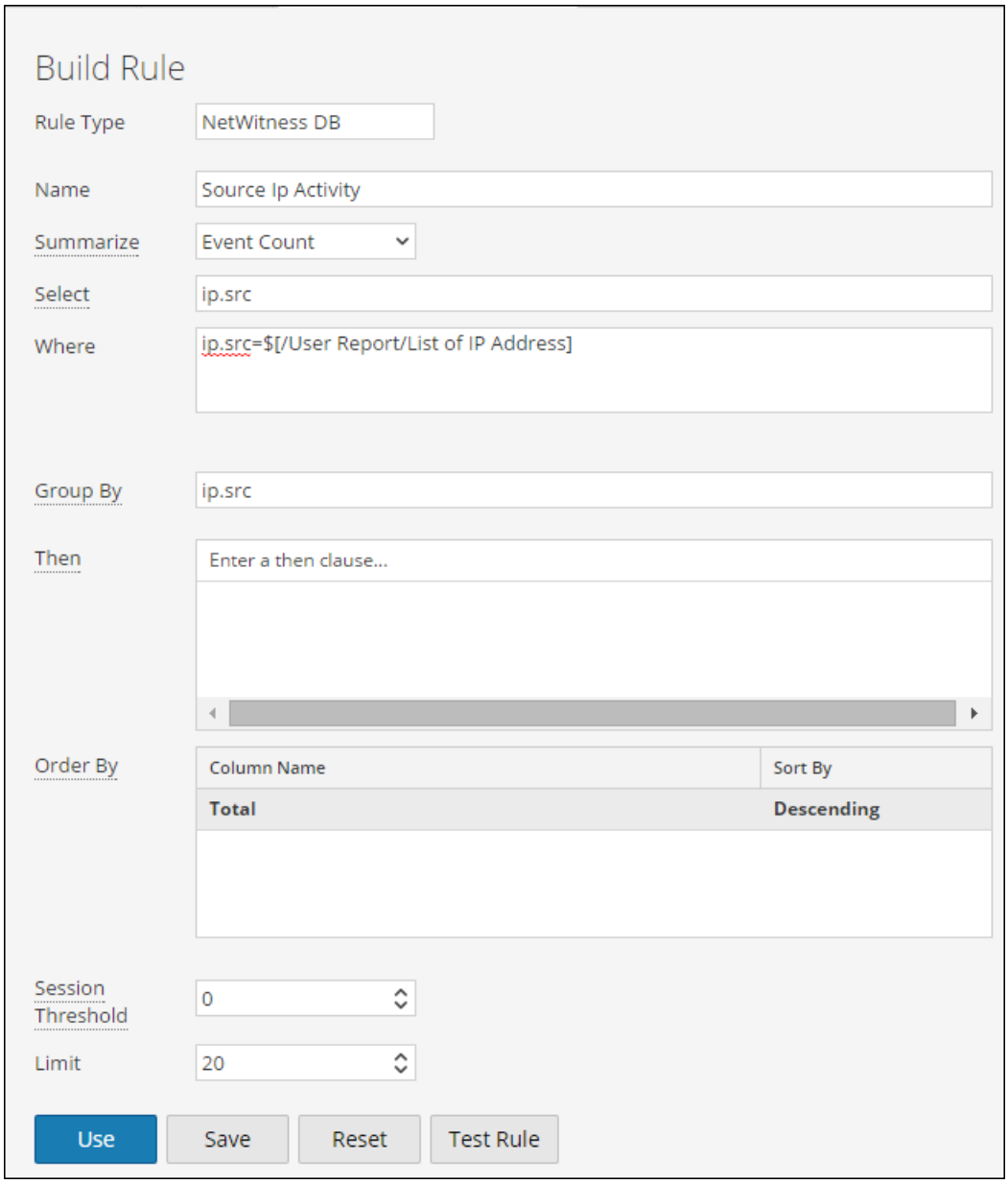
Si les entités de reporting (rapports, alertes ou graphiques) contiennent des règles NWDB (dans la plupart des cas où la requête contient Group By), le processus mettra beaucoup de temps à s'exécuter, et dans ce cas, vous pourrez effectuer les opérations suivantes :

1. Affiner la clause Where :

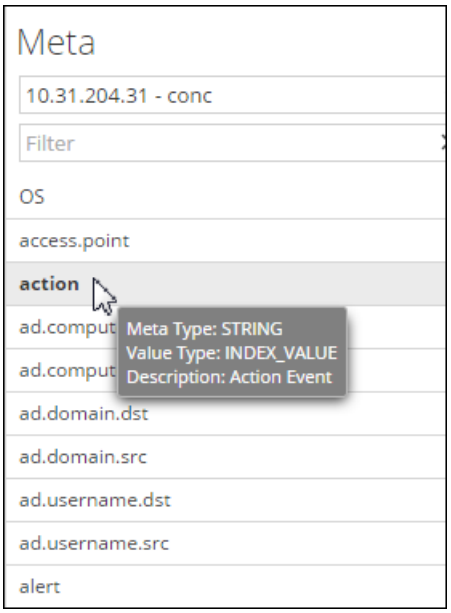
   Vous pouvez limiter le nombre de sessions analysées en utilisant ou affinant la clause Where (en particulier lorsque vous utilisez l'option Grouper par). Par exemple, envisageons la règle suivante.



Si vous utilisez une clause Where comme mentionnée ci-dessus, le nombre de sessions agrégées sera énorme. Pour éviter cela, vous pouvez filtrer uniquement les sessions requises en spécifiant la liste des adresses IP ou en créant une liste (liste des adresses IP) qui contient les adresses IP pertinentes.



2. Utilisation des clés méta indexées dans la clause Where :
   Pour savoir si la métadonnée est indexée ou non, placez la souris sur la clé méta. Si la valeur est du type INDEX_VALUE, alors la métadonnée est indexée. La valeur est du type INDEX_KEY ou INDEX_NONE si la métadonnée n'est pas indexée.
   Voici un aperçu d'une clé méta qui est indexée.



3. Configurer l'option Timeout :
   Si la requête met beaucoup de temps à s'exécuter et échoue en raison d'un problème d'expiration du délai, configurez le délai d'attente pour les exécutions de la règle NWDB. Pour plus d'informations, reportez-vous à la rubrique Configuration du délai d'expiration des règles NWDB qui figure ci-après.
4. Planifier les requêtes pour qu'elles s'exécutent à des moments différents :
   Si plusieurs agrégats de requête sont exécutés simultanément et que la temporisation se déclenche, vous pouvez planifier les requêtes pour qu'elles s'exécutent à des moments différents, sans trop de chevauchement.

Configuration du délai d'expiration des règles NWDB

Remarque : Il est conseillé de vérifier les statistiques du Reporting Engine et des sources de données NWDB avant de modifier la configuration. Pour plus d'informations, reportez-vous aux rubriques « Contrôler les détails d'un service » pour Reporting Engine, et « Contrôler les statistiques du système » dans le *Guide de maintenance du système*.

Si l'exécution de la règle NWDB échoue en raison du délai d'expiration, les erreurs suivantes peuvent s'afficher sur la page Afficher un rapport :

- Erreur liée à l'expiration du délai d'exécution du Reporting Engine
  - « Data source ‘`10.31.x.x Concentrator`' did not respond within the configured time `30` minutes for the ‘`/sdk/values`' request. »

- Erreur liée à l'expiration du délai d'exécution d'une source de données NWDB
  - « Error occurred while fetching data from source '`10.31.x.x Concentrator`'. `{Timeout message from NWDB}` »

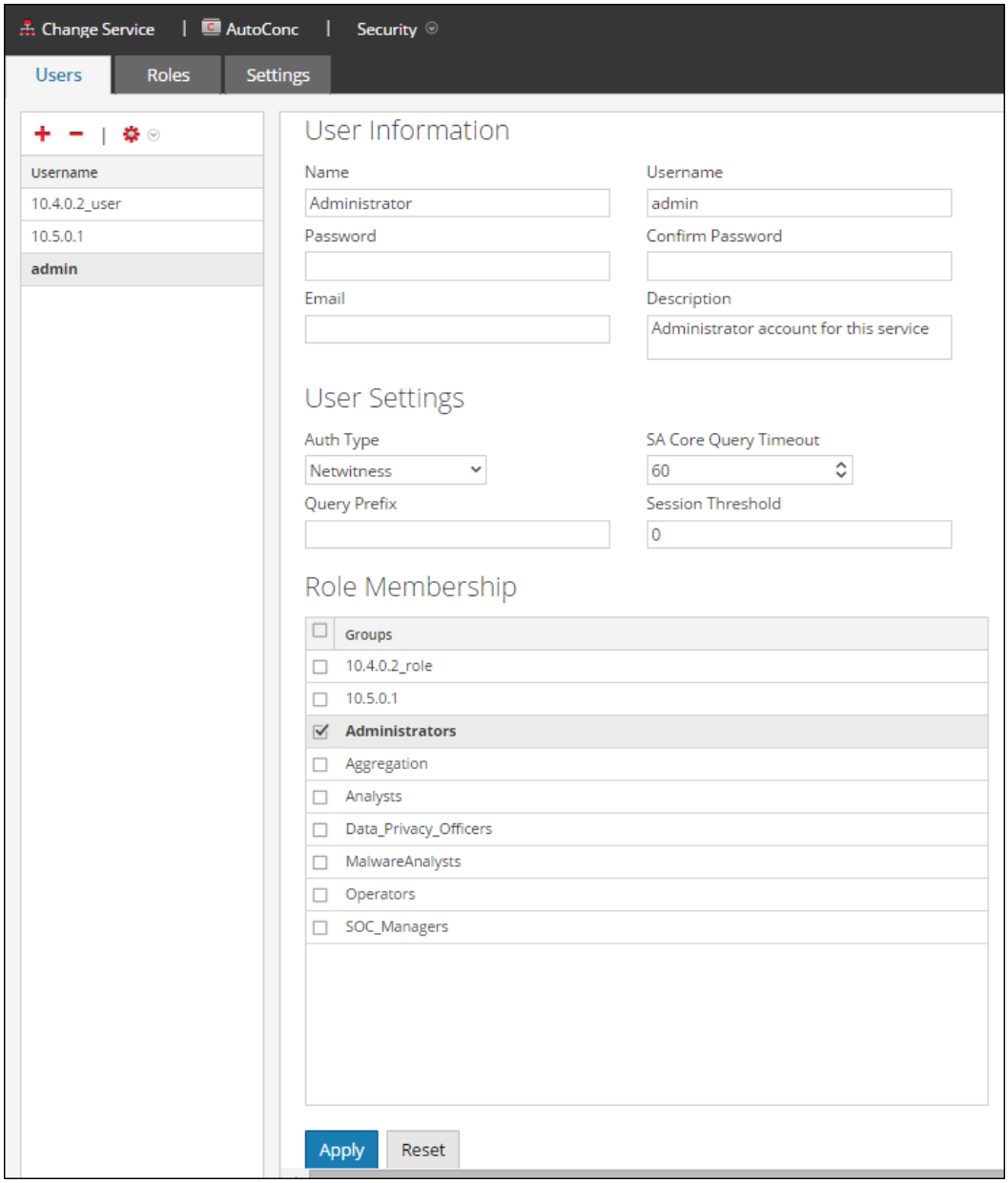
  Dans ce cas, procédez comme suit :
  - Expiration du délai d'exécution du Reporting Engine

    En cas d'expiration du délai d'exécution du Reporting Engine, vous pouvez définir un délai d'une durée plus longue de sorte que les requêtes longues puissent être exécutées. Pour plus d'informations sur la configuration des options `NWDB Queries Time Out` et `NWDB Info Queries Time Out` pour le Reporting Engine, reportez-vous à la rubrique « Étape 2. Configurer les paramètres du Reporting Engine » dans le *Guide de Configuration de Reporting Engine*. RSA vous recommande de définir l'option `NWDB Query Time Out` sur zéro minute (pas de délai) et l'option `NWDB Info Queries Time Out` sur 60 minutes.
  - Délai d'expiration NWDB

    En cas d'expiration du délai NWDB, vous pouvez configurer les paramètres `query.level.timeout` et `max.concurrent.queries` pour la source de données NWDB basée sur les recommandations du *Guide d'optimisation de base de données principale* en vue d'affiner les requêtes.

    La figure suivante présente un exemple de la vue Explorer qui vous permet de définir

les paramètres de la source de données NWDB.



- Planifier des rapports à des heures différentes

  Si les périphériques de base NWDB sont lourdement sollicités, vous pouvez planifier l'exécution des rapports à des moments différents, sans chevauchement.

- Fractionner le rapport

  Si votre rapport contient de nombreuses règles, fractionnez le rapport en plusieurs rapports contenant chacun un ensemble logique de règles. Si vous avez plusieurs règles,

toutes les règles vont commencer à s'exécuter en même temps, sur la base de threads disponibles, donc vous pouvez regrouper les règles de manière logique dans des rapports distincts.

Action de la règle LookupAndAdd

Si une règle composée d'une ou de plusieurs actions de règle `lookup_and_add` prend beaucoup de temps à exécuter le rapport, c'est parce que chaque action de règle déclenche plusieurs requêtes de recherche sur la source de données NWDB, ce qui implique un temps d'exécution plus long.

Pour améliorer le temps d'exécution des rapports, vous pouvez effectuer les opérations suivantes :

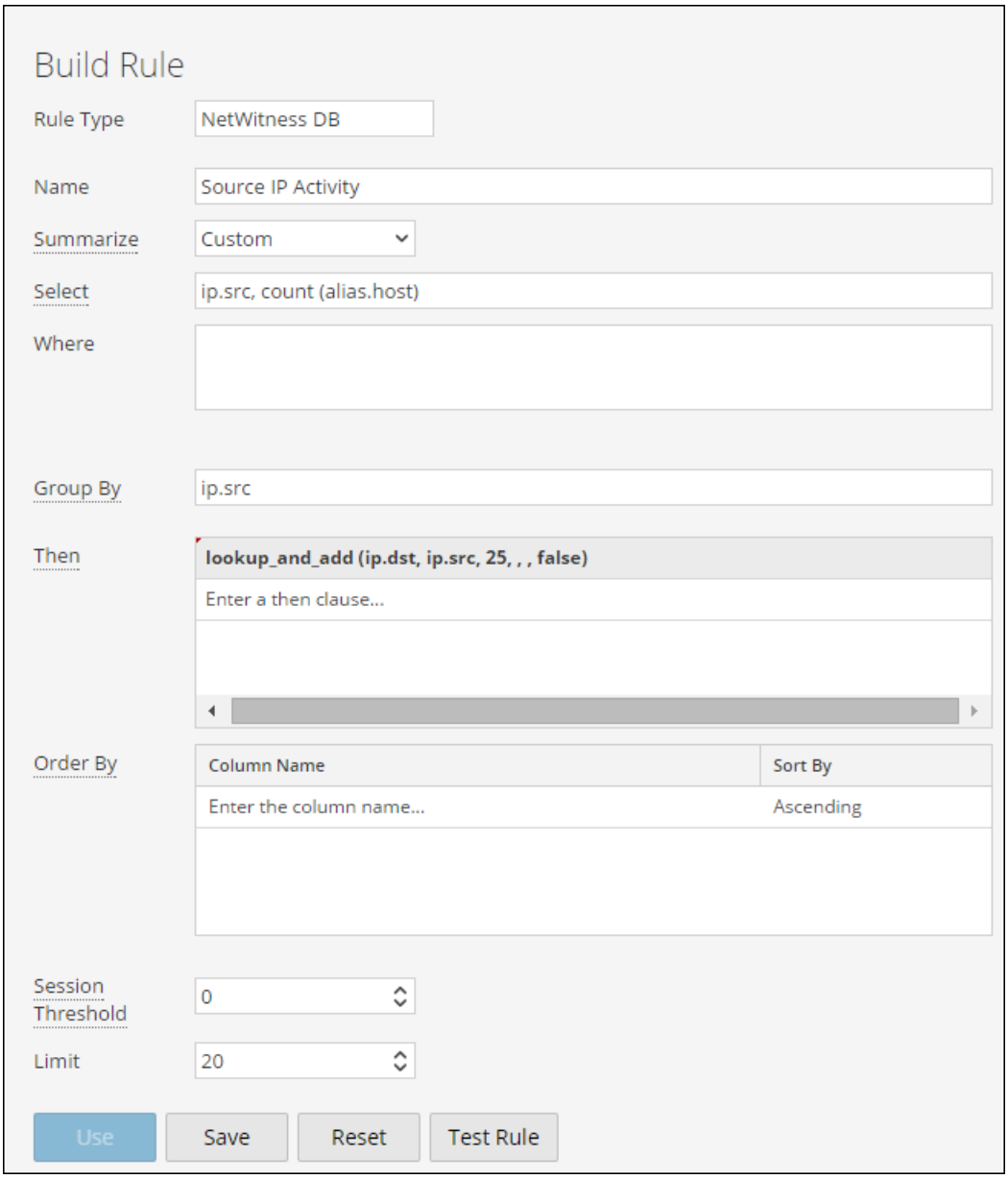
- Affiner la clause Where comme suit :
  - Règle contenant l'action de règle `lookup_and_add`
  - Action de règle `lookup_and_add`
- Définir des limites

  Vous devez définir des limites appropriées pour la règle et les actions de la règle. Si la limite est élevée, cela se traduira par le déclenchement de nombreuses requêtes, et donc le rapport prendra beaucoup de temps à s'exécuter.
- Définir le paramètre booléen aggregate

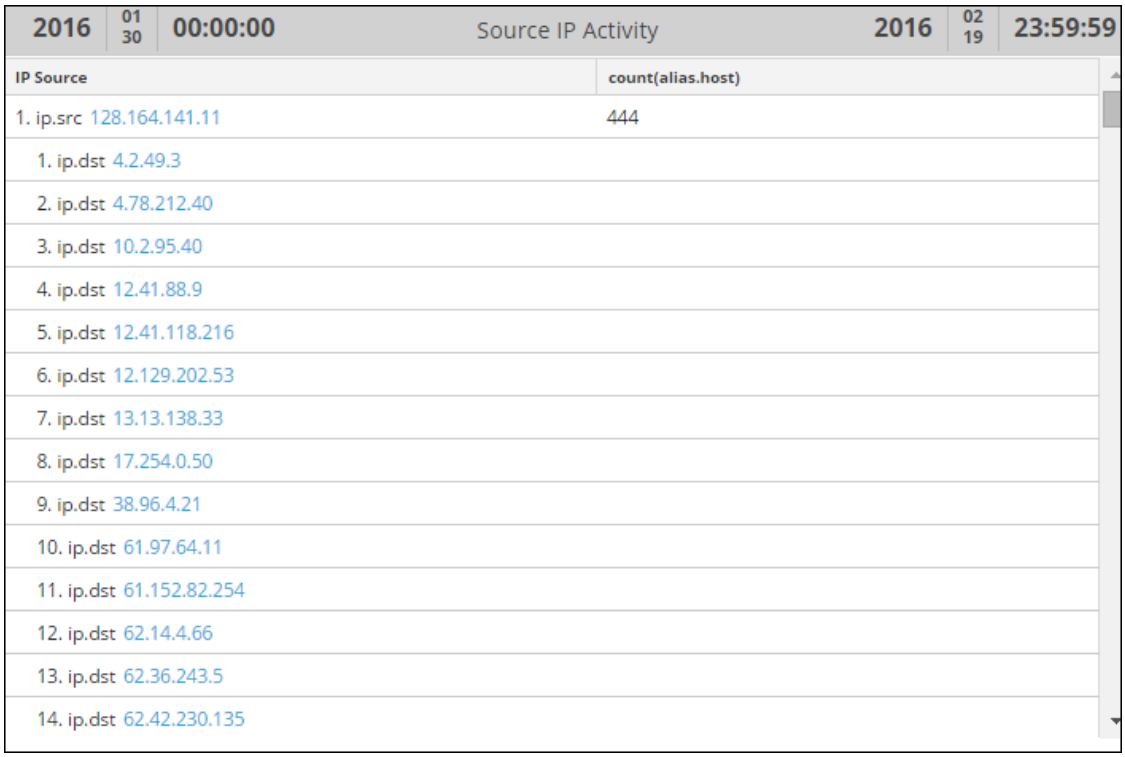
  Si vous ne souhaitez pas de valeur d'agrégat, comme `sum(meta)`, `count(meta)`, etc. pour les valeurs de recherche, définissez le paramètre booléen aggregate sur false dans l'action de la règle `lookup_and_add`. Pour plus d'informations, reportez-vous à la rubrique Syntaxe des règles NWDB dans Syntaxe de la règle .

  ```
  lookup_and_add(string select, string field, int limit, boolean
  inherit, string extraWhere, boolean aggregate)
  ```

  Envisageons la règle contenant l'action de la règle lookup_and_add :



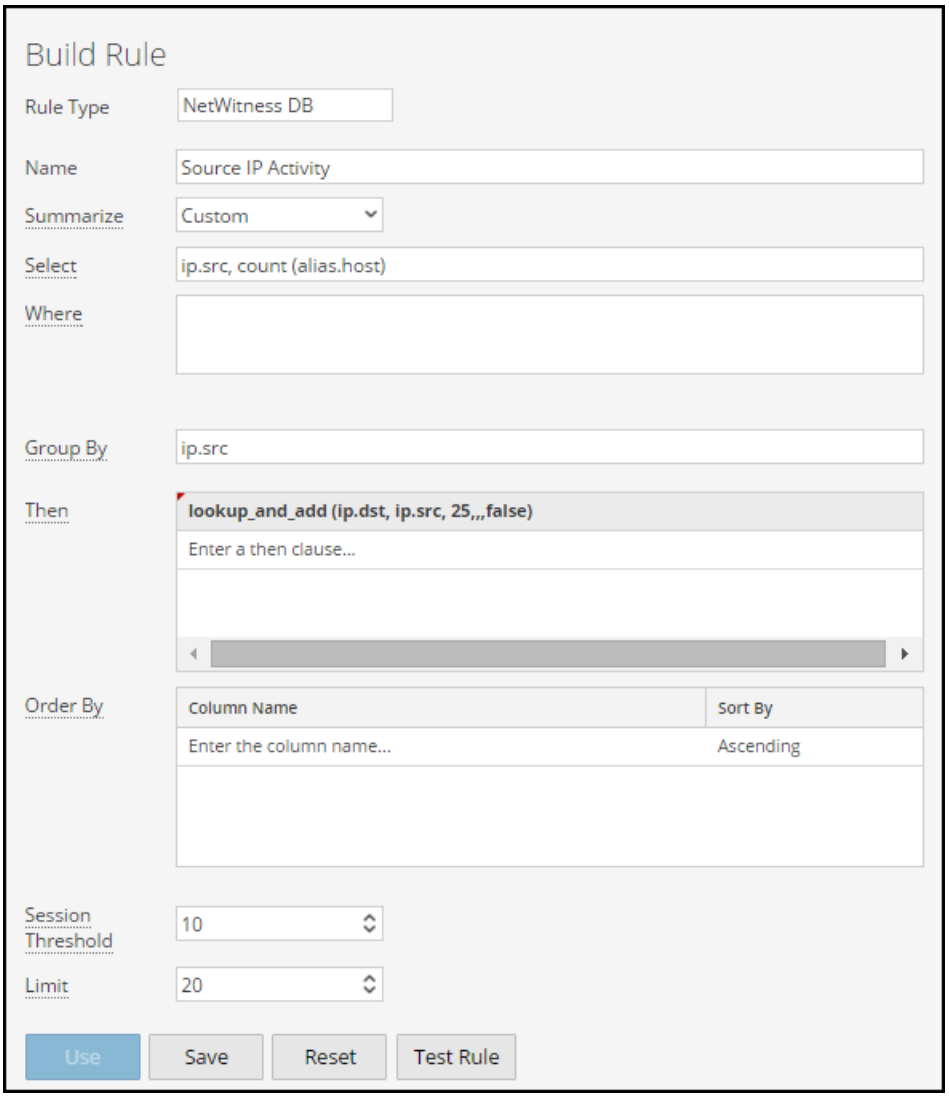
Le résultat s'affiche :



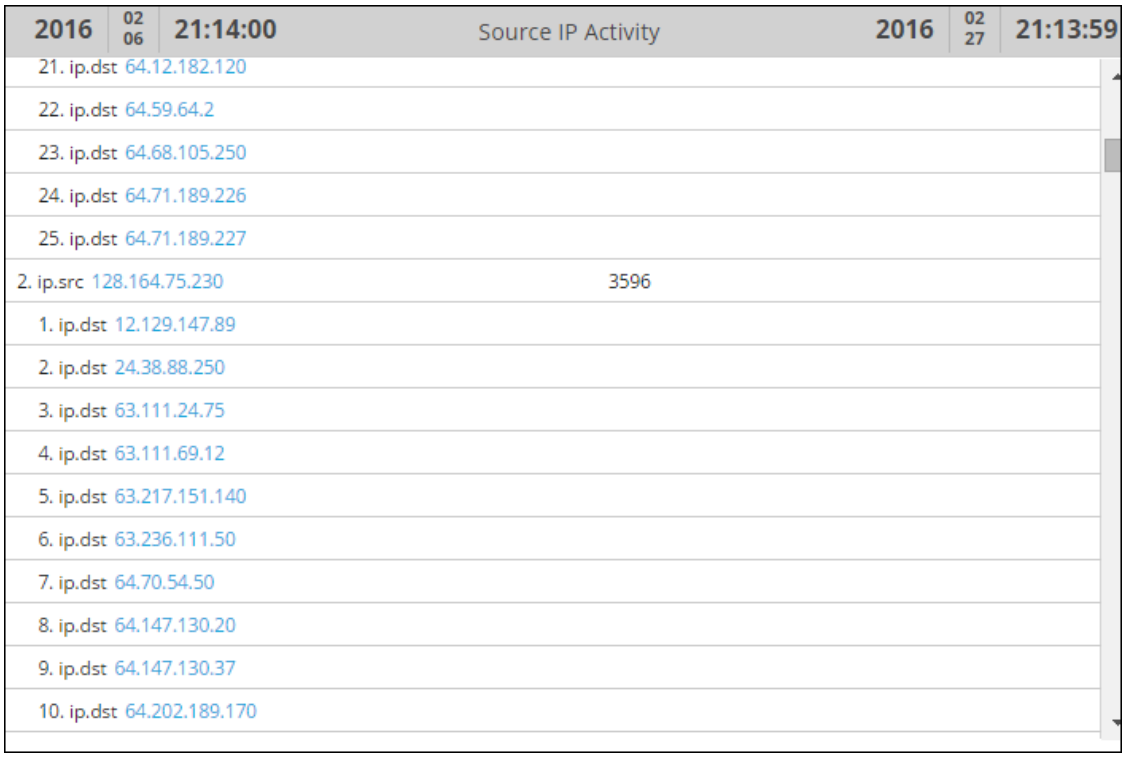
- Chaque action de la règle `lookup_and_add` déclenche par défaut deux requêtes de recherche simultanées sur la source de données. RSA recommande de conserver la configuration par défaut, mais si vous souhaitez augmenter la valeur, vérifiez que la valeur du paramètre `Max # of Concurrent LookupAndAdd Queries` dans Reporting Engine est inférieure à la valeur `Max Concurrent Queries` dans la configuration de la source de données NWDB.

  Si la source de données NWDB est partagée entre d'autres services, alors vous pourrez conserver une faible valeur pour le paramètre `Max # of Concurrent LookupAndAdd Queries` dans Reporting Engine, car le fait de l'augmenter pourrait avoir un impact sur les requêtes issues d'autres services. Pour plus d'informations, consultez la rubrique « Onglet général du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
- Si vous êtes intéressé(e) uniquement par les valeurs uniques au lieu des valeurs agrégées précises, alors définissez le `Session Threshold` à une valeur non nulle pour la règle NWDB. Pour plus d'informations, voir la rubrique Création d'une règle à l'aide de la source de données NetWitness dans Configurer une règle. Plus la valeur est haute, plus l'exécution de la règle est longue. Si la valeur est définie sur zéro, il faudra plus de temps, mais elle fournira des agrégats précis.

  Envisagez une règle avec l'action de règle lookup_and_add et un seuil de session sur 10.



Le résultat s'affiche :



Rapports de listes de valeurs

Utiliser une liste affinée :

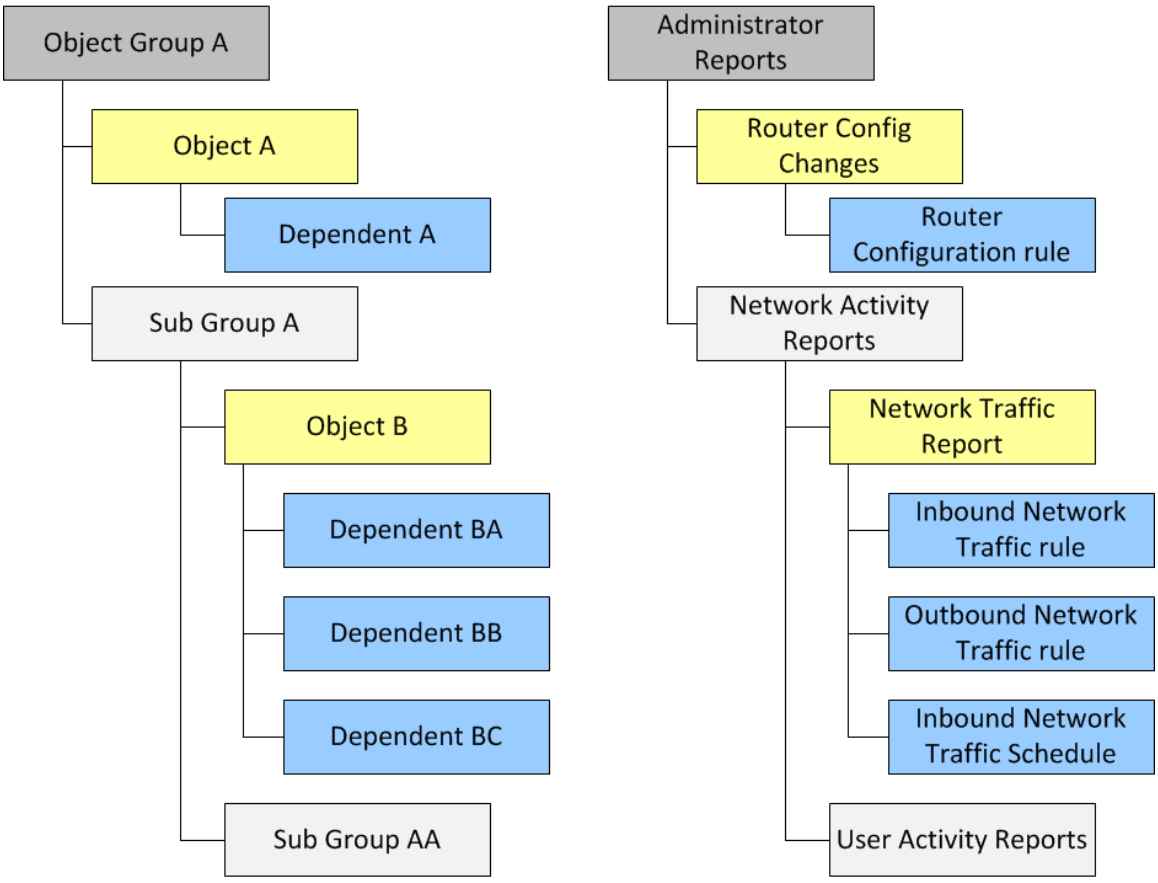
Dans le cas des rapports de listes de valeurs (pour n'importe quel type de source de données), les rapports individuels seront générés pour chaque valeur de la liste. Par conséquent, plus la liste contient de valeurs, plus les rapports prendront du temps à s'exécuter. De ce fait, vous devez utiliser une liste affinée pour produire ces rapports.

Contrôler l'accès à Reporting

Le module Reporting vous offre la possibilité de configurer un contrôle d'accès à tous les composants du module. Dans NetWitness Suite, vous pouvez définir différents rôles et spécifier le contrôle d'accès pour chacun des rôles du module de sécurité du système. Vous pouvez définir le contrôle d'accès à fournir pour le module Reporting pour chaque rôle. Pour plus d'informations, reportez-vous à « Étape 1 : Passer en revue les rôles préconfigurés NetWitness Suite » et « Étape 2 : (Facultatif) Ajouter un rôle et attribuer des autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Dans le module Rapports, vous pouvez modifier les autorisations des rôles ou accéder aux objets Reporting suivants :

Voici un exemple de la hiérarchie des groupes d'objets, des objets et des dépendants. Il s'agit d'une illustration de la hiérarchie des groupes de rapports et des rapports.



Hiérarchie des groupes de rapports et des rapports

Autorisation pour les groupes d'objets

- Vous devez avoir l'autorisation Lecture et écriture pour définir les autorisations pour les groupes d'objets, les objets ou les dépendants. Les dépendants avec l'autorisation « Aucun accès » sont grisés et les dépendants avec l'autorisation « Lecture seule » sont signalés par une icône.
- Lorsque vous définissez l'autorisation pour le groupe d'objets, les objets et les dépendants du groupe d'objets, n'attribuez pas l'autorisation automatiquement. Vous devez sélectionner le paramètre « Appliquer ces autorisations aux sous-groupes et <Objets> dans ce groupe » pour effectuer l'opération. Par exemple, si vous ne souhaitez pas que les rôles Opérateurs accèdent aux rapports du Groupe de rapports A, vous devez alors appliquer l'autorisation Aucun accès au groupe A pour le rôle Opérateur. Ensuite, vous devez sélectionner l'option « Appliquer ces autorisations aux sous-groupes et rapports dans ce groupe ».
- Lorsque vous définissez les autorisations pour le groupe d'objets et sélectionnez l'option « Appliquer ces autorisations aux sous-groupes et <Objets> dans ce groupe », les dépendants

comme les règles ou les plannings en tant qu'objets n'héritent pas des autorisations automatiquement. Vous devez utiliser l'option « Appliquer l'autorisation de lecture seule aux <Objets> » pour appliquer l'autorisation aux règles.

- Lorsque vous définissez des autorisations pour les objets, vous devez vous assurer que les objets de la hiérarchie ont toujours une autorisation qui est inférieure ou égale à celle au-dessus dans la hiérarchie pour que l'autorisation soit appliquée. Par exemple, les rapports contenus dans un groupe de rapports ont l'autorisation Lecture et écriture. Vous appliquez une autorisation Lecture seule ou Aucun accès au niveau du groupe de rapports et vous sélectionnez l'option « Appliquer ces autorisations aux sous-groupes et rapports dans ce groupe », alors l'autorisation sur les règles restera inchangée.
- Les autorisations sont mises en cascade du haut vers le bas dans la hiérarchie et non vice-versa. Par exemple, si vous appliquez une autorisation à une règle, elle ne changera pas l'autorisation du rapport qui contient la règle.

Autorisation pour les objets ou les dépendants

- Vous devez avoir l'autorisation Lecture et écriture pour définir les autorisations pour les objets ou les dépendants.
- Vous pouvez spécifier l'autorisation pour plusieurs objets à la fois au lieu de définir l'autorisation pour chaque objet.
- Lorsque vous définissez l'autorisation pour l'objet et les dépendants de l'objet, n'attribuez pas l'autorisation automatiquement. Vous devez sélectionner l'option « Appliquer l'autorisation de lecture seule aux <Objets> » pour exécuter l'opération.

Lorsque vous appliquez l'autorisation aux dépendants, elle est appliquée sur la base de l'autorisation existante pour le rôle. Prenons par exemple un analyste et un opérateur avec les autorisations suivantes pour les différents dépendants (l'objet du Rapport A a la Règle AA, la Règle AB et la Règle AC comme dépendants).

Objet ou Dépendant	Analyste	Opérateur
Rapport A	Lecture et écriture	Aucun accès
Règle AA	Lecture et écriture	Aucun accès
Règle AB	Lecture et écriture	Lecture et écriture
Règle AC	Lecture seule	Aucun accès

Si l'analyste applique une autorisation de lecture et écriture pour le rôle Opérateur et sélectionne l'option « Appliquer l'autorisation de lecture seule aux <Objets> », les autorisations seront définies pour les différents dépendants comme suit :

Modifiez les autorisations.

- **Niveau du groupe :** Définissez les autorisations au niveau du groupe d'objets et pour tous les objets et entités du Groupe. Par exemple, si vous avez 80 rapports dans le groupe Rapports administrateurs rapports et que vous souhaitez que seul l'administrateur ajoute ou modifie ces rapports, vous pouvez définir l'autorisation pour tous les autres rôles au niveau du groupe en lecture seule, et sélectionnez la possibilité de l'appliquer à tous les rapports et les sous-groupes au sein du groupe de rapports.
- **Objets multiples :** Sélectionnez plusieurs objets et spécifiez l'accès à tous les objets sélectionnés. Par exemple, si vous avez 10 rapports dans le sous-groupe Trafic réseau avec des informations sensibles que vous ne souhaitez pas laisser accessibles, sélectionnez les 10 rapports, puis définissez l'autorisation « Aucun accès » pour tous les rôles.
- **Objet unique :** Sélectionnez uniquement l'objet et spécifiez l'autorisation. Par exemple, sélectionnez le rapport Trafic réseau et spécifiez l'autorisation de lecture-écriture pour le rôle Analyste de sécurité, ou sélectionnez l'alerte en cas d'échec de la connexion et spécifiez l'autorisation de lecture-écriture pour le rôle Analyste de sécurité.

Objet ou Dépendant	Opérateur (avant l'application de l'autorisation)	Opérateur (après l'application de l'autorisation)
Rapport A	Aucun accès	Lecture et écriture
Règle AA	Aucun accès	Lecture seule
Règle AB	Lecture et écriture	Lecture et écriture
Règle AC	Aucun accès	Lecture seule

Rôles et autorisations pour le module de reporting

Bien que NetWitness Suite inclue cinq rôles préconfigurés, vous pouvez ajouter des rôles personnalisés. Par exemple, parallèlement au rôle préconfiguré Analystes, vous pouvez ajouter les rôles personnalisés AnalystesEurope et AnalystesAsia.

Rôle	Autorisation
Administrateurs	Accès complet au système
Opérateurs	Accès aux configurations mais pas aux données
Analystes	Accès aux données mais pas aux configurations
SOC_Managers (Responsables de SOC)	Même accès que les Analystes avec des autorisations supplémentaires pour gérer les incidents
Malware_Analysts (Analystes du malware)	Accès aux événements de malware uniquement

En fonction du rôle d'utilisateur, vous pouvez définir les autorisations d'accès suivante pour accéder aux composants du module Reporting (Règles, Rapports, Graphiques, Alertes et Listes) :

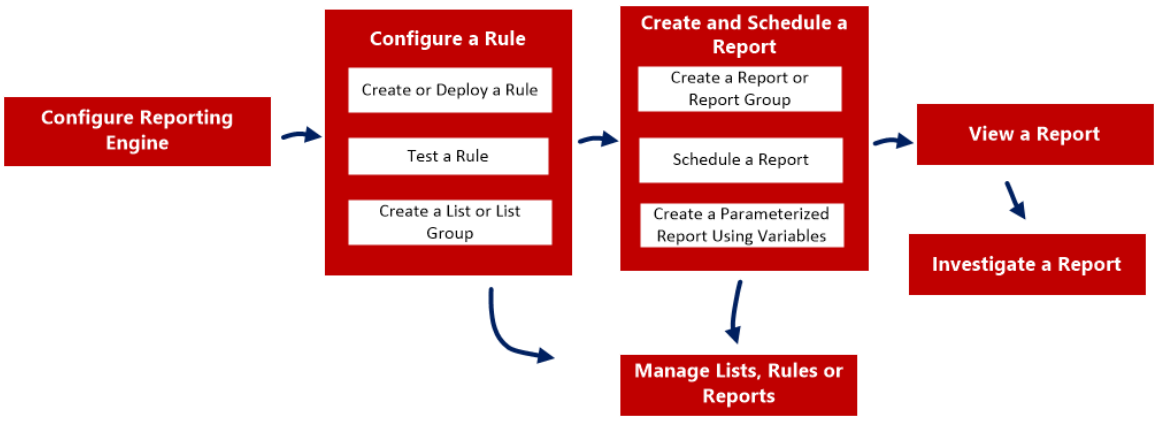
- Créer
- Supprimer
- Exporter
- Manage
- Afficher

Remarque : Vous devez activer toutes les autorisations pour qu'un rôle d'utilisateur puisse définir, supprimer, gérer et consulter chacun des modules Reporting. Vous devez également disposer des autorisations appropriées pour que la source de données soit répertoriée tout en définissant les rapports, graphiques ou alertes. Pour plus d'informations, reportez-vous à la rubrique « Configurer les autorisations d'accès aux sources de données » dans le *Guide de configuration de Reporting Engine*.

Pour obtenir une liste détaillée des autorisations et savoir comment ajouter un rôle et attribuer des autorisations, reportez-vous à la rubrique « Autorisations de rôle » et « Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Configurer et générer un rapport

Cette figure est une vue d'ensemble de tout le processus de configuration et de génération d'un rapport.



Pour configurer et générer un rapport, procédez comme suit :

1. Configurer Reporting Engine - Vvous devez configurer le Reporting Engine avant de pouvoir configurer et générer un rapport. Vous devez également spécifier la source de données dans le Reporting Engine à partir de laquelle les données sont extraites. Pour plus d'informations sur la façon de configurer Reporting Engine, reportez-vous à la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting*.
2. Configurer une règle
3. Créer et planifier un rapport
4. Afficher un rapport
5. Analyser un rapport
6. Gérer les listes, les règles ou les rapports

Configurer une règle

Vous pouvez créer une nouvelle règle ou déployer une règle existante à partir de Services Live qui peut être utilisée dans un rapport. Vous pouvez utiliser différentes conditions pour affiner les données ou les informations contenues dans les sources de données telles que :

- Clause select
- Clause where
- Regrouper par
- Trier par, etc.

Par exemple, vous pouvez écrire une règle pour afficher les 20 adresses principales que les utilisateurs visitent quotidiennement.

Vous pouvez créer différents types de règles à l'aide de différentes sources de données. Selon vos exigences, vous pouvez sélectionner l'une des options suivantes pour créer une règle :

- Créer une règle avec une source de données NetWitness
- Créer une règle avec une source de données Warehouse
- Créer une règle avec une source de données Respond

Vous pouvez également utiliser une liste dans une règle pour affiner les résultats de recherche à partir de la source de données. Lorsqu'une règle est créée, vous pouvez tester une règle pour consulter les résultats renvoyés par la règle.

Créer un groupe de règles

Pour créer un groupe de règles ou un sous-groupe de règles, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Exécutez l'une des opérations suivantes :
   - Pour définir un groupe de règles :
     a. Dans le panneau Groupes de règles, cliquez sur  .
        Un nouveau groupe de règles est ajouté au panneau Groupes de règles.
     b. Saisissez le nom du groupe de règles et appuyez sur ENTRÉE.

- Pour ajouter un sous-groupe de règles :
  a. Dans le panneau Groupes de règles, sélectionnez le groupe de règles auquel ajouter un sous-groupe.
  b. Cliquez sur + .
     Un nouveau sous-groupe de règles est ajouté au groupe de règles.
  c. Saisissez le nom du sous-groupe de règles et appuyez sur ENTRÉE.

Créer une règle avec une source de données NetWitness

Vous pouvez créer une règle afin d'extraire des données ou des événements à partir d'une source de données NetWitness. La même procédure permet de définir une règle afin d'extraire des données ou événements à partir d'une source de données Archiver.

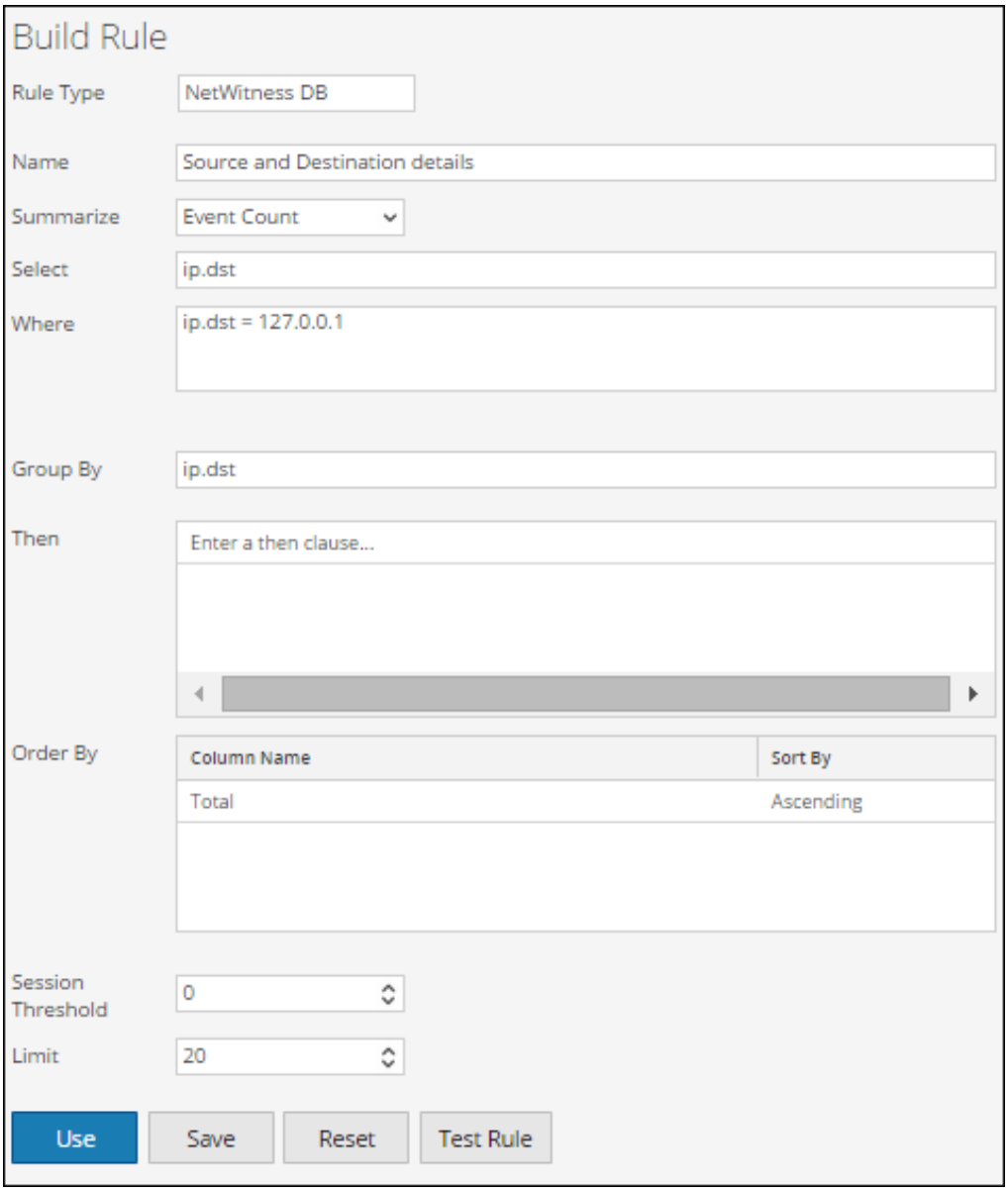
Les sources de données Archiver peuvent être ajoutées dans la vue Configuration des services du Reporting Engine. Pour plus d'informations, consultez la section (Facultatif) « Ajouter Archiver comme source de données au Reporting Engine » dans le *Guide de configuration Archiver*.

Conditions préalables

Veillez à comprendre la manière dont les clés méta personnalisées sont créées à l'aide des feeds personnalisés. Pour plus d'informations, reportez-vous à la rubrique « Créer des clés méta personnalisées à l'aide d'un feed personnalisé » dans le *Guide de configuration de Decoder et Log Decoder*.

Pour créer une règle afin d'extraire des données ou événements à partir d'une source de données NetWitness, procédez comme suit :

1. Sélectionnez **SURVEILLER**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans la barre d'outils, cliquez sur + > **Base de données NetWitness**.
   L'onglet de la vue Élaborer une règle s'affiche.



3. Dans le champ **Type de règle**, **Base de données NetWitness** est sélectionné par défaut.
4. Dans le champ **Nom**, saisissez un nom utilisé pour identifier ou libeller la règle dans les alertes et rapports.
5. Le champ **Résumé** détermine le type de résumé ou d'agrégation correspondant à la règle. En fonction du type de règle à définir, vous devez sélectionner l'une des options suivantes :
   - Pour définir une règle **Sans agrégation** sans regroupement, sélectionnez : **Aucune**
   - Pour définir une règle **Agrégation** avec une agrégation spéciale comme les agrégats associés à une collection (sessions/événements/paquets), sélectionnez l'une des options suivantes :

- Décompte d'événements
- Nombre de paquets
- Taille des sessions

- Pour définir une règle **Agrégation** avec des métavaleurs et des agrégats personnalisés tels que sum(), count(), etc., sélectionnez : **Custom**

  Choisir « Personnalisé » dans le champ **Résumé** vous permet de définir la fonction d'agrégation de votre choix dans la clause *Select*. Par exemple, select ip.src, countdistinct (ip.dst), distinct(ip.dst). Les fonctions d'agrégation prises en charge sont les suivantes :

  - sum (<meta>)
  - count(<meta>)
  - countdistinct(<meta>)
  - min(<meta>)
  - max(<meta>)
  - avg(<meta>)
  - first(<meta>)
  - last(<meta>)
  - len(<meta>)
  - distinct(<meta>)

  Pour plus d'informations détaillées sur les règles agrégées et non agrégées, reportez-vous à la rubrique Syntaxe des règles NWDB dans Syntaxe de la règle .

6. Dans le champ **Select**, saisissez un méta ou sélectionnez-en un dans la liste des types de métas disponibles fournis dans la bibliothèque des méta. Pour plus d'informations, reportez-vous à la section « Panneau méta » dans la Vue Élaborer une règle. Le nom du méta permettant de récupérer le log brut est raw. Raw peut uniquement être utilisé dans le champ **Select**. Il ne peut pas être utilisé dans les champs **Where** et **Then**. Plusieurs fonctions d'agrégation sont prises en charge pour la règle d'agrégation personnalisée dans le champ **Select**.

   Remarque : Dans les versions antérieures de NetWitness Suite, une seule fonction d'agrégation était prise en charge pour la règle d'agrégation personnalisée dans la clause **Select**. Désormais, plusieurs fonctions d'agrégation sont prises en charge dans la clause **Select**. Par exemple, Select: *ip.src, username, service, distinct(country.src), sum (payload)*.

7. Dans le champ **Alias**, saisissez le nom d'alias des colonnes utilisées dans la clause Select.

8. Dans le champ **Where**, saisissez un méta ou sélectionnez un méta dans la liste des types de méta disponibles, puis utilisez les opérateurs permettant de construire la clause Where pour les critères de requête de base.
9. Le champ **Regrouper par** est un champ en lecture seule qui fournit les méta qui sont définis dans la clause Select. Pour une fonction sans agrégation, ce champ n'est pas visible. Un maximum de six méta sont pris en charge dans le champ **Regrouper par**.

   Remarque : Dans les versions antérieures de NetWitness Suite, un seul méta était pris en charge pour la règle d'agrégation personnalisée dans la clause **Group By**. Désormais, un maximum de six méta est pris en charge dans la clause **Group By** .
10. Dans le champ **Then**, saisissez les actions de règle qui manipulent l'ensemble des résultats d'origine d'une règle afin de rendre la sortie du rapport plus concrète ou d'ajouter d'autres fonctionnalités que l'interrogation des données et leur affichage. Par exemple, la création d'un feed issu des résultats. Pour obtenir la liste complète des actions de règle disponibles, reportez-vous à la rubrique Syntaxe des règles NWDB dans Syntaxe de la règle .

    Remarque : Lorsqu'une règle est exécutée pour une source de données Archiver, il est recommandé de ne pas utiliser les actions de règles intensives pour les requêtes telles que lookup_and_add() et show_whats_new().
11. Dans le champ **Réorganiser par**, procédez comme suit :
    a. Dans la colonne **Nom de la colonne**, saisissez le nom des colonnes dont vous souhaitez trier les résultats. Par défaut, la valeur est vide. La valeur est renseignée en fonction de la valeur sélectionnée dans le champ **Résumé**.
       - Pour la valeur « Aucun » du champ Résumé, si aucune valeur **Réorganiser par** n'est sélectionnée, par défaut le tri s'effectue en fonction de l'heure de la session ou de la collecte.
       - Pour les valeurs du champ Résumé, le tri par défaut est basé sur le premier méta « group by » sélectionné lorsqu'aucune valeur « order by » n'est définie. Pour les zones Décompte d'événements, Nombre de paquets et Taille des sessions, les valeurs acceptées sont Total et Valeur.

    b. Dans la colonne **Trier par**, sélectionnez l'une des méthodes suivantes pour trier les résultats :
       - Ordre croissant
       - Ordre décroissant
12. Dans le **seuil de session**, saisissez le paramètre d'optimisation qui permet de rechercher chaque valeur unique possible de la métadonnée sélectionnée dans les sessions correspondantes. Le seuil est un nombre entier compris entre 0 (par défaut) et 2147483647.

Remarque : Cela ne s'applique qu'aux règles agrégées NWDB. Si la valeur par défaut est spécifiée, toutes les sessions correspondantes seront numérisées et la valeur exacte sera retournée. Un seuil de session supérieur permet des comptages précis pour une valeur. Toutefois, cela entraîne la plus longue durée d'exécution de règle. Par exemple, imaginez que vous définissez le seuil de session 1000 pour ip.src. Si 5 000 sessions correspondent à une valeur ip.src particulière qui est présente dans plus de 1 000 sessions, NWDB arrêtera l'analyse après 1 000 sessions et retournera la valeur agrégée extrapolée. Cela optimise le temps d'exécution de la requête. Si la valeur est présente dans moins de 1 000 sessions, la valeur réelle sera retournée.

13. Dans le champ **Limite**, saisissez la limite à appliquer à la requête lors de l'extraction des données à partir de la base de données. Si l'ensemble des résultats est trié par nombre d'événements, nombre de paquets ou taille de session, la limite représentera les premières (ou dernières) valeurs N à renvoyer. Si l'ensemble de résultats n'est pas trié, les premières valeurs N sont renvoyées.
14. Cliquez sur **Enregistrer**.

Remarque : Contrairement aux méta analysées, les logs bruts sont extraits des Decoders. Si les logs bruts et les méta analysés sont interrogés à l'aide d'une seule règle, à cause des différentes périodes de rétention, les méta analysés pourraient être disponibles et les logs bruts manquants dans la même session. Donc, le résultat aura analysé les métavaleurs et la valeur brute vide pour ces sessions. Par exemple, pour la règle « Select **ip.src**, **ip.dst**, **service**, **username**, **raw** », le méta analysé peut être renseigné et le méta **raw** peut rester vide pour quelques sessions.

Créer une règle avec une source de données Warehouse

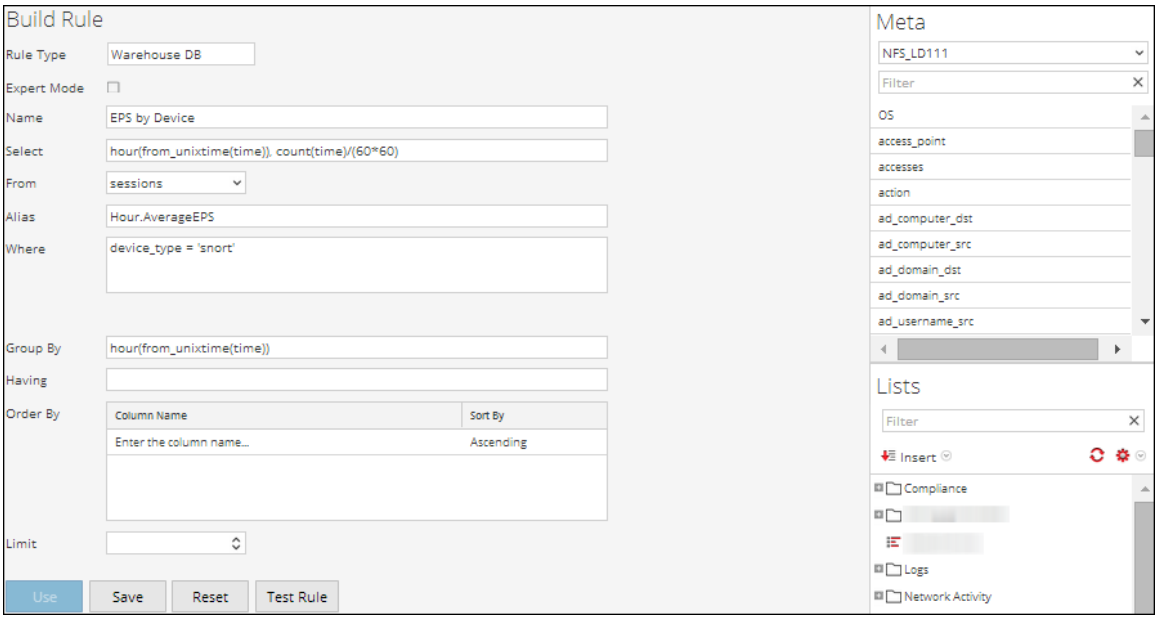
Vous pouvez créer une règle afin d'extraire des données ou des événements à partir d'une source de données Warehouse. Vous pouvez définir les règles en fonction de deux modes :

- Mode par défaut
- Mode Expert

Mode par défaut

Dans ce mode, vous pouvez créer des règles contenant des instructions SQL simples comme des requêtes HIVE contenant des clauses Select, Where, Group By et Having. Par défaut, vous pouvez créer des règles pour les sessions de requête ou les logs bruts. Pour plus d'informations sur la syntaxe des requêtes simples et pour obtenir des exemples, reportez-vous à la rubrique Règles de syntaxe simples liées à une base de données Warehouse.

La figure suivante illustre la vue **Élaborer une règle** qui s'affiche lorsque vous sélectionnez **Base de données Warehouse** pour **Type de règle** (mode expert non sélectionné).

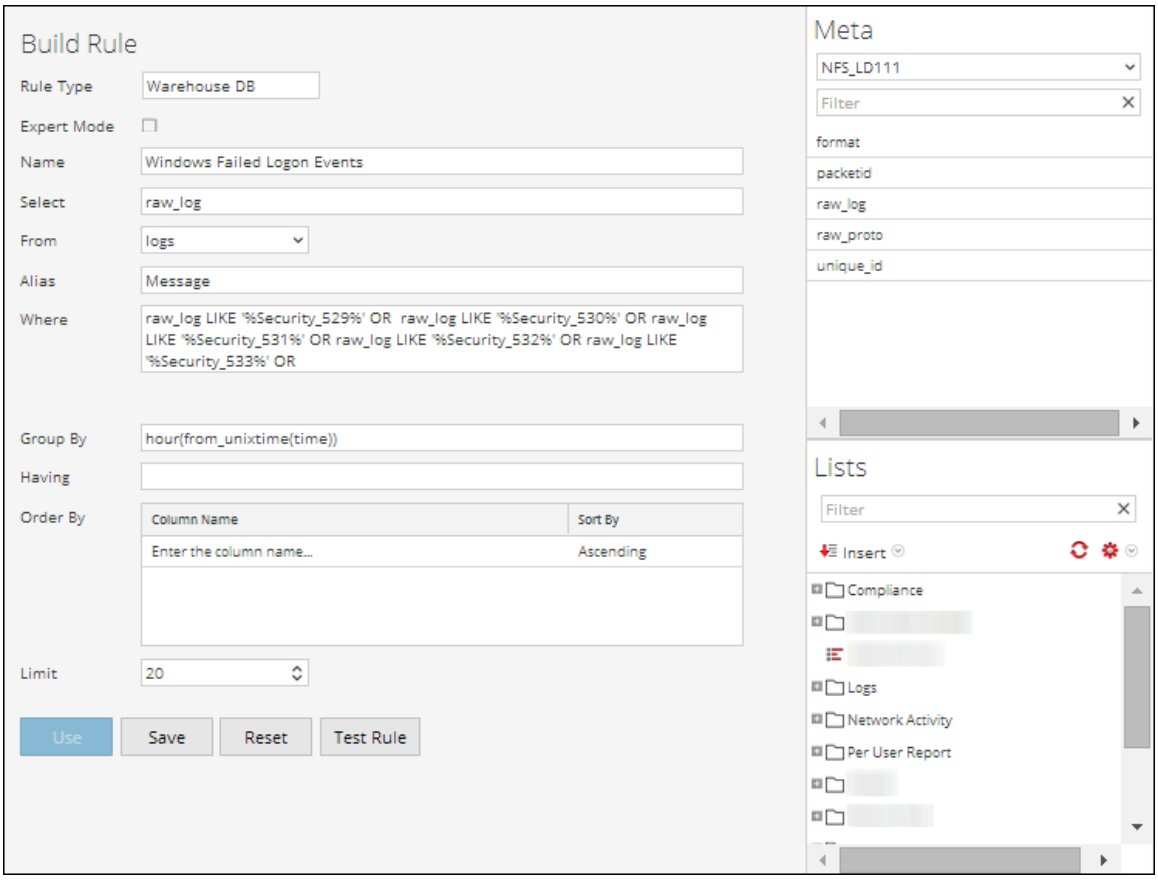


Interrogation des logs bruts

Le format de log brut est utilisé dans les clauses select ou where pour interroger les logs bruts.

Remarque : La période que vous pouvez définir dans votre requête est d'une journée (24 heures). Si vous avez spécifié une période inférieure à un jour dans votre requête, les résultats contiennent les données d'au moins un jour (24 heures).

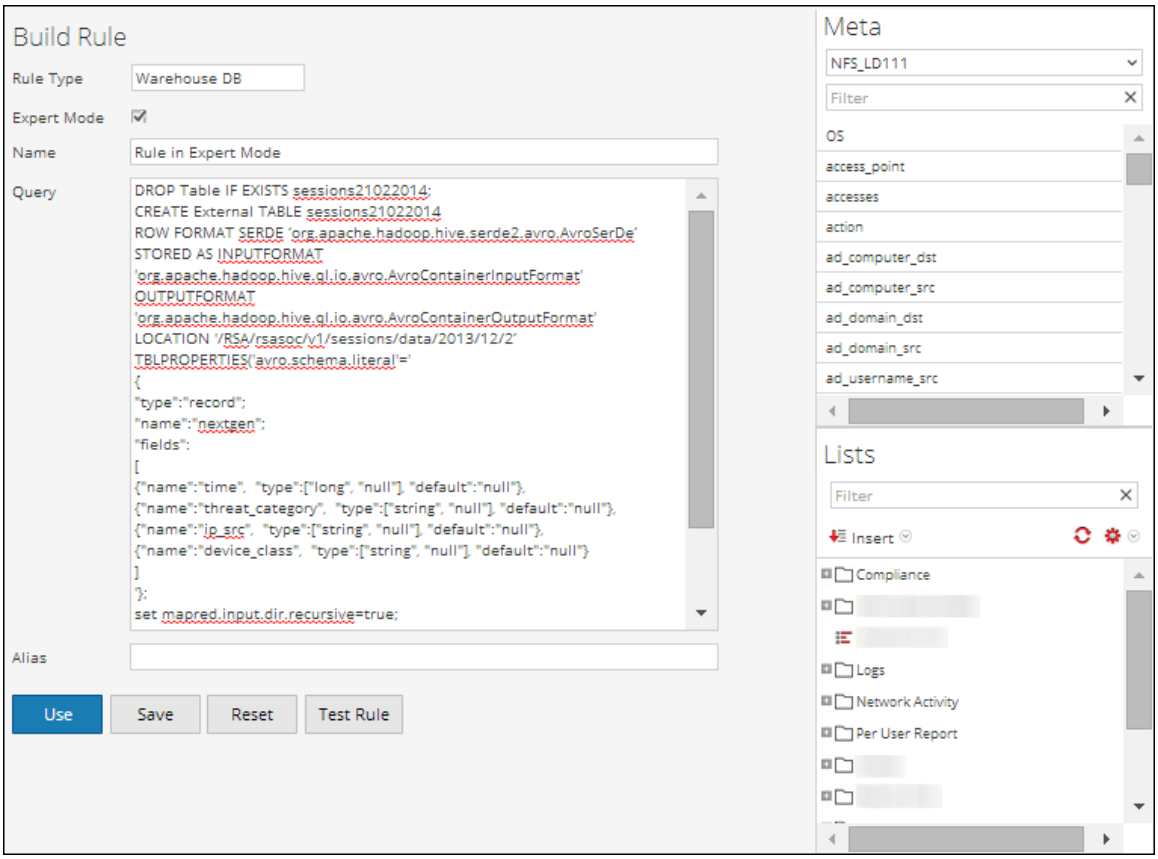
La figure suivante illustre la vue **Élaborer une règle** qui s'affiche lorsque vous sélectionnez **Base de données Warehouse** pour **Type de règle** et que vous créez une règle pour interroger les logs bruts.



Mode Expert

Des règles avancées sont définies à l'aide de requêtes HIVE complexes, via les clauses DROP, CREATE, etc. Contrairement aux règles simples, nous insérons toujours les résultats dans une table. Pour plus d'informations sur le langage de requête avancée HIVE, consultez le *manuel du langage HIVE*.

La figure suivante illustre la vue Élaborer **une règle** qui s'affiche lorsque vous sélectionnez **Base de données Warehouse** pour **Type de règle** (mode expert sélectionné).



Si vous souhaitez générer un rapport pour une période spécifique, vous devez définir manuellement la période dans la requête à l'aide des deux variables suivantes :

- ${report_starttime} - Date de début de la période en secondes.
- ${report_endtime} - Date de fin de la période en secondes.

Par exemple, **SELECT col1, col2 FROM custom_table WHERE timecol >= ${report_starttime} AND timecol <= ${report_endtime};**

Remarque : Par défaut, Reporting Engine traite `${keyword}` comme une variable. Si vous souhaitez spécifier des variables HIVE, mentionnez la syntaxe complète d'une variable. Par exemple, `${hiveconf:hive.exec.scratchdir}`.

Conditions préalables

Veillez à comprendre la manière dont les clés méta personnalisées sont créées à l'aide des feeds personnalisés. Pour plus d'informations, reportez-vous à la rubrique « Créer des clés méta personnalisées à l'aide d'un feed personnalisé » dans le *Guide de configuration de l'hôte et des services*.

Pour créer une règle afin d'extraire des données ou événements à partir d'une source de données Warehouse, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Dans la barre d'outils Règle, cliquez sur + > **Base de données Warehouse.**

   La vue Élaborer une règle s'affiche.

3. Dans le champ **Type de règle**, le paramètre **Base de données Warehouse** est sélectionné par défaut.

   Si vous définissez la règle en mode Par défaut, effectuez les opérations suivantes :

   a. Dans le champ **Nom**, saisissez un nom utilisé pour identifier ou libeller la règle dans les alertes et rapports.

   b. Dans le champ **Sélection**, saisissez un méta ou sélectionnez-en un dans la liste des types de métadonnées disponibles fournis dans le panneau Méta. Pour plus d'informations, consultez Panneau Méta dans la vue Vue Élaborer une règle.

   c. Dans le menu déroulant **De**, sélectionnez l'une des options suivantes :

      - Session
      - Logs

   d. Dans le champ **Alias**, saisissez le nom d'alias des colonnes utilisées dans la clause Select.

   e. Dans le champ **Où**, saisissez un méta ou sélectionnez-en un dans la liste des types de métadonnées disponibles fournis dans le panneau Méta. La clause Where fournit les critères de requête de base pour la règle.

   f. Dans le champ **Regrouper par**, saisissez le méta sélectionné dans la clause Select, de sorte que l'ensemble de résultats soit regroupé d'après le méta.

   g. Dans le champ **Having**, saisissez les critères permettant de filtrer l'ensemble de résultats des requêtes agrégées.

   h. Dans le champ **Réorganiser par**, procédez comme suit :

      1. Dans la colonne **Nom de la colonne**, saisissez le nom des colonnes selon lesquelles vous souhaitez regrouper les résultats.
      2. Dans la colonne **Trier par**, sélectionnez l'une des méthodes suivantes pour trier les résultats :

- Ordre croissant
- Ordre décroissant

i. Dans le champ **Limite**, saisissez la limite à appliquer à la requête lors de l'extraction des données à partir de la base de données. Si l'ensemble de résultats est trié par nombre de sessions, nombre de paquets ou taille de session, la limite représente les premières (ou dernières) valeurs N à renvoyer. Si l'ensemble de résultats n'est pas trié, les premières valeurs N sont renvoyées.

j. Cliquez sur **Enregistrer**.

4. Si vous définissez la règle en mode Expert, activez la case à cocher **Mode Expert** et effectuez les opérations suivantes :

   a. Dans le champ **Nom**, saisissez un nom utilisé pour identifier ou libeller la règle dans les alertes et rapports.

   b. Dans le champ **Requête**, saisissez l'instruction de requête Hive pour interroger la source de données.

   c. Dans le champ **Alias**, saisissez le nom d'alias des colonnes utilisées dans la clause Select.

   d. Cliquez sur **Enregistrer**.

Créer une règle avec une source de données Respond

Vous pouvez créer une règle afin d'extraire des incidents ou des alertes à partir d'une source de données Respond.

Conditions préalables

Vérifiez que :

- Le service Reporting Engine est en cours d'exécution.
- Le service Incident Management est en cours d'exécution. Pour plus d'informations, consultez la rubrique « Configurer une base de données pour le service Respond Server » dans le *Guide de configuration de NetWitness Respond*.
- (Facultatif) Assurez-vous que le service Event Stream Analysis est en cours d'exécution. Pour plus d'informations, reportez-vous à la rubrique « Étape 2. Configurer les paramètres avancés d'un service ESA » dans le *Guide de Configuration ESA*.

- (Facultatif) Assurez-vous que le service Malware Analysis est en cours d'exécution. Pour plus d'informations, consultez la rubrique « (Facultatif) Configurer l'auditing sur l'hôte Malware Analysis » dans le *Guide de configuration de Malware*.

Remarque : Vous devez configurer l'un des services (Event Stream Analysis, Reporting Engine, Malware Analysis ou Endpoint) en fonction de vos besoins et du type d'alertes ou d'incidents que vous souhaitez générer.

Pour créer une règle afin d'extraire des données ou événements à partir d'une source de données Respond, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

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

   L'onglet de la vue Élaborer une règle s'affiche.

3. Dans le champ **Type de règle**, Respond est sélectionné par défaut.

4. Dans le champ **Nom**, saisissez un nom utilisé pour identifier ou libeller la règle dans les alertes et rapports d'incidents.

5. Le champ **Résumé** détermine le type de résumé ou d'agrégation correspondant à la règle. En fonction du type de règle à définir, vous devez sélectionner l'une des options suivantes :

   - Pour définir une règle **Sans agrégation** sans regroupement, sélectionnez **Aucun**
   - Pour définir une règle **Agrégation** avec des métavaleurs et des agrégats personnalisés, sélectionnez **Personnalisé**

     Choisir « Personnalisé » dans le champ **Résumé** vous permet de définir la fonction d'agrégation de votre choix dans la clause *Select* en fonction du type de rapport que vous avez sélectionné.

     Pour plus d'informations détaillées sur les règles agrégées et non agrégées, reportez-vous à la rubrique Syntaxe de la règle .

6. Dans le champ **De**, en fonction du type de rapport de sortie à afficher, vous devez sélectionner l'une des options suivantes :

   - Alerte
   - Incident

7. Dans le champ **Sélectionner**, saisissez une métadonnée ou sélectionnez-en une dans la liste des types de métadonnées disponibles fournis dans la bibliothèque de métadonnées. Pour plus d'informations, reportez-vous à la section «Panneau Métadonnées» dans la Vue Élaborer une règle. Il est impossible de l'utiliser dans le champ **Où**. Plusieurs fonctions d'agrégation sont

prises en charge pour la règle d'agrégation personnalisée dans le champ **Select**.

Par exemple, les fonctions d'agrégation prises en charge pour l'alerte sont les suivantes :

- alert_host_summary
- alert.name
- alert.numEvents
- alert.severity
- alert.source
- alert.timestamp
- incidentCreated
- incidentId
- receivedTime

Par exemple, les fonctions d'agrégation prises en charge pour l'incident sont les suivantes :

- categories
- created
- priority
- riskScore
- sealed
- status

Pour plus d'informations détaillées sur les règles agrégées et non agrégées, reportez-vous à la rubrique Syntaxe de la règle .

8. Dans le champ **Alias**, saisissez le nom d'alias des colonnes utilisées dans la clause Select.
9. Dans le champ **Where**, saisissez un méta ou sélectionnez un méta dans la liste des types de méta disponibles, puis utilisez les opérateurs permettant de construire la clause Where pour les critères de requête de base.
10. Le champ **Regrouper par** est un champ en lecture seule qui fournit les méta qui sont définis dans la clause Select. Pour une fonction Sans agrégation, ce champ n'est pas visible. Un maximum de six méta est pris en charge dans le champ **Group By**.
11. Dans le champ **Réorganiser par**, procédez comme suit :
    a. Dans la colonne **Nom de la colonne**, saisissez le nom des colonnes dont vous souhaitez trier les résultats. Par défaut, la valeur est vide.
    b. Dans la colonne **Trier par**, sélectionnez l'une des méthodes suivantes pour trier les

résultats :

- Ordre croissant
- Ordre décroissant

12. Dans le champ **Limite**, saisissez la limite à appliquer à la requête lors de l'extraction des données à partir de la base de données. Si l'ensemble de résultats est trié, la limite représente les premières (ou dernières) valeurs N à renvoyer. Si l'ensemble de résultats n'est pas trié, les premières valeurs N sont renvoyées.
13. Cliquez sur **Enregistrer**.

Déployer une règle

Dans RSA NetWitness Suite, vous pouvez déployer les règles sélectionnées sur le service (par exemple, Reporting Engine), à l'aide de l'Assistant de déploiement.

Conditions préalables

Vérifiez que :

- Les services sur lesquels vous déployez une règle sont en cours d'exécution.
- Services Live est configuré.

Pour déployer une règle, procédez comme suit :

1. Sélectionnez **CONFIGURER > CONTENU LIVE**.
2. Dans le panneau **Critères de recherche**, recherchez des ressources Live (par exemple, recherchez le type de ressource **Règle d'application**).
3. Dans le panneau **Ressources correspondantes**, sélectionnez **Afficher les résultats > Grille**.
4. Cochez la case à gauche ou les ressources que vous souhaitez déployer.
5. Dans la barre d'outils **Ressources correspondantes**, cliquez sur 

.
6. Cliquez sur **Suivant**.
7. Sélectionnez le service sur lequel vous déployez une règle (par exemple, Reporting Engine), puis cliquez sur **Suivant**.
8. Cliquez sur **Déployer**.
   La règle est déployée avec succès.

Utiliser les alias de métadonnées pour Reporting

Lorsque vous faites référence à des métadonnées dans les rapports et les graphiques, vous ne pouvez afficher que les alias des noms des métadonnées. Ces alias les rendent plus compréhensibles pour une audience plus large.

Vous ne pouvez utiliser que les alias prédéfinis pour les métadonnées. En effet, vous ne pouvez pas modifier ces valeurs.

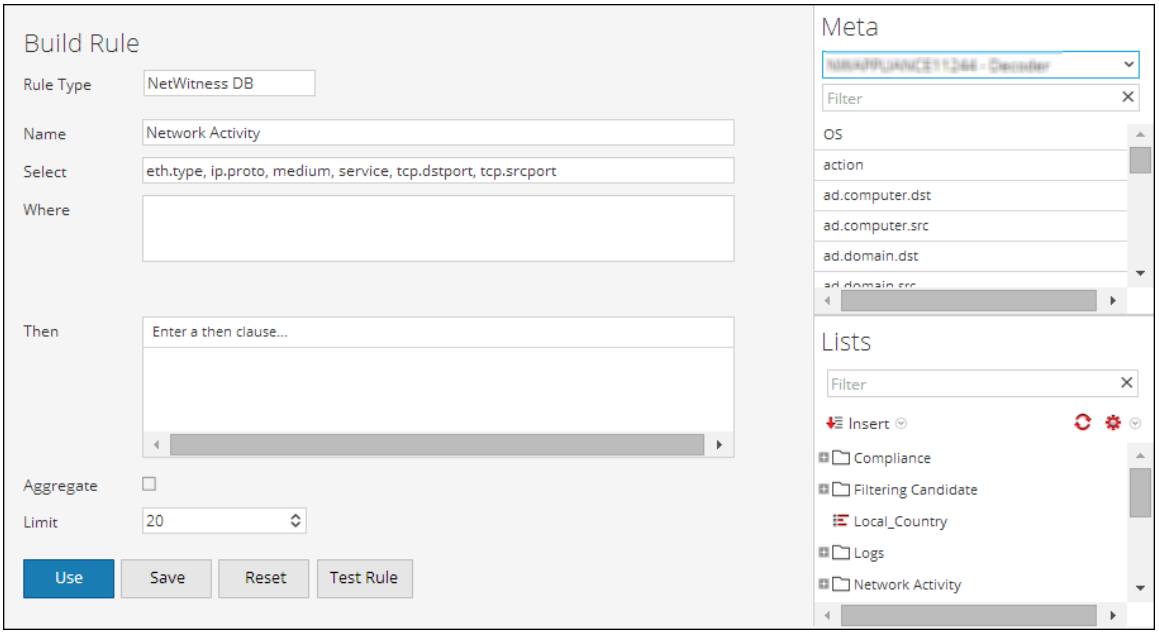
Vous ne pouvez pas fournir de valeurs d'alias pour les métadonnées dans la clause WHERE, car NetWitness Suite utilise la clause WHERE pour extraire les données de la source de données (par exemple dans Concentrator). Par ailleurs, les sources de données ne prennent pas en charge les alias. En d'autres termes, vous ne pouvez pas fournir la valeur d'alias **HTTP** pour le port HTTP 80.

Remarque : * Vous ne pouvez pas créer d'alias pour d'autres métadonnées que celles ayant déjà des alias attribués par Reporting Engine. En outre, vous ne pouvez pas modifier le format des alias.
* Les alias ne sont pas pris en charge pour les alertes et les rapports CSV.

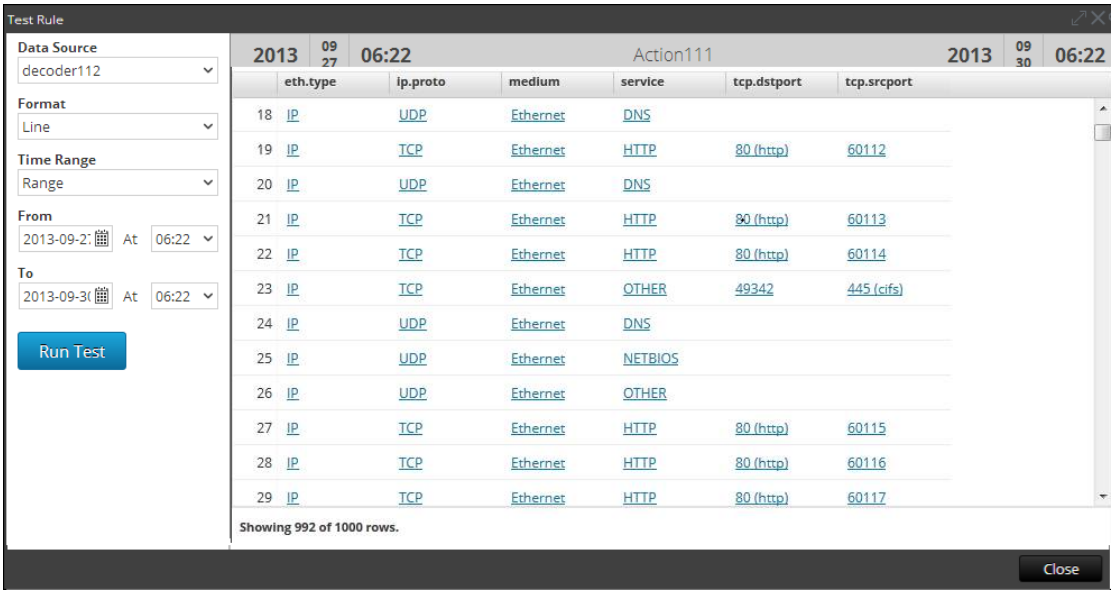
Pour utiliser un alias dans une règle, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau Liste de règles, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle, puis cliquez sur dans la barre d'outils Règles.
   - Cliquez sur > **Modifier**.
3. Spécifiez les métadonnées avec alias dans le champ **Select**.

L'exemple suivant spécifie les métadonnées **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport** et **tcp.srcport** dans le champ Select.



4. Cliquez sur **Tester la règle**.
   L'exemple suivant affiche les résultats des colonnes d'alias **eth.type**, **ip.proto**, **medium**, **service**, **tcp.dstport** et **tcp.srcport** qui ont été spécifiées dans le champ **Select** de la règle.



Définitions d'alias fournis par RSA

Les fichiers d'alias de cette section ne sont que des exemples. Ils sont basés sur les définitions d'alias actuelles de Reporting Engine. NetWitness Suite ne peut pas modifier ces définitions dans Reporting Engine en fonction des modifications apportées au fichier xml de Concentrator. Les modifications apportées au fichier xml de Concentrator ne sont pas répercutées dans Reporting Engine.

Les différentes métadonnées sont expliquées en détail dans chacun des **alias de métadonnées**.

eth.type

```
ALIAS_FORMAT=$alias
 0=802.3
 257=Experimental
 512=Xerox PUP
 513=Xerox PUP
 1024=Nixdorf
 1536=Xerox NS IDP
 1537=XNS Address Translation (3Mb only)
 2048=IP
 2049=X.75 Internet
 2050=NBS Internet
 2051=ECMA Internet
 2052=CHAOSnet
 2053=X.25 Level 3
 2054=ARP
 2055=XNS Compatibility
 2076=Symbolics Private
 2184=Xyplex
 2304=Ungermann-Bass network debugger
 2560=Xerox IEEE802.3 PUP
 2561=Xerox IEEE802.3 PUP Address Translation
 2989=Banyan Systems
 2991=Banyon VINES Echo
 4096=Berkeley Trailer negotiation
 4097=Berkeley Trailer encapsulation for IP
 4660=DCA - Multicast
 5632=VALID system protocol
 6537=Artificial Horizons
 6549=Datapoint Corporation (RCL lan protocol)
 15360=3Com NBP virtual circuit datagram (like XNS SPP) not registered
 15361=3Com NBP System control datagram not registered
 15362=3Com NBP Connect request (virtual cct) not registered
 15363=3Com NBP Connect repsonse not registered
 15364=3Com NBP Connect complete not registered
 15365=3Com NBP Close request (virtual cct) not registered
 15366=3Com NBP Close response not registered
 15367=3Com NBP Datagram (like XNS IDP) not registered
 15368=3Com NBP Datagram broadcast not registered
 15369=3Com NBP Claim NetBIOS name not registered
 15370=3Com NBP Delete Netbios name not registered
```

```
15371=3Com NBP Remote adaptor status request not registered
15372=3Com NBP Remote adaptor response not registered
15373=3Com NBP Reset not registered
16972=Information Modes Little Big LAN diagnostic
17185=THD - Diddle
19522=Information Modes Little Big LAN
21000=BBN Simnet Private
24576=DEC unassigned
24577=DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
24578=DEC Maintenance Operation Protocol (MOP) Remote Console
24579=DECNET Phase IV
24580=DEC Local Area Transport (LAT)
24581=DEC diagnostic protocol (at interface initialization?)
24582=DEC customer protocol
24583=DEC Local Area VAX Cluster (LAVC)
24584=DEC AMBER
24585=DEC MUMPS
24592=3Com Corporation
28672=Ungermann-Bass download
28673=Ungermann-Bass NIUs
28674=Ungermann-Bass diagnostic/loopback
28675=Ungermann-Bass ??? (NMC to/from UB Bridge)
28677=Ungermann-Bass Bridge Spanning Tree
28679=OS/9 Microware
28681=OS/9 Net?
28704=LRT (England) (now Sintrom)
28720=Racal-Interlan
28721=Prime NTS (Network Terminal Service)
28724=Cabletron
32771=Cronus VLN
32772=Cronus Direct
32773=HP Probe protocol
32774=Nestar
32776=AT&amp;amp;T/Stanford Univ.
32784=Excelan
32787=Silicon Graphics diagnostic
32788=Silicon Graphics network games
32789=Silicon Graphics reserved
32790=Silicon Graphics XNS NameServer
32793=Apollo DOMAIN
32814=Tymshare
32815=Tigan
32821=Reverse Address Resolution Protocol (RARP)
32822=Aeonic Systems
32823=IPX (Novell Netware?)
32824=DEC LanBridge Management
32825=DEC DSM/DDP
32826=DEC Argonaut Console
```

```
32827=DEC VAXELN
32828=DEC DNS Naming Service
32829=DEC Ethernet CSMA/CD Encryption Protocol
32830=DEC Distributed Time Service
32831=DEC LAN Traffic Monitor Protocol
32832=DEC PATHWORKS DECnet NETBIOS Emulation
32833=DEC Local Area System Transport
32834=DEC unassigned
32836=Planning Research Corp.
32838=AT&amp;amp;T
32839=AT&amp;amp;T
32840=DEC Availability Manager for Distributed Systems DECamds
32841=ExperData
32859=VMTP
32860=Stanford V Kernel
32861=Evans &amp;amp; Sutherland
32864=Little Machines
32866=Counterpoint Computers
32869=University of Mass. at Amherst
32870=University of Mass. at Amherst
32871=Veeco Integrated Automation
32872=General Dynamics
32873=AT&amp;amp;T
32874=Autophon
32876=ComDesign
32877=Compugraphic Corporation
32878=Landmark Graphics Corporation
32890=Matra
32891=Dansk Data Elektronik
32892=Merit Internodal
32893=Vitalink Communications
32896=Vitalink TransLAN III Management
32897=Counterpoint Computers
32904=Xyplex
32923=EtherTalk - AppleTalk over Ethernet
32924=Datability
32927=Spider Systems Ltd.
32931=Nixdorf Computers
32932=Siemens Gammasonics Inc.
32960=DCA Data Exchange Cluster
32966=Pacer Software
32967=Applitek Corporation
32968=Intergraph Corporation
32973=Harris Corporation
32975=Taylor Instrument
32979=Rosemount Corporation
32981=IBM SNA Services over Ethernet
32989=Varian Associates
```

```
32990=TRFS (Integrated Solutions Transparent Remote File System)
32992=Allen-Bradley
32996=Datability
33010=Retix
33011=AppleTalk Address Resolution Protocol (AARP)
33012=Kinetics
33015=Apollo Computer
33023=Wellfleet Communications
33026=Wellfleet BOFL
33027=Wellfleet Communications
33031=Symbolics Private
33067=Talaris
33072=Waterloo Microsystems Inc.
33073=VG Laboratory Systems
33079=IPX
33080=Novell Inc
33081=KTI
33087=M/MUMPS data sharing
33093=Vrije Universiteit (NL)
33094=Vrije Universiteit (NL)
33095=Vrije Universiteit (NL)
33100=SNMP
33103=Technically Elite Concepts
33169=PowerLAN
33149=XTP
33238=Artisoft Lantastic
33239=Artisoft Lantastic
33283=QNX Software Systems Ltd.
33680=Accton Technologies (unregistered)
34091=Talaris multicast
34178=Kalpana
34525=IPv6
34617=Control Technology Inc.
34618=Control Technology Inc.
34619=Control Technology Inc.
34620=Control Technology Inc.
34848=Hitachi Cable (Optoelectronic Systems Laboratory)
34902=Axis Communications AB
34952=HP LanProbe test?
36864=Loopback (Configuration Test Protocol)
36865=3Com XNS Systems Management
36866=3Com TCP/IP Systems Management
36867=3Com loopback detection
43690=DECNET
64245=Sonix Arpeggio
65280=BBN VITAL-LanBridge cache wakeups
34915=PPPoe
34916=PPPoe
```

```
 2056=Frame Relay ARP
 16962=IEEE bridge spanning protocol
 25944=Bridged Ethernet/802.3 packet
 65278=ISO CLNP/ISO ES-IS DSAP/SSAP
```

ip.proto

```
ALIAS_FORMAT=$alias
 0=HOPOPT
 1=ICMP
 2=IGMP
 3=GGP
 4=IP
 5=ST
 6=TCP
 7=CBT
 8=EGP
 9=IGP
 10=BBN-RCC-M
 11=NVP-II
 12=PUP
 13=ARGUS
 14=EMCON
 15=XNET
 16=CHAOS
 17=UDP
 18=MUX
 19=DCN-MEAS
 20=HMP
 21=PRM
 22=XNS-IDP
 23=TRUNK-1
 24=TRUNK-2
 25=LEAF-1
 26=LEAF-2
 27=RDP
 28=IRTP
 29=ISO-TP4
 30=NETBLT
 31=MFE-NSP
 32=MERIT-INP
 33=SEP
 34=3PC
 35=IDPR
 36=XTP
 37=DDP
 38=IDPR-CMTP
 39=TP++
 40=IL
```

```
41=IPv6
42=SDRP
43=IPv6-Rout
44=IPv6-Frag
45=IDRP
46=RSVP
47=GRE
48=MHRP
49=BNA
50=ESP
51=AH
52=I-NLSP
53=SWIPE
54=NARP
55=MOBILE
56=TLSP
57=SKIP
58=IPv6-ICMP
59=IPv6-NoNx
60=IPv6-Opts
61=AnyHost
62=CFTP
63=AnyNetwork
64=SAT-EXPAK
65=KRYPTOLAN
66=RVD
67=IPPC
68=AnyFile
69=SAT-MON
70=VISA
71=IPCV
72=CPNX
73=CPHB
74=WSN
75=PVP
76=BR-SAT-MO
77=SUN-ND
78=WB-MON
79=WB-EXPAK
80=ISO-IP
81=VMTP
82=SECURE-VM
83=VINES
84=TTP
85=NSFNET-IG
86=DGP
87=TCF
88=EIGRP
```

```
89=OSPFIGP
90=Sprite-RP
91=LARP
92=MTP
93=AX.25
94=IPIP
95=MICP
96=SCC-SP
97=ETHERIP
98=ENCAP
99=AnyPrivate
100=GMTP
101=IFMP
102=PNNI
103=PIM
104=ARIS
105=SCPS
106=QNX
107=A/N
108=IPComp
109=SNP
110=Compaq-Pe
111=IPX-in-IP
112=VRRP
113=PGM
114=AnyHop
115=L2TP
116=DDX
117=IATP
118=STP
119=SRP
120=UTI
121=SMP
122=SM
123=PTP
124=ISIS
125=FIRE
126=CRTP
127=CRUDP
128=SSCOPMCE
129=IPLT
130=SPS
131=PIPE Pr
132=SCTP St
133=FC Fi
134=RSVP-E2E-
255=Reserved
```

medium

```
ALIAS_FORMAT=$alias
 1=Ethernet
 2=Tokenring
 3=FDDI
 4=HDLC
 5=NetWitness
 6=802.11
 7=802.11 Radio
 8=802.11 AVS
 9=802.11 PPI
 10=802.11 PRISM
 11=802.11 Management
 12=802.11 Control
 13=DLT Raw
 32=Logs
```

service

```
ALIAS_FORMAT=$alias
 0=OTHER
 20=FTPD
 21=FTP
 22=SSH
 23=TELNET
 25=SMTP
 53=DNS
 67=DHCP
 69=TFTP
 80=HTTP
 110=POP3
 111=SUNRPC
 119=NNTP
 123=NTP
 135=RPC
 137=NETBIOS
 139=SMB
 143=IMAP
 161=SNMP
 179=BGP
 443=SSL
 502=MODBUS
 520=RIP
 1024=EXCHANGE
 1080=SOCKS
 1122=MSN IM
 1344=ICAP
 1352=NOTES
 1433=TDS
```

```
 1521=TNS
 1533=SAMETIME
 1719=H.323
 1720=RTP
 2000=SKINNY
 2040=SOULSEEK
 2049=NFS
 3270=TN3270
 3389=RDP
 3700=DB2
 5050=YAHOO IM
 5060=SIP
 5190=AOL IM
 5222=Google Talk
 5900=VNC
 6346=GNUTELLA
 6667=IRC
 6801=Net2Phone
 6881=BITTORRENT
 8000=QQ
 8002=YCHAT
 8019=WEBMAIL
 8082=FIX
 20000=DNP3
 1000000=KERNEL
 1000001=USER
 1000003=SYSTEM
 1000004=AUTH
 1000005=LOGGER
 1000006=LPD
 1000008=UUCP
 1000009=SCHEDULE
 1000010=SECURITY
 1000013=AUDIT
 1000014=ALERT
 1000015=CLOCK
```

tcp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
```

```
25=smtp
37=time
42=nameserver
43=nicname
53=domain
70=gopher
79=finger
80=http
88=kerberos
101=hostname
102=iso-tsap
107=rtelnet
109=pop2
110=pop3
111=sunrpc
113=auth
117=uucp-path
119=nntp
135=epmap
137=netbios-ns
139=netbios-ssn
143=imap
158=pcmail-srv
170=print-srv
179=bgp
194=irc
389=ldap
443=https
445=cifs
464=kpasswd
512=exec
513=login
514=cmd
515=printer
520=efs
526=tempo
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
```

```
 1433=ms-sql-s
 1434=ms-sql-m
 1512=wins
 1524=ingreslock
 1723=pptp
 2053=knetd
 1122=msn im
 1352=notes
 1521=tns
 1533=sametime
 1718=h323
 1720=rtp
 1863=msn im
 2049=nfs
 3389=rdp
 5050=yahoo im
 5060=sip
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

tcp.srcport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 20=ftp-data
 21=ftp
 22=ssh
 23=telnet
 25=smtp
 37=time
 42=nameserver
 43=nicname
 53=domain
 70=gopher
 79=finger
 80=http
 88=kerberos
 101=hostname
 102=iso-tsap
 107=rtelnet
 109=pop2
```

```
110=pop3
111=sunrpc
113=auth
117=uucp-path
119=nntp
135=epmap
137=netbios-ns
139=netbios-ssn
143=imap
158=pcmail-srv
170=print-srv
179=bgp
194=irc
389=ldap
443=https
445=cifs
464=kpasswd
512=exec
513=login
514=cmd
515=printer
520=efs
526=tempo
530=courier
531=conference
532=netnews
540=uucp
543=klogin
544=kshell
556=remotefs
636=ldaps
749=kerberos-adm
993=imaps
995=pop3s
1109=kpop
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1524=ingreslock
1723=pptp
2053=knetd
1122=msn im
1352=notes
1521=tns
1533=sametime
1718=h323
1720=rtp
1863=msn im
```

```
 2049=nfs
 3389=rdp
 5050=yahoo im
 5060=sip
 5190=aim
 6346=gnuetella
 6667=irc
 9001=tor
 9030=tor
 9535=man
```

udp.dstport

```
ALIAS_FORMAT=$value ($alias)
 7=echo
 9=discard
 13=daytime
 17=qotd
 19=chargen
 37=time
 39=rlp
 42=nameserver
 53=domain
 67=bootps
 68=bootpc
 69=tftp
 88=kerberos
 111=sunrpc
 123=ntp
 135=epmap
 137=netbios-ns
 138=netbios-dgm
 161=snmp
 162=snmptrap
 213=ipx
 443=https
 445=cifs
 464=kpasswd
 500=isakmp
 512=biff
 513=who
 514=syslog
 517=talk
 518=ntalk
 525=timed
 533=netwall
 550=new-rwho
 560=rmonitor
 561=monitor
```

```
749=kerberos-adm
1167=phone
1433=ms-sql-s
1434=ms-sql-m
1512=wins
1701=l2tp
1812=radiusauth
1813=radacct
2049=nfsd
2504=nlbs
```

Tester une règle

Vous pouvez tester une règle en fonction de la période et de la source de données sélectionnée.

Pour tester une règle, effectuez les étapes suivantes :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau Liste de règles, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle, puis cliquez sur  dans la barre d'outils Règles.
   - Cliquez sur  > **Modifier**.
     L'onglet de la vue Élaborer une règle s'affiche.

3. Cliquez sur **Tester la règle**.
   La vue Tester la règle s'affiche.

> **Remarque :** Lorsque vous cliquez sur **Tester la règle**, celle-ci n'est pas enregistrée. Vous devez cliquer sur **Enregistrer** dans la vue Élaborer une règle pour l'enregistrer.

4. Sélectionnez une option dans la liste déroulante **Source de données**.
   Vous devez sélectionner la source de données adaptée à la règle définie.
5. Dans la liste déroulante **Format**, sélectionnez le format dans lequel vous souhaitez afficher le résultat.
6. Dans la liste déroulante **Période**, sélectionnez l'une des options suivantes.
   - **Passé** - Pour spécifier le nombre d'années, jours, semaines, mois ou heures.
   - **Plage** - Pour spécifier une plage de données et une période.

   > **Remarque :** Dans l'interface utilisateur, la date ou l'heure qui s'affiche dépend du profil de fuseau horaire sélectionné par l'utilisateur.
7. **Axe X** et **Axe Y** permettent de spécifier les métas à tracer dans les tableaux.
   Dans **Axe X**, le méta de la règle « Regrouper par » s'affiche. Dans **Axe Y**, les fonctions agrégées utilisées dans la règle s'affichent.

> **Remarque :** Sommes, Nombre, Countdistinct et Moyenne sont les fonctions agrégées prises en charge pour la règle. Par défaut, pour les règles personnalisées avec plusieurs « Regrouper par », vous pouvez sélectionner uniquement les premiers métas dans **Axe X**.

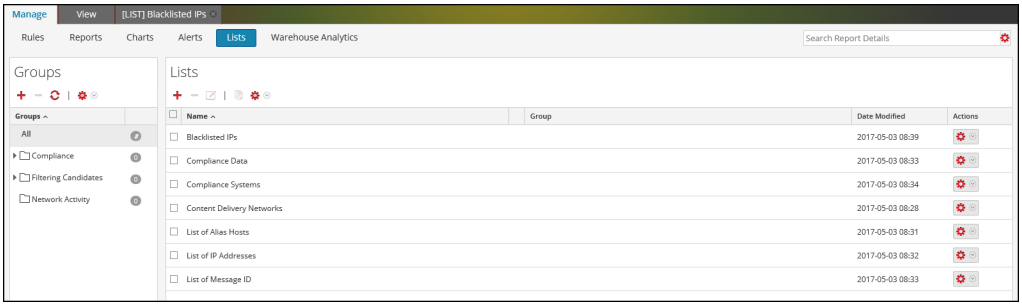
8. Cliquez sur **Exécuter le test** pour exécuter la règle.
   Les données de la règle (cas échéant) de la période sélectionnée s'affichent.

Créer des listes ou un groupe de listes

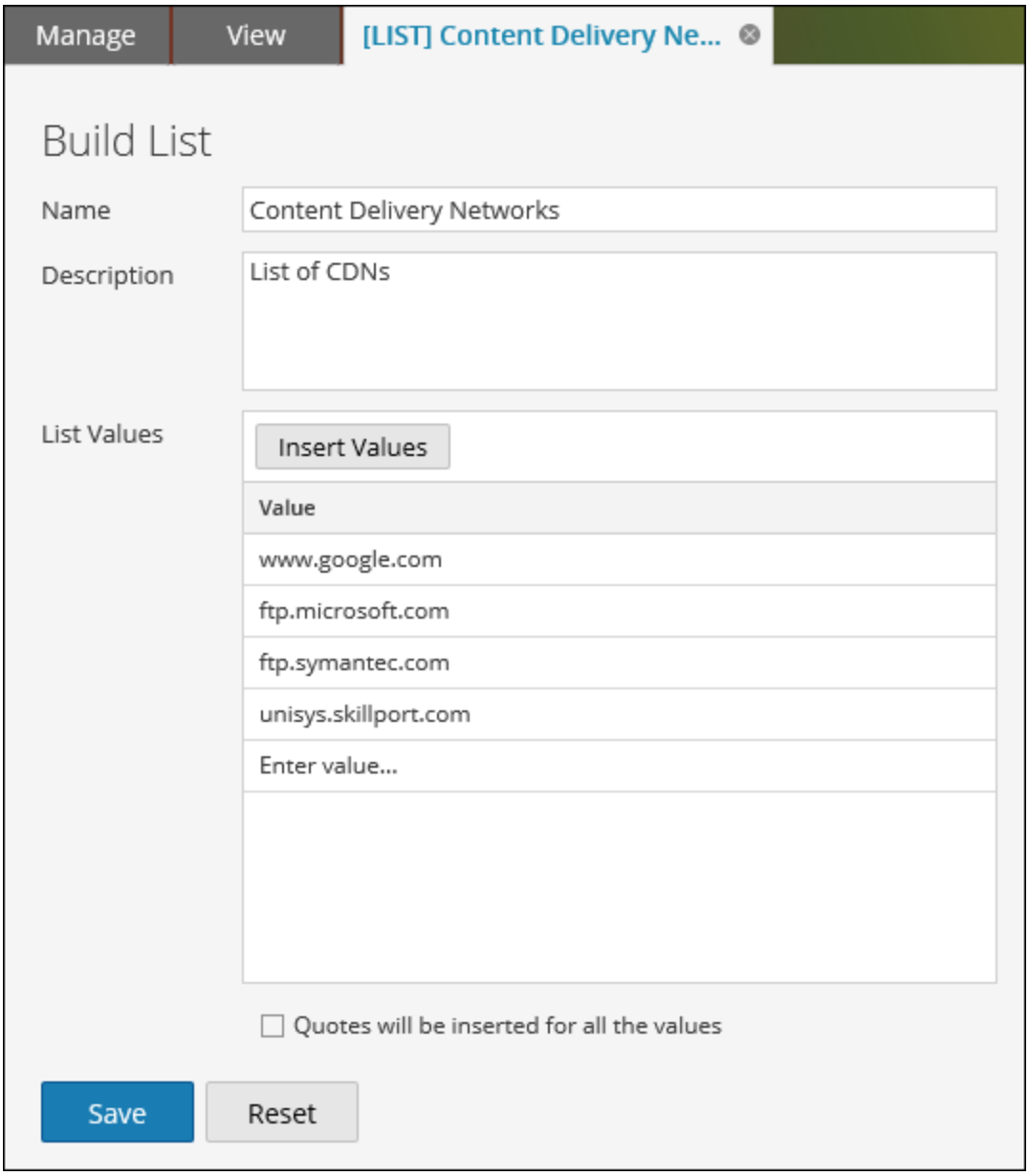
Pour créer une liste, procédez comme suit :

Les listes peuvent être ajoutées à un groupe ou au dossier racine.

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans la barre d'outils **Liste**, cliquez sur +.
   L'onglet de la vue Créer la liste s'affiche.

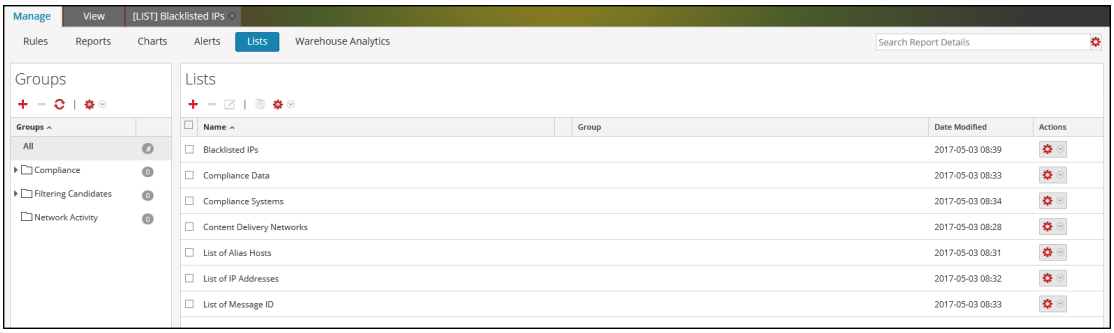


4. Dans le champ **Nom**, saisissez le nom spécifique de la liste.
5. Dans le champ **Description**, saisissez la description de la liste.
6. Dans le champ **Valeurs de la liste**, effectuez l'une des opérations suivantes :
   - Cliquez sur **Insérer** et entrez les valeurs séparées par des virgules. Vous pouvez coller une liste de valeurs à partir d'un fichier ou d'autres listes définies.
   - Dans la colonne **Valeur**, saisissez les valeurs.
7. Pour que des guillemets soient insérés directement pour les valeurs au moment de l'exécution, sélectionnez **Des guillemets seront insérés pour toutes les valeurs**.

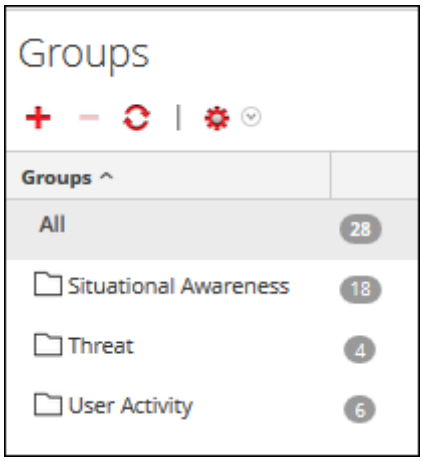
8. Cliquez sur **Enregistrer**.

Pour créer un groupe de liste, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Effectuez ce qui suit :
   - Pour créer un groupe de listes
     1. Dans le panneau Groupes de listes, cliquez sur +.
        Un nouveau groupe de listes est ajouté au groupe de listes.



     2. Saisissez le nom du groupe de listes et appuyez sur ENTRÉE.
   - Pour créer un sous-groupe de listes :
     1. Dans le panneau Groupes de listes, sélectionnez le groupe de listes auquel ajouter un sous-groupe.
     2. Cliquez sur +.

Un nouveau sous-groupe de listes est ajouté au groupe de listes.

3. Saisissez le nom du sous-groupe de listes et appuyez sur ENTRÉE.

Créer et planifier un rapport

Vous pouvez créer un rapport simple ou complexe et configurer ses propriétés d'exécution en planifiant un rapport. Un rapport peut inclure plusieurs règles, et vous pouvez planifier une période différente pour exécuter le même rapport. Par exemple, en fonction de vos besoins, vous pouvez planifier un rapport pour une exécution quotidienne, hebdomadaire ou mensuelle.

Lorsque vous exécutez un rapport, les résultats sont stockés dans Reporting Engine.

Après avoir généré un rapport, vous pouvez effectuer les opérations suivantes :

- Envoyer les rapports par e-mail à d'autres utilisateurs en configurant les actions de résultat. Vous pouvez également configurer les actions de résultat avant de générer un rapport.
- Télécharger les rapports au format de fichier PDF ou CSV.

Remarque : L'opération d'annulation n'est pas prise en charge pour les rapports de réponse.

Créer un rapport ou un groupe de rapports

Pour créer un rapport sur un groupe ou un sous-groupe, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans la barre d'outils **Rapports**, cliquez sur  .
   L'onglet Élaborer le rapport s'affiche.
4. Saisissez le nom du rapport.
5. Faites glisser le texte et les règles sur le rapport.

   Remarque : Le texte saisi est facultatif et cette option sera nécessaire seulement pour afficher les en-têtes et le contenu définis par l'utilisateur.
6. Cliquez sur **Enregistrer**.
   Un message de confirmation de l'enregistrement du rapport s'affiche.

Pour ajouter un groupe au dossier par défaut ou ajouter des sous-groupes sous un groupe de rapports, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Groupes de rapports**, cliquez sur  .
   Un groupe par défaut est ajouté dans le panneau Groupes de rapports.
4. Saisissez le nom du nouveau groupe.
5. Appuyez sur **Entrée**.
   Le groupe est ajouté dans le panneau Groupes de rapports.

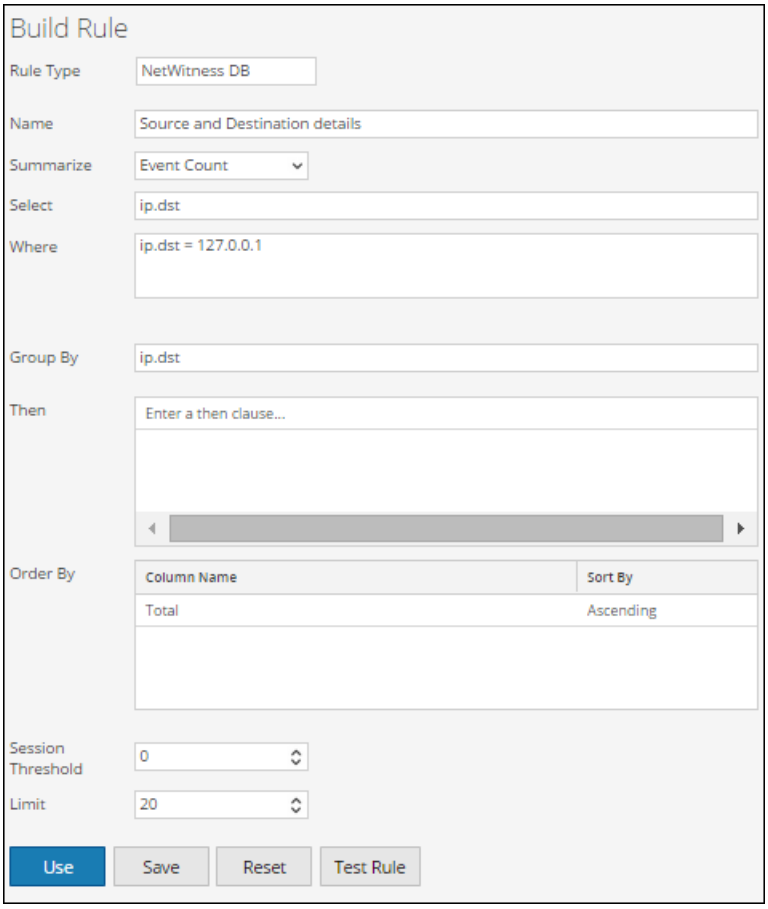
Planifier un rapport

Remarque : Lorsque vous planifiez un rapport Warehouse, vous pouvez utiliser un planificateur de tâches pris en charge pour allouer des ressources dans un cluster pour la tâche planifiée. Pour plus d'informations sur les planificateurs de tâches pris en charge, consultez la rubrique Planificateur de tâches pour Warehouse Reporting.

Pour planifier un rapport, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans la page **Élaborer une règle**, cliquez sur  pour créer une règle.
4. Cliquez sur **Enregistrer**.

5. Cliquez sur **Utiliser**.



6. Sélectionnez le **Nouveau rapport** ou le **Rapport existant**.
7. Sélectionnez un groupe de rapports et cliquez sur **Sélectionner**.
8. Indiquez le nom du rapport et sélectionnez la règle.
9. Cliquez sur **Planifier**.
   La vue Planifier un rapport s'affiche.

> **Remarque :** Si vous fournissez des autorisations d'accès à un rapport, vous devez aussi fournir les autorisations au groupe de rapports, aux règles utilisées dans le rapport et aux groupes de règles, sinon un message d'erreur s'affiche.

8. Pour exécuter les rapports selon le planning, cochez la case **Activer**.
9. Dans le champ **Nom de planning**, saisissez le nom de la configuration du rapport pour le planning.
10. Dans le champ Source de données, sélectionnez la source de données.

> **Remarque :** Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB, Répondre et Warehouse. Pour plus d'informations, reportez-vous à la rubrique « Configurer les autorisations des sources de données » dans le *Guide de configuration de Reporting Engine*.

11. (Facultatif) Dans le menu déroulant **Pool de ressource Warehouse**, sélectionnez les pools ou les files d'attentes disponibles dans le cluster afin de planifier le rapport à exécuter sur le pool ou la file d'attente. Ce menu déroulant n'est disponible que si vous avez sélectionné un rapport de base de données Warehouse.

    > **Remarque :** Tous les pools ou files d'attente que vous avez spécifiés à la page Explorer du Reporting Engine sont répertoriés. Si aucun pool ou file d'attente n'est configuré à la page Explorer, ce menu déroulant est désactivé et les tâches sont envoyées aux clusters sans aucun nom de file d'attente ou de pool.

    > **Remarque :** Si la file d'attente ou le pool configuré dans le planning du rapport est supprimé du cluster, alors le nom de la file d'attente dans le Planificateur de capacité reste inchangé. Toutefois, dans le planificateur, le nom de pool spécifié sera créé à l'aide du paramètre de propriété mapred.fairscheduler.allow.undeclared.pool.

12. Dans le menu déroulant Fuseau horaire, sélectionnez un fuseau horaire pour afficher toutes les données de temps dans un résultat de rapport au format spécifié. Ce paramètre est configurable dans la vue Explorer le Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).

13. Dans le champ **Exécuter** , sélectionnez le type de planification d'exécution. (Par exemple, Maintenant ou Toutes les heures).

    En fonction du type de planning d'exécution, effectuez l'une des opérations suivantes :

    - Si vous sélectionnez le planning d'exécution **Ultérieurement** ou **Tous les mois**, vous devez proposer une valeur pour le jour et l'heure dans le champ respectif.
    - Si vous sélectionnez un planning d'exécution **Toutes les heures**, vous devez spécifier les minutes dans le champ **À la minute**.
    - Si vous sélectionnez le planning d'exécution **Tous les jours**, vous devez saisir une valeur dans le champ **À**.
    - Si vous sélectionnez le planning d'exécution **Toutes les semaines**, vous devez saisir une valeur dans le champ **À** et sélectionner les jours de la semaine.

Remarque : Lorsque vous planifiez un rapport, si vous sélectionnez l'option **Derniers/Dernières** ou **Plage (spécifique/générique)** ou une heure de fin très proche de l'heure actuelle, vous devez vous assurer que les données agrégées dans la source de données sont retournées. S'il existe un délai d'agrégation dans la source de données, l'heure de fin que vous choisissez doit tenir compte de ce délai, sinon les rapports perdront des données non agrégées pour cette période.

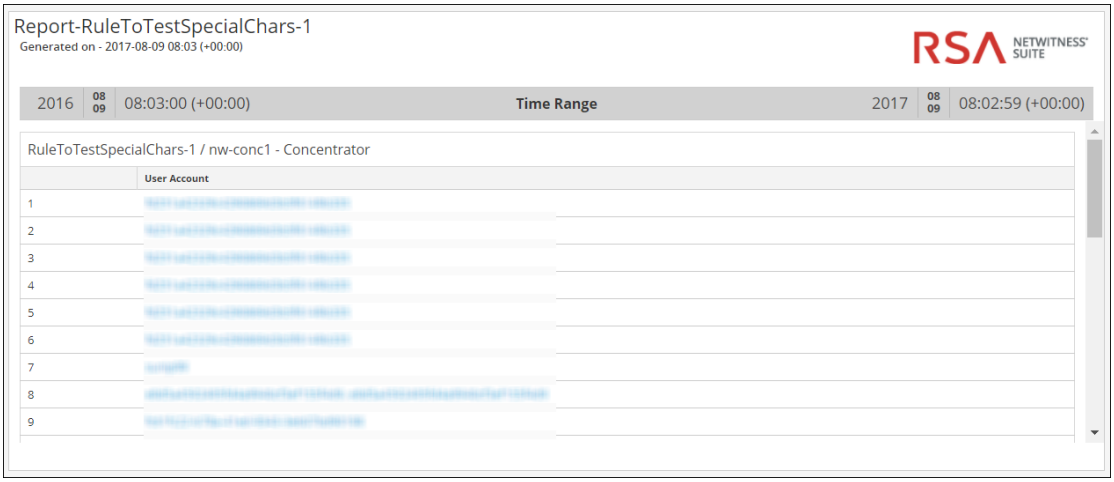
Pour plus d'informations sur la procédure à suivre pour générer un rapport avec des variables, reportez-vous à la rubrique Créer un rapport paramétré à l'aide d'une variable.

14. (Facultatif) Dans le panneau **Actions de résultat**, effectuez les opérations suivantes :
    a. Saisissez l'adresse e-mail et l'objet.
    b. Modifiez le corps de message du rapport.
    c. Sélectionnez le format de la pièce jointe.
    d. Saisissez une valeur pour les séparateurs à valeurs multiples et CSV.
    e. (Facultatif) Dans le champ Autres options, procédez comme suit :
        i. Cliquez sur  et sélectionnez le résultat de résultat SFTP, URL ou Partage réseau. Une ligne est ajoutée avec l'action de résultat sélectionnée.
        ii. Sélectionnez les options adéquates pour envoyer le rapport au format PDF ou CSV (ou les deux), vers l'action de résultat SFTP, URL ou Partage réseau configurée dans RE.
15. (Facultatif) Pour ajouter une liste dans le panneau Liste dynamique, consultez la rubrique Générer une liste à partir du rapport planifié.
16. (Facultatif) Pour choisir un logo dans le panneau Logo, reportez-vous à la rubrique *Gérer et sélectionner un logo de rapport* dans la rubrique Gérer les listes, les règles ou les rapports .

    Remarque : Si vous ne sélectionnez pas de logo, le logo RSA par défaut est utilisé.

17. Cliquez sur **Planifier**.

    Le rapport planifié s'exécute comme prévu et fournit les résultats configurés.



Après avoir créé et planifié un rapport, vous pouvez effectuer les tâches suivantes :

1. Vous pouvez notifier le destinataire de l'e-mail à la fin de l'exécution du rapport et envoyer les rapports au format PDF et CSV sous forme de pièces jointes à l'e-mail.
2. Vous pouvez générer une liste basée sur le rapport planifié et les afficher dans le module **Listes**.
3. Vous pouvez envoyer un rapport planifié au format PDF ou CSV (ou les deux) à l'emplacement SFTP, URL ou Partage réseau configuré dans RE.
4. Vous pouvez modifier le logo par défaut et l'afficher dans le rapport planifié.
5. Vous pouvez modifier les NetWitness Suitedétails de configuration de Reporting Engine en naviguant dans l'onglet Général du Reporting Engine. Consultez la rubrique « Onglet général du Reporting Engine » dans *l'Onglet général du Reporting Engine*.

Exemples

Par défaut, lorsque vous planifiez des rapports dans la vue Planifier un rapport, les résultats de l'option **Derniers/Dernières** sont présentées en fonction du fuseau horaire de l'utilisateur. Les exemples suivants permettent d'évaluer clairement les résultats des options **Heures**, **Jours**, **Semaines**, **Mois**, ou **Années** pour l'option **Derniers/Dernières** en fonction d'une durée absolue ou relative.

Remarque : Par défaut, la case de la durée relative est décochée. Cela implique que les résultats de l'option **Derniers/Dernières** sont présentés selon la durée absolue.

- **Selon une durée absolue** - La durée absolue permet de planifier un rapport à une heure absolue par rapport à l'heure actuelle (sans les secondes), et en prenant en considération

l'intervalle de temps dans son ensemble. Par exemple, 12h00 est une heure absolue par rapport à l'heure actuelle (12h45).

- Heures - Supposons que vous sélectionniez Heures et que vous spécifiiez une heure. Si l'heure spécifiée par l'utilisateur actuel est 16h20, le rapport est généré pour la période 15h00-16h00.
- Jours - Supposons que vous sélectionniez Jours et que vous spécifiiez un jour. Si la date du jour est le 27 août 2014 et que l'utilisateur actuel a spécifié 10:15 comme heure, le rapport sera généré pour la plage : Du 26 août 2014 à 12h00 au 27 août 2014 à 12h00.
- Semaines - Supposons que vous sélectionniez Semaines et que vous spécifiiez une semaine. Si la date du jour est le 27 août 2014, 14h30 (mercredi), le rapport sera généré pour la plage : Du samedi 16 août 2014 à 12h00 au samedi 23 août 2014 à 12h00.
- Mois - Supposons que vous sélectionniez Mois et que vous spécifiiez un mois. Si la date du jour est le 27 août 2014, 14h30, le rapport sera généré pour la plage : du 1er juillet 2014, 00h00 au 31 juillet 2014, 00h00.
- Années - Supposons que vous sélectionniez Années et que vous spécifiiez une année. Si la date du jour est le 27 août 2014 14h30, le rapport sera généré pour la plage : du 1er janvier 2013, 00h00 au 31 décembre 2013, 00h00.

- **Selon une durée relative** - La durée relative permet à un rapport d'être planifié à une heure relative par rapport à l'heure actuelle, et peut varier en fonction de l'heure actuelle. Par exemple, 12h45 est l'heure relative par rapport à l'heure actuelle (12h45).
  - Heures - Supposons que vous sélectionniez Heures et que vous spécifiiez une heure. Si l'heure spécifiée par l'utilisateur actuel est 16h20, le rapport est généré pour la période 15h20-16h20.
  - Jours - Supposons que vous sélectionniez Jours et que vous spécifiiez un jour. Si la date du jour est le 27 août 2014 et que l'utilisateur actuel a spécifié 10:15 comme heure, le rapport sera généré pour la plage : du 26 août 2014, 10h15 au 27 août 2014, 10h15.
  - Semaines - Supposons que vous sélectionniez Semaines et que vous spécifiiez une semaine. Si la date du jour est le 27 août 2014, 12h30 (mercredi), le rapport sera généré pour la plage : du jeudi 21 août 2014, 12h30 au mercredi 27 août 2014, 12h30.
  - Mois - Supposons que vous sélectionniez Mois et que vous spécifiiez un mois. Si la date du jour est le 27 août 2014, 14h30, le rapport sera généré pour la plage : du 27 juillet 2014, 14h30 au 27 août 2014, 14h30.

- Années - Supposons que vous sélectionniez Années et que vous spécifiiez une année. Si la date du jour est le 27 août 2014 14h30, le rapport sera généré pour la plage : Du 27 août 2013 à 14h30 au 27 août 2014 à 14h30.

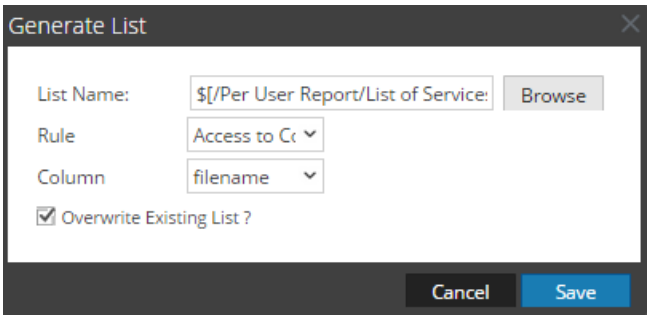
Procédures supplémentaires

Générer une liste à partir du rapport planifié

Vous pouvez générer une liste à partir du rapport planifié. Assurez-vous que vos listes sont créées dans NetWitness Suite avant de générer une liste pour planifier un rapport.

Pour générer une liste à partir de la vue Élaborer le rapport, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport et cliquez sur  > **Planifier un rapport**.
   L'onglet de la vue Planifier un rapport s'affiche.
4. Dans le panneau **Liste dynamique**, cliquez sur  .
   La boîte de dialogue Générer une liste s'ouvre.
5. Cliquez sur **Parcourir**.
   Le panneau Sélection de listes s'affiche.
6. Choisissez un élément de liste et cliquez sur **Sélectionner**.
   Le nom de la liste apparaît dans le champ Nom de la liste.
7. Sélectionnez une règle valide pour filtrer les résultats du rapport en fonction de la définition de la règle.
8. Sélectionnez une valeur pour le champ **Colonne**.
   La colonne forme les valeurs de la liste créée.
9. Pour remplacer la liste existante, activez la case à cocher **Remplacer la liste existante ?**
10. Cliquez sur **Enregistrer**.
    Le nom de la liste apparaît dans le panneau Générer une liste.



11. (Facultatif) Sélectionnez une liste dans le panneau Générer une liste et cliquez sur pour supprimer la liste sélectionnée.
12. (Facultatif) Sélectionnez une liste dans le panneau Générer une liste et cliquez sur pour modifier les détails de la liste.

Créer un rapport paramétré à l'aide d'une variable

Vous utilisez des variables pour le reporting dans le module RSA NetWitness Suite Reporting. Les rapports paramétrés vous permettent de spécifier des valeurs de manière dynamique lors de l'exécution sans modifier la définition des règles afin d'afficher les résultats en fonction d'une valeur particulière. Vous pouvez obtenir des rapports paramétrés en utilisant des variables dans la requête ou la règle. Pour plus d'informations sur l'ajout d'une règle, reportez-vous à la rubrique Configurer une règle. Lors de l'exécution, vous pouvez saisir la valeur de la variable ou sélectionner la valeur dans la liste en fonction de laquelle l'ensemble des résultats est affiché.

La syntaxe permettant de spécifier la variable est la suivante :

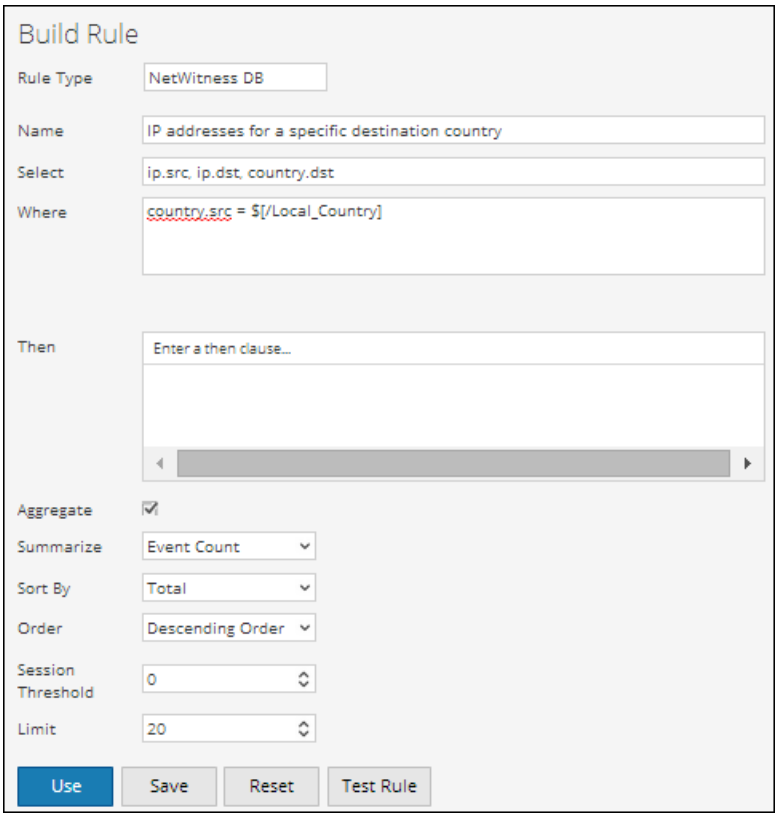
Description	Exemples de syntaxe prise en charge
Insérez `$` avant une variable. Placez une variable entre parenthèses.	`columnname=${<variable>}`

La syntaxe permettant de définir la variable est la même pour les sources de bases de données NetWitness, IPDB et Warehouse. Lorsque vous attribuez la valeur de la variable dans une configuration d'exécution, vous devez placer la valeur entre des guillemets simples : `'<value>'` .

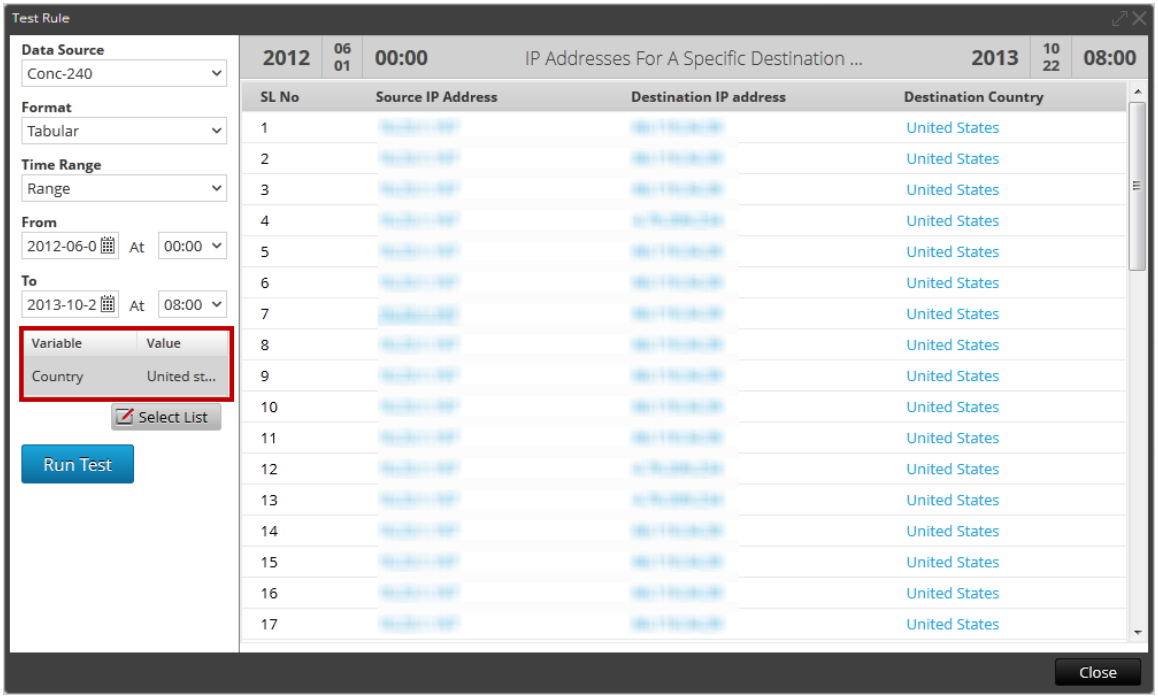
Certains exemples d'utilisation de variables peuvent être fournis dans cette rubrique.

Afficher les adresses IP source pour un pays de destination spécifique

Voici un exemple de règle de base de données NetWitness permettant d'afficher les adresses IP source et de destination pour un pays de destination spécifique. Ici la valeur du pays source est définie en tant que variable `${local_country}`.



Au moment de l'exécution, vous êtes invité(e) à saisir la valeur de la variable. La figure ci-dessous affiche la variable `local_Country` où vous pouvez saisir la valeur. Si vous saisissez la valeur **United states**, toutes les adresses IP source et de destination avec le pays de destination United states s'affichent.



Vous pouvez utiliser la règle ci-dessus pour planifier un rapport. Vous pouvez planifier deux types de rapports :

- Rapport avec des variables dynamiques
- Rapport itératif

Rapport avec des variables dynamiques

Les variables dynamiques permettent à l'utilisateur de spécifier les valeurs d'une variable définie dans une règle lors de la planification d'un rapport.

Pour planifier un rapport avec une variable dynamique, procédez comme suit :

1. Sélectionnez **SURVEILLER** > Rapports.

   L'onglet Gérer s'affiche.

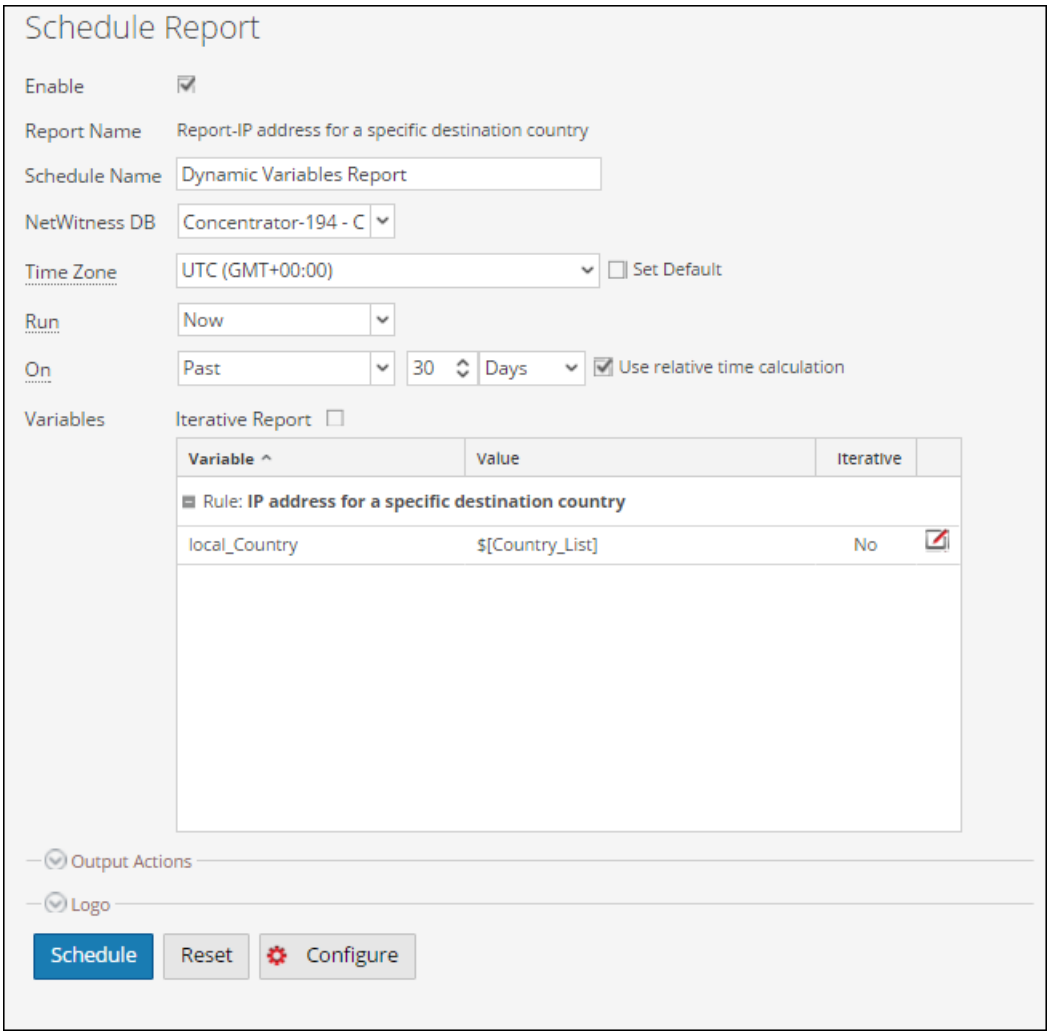
2. Cliquez sur **Rapports**.

   La vue Rapport s'affiche.

3. Sur la page **Élaborer le rapport**, cliquez sur + pour créer un rapport.

4. Ajoutez la règle ayant la variable définie par l'utilisateur à partir de l'onglet Règles.

5. Cliquez sur **Planifier**.
   L'onglet de la vue Planifier un rapport s'affiche.



6. Pour exécuter les rapports selon le planning, cochez la case **Activer**.
7. Dans le champ **Nom de planning**, saisissez le nom de la configuration du rapport pour le planning.
8. Dans le champ **Source de données**, sélectionnez la source de données.

   Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubrique « Configurer les autorisations d'accès aux sources de données » dans le *Guide de configuration de Reporting Engine*.

9. (Facultatif) Dans le menu déroulant **Pool de ressource Warehouse**, sélectionnez les pools ou les files d'attentes disponibles dans le cluster afin de planifier le rapport à exécuter sur le pool ou la file d'attente. Ce menu déroulant n'est disponible que si vous avez sélectionné un rapport de base de données Warehouse.

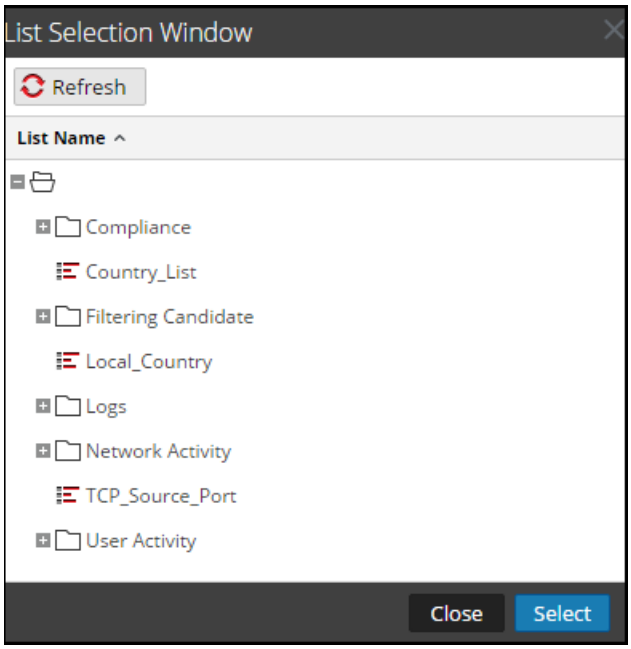
Remarque : Tous les pools ou files d'attente que vous avez spécifiés à la page Explorer du Reporting Engine sont répertoriés. Si aucun pool ou file d'attente n'est configuré à la page Explorer, ce menu déroulant est désactivé et les tâches sont envoyées aux clusters sans aucun nom de file d'attente ou de pool.

Remarque : Si la file d'attente ou le pool configuré dans le planning du rapport est supprimé du cluster, alors le nom de la file d'attente dans le Planificateur de capacité reste inchangé. Toutefois, dans le planificateur, le nom de pool spécifié sera créé à l'aide du paramètre de propriété `mapred.fairscheduler.allow.undeclared.pool`.

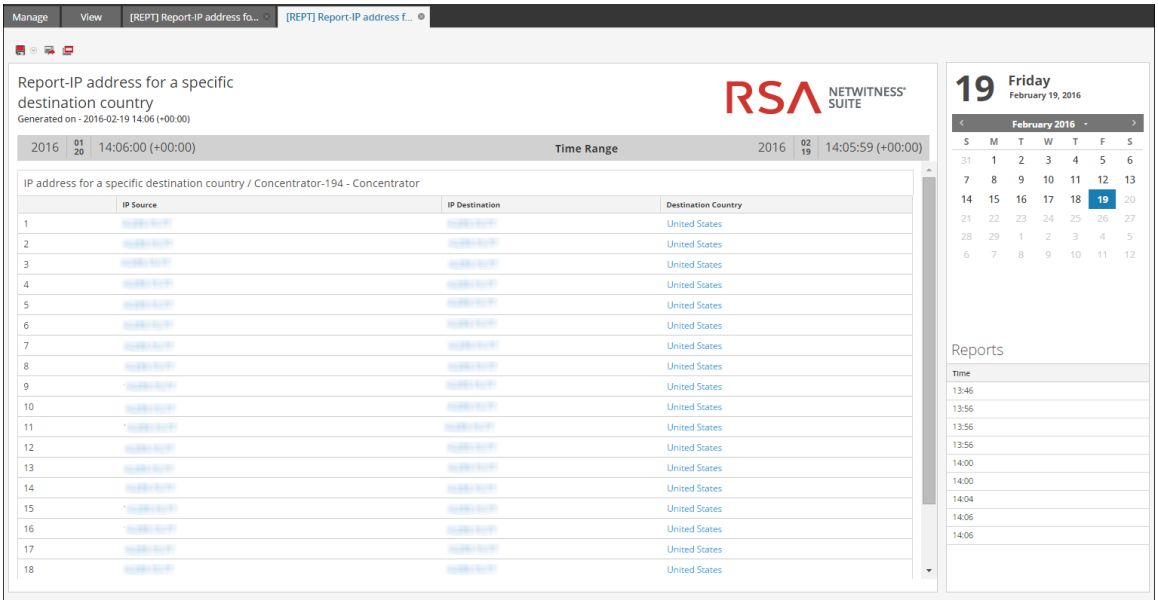
10. Dans le menu déroulant Fuseau horaire, sélectionnez un fuseau horaire pour afficher toutes les données liées au temps dans un résultat de rapport au format spécifié. Ce paramètre est configurable dans la vue Explorer du Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. Dans le champ **Exécuter** , sélectionnez le type de planification d'exécution. (Par exemple, Maintenant ou Toutes les heures). En fonction du type de planning d'exécution, effectuez l'une des opérations suivantes :
    - Si vous sélectionnez le planning d'exécution **Ultérieurement** ou **Tous les mois**, vous devez proposer une valeur pour le jour et l'heure dans le champ respectif.
    - Si vous sélectionnez un planning d'exécution **Toutes les heures**, vous devez spécifier les minutes dans le champ **À la minute**.
    - Si vous sélectionnez le planning d'exécution **Tous les jours**, vous devez saisir une valeur de temps dans le champ **À**.
    - Si vous sélectionnez le planning d'exécution **Toutes les semaines**, vous devez saisir une valeur dans le champ **À** et sélectionner les jours de la semaine.

    Remarque : Lorsque vous planifiez un rapport, si vous sélectionnez l'option **Coller** ou **Plage (spécifique/générique)** ou une heure de fin très proche de l'heure actuelle, vous devez vous assurer que les données agrégées dans la source de données sont retournées. S'il existe un délai d'agrégation dans la source de données, l'heure de fin que vous choisissez doit tenir compte de ce délai, sinon les rapports perdront des données non agrégées pour cette période.
12. Dans le champ des variables, cliquez sur  .
13. Exécutez l'une des opérations suivantes :

- Saisissez la valeur de la variable, ou
- Choisissez la valeur de liste pour la variable.

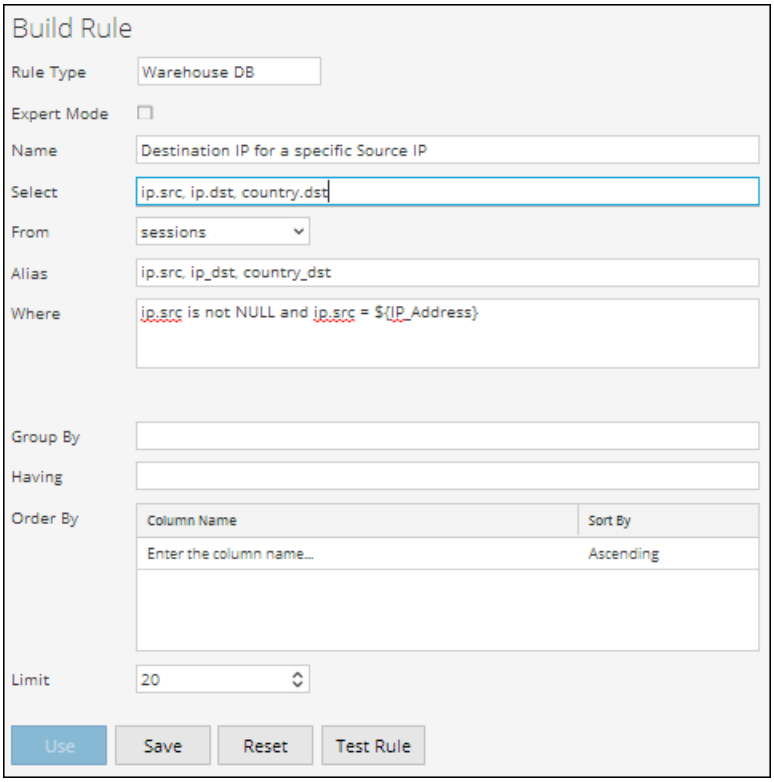


14. Cliquez sur **Sélectionner**.
15. Cliquez sur **Planifier**.
    Le rapport planifié s'exécute comme prévu et fournit les résultats configurés.

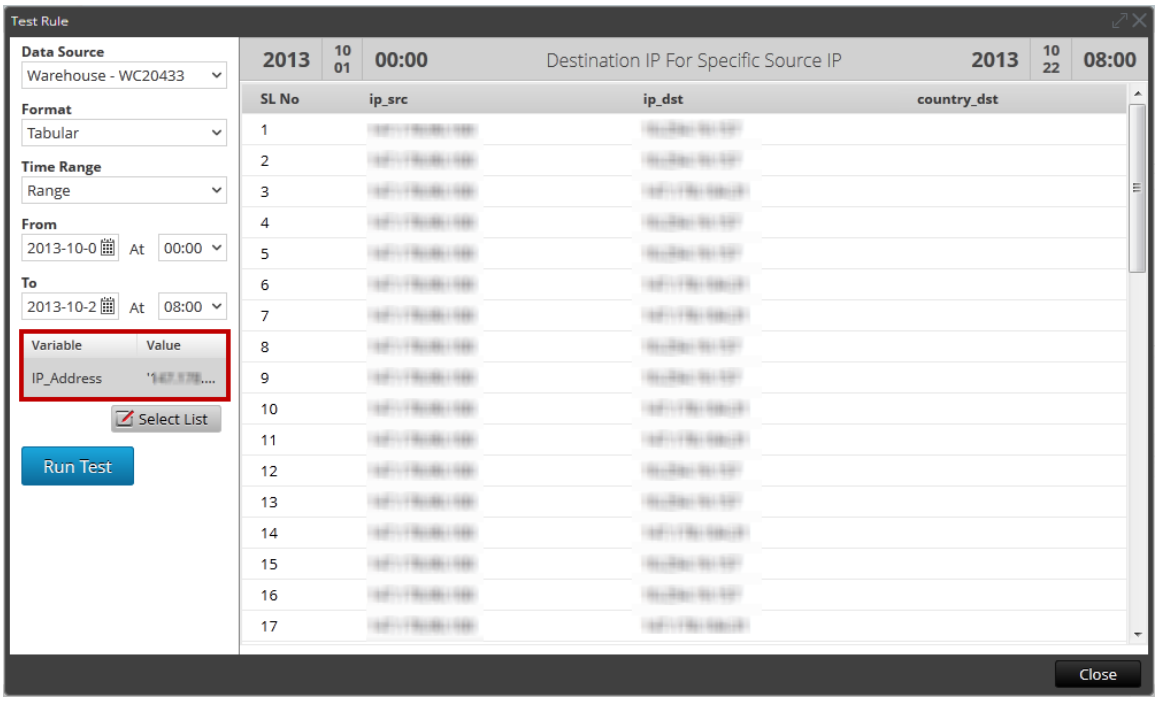


Afficher toutes les adresses IP de destination pour une adresse IP source

Voici un exemple de règle Warehouse permettant d'afficher toutes les adresses IP de destination pour une adresse IP source spécifique. L'adresse IP source `ip_src` est définie en tant que variable `${IP_Address}`.

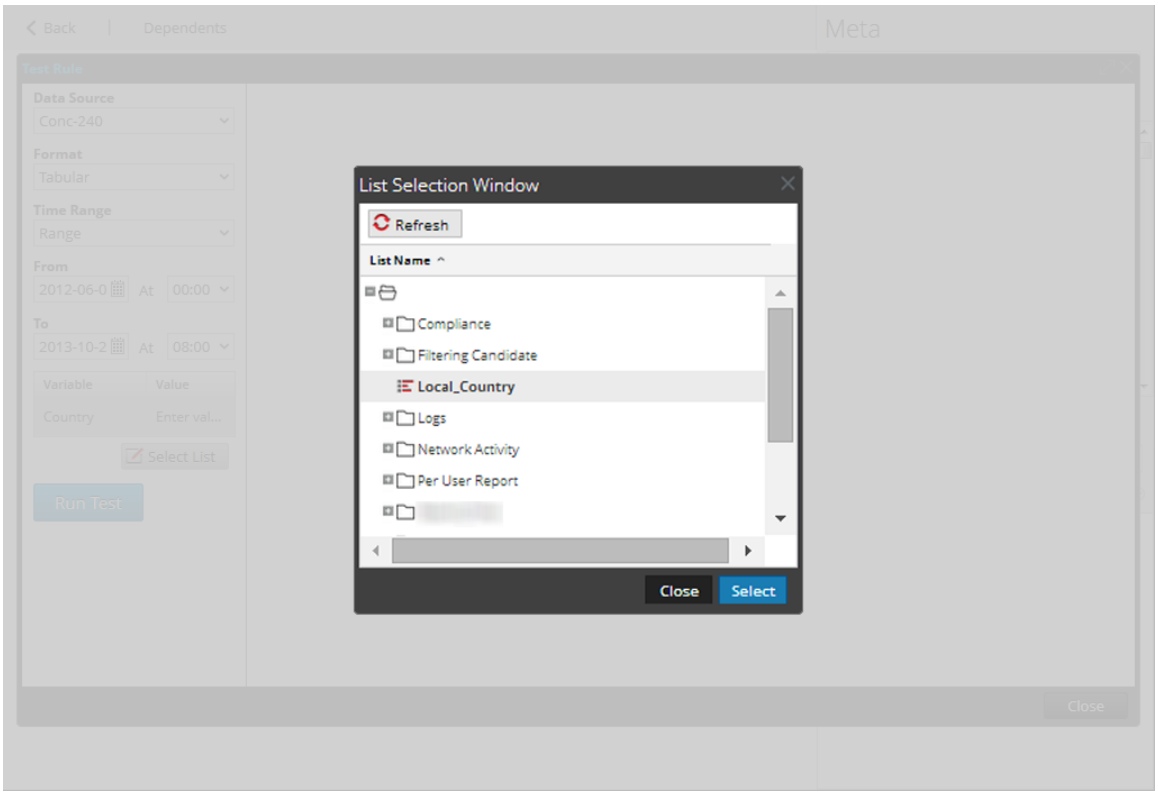


Au moment de l'exécution, vous êtes invité(e) à saisir l'adresse IP source. La figure affiche la variable `IP_Address` qui vous permet de saisir une adresse IP source valide. Toutes les adresses IP de destination avec l'adresse IP source spécifiée sont répertoriées.



Associer une variable à une liste de valeurs

Vous pouvez associer la variable à une liste. Par exemple, vous pouvez créer une liste nommée `Local_Country`, puis saisir tous les noms des pays en tant que valeurs. Vous pouvez sélectionner la liste `Local_Country` comme valeur pour la variable `Local_Country`. Lors de la configuration de l'exécution, la liste `Local_Country` est renseignée et vous pouvez sélectionner le pays en fonction des résultats affichés.



Rapport itératif

Un rapport itératif génère un rapport pour chaque valeur dans la liste.

Pour planifier un rapport, procédez comme suit :

1. Sélectionnez **SURVEILLER** > Rapports.

   L'onglet Gérer s'affiche.

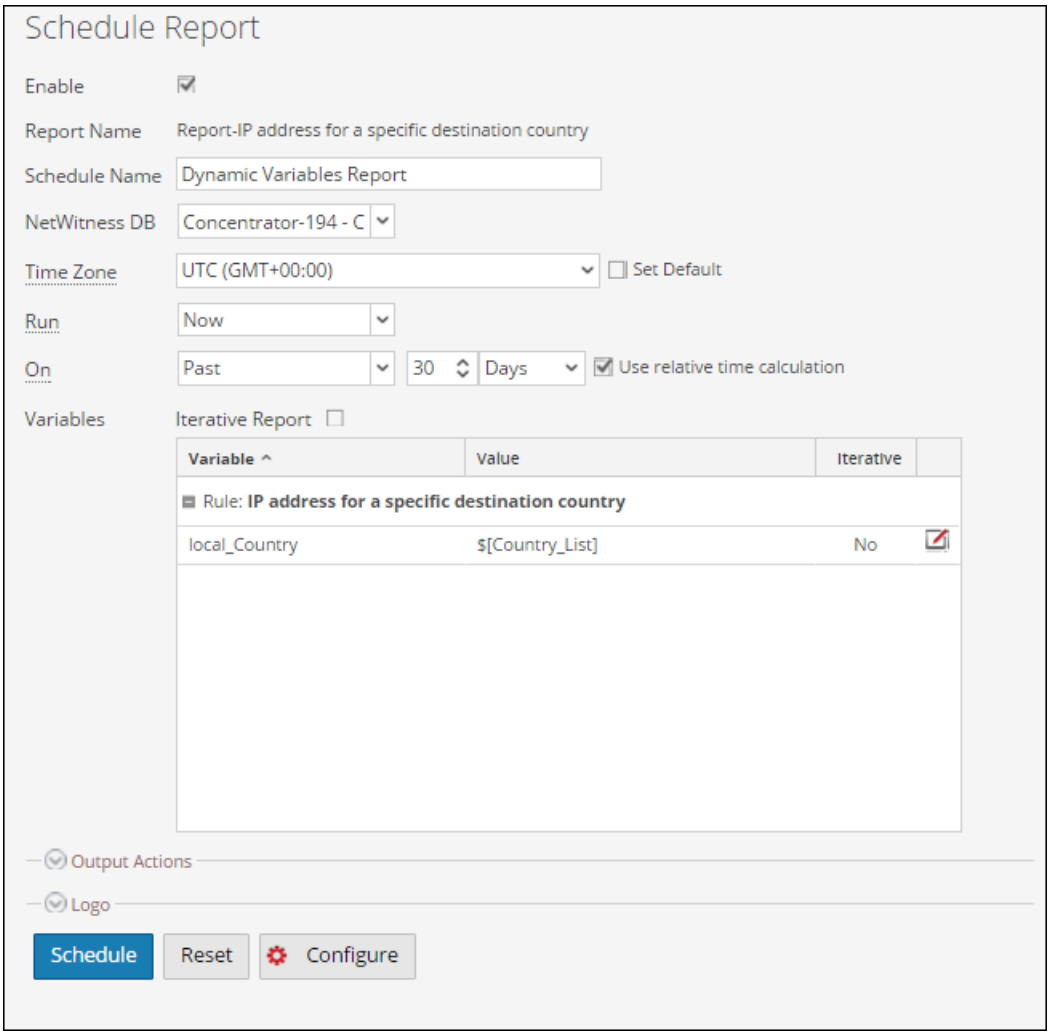
2. Cliquez sur **Rapports**.

   La vue Rapport s'affiche.

3. Sur la page **Élaborer le rapport**, cliquez sur + pour créer un rapport.

4. Ajoutez la règle ayant la variable définie par l'utilisateur à partir de l'onglet Règles.

5. Cliquez sur **Planifier**.
   L'onglet de la vue Planifier un rapport s'affiche.



6. Pour exécuter les rapports selon le planning, cochez la case **Activer**.
7. Dans le champ **Nom de planning**, saisissez le nom de la configuration du rapport pour le planning.
8. Dans le champ **Source de données**, sélectionnez la source de données.

   Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubqirue « Configurer les autorisations d'accès aux sources de données » dans le *Guide de configuration de Reporting Engine*.

9. (Facultatif) Dans le menu déroulant **Pool de ressource Warehouse**, sélectionnez les pools ou les files d'attentes disponibles dans le cluster afin de planifier le rapport à exécuter sur le pool ou la file d'attente. Ce menu déroulant n'est disponible que si vous avez sélectionné un rapport de base de données Warehouse.

Remarque : Tous les pools ou files d'attente que vous avez spécifiés à la page Explorer du Reporting Engine sont répertoriés. Si aucun pool ou file d'attente n'est configuré à la page Explorer, ce menu déroulant est désactivé et les tâches sont envoyées aux clusters sans aucun nom de file d'attente ou de pool.

Remarque : Si la file d'attente ou le pool configuré dans le planning du rapport est supprimé du cluster, alors le nom de la file d'attente dans le Planificateur de capacité reste inchangé. Toutefois, dans le planificateur, le nom de pool spécifié sera créé à l'aide du paramètre de propriété `mapred.fairscheduler.allow.undeclared.pool`.

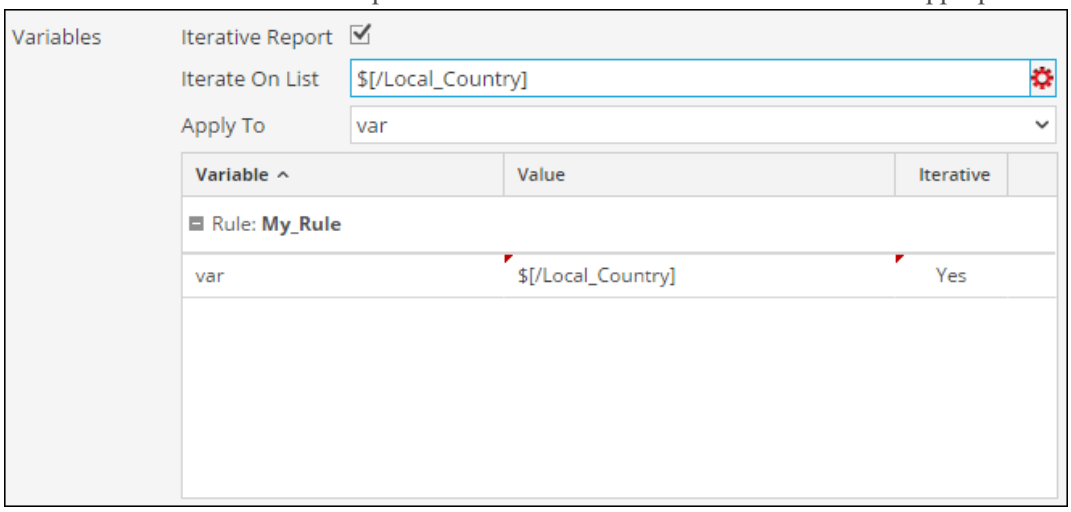
10. Dans le menu déroulant Fuseau horaire, sélectionnez un fuseau horaire pour afficher toutes les données liées au temps dans un résultat de rapport au format spécifié. Ce paramètre est configurable dans la vue Explorer du Reporting Engine (/com.rsa.soc.re/configuration/reportoutputformatterconfig/reportoutputformatterconfig).
11. Dans le champ **Exécuter** , sélectionnez le type de planification d'exécution. (Par exemple, Maintenant ou Toutes les heures). En fonction du type de planning d'exécution, effectuez l'une des opérations suivantes :
    - Si vous sélectionnez le planning d'exécution **Ultérieurement** ou **Tous les mois**, vous devez proposer une valeur pour le jour et l'heure dans le champ respectif.
    - Si vous sélectionnez un planning d'exécution **Toutes les heures**, vous devez spécifier les minutes dans le champ **À la minute**.
    - Si vous sélectionnez le planning d'exécution **Tous les jours**, vous devez saisir une valeur de temps dans le champ **À**.
    - Si vous sélectionnez le planning d'exécution **Toutes les semaines**, vous devez saisir une valeur dans le champ **À** et sélectionner les jours de la semaine.

    Remarque : Lorsque vous planifiez un rapport, si vous sélectionnez l'option **Coller** ou **Plage (spécifique/générique)** ou une heure de fin très proche de l'heure actuelle, vous devez vous assurer que les données agrégées dans la source de données sont retournées. S'il existe un délai d'agrégation dans la source de données, l'heure de fin que vous choisissez doit tenir compte de ce délai, sinon les rapports perdront des données non agrégées pour cette période.
12. Dans le champ des variables, effectuez les opérations suivantes :
    a. Pour exécuter des rapports itératifs, cochez la case **Rapport itératif**.
    b. Pour effectuer une itération en fonction de la valeur de liste, cliquez sur  .

       La fenêtre de sélection de liste s'ouvre.
    c. Choisissez un élément de liste, puis cliquez sur **Sélectionner**.

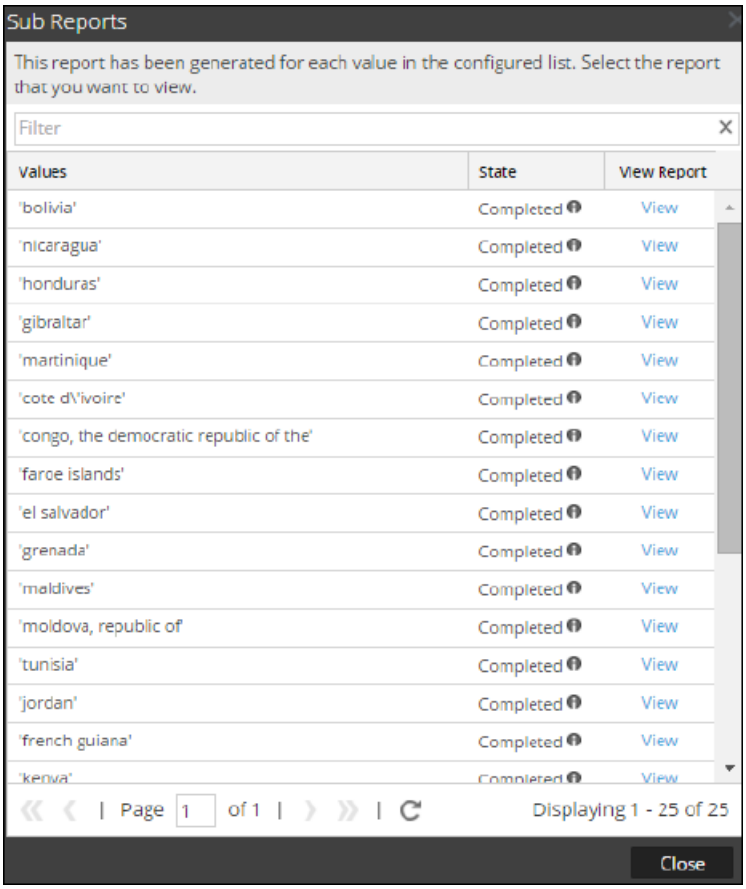
       L'élément de liste sélectionné est ajouté au champ **Itérer sur la liste**.

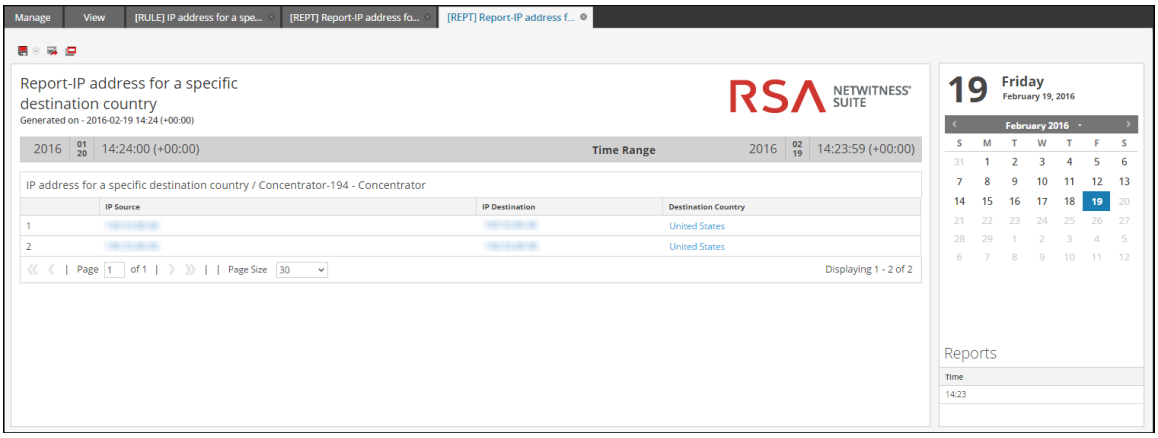
d. Sélectionnez la variable sur laquelle la valeur de liste sélectionnée doit être appliquée.



13. Cliquez sur **Planifier**.
    Le rapport planifié s'exécute comme prévu et fournit les résultats configurés.

La figure ci-dessous illustre la vue Rapport itératif.





Créer un rapport à l'aide d'une règle

Vous pouvez créer un rapport à l'aide d'une règle. Lorsque vous créez un rapport à l'aide d'une règle, un rapport par défaut est créé avec cette règle unique. Vous pouvez modifier davantage le rapport pour ajouter d'autres règles.

Pour créer un rapport à l'aide d'une règle, procédez comme suit :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Exécutez l'une des opérations suivantes :
   - Vous pouvez créer un rapport à l'aide d'une règle lorsque vous créez ou modifiez la règle. Effectuez les opérations suivantes :
     a. Dans la vue **Créer une règle,** cliquez sur **Utiliser**.
        La boîte de dialogue Règle d'utilisation s'affiche.
     b. Cliquez sur **Rapport**.
     c. Sélectionnez **Nouveau rapport** ou **Rapport existant** selon vos besoins.
     d. Cliquez sur **Sélectionner**.
   - Sélectionnez une règle dans le panneau Liste de règles, puis cliquez sur  dans la barre d'outils Règle. Dans le menu déroulant, sélectionnez **Utiliser**>**Rapport**.
   - Dans le panneau Liste des règles, puis cliquez sur  > **Créer un rapport**.

Remarque : Des règles personnalisées peuvent être utilisées pour créer un rapport. Si vous sélectionnez la vue « Aire » ou « Sectoriel » pour la règle, une fenêtre apparaît pour les entrées **Axe X** et **Axe Y**. Par défaut, vous ne pouvez sélectionner que la première méta dans **Axe X**.

Afficher un rapport

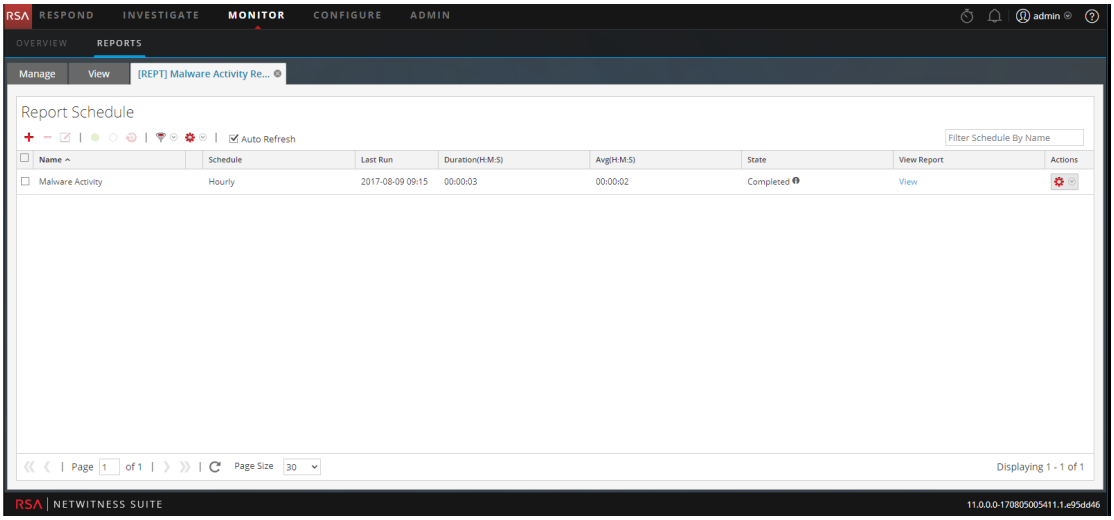
Vous pouvez afficher un rapport ou une liste de tous les rapports. Vous pouvez également afficher les rapports planifiés pour connaître l'état du rapport planifié. Si le rapport planifié est à l'état d'arrêt ou de désactivation, vous pouvez le démarrer ou l'activer.

Après avoir vu un rapport, vous pouvez effectuer les opérations suivantes :

1. Vous pouvez imprimer, enregistrer, envoyer par e-mail et afficher des rapports en mode plein écran.
2. Vous pouvez aussi sélectionner une date du calendrier pour afficher la liste des rapports exécutés correctement à la date choisie.

Pour afficher un rapport, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports** cliquez sur  > **Afficher les rapports planifiés**.
4. Cliquez sur la colonne **#Schedules**.
   L'onglet de la vue Planifier des rapports affiche l'état de chaque rapport planifié.



5. Sélectionnez un rapport planifié et cliquez sur **Afficher**.
   L'un des éléments suivants s'affiche :

- Le rapport sélectionné.
- Le panneau Sous-rapports pour un rapport planifié dont l'option Itératif est sélectionnée.

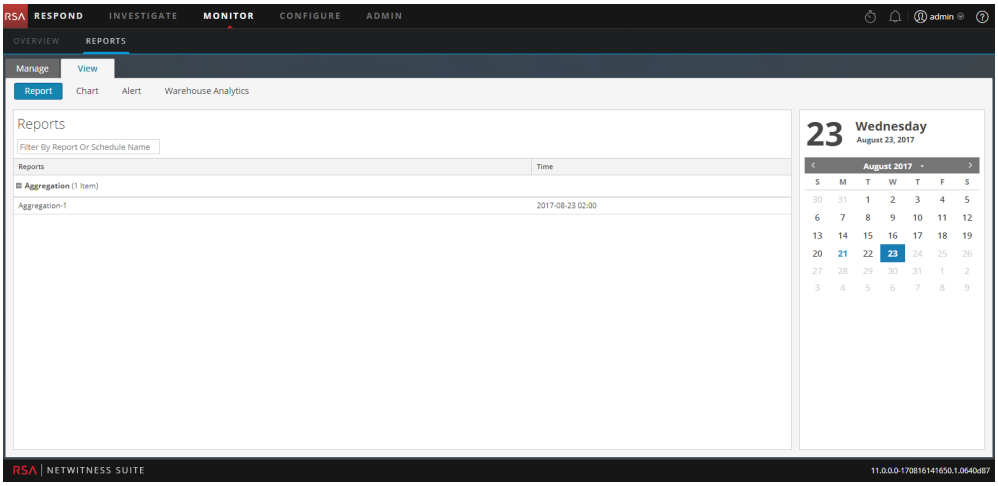
Pour chaque valeur de la liste configurée, un rapport s'affiche.

> **Remarque :** Si l'état du rapport est partiel ou complet, les paramètres "last run timestamp" et "last run (seconds)" sont mis à jour. En revanche, la durée moyenne d'exécution du rapport est mise à jour uniquement si l'état du rapport est complet et non partiel.

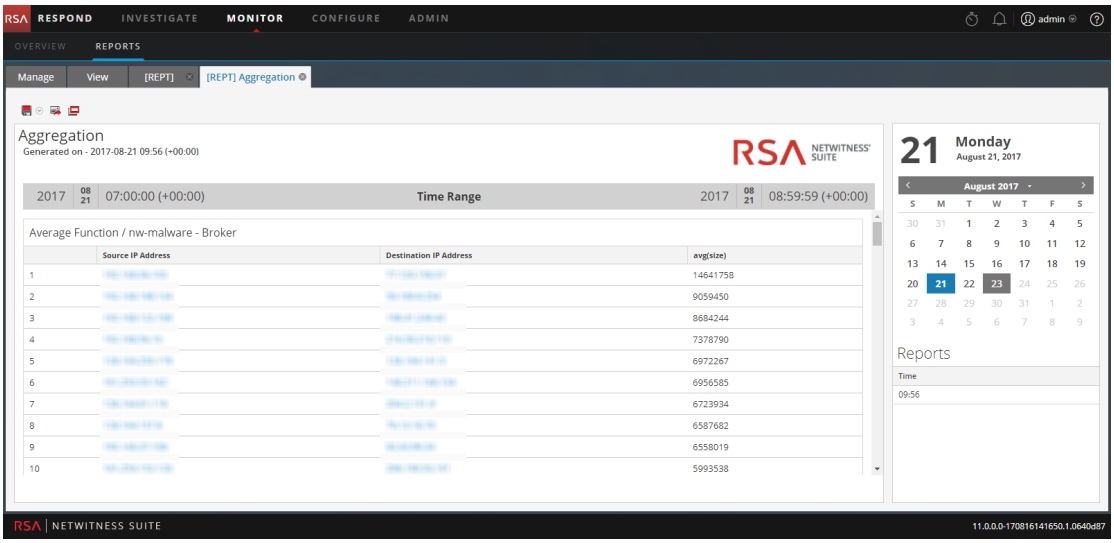
Pour afficher une liste de tous les rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet **Gérer** s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Rapport**, cliquez sur **Afficher tous les rapports**.
   La liste des rapports, ainsi que leur nom et heure de planification s'affichent sous l'onglet Vue.

> **Remarque :** Si aucune liste ne s'affiche, sélectionnez une date dans le calendrier pour afficher la liste des rapports pour cette date.



4. Vous pouvez cliquer sur un rapport planifié et l'imprimer, l'enregistrer sous forme de fichier PDF/CSV, envoyer des notifications par e-mail ou l'afficher en mode plein écran.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
OVERVIEW
REPORTS
Manage
View
[REPT]
[REPT] Aggregation
Aggregation
Generated on - 2017-08-21 09:56 (+00:00)
RSA NETWITNESS SUITE
2017 08 21 07:00:00 (+00:00)
Time Range
2017 08 21 08:59:59 (+00:00)
Average Function / nw-malware - Broker
Source IP Address
Destination IP Address
avg(size)
1 14641758
2 9059450
3 8684244
4 7378790
5 6972267
6 6956585
7 6723934
8 6587682
9 6558019
10 5993538
21 Monday
August 21, 2017
August 2017
S M T W T F S
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Reports
Time
09:56
RSA | NETWITNESS SUITE
11.0.0.0-170816141650.1.0640d87

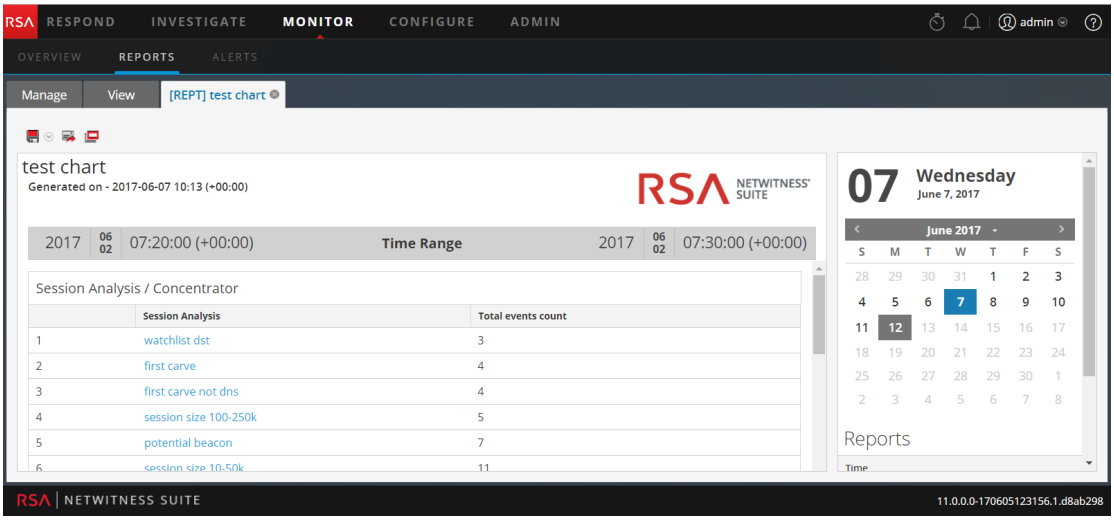
Analyser un rapport

Vous pouvez analyser un rapport en accédant directement à la vue Investigation à partir du rapport. À l'aide de l'option Analyser un rapport, vous pouvez analyser chaque événement mentionné dans le rapport.

Pour analyser un rapport, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans la barre d'outils **Rapport**, cliquez sur **Afficher tous les rapports**.
   L'onglet Afficher tous les rapports s'affiche.

   Remarque : Si aucun rapport ne s'affiche sous l'onglet Afficher tous les rapports, sélectionnez une date pour laquelle vous souhaitez afficher les rapports.
4. Double-cliquez sur le nom du rapport pour afficher ses détails.
   L'écran Détails du rapport s'affiche.



   Vous pouvez cliquer sur l'analyse de session à analyser dans le rapport.

Remarque : Pour copier manuellement les données du résultat et les utiliser pour l'investigation, assurez-vous que les valeurs binaires comportent le préfixe « hex: ».

Gérer les listes, les règles ou les rapports

Vous pouvez définir un contrôle d'accès, supprimer, modifier, importer ou exporter une liste, une règle ou un rapport.

Gérer une liste

Définir le contrôle d'accès pour une liste ou un groupe de listes

Vous pouvez configurer les autorisations d'accès pour les rôles d'utilisateur permettant de gérer les listes ou les groupes de listes. Le Reporting fournit un contrôle d'accès au niveau de la liste et du groupe de listes. Seul un utilisateur disposant de l'ensemble d'autorisations approprié peut effectuer les tâches du Reporting. Le contrôle d'accès est géré par l'administrateur à partir de l'onglet **ADMIN > Sécurité > Rôles**.

En tant qu'administrateur, vous devez vous assurer que les rôles créés pour les tâches spécifiques ont accès à toutes les autorisations supérieures dans la hiérarchie de rôles.

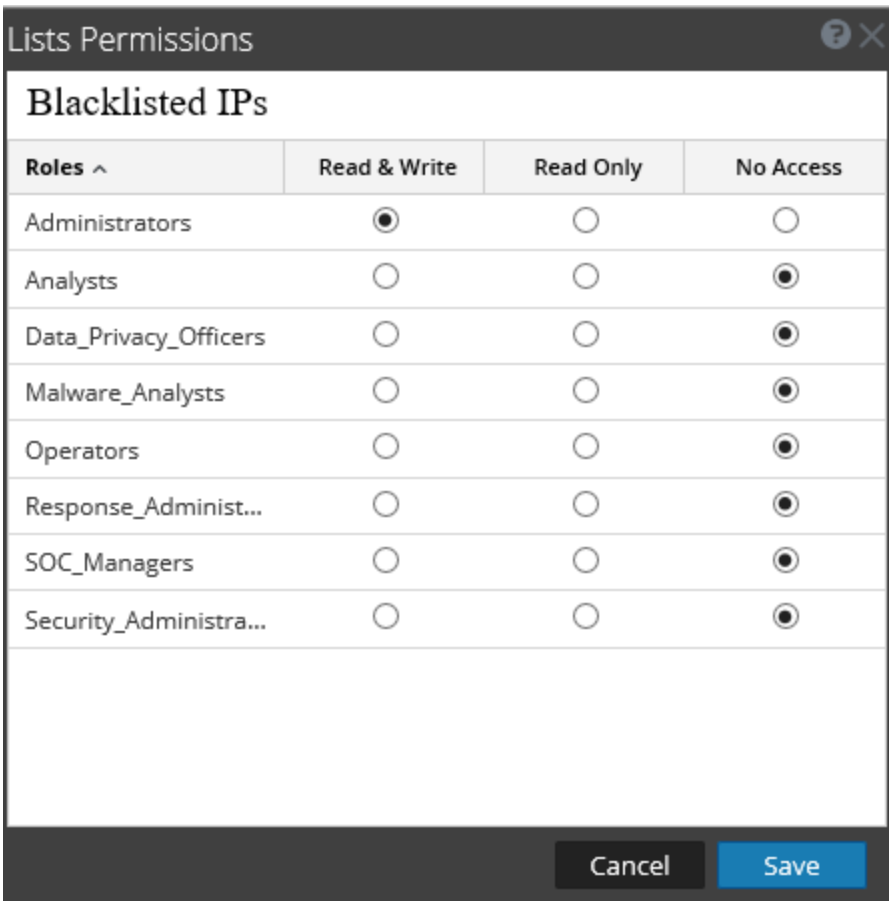
Les listes ou groupes de listes peuvent être attribués à un ensemble spécifique de rôles d'utilisateur. Lorsque les utilisateurs se connectent à NetWitness Suite, ils peuvent accéder uniquement aux listes auxquelles ils appartiennent. Les utilisateurs appartenant à un rôle d'utilisateur avec le droit d'accès **Lecture et écriture** doivent posséder des privilèges d'accès complets sur les listes. De plus, l'accès peut être renforcé afin que les listes soient accessibles uniquement pour les personnes possédant l'accès **Lecture seule**.

Remarque : Vous devez avoir l'autorisation de **Lecture seule** sur un groupe de listes pour afficher les listes de ce groupe.

Par exemple, si vous souhaitez que les **analystes de la sécurité** aient accès à toutes les listes d'un groupe de listes, vous pouvez alors définir l'autorisation **Lecture et écriture** au niveau du groupe de listes. Et si vous ne souhaitez pas que le rôle **Opérateur** ait accès à un ensemble spécifique de listes dans un groupe de listes, vous pouvez définir l'autorisation **Aucun accès** au niveau du groupe de listes.

Au niveau de la règle, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness Suite. Pour plus d'informations, reportez-vous à la rubrique Vue Liste :

- Lecture et écriture
- Lecture seule
- Aucun accès



Le tableau suivant répertorie les différentes colonnes du panneau Autorisations des listes :

Colonne	Description
Rôles	Décrit les rôles des utilisateurs connectés à l'interface utilisateur NetWitness Suite.
Lecture et écriture	Permet aux utilisateurs d'accéder, afficher, modifier, supprimer, importer et exporter les listes de la vue Listes. Les utilisateurs ne peuvent pas modifier l'autorisation dans la règle.
Lecture seule	Permet uniquement aux utilisateurs d'accéder à la liste et de l'afficher dans la vue Listes.
Aucun accès	Ne permet pas aux utilisateurs d'accéder aux listes ni de les afficher.

Contrôle d'accès pour une liste

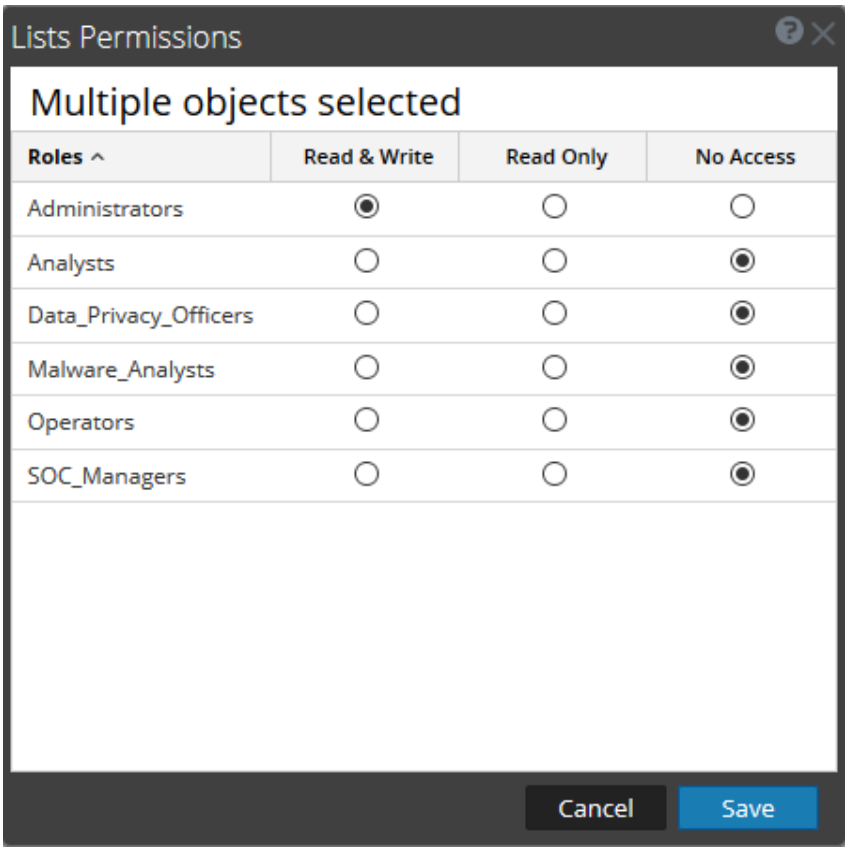
Pour modifier les autorisations de listes, vous devez sélectionner une liste et définir les autorisations d'accès à l'aide du panneau Autorisations des listes.

Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez la définir au niveau de la liste. Excepté pour les administrateurs, l'autorisation par défaut définie pour tous les autres rôles d'utilisateur est **Aucun accès** avant l'application des autorisations de tâche.

Contrôle de l'accès à plusieurs listes

Vous pouvez sélectionner plusieurs listes à la fois et définir les autorisations d'accès à l'aide du panneau Autorisations des listes. L'autorisation d'accès que vous choisissez s'applique à toutes les listes.

Remarque : Le caractère * en regard du nom du rôle indique les autres autorisations disponibles pour le rôle d'utilisateur. Si vous souhaitez modifier l'autorisation d'accès du rôle d'utilisateur requis, sélectionnez le rôle d'utilisateur et modifiez l'autorisation d'accès.



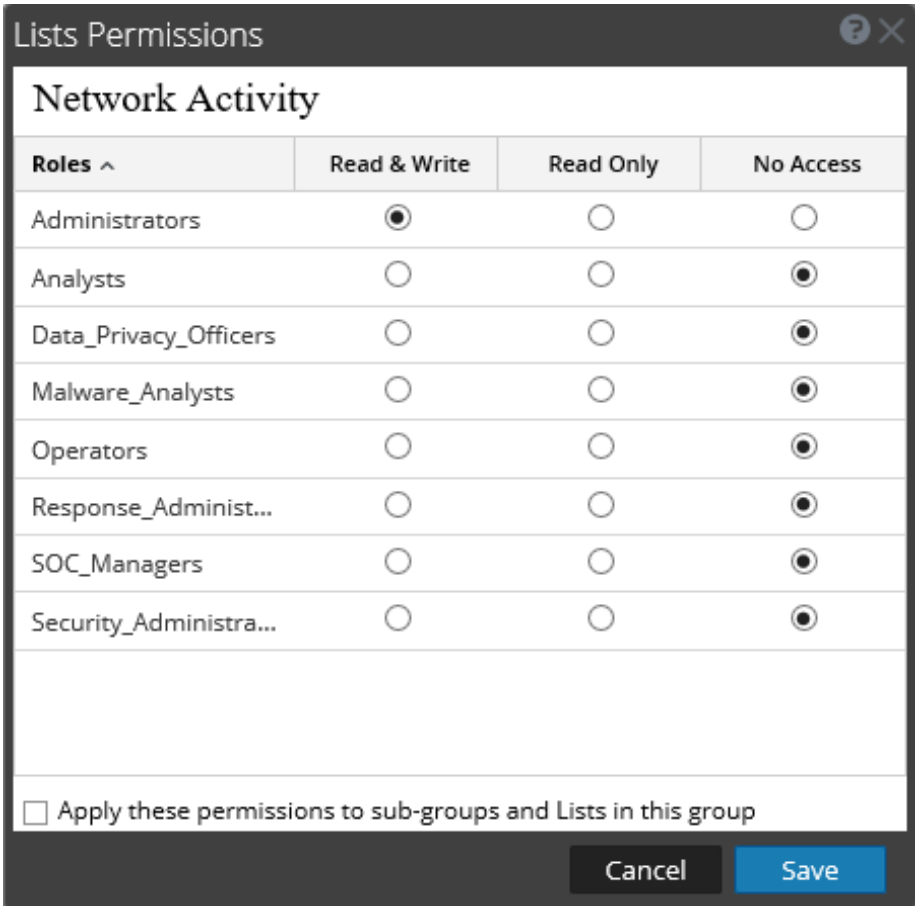
Remarque : Si un utilisateur (autre que ADMIN) crée une liste, ADMIN ne pourra pas accéder à cette liste.

Définir le contrôle d'accès pour un groupe de listes

Pour modifier les autorisations du groupe de listes, vous devez sélectionner un groupe de listes et définir leurs autorisations d'accès à l'aide du panneau Autorisations des listes.

Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez la définir au niveau du groupe de listes. Excepté pour les administrateurs, l'autorisation par défaut définie pour tous les autres rôles d'utilisateur est **Aucun accès** avant l'application des autorisations de tâche.

Vous pouvez également appliquer l'autorisation aux sous-groupes et aux listes du groupe en cochant la case.



Les scénarios suivants décrivent la définition d'autorisations pour les groupes de listes ou les sous-groupes et les listes dans les groupes :

- Scénario 1: Autorisations appliquées au groupe de listes ou sous-groupe en fonction du rôle d'utilisateur.

  Chacun des niveaux aura un ensemble d'autorisations en fonction du rôle d'utilisateur. Par exemple, s'il est attribué au groupe de listes le rôle d'analyste en sécurité, les autorisations sont définies en Lecture et écriture pour le groupe de listes.

- Scénario 2: Autorisations appliquées aux sous-groupes et aux listes dans le groupe.
  Les autorisations d'accès que vous définissez peuvent être appliquées à des sous-groupes et aux objets enfants de ce groupe. Les autorisations au niveau du groupe de listes sont héritées par les sous-groupes et les listes du groupe.

Rôle (Analystes)	Autorisations appliquées au groupe de listes ou sous-groupe en fonction du rôle d'utilisateur	Autorisations appliquées au sous-groupe et aux listes dans le groupe
Groupe	Lecture et écriture	Lecture et écriture
Sous-groupe	Lecture	Lecture et écriture - Héritée
Listes	Lecture	Lecture écriture - Héritée

Autorisation d'accès pour une liste ou un groupe de listes

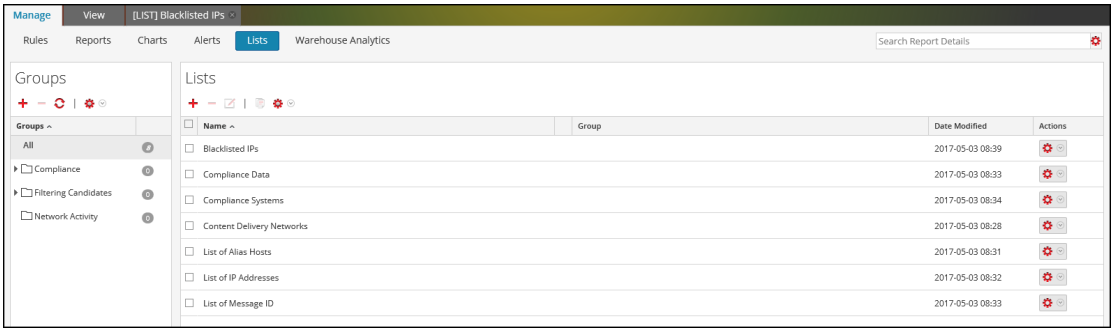
Veillez à disposer d'au moins une autorisation d'accès **en lecture et écriture** afin d'accéder aux listes ou groupes de listes.

Pour définir les autorisations d'accès pour une liste, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

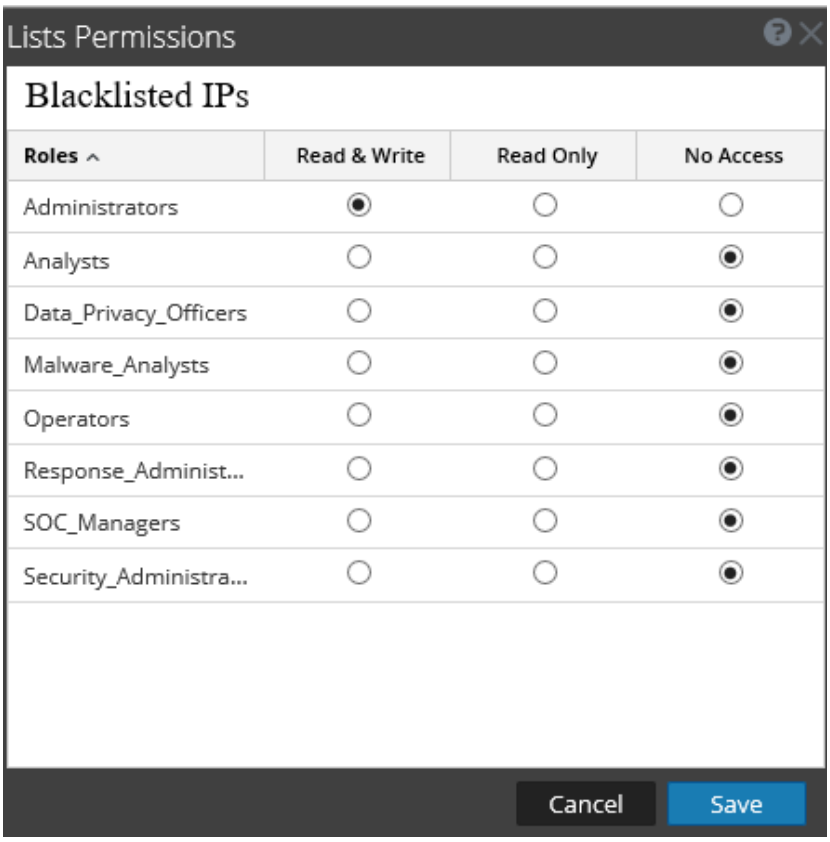
   L'onglet Gérer s'affiche.

2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Vue Liste**, sélectionnez une liste.

4. Cliquez sur  > **Autorisations** dans la barre d'outils Liste.
   La boîte de dialogue Autorisations des listes s'affiche.



5. Sélectionnez l'autorisation d'accès appropriée pour chacun des rôles d'utilisateur et cliquez sur **Enregistrer**.

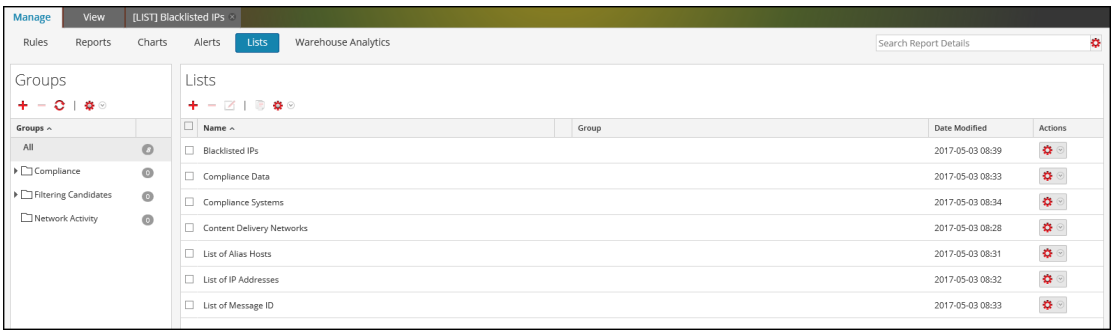
   Un message de confirmation s'affiche indiquant que l'autorisation a été définie pour la liste sélectionnée.

Pour définir le contrôle d'accès pour un groupe de listes, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

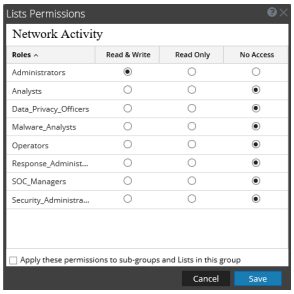
   L'onglet Gérer s'affiche.

2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Groupes de listes**, sélectionnez un groupe de listes.

4. Cliquez sur  > **Autorisations**.
   La boîte de dialogue Autorisations des listes s'affiche.



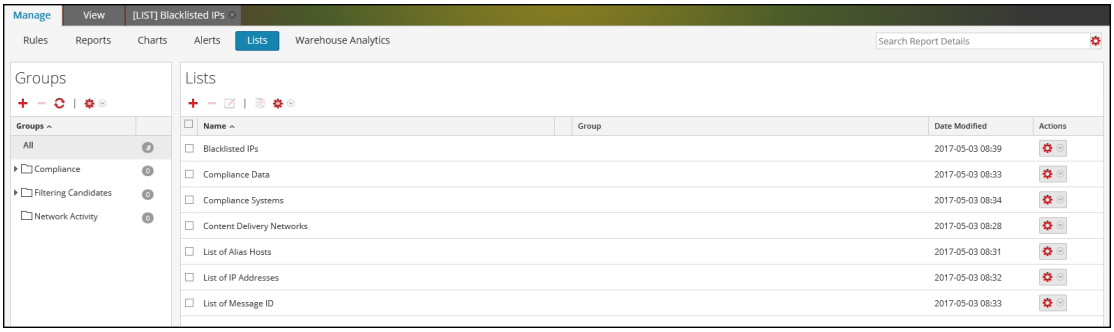
5. (Facultatif) Cochez la case appropriée pour appliquer ces autorisations à des sous-groupes et aux objets enfants de ce groupe.
6. Cliquez sur **Enregistrer**.

   Un message de confirmation s'affiche indiquant que l'autorisation a été définie pour le groupe de listes sélectionné.

Modifier une liste

Pour modifier une liste, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Vue Liste**, sélectionnez une liste que vous souhaitez modifier et procédez comme suit.
   - Cliquez sur  dans la barre d'outils Liste.
   - Dans le panneau Vue Liste, cliquez sur  > **Modifier**.

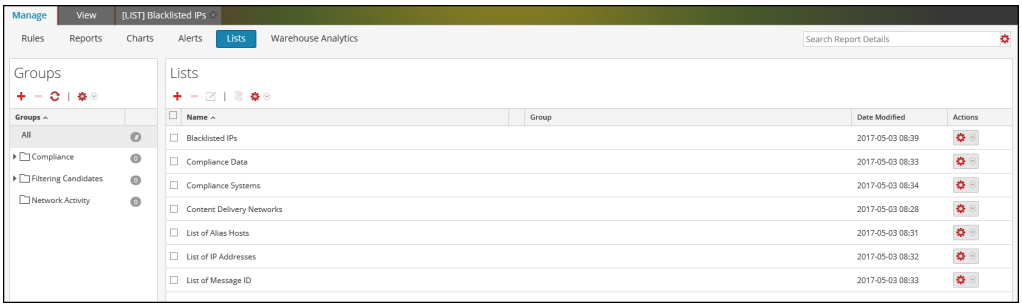
Remarque : Vous ne pouvez modifier qu'une seule liste à la fois.

4. Modifiez les champs obligatoires et ajoutez de nouvelles valeurs à la liste.
5. Cliquez sur **Enregistrer**.
   Un message de confirmation indiquant que la liste a été enregistrée correctement s'affiche.

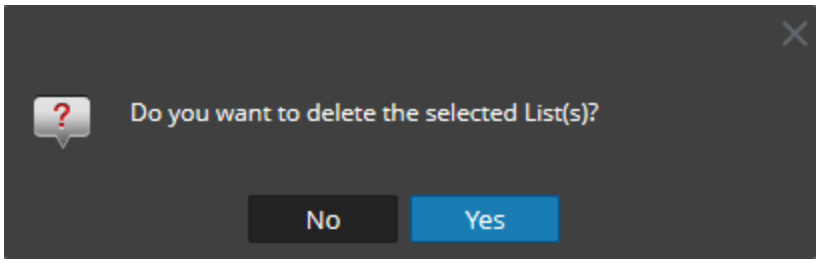
Supprimer une liste ou un groupe de listes

Pour supprimer une liste, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Vue Liste**, effectuez l'une des opérations suivantes :
   - Sélectionnez une ou plusieurs listes à supprimer et cliquez sur dans la barre d'outils **Listes**.
   - Dans la colonne **Actions**, cliquez sur > **Supprimer**.
     Une boîte de dialogue de confirmation s'affiche.



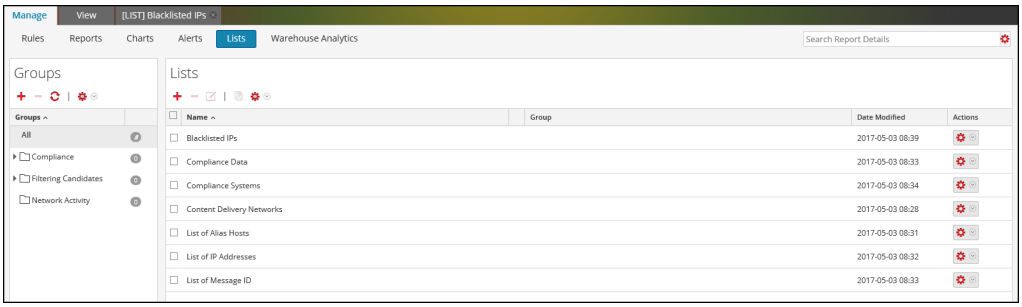
Remarque : Avant de supprimer une liste, vérifiez que cette liste n'est pas associée à une règle.

4. Cliquez sur **Oui** pour supprimer la liste.
   Un message de confirmation indiquant la suppression de la liste s'affiche et la liste

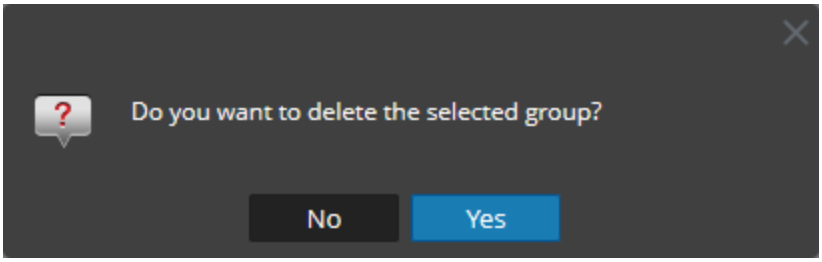
sélectionnée est supprimée du panneau Vue Liste.

Pour supprimer un groupe de listes, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Groupes de listes**, sélectionnez le groupe et cliquez sur .
   Une boîte de dialogue de confirmation s'affiche.



Attention : Si vous supprimez un groupe, tous les sous-groupes et toutes les listes de ce groupe sont supprimés.

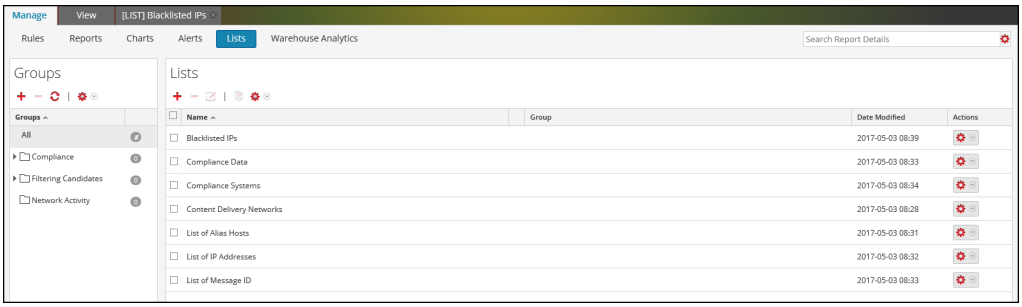
4. Cliquez sur **Oui** pour supprimer le groupe sélectionné.

Remarque : Si vous tentez de supprimer un groupe de listes qui contient des listes référencées dans une règle, un message d'avertissement s'affiche indiquant que **les listes sont référencées dans une règle**.

Dupliquer une liste

Pour dupliquer une liste, effectuez les étapes suivantes :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Vue Liste**, sélectionnez une liste à dupliquer.

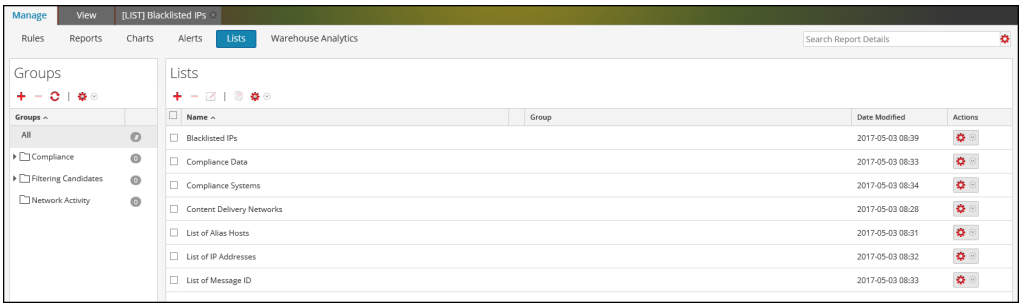
   Remarque : Vous ne pouvez dupliquer qu'une liste à la fois.

4. Dans la barre d'outils **Liste**, cliquez sur .

Exporter une liste ou un groupe de listes

Pour exporter une liste, effectuez les étapes suivantes :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Vue Liste**, effectuez l'une des opérations suivantes :

   - Sélectionnez une liste, puis cliquez sur  > **Exporter** dans la barre d'outils Liste.
   - Dans la colonne **Actions**, cliquez sur  > **Exporter**

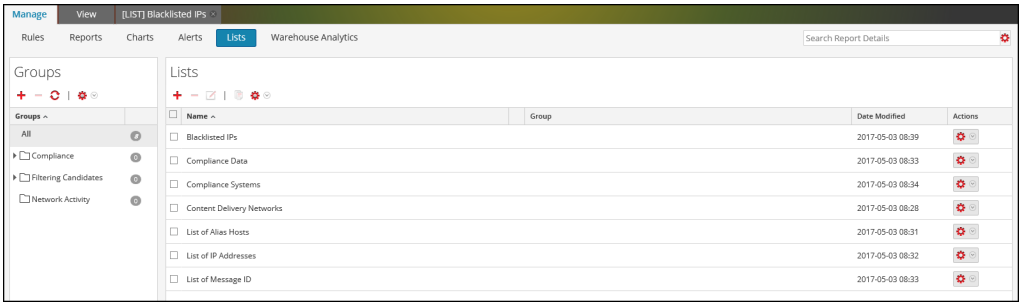
   Vous pouvez exporter plusieurs listes à la fois. Pour sélectionner plusieurs listes, sélectionnez la case à cocher des listes à exporter. Une boîte de dialogue d'exportation spécifique au navigateur peut s'afficher, vous permettant d'ouvrir ou d'enregistrer le fichier.

   Remarque : Vous ne pouvez exporter qu'une liste à la fois.

Pour exporter un groupe de listes, effectuez les étapes suivantes :

Vous pouvez exporter des groupes de listes sélectionnés dans un fichier externe qui pourra être importé ultérieurement dans NetWitness Suite. Si aucun élément n'est sélectionné dans le panneau Librairie de liste, l'arborescence des listes intégrale est exportée. Lorsque vous exportez, le résultat est un fichier d'exportation unique au format binaire.

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



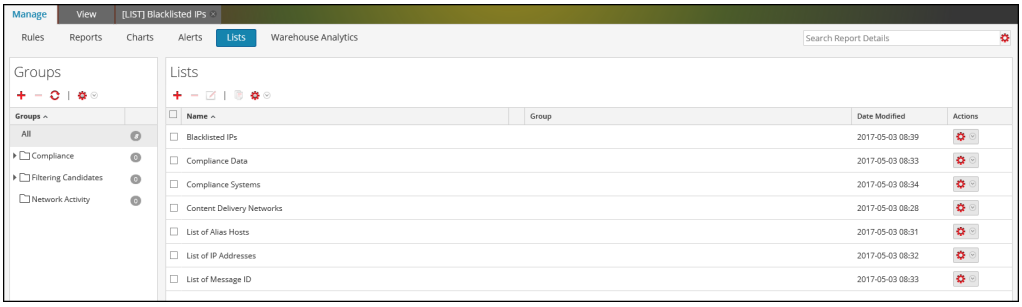
3. Dans le panneau **Groupes de listes**, sélectionnez le groupe de listes contenant les listes à exporter.
4. Cliquez sur  > **Exporter**
   .Vous pouvez exporter plusieurs groupes de listes à la fois. Pour sélectionner plusieurs groupes de listes, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les groupes de listes à exporter. Le fichier exporté est enregistré sur le disque local.

Importer une liste ou un groupe de listes

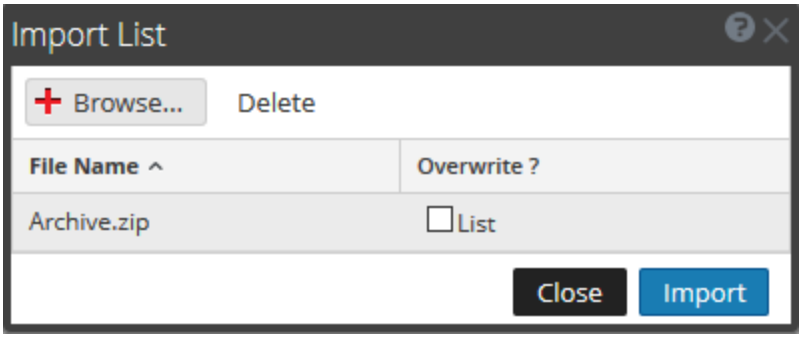
Pour importer une liste, procédez comme suit :

Vous pouvez importer des listes d'instances de NetWitness Suite dans l'arborescence du panneau de la vue Liste. Les listes doivent figurer dans un fichier binaire valide exporté depuis une instance de NetWitness Suite.

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans la barre d'outils **Liste**, cliquez sur  > **Importer**.
   La boîte de dialogue Importer la liste s'affiche. Vous pouvez importer plusieurs listes à la fois. Pour sélectionner plusieurs listes, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les groupes de listes à importer.
4. Cliquez sur **Parcourir** et sélectionnez le fichier archivé qui contient les listes.



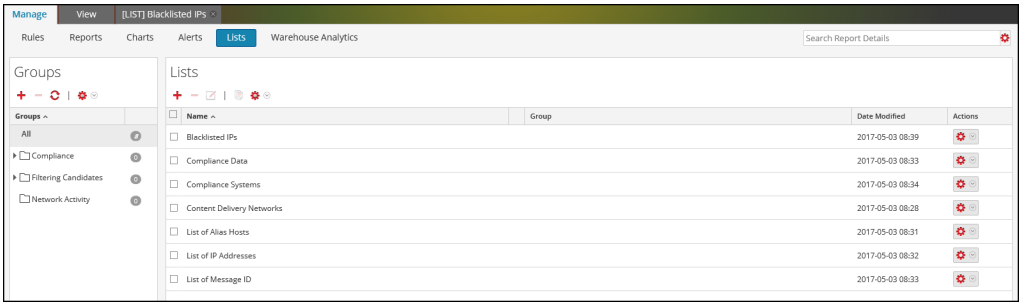
5. Cliquez sur **Importer**.

Remarque : Pendant le processus d'importation, s'il existe une liste dupliquée et que vous ne sélectionnez pas l'option Remplacer, la liste est importée et aucun message concernant les listes dupliquées ne s'affiche.

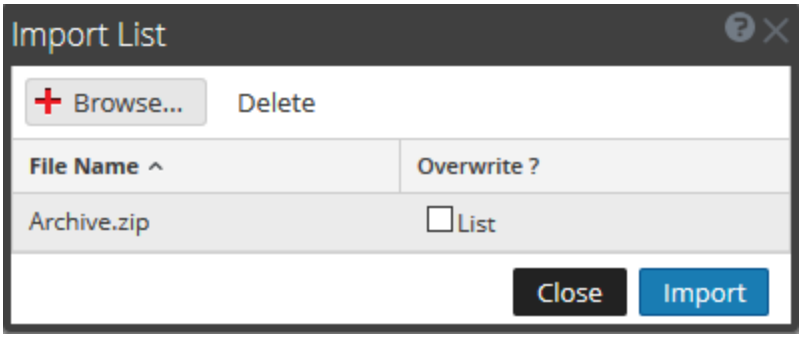
Pour importer un groupe de listes, procédez comme suit :

Vous pouvez importer des groupes de listes provenant d'instances de NetWitness Suite dans l'arborescence du panneau de la vue Groupes de listes. Les listes doivent figurer dans un fichier binaire valide exporté depuis une instance de NetWitness Suite.

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Liste s'affiche.



3. Dans le panneau **Groupes de listes**, cliquez sur  > **Importer**.
   La boîte de dialogue Importer la liste s'affiche.
4. Cliquez sur **Parcourir** et sélectionnez le fichier archivé qui contient les groupes de listes.



   Vous pouvez importer plusieurs groupes de listes à la fois. Pour sélectionner plusieurs groupes de listes, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les groupes de listes à importer.
5. Cliquez sur **Importer**.

Remarque : Pendant le processus d'importation, s'il existe un groupe de listes dupliqué et que vous ne sélectionnez pas l'option Remplacer, le groupe de listes est importé et aucun message concernant le groupe de listes dupliqué ne s'affiche.

Gérer une règle

Contrôle d'accès pour une règle et un groupe de règles

Pour définir les autorisations d'accès dont l'utilisateur bénéficiera selon son rôle afin de gérer une règle ou un groupe de règles. Le Reporting fournit un contrôle d'accès au niveau de la règle et du groupe de règles. Seul un utilisateur disposant de l'ensemble d'autorisations approprié peut effectuer les tâches du Reporting. Le contrôle d'accès est géré par l'administrateur à partir de l'onglet **ADMIN > Sécurité > Rôles**.

Lorsqu'il crée des utilisateurs et des rôles d'utilisateur, l'administrateur doit s'assurer que les rôles créés pour les tâches spécifiques ont accès à toutes les autorisations supérieures dans la hiérarchie de rôles.

Les règles et les groupes de règles peuvent être liés à un ensemble spécifique de rôles d'utilisateur de telle sorte que lorsqu'un utilisateur se connecte à NetWitness Suite, les seules règles auxquelles il peut accéder sont celles qui sont accessibles par le groupe auquel il appartient. Les utilisateurs appartenant à un rôle d'utilisateur avec le droit d'accès « Lecture et écriture » doivent posséder des privilèges d'accès complets sur la règle. En outre, l'accès peut être limité pour que les règles ne soient accessibles que par ceux qui ont l'accès en « lecture seule ».

Remarque : Vous devez avoir au moins l'autorisation de « Lecture seule » pour un groupe pour afficher les règles de ce groupe.

Au niveau de la règle, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur :

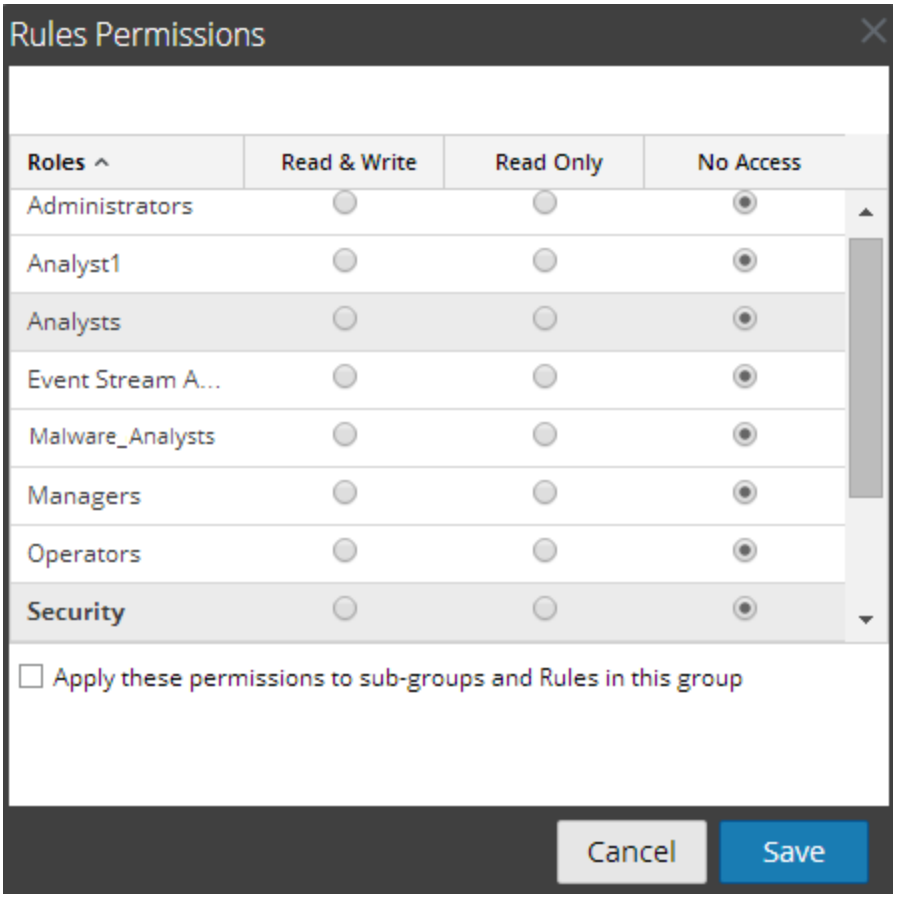
- Lecture et écriture
- Lecture seule
- Aucun accès

Supposons que vous souhaitiez que les **analystes de la sécurité** aient accès à toutes les règles d'un groupe de règles, vous pourriez alors définir l'autorisation **Lecture et écriture** au niveau du Groupe de règles. Et si vous ne souhaitez pas que le rôle **Opérateur** ait accès à un ensemble spécifique de règles dans un groupe de règles, vous pouvez définir l'autorisation **Aucun accès** au niveau du Groupe de règles. L'autorisation n'est configurée que pour le groupe de règles, et non les règles ou les sous-groupes dans le groupe de règles.

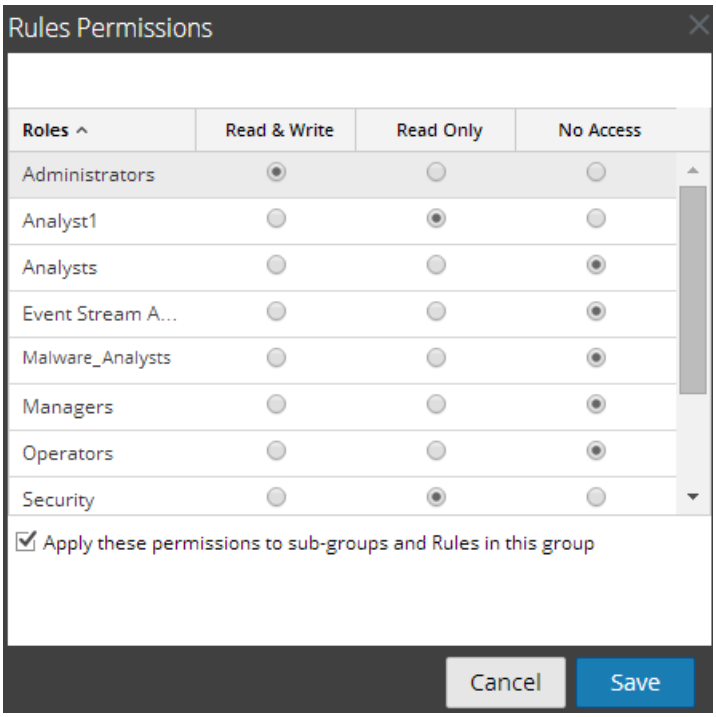
Contrôle d'accès pour un groupe de règles

Lorsque vous souhaitez modifier les autorisations du groupe de règles, vous devez sélectionner un groupe de règles et définir les autorisations d'accès à l'aide du panneau Autorisations des règles.

Avant d'appliquer les autorisations des groupes de règles, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « Aucun accès » et les cases sont décochées.



Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez le faire au niveau du groupe de règles, comme l'indique la figure. Supposons que vous souhaitiez que les **administrateurs** aient accès à toutes les règles d'un groupe de règles, vous pourriez alors définir l'autorisation **Lecture et écriture** dans le panneau Autorisations sur les groupes de règles.



Vous pouvez également appliquer des autorisations aux sous-groupes et aux règles du groupe en cochant la case.

Ces deux scénarios sont expliqués brièvement :

- Scénario 1 : Autorisations appliquées au groupe de règles, au sous-groupe et aux règles en fonction du rôle d'utilisateur.
- Scénario 2 : Autorisations appliquées au sous-groupe et aux règles dans le groupe.

Rôle (Analystes)	Autorisations appliquées au groupe de règles, au sous-groupe et aux règles en fonction du rôle d'utilisateur.	Autorisations appliquées au sous-groupe et aux règles dans le groupe.
Groupe	**Lecture et écriture**	**Lecture et écriture**
Sous-groupe	**Lecture**	**Lecture et écriture - Héritée**
Règles	**Lecture**	**Lecture et écriture - Héritée**

Les autorisations d'accès que vous définissez peuvent être appliquées à des sous-groupes et aux objets enfants de ce groupe.

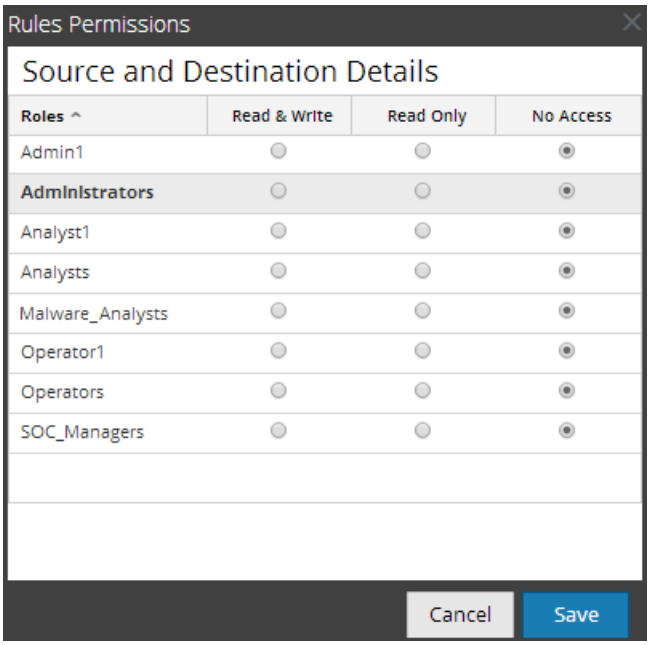
Il sera attribué au groupe de règles le rôle d'un **Analyste de sécurité** et les autorisations sont définies en **Lecture et écriture** du groupe de règles.

Pour le scénario 1, chacun des niveaux aura un ensemble d'autorisations en fonction du rôle d'utilisateur. Pour le scénario 2, les autorisations au niveau du groupe de règles sont héritées par le sous-groupe et les règles du groupe.

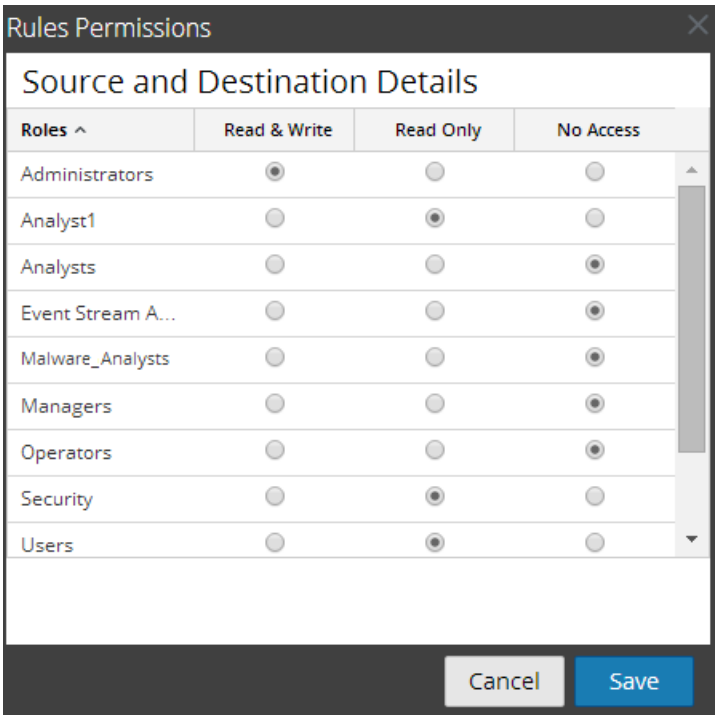
Contrôle d'accès pour une règle

Lorsque vous souhaitez modifier les autorisations des règles, vous devez sélectionner une règle et définir leurs autorisations d'accès à l'aide du panneau Autorisations des règles.

Avant d'appliquer les autorisations des règles, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « Aucun accès » et la case est décochée.



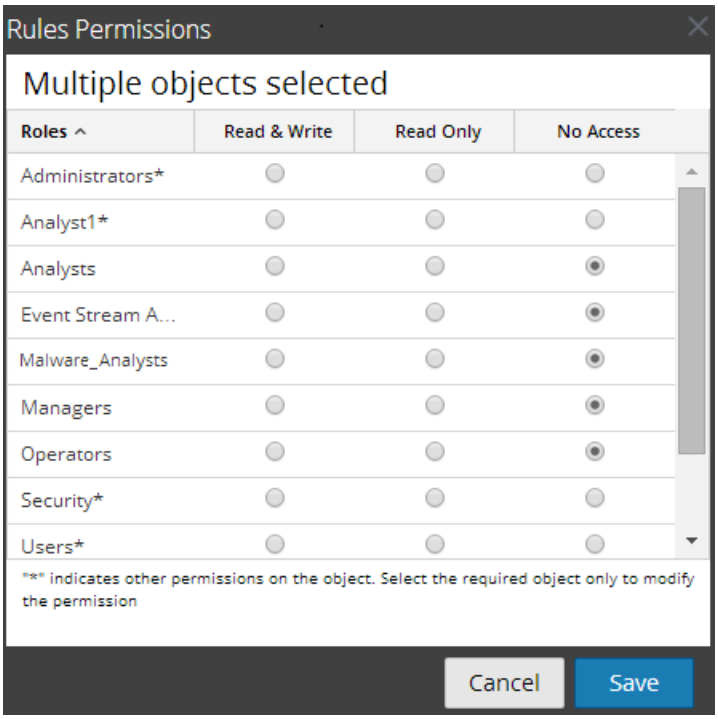
Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez définir cela au niveau de la règle, comme le montre la figure. Supposons que vous souhaitiez que les **Administrateurs** aient accès à toutes les règles d'un groupe de règles, vous pouvez définir l'autorisation **Lecture et écriture** dans le panneau Autorisations de la règle.



Contrôle d'accès pour une règle lorsque plusieurs règles sont sélectionnées

Lorsque vous souhaitez modifier les autorisations de plusieurs règles, vous pouvez sélectionner plusieurs règles simultanément et paramétrer leurs autorisations d'accès dans le panneau Autorisations des règles. L'autorisation d'accès que vous choisissez s'applique à toutes les règles sélectionnées.

Remarque : Le caractère « * » en regard du nom du rôle indique les autres autorisations disponibles pour le rôle d'utilisateur. Si vous souhaitez modifier l'autorisation d'accès du rôle d'utilisateur requis, sélectionnez le rôle d'utilisateur et modifiez l'autorisation d'accès.



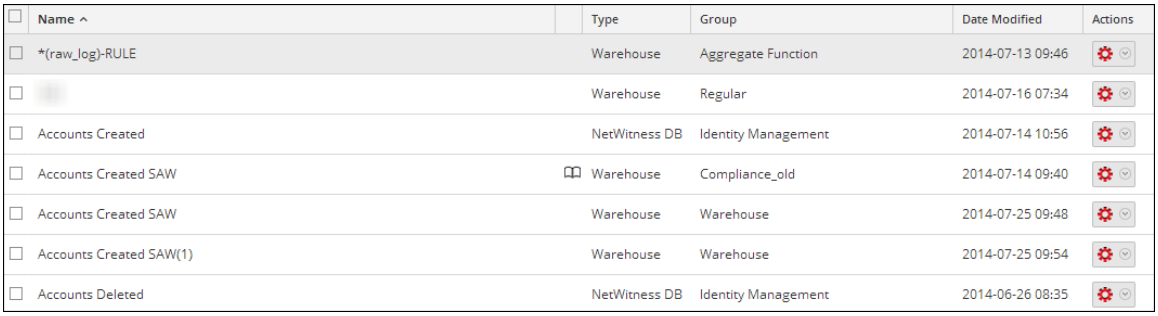
Se connecter en tant qu'utilisateur spécifique et afficher les détails d'accès

Lorsque vous vous connectez à l'interface utilisateur de NetWitness Suite en tant qu'utilisateur avec une autorisation de lecture seule, toutes les règles sont annotées du symbole (🕮). Lorsque vous cliquez sur ce symbole, la légende « Lecture seule » s'affiche dans le panneau Liste de règles.

Lorsque vous vous connectez à l'interface utilisateur de NetWitness Suite

en tant qu'utilisateur ne détenant pas l'autorisation d'accès en lecture/écriture à une règle, toutes les règles sont marquées du symbole et elles sont grisées dans le panneau Liste des règles.

La figure suivante montre le panneau Liste des règles d'un utilisateur connecté avec l'autorisation d'accès en lecture/écriture minimale.



Remarque : Si un utilisateur (autre que l'administrateur) crée une règle, ADMIN ne pourra pas accéder à cette règle.

Liste tabulaire

Le tableau suivant répertorie les colonnes du panneau Autorisations des règles :

Colonne	Description
Rôles	Le rôle de l'utilisateur connecté dans l'interface utilisateur de NetWitness Suite.
Lecture et écriture	L'utilisateur peut accéder, afficher, modifier, importer et exporter les règles de la vue Règles. L'utilisateur ne peut pas modifier l'autorisation dans la règle.
Lecture seule	L'utilisateur peut uniquement accéder à la règle et l'afficher dans la vue Règles.
Aucun accès	L'utilisateur ne peut pas accéder à la règle pour laquelle cette autorisation est définie, ou l'afficher.

Définir le contrôle d'accès pour une règle

Vous pouvez définir le contrôle d'accès pour une règle. Le Reporting Engine fournit un contrôle d'accès au niveau de la règle. Seul un utilisateur possédant le bon ensemble d'autorisations peut effectuer des tâches sur la règle. Lorsqu'il crée des utilisateurs et rôles, l'administrateur doit s'assurer que les rôles créés pour les tâches spécifiques ont accès à toutes les autorisations supérieures dans la hiérarchie de rôles.

Au niveau de la règle, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness Suite :

- Lecture et écriture – Affichez ou modifiez les règles dans le groupe de règles.
- Lecture seule – Affichez les règles dans le groupe de règles.
- Aucun accès – Vous ne pouvez pas afficher ou modifier les règles dans le groupe de règles.

Conditions préalables

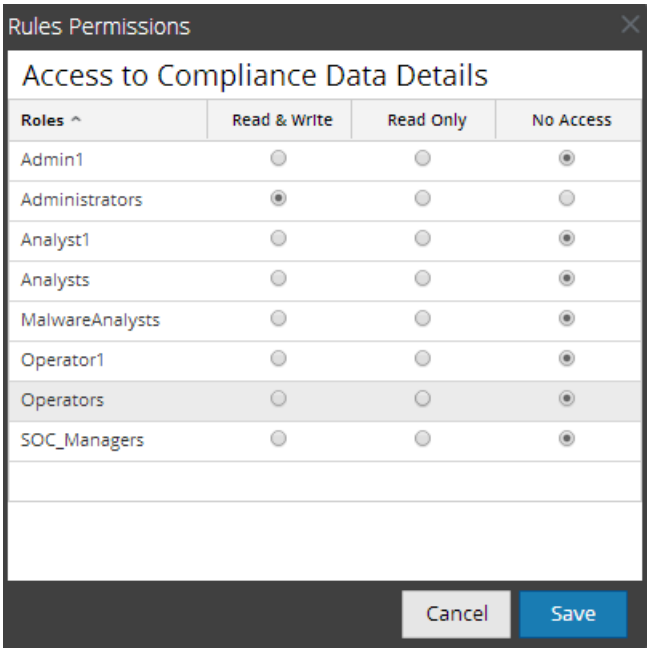
Veillez à disposer d'une autorisation d'accès minimale en lecture et écriture pour définir les autorisations d'accès d'une règle.

Pour définir le contrôle d'accès pour une règle, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau de la liste de **Règles**, sélectionnez la règle.

3. Cliquez sur  > **Autorisations** dans la barre d'outils Règle.

   La boîte de dialogue **Autorisations des règles** s'affiche.



4. Sélectionnez l'autorisation d'accès appropriée pour le rôle d'utilisateur, puis cliquez sur **Enregistrer**.

   - Lecture et écriture
   - Lecture seule
   - Aucun accès

Définir le contrôle d'accès pour un groupe de règles

Vous pouvez définir le contrôle d'accès au niveau du groupe de règles. Seul un utilisateur possédant le bon ensemble d'autorisations peut effectuer les tâches sur la règle. Lorsqu'il crée des utilisateurs et rôles, l'administrateur doit s'assurer que les rôles créés pour les tâches spécifiques ont accès à toutes les autorisations supérieures dans la hiérarchie de rôles.

Au niveau du groupe de règles, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness Suite :

- Lecture et écriture – Affichez ou modifiez les règles dans le groupe de règles.
- Lecture seule – Affichez les règles dans le groupe de règles.
- Aucun accès – Vous ne pouvez pas afficher ou modifier la règle dans les groupes de règles.

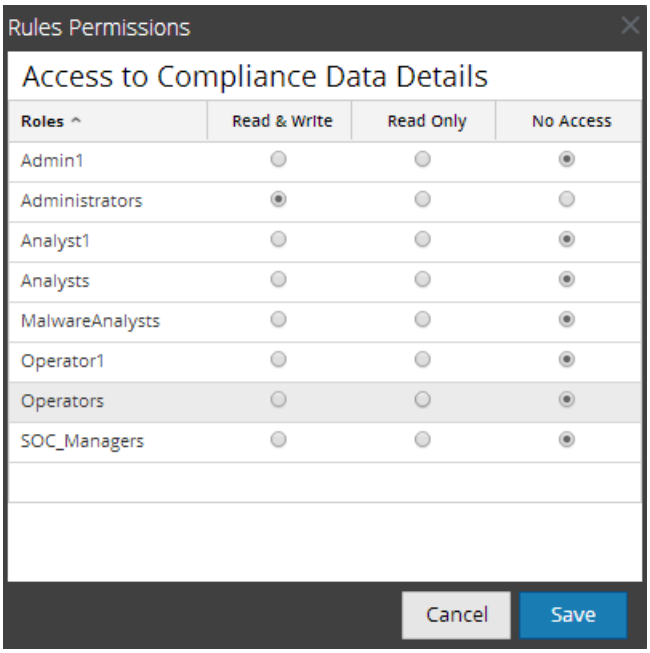
Conditions préalables

Veillez à disposer d'une autorisation d'accès minimale en lecture et écriture pour définir les autorisations d'accès d'un groupe de règles.

Pour définir le contrôle d'accès pour un groupe de règles, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau **Groupes de règles**, sélectionnez le groupe de règles et effectuez l'une des actions suivantes :
   - Cliquez sur  et sélectionnez **Autorisations**.
   - Cliquez avec le bouton droit de la souris sur le groupe de règles sélectionné et choisissez **Autorisations**.

   La boîte de dialogue **Autorisations des règles** s'affiche.



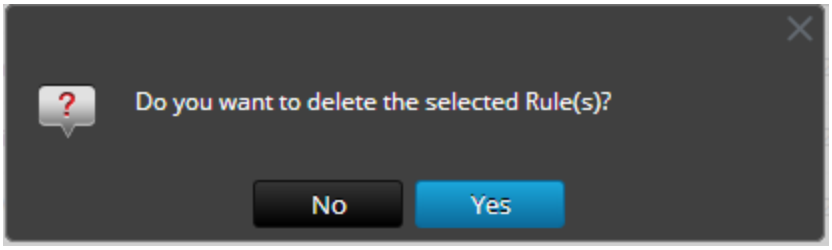
3. (Facultatif) Cochez la case appropriée pour appliquer ces autorisations à des sous-groupes et aux objets enfants de ce groupe.
4. Cliquez sur **Enregistrer**.
   Un message de confirmation de la définition de l'autorisation pour le groupe de règles sélectionné s'affiche.

Supprimer une règle ou un groupe de règles

Pour supprimer une règle, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau **Règles**, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle et cliquez sur dans la barre d'outils Règle.
   - Cliquez sur > **Supprimer**.

     Une boîte de dialogue de confirmation s'affiche.



Remarque : Si une règle est en cours d'utilisation dans un rapport, un avertissement s'affiche indiquant que la règle est en cours d'utilisation et ne peut pas être supprimée.

3. Cliquez sur **Oui** pour supprimer la règle.

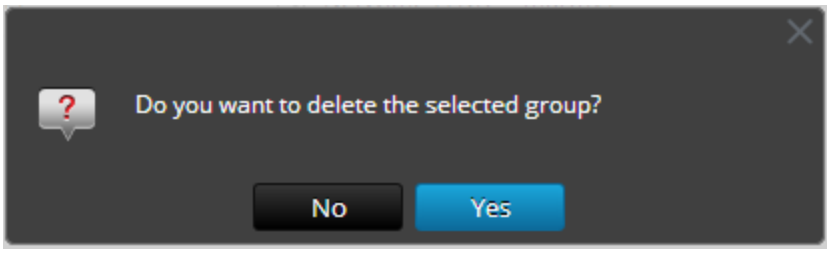
   Un message de confirmation indiquant que la suppression de la règle s'est déroulée correctement s'affiche et la règle sélectionnée est supprimée du panneau Liste de règles.

Pour supprimer un groupe de règles, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.
2. Dans le panneau **Groupes de règles**, sélectionnez le groupe de règles que vous souhaitez supprimer.
3. Cliquez sur .

   Une boîte de dialogue de confirmation s'affiche.



Remarque : Si l'une des règles du groupe est utilisée dans des rapports, un avertissement s'affiche indiquant que la règle est en cours d'utilisation et ne peut pas être supprimée.

4. Cliquez sur **Oui** pour supprimer le groupe.

   Un message de confirmation de la suppression du groupe s'affiche et le groupe sélectionné est supprimé du panneau Groupes de règles.

Dupliquer une règle

Pour dupliquer une règle, effectuez les étapes suivantes :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau de liste **Règles**, sélectionnez la règle à dupliquer.
3. Dans la barre d'outils, cliquez sur  .

Modifier une règle

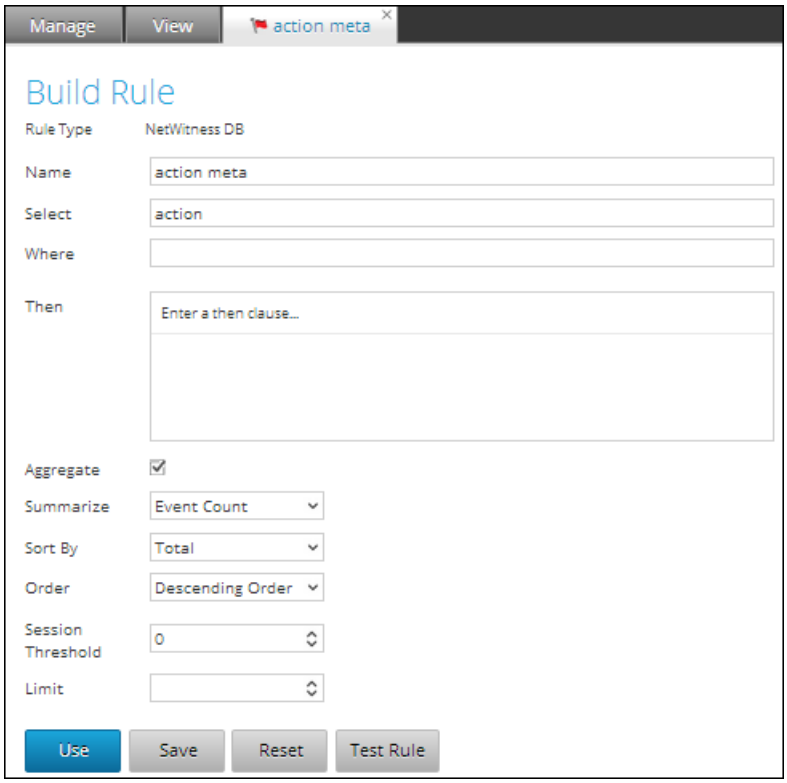
Conditions préalables

Pour modifier une règle, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau **Liste de règles**, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle et cliquez sur  dans la barre d'outils Règle.

- Cliquez sur  > **Modifier**.

  L'onglet de la vue Élaborer une règle s'affiche.



Remarque : Si une règle est modifiée, la définition de règle mise à jour est appliquée aux rapports, graphiques et alertes qui contiennent cette règle.

3. Modifiez les champs obligatoires.
4. Cliquez sur **Enregistrer**.

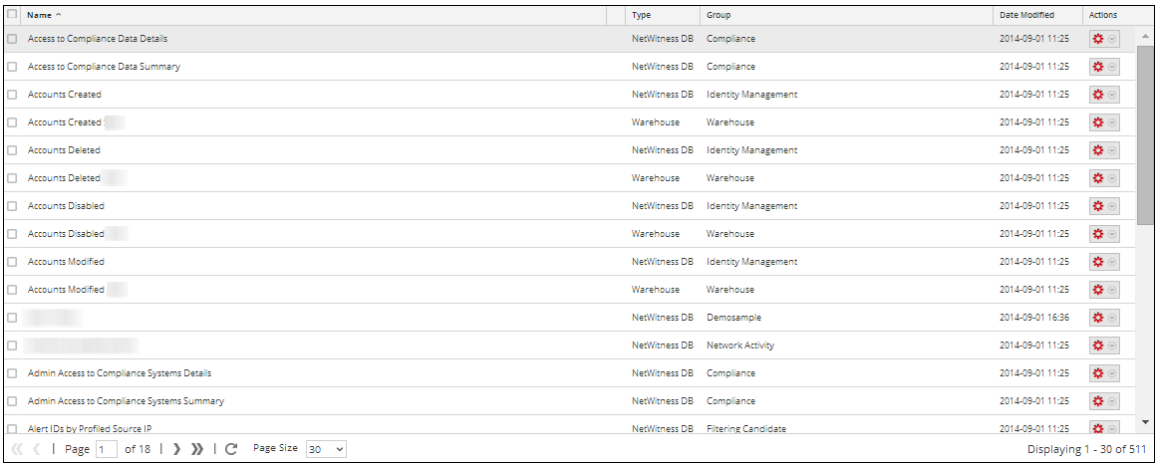
   Un message de confirmation de l'enregistrement de la règle s'affiche.

Lorsque vous modifiez une règle, veillez à sélectionner de nouveau la règle pour laquelle vous souhaitez que le graphique soit généré, de sorte que la règle modifiée soit appliquée. Si vous ne resélectionnez pas la règle et tentez d'enregistrer ou de tester la règle, la règle est enregistrée et un message d'avertissement s'affiche.

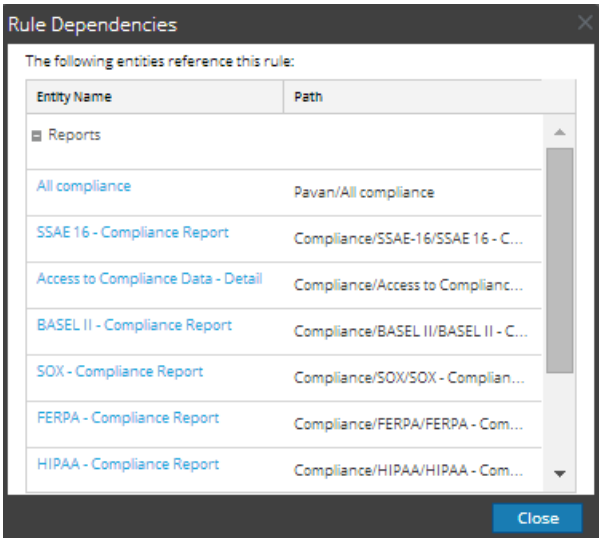
Afficher les dépendances d'une règle

Vous pouvez afficher les dépendances d'une règle. Vous devez parcourir une liste de règles, sélectionner une règle dont vous voulez identifier la dépendance pour un rapport, un graphique ou une alerte.

La figure suivante illustre la vue Règle dans laquelle vous sélectionnez la règle "Accès aux données de conformité".



La figure suivante illustre la dépendance de la règle pour les alertes et les rapports.



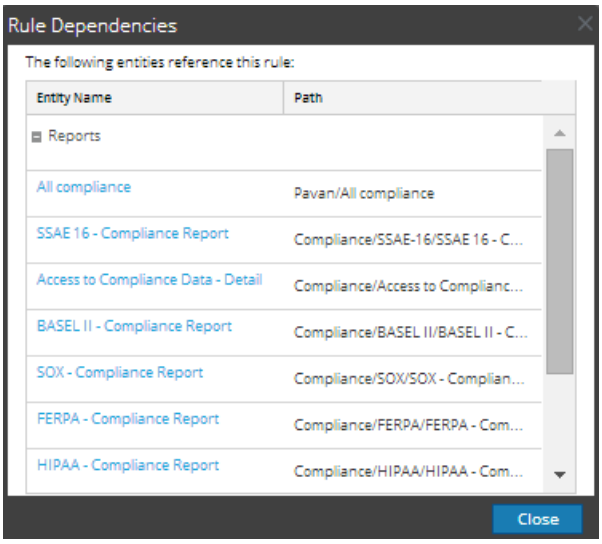
Le tableau suivant répertorie les différentes colonnes de la boîte de dialogue Dépendances des règles avec leur description.

Colonne	Description
Nom de l'entité	Nom de l'entité qui fait référence à la règle.
Chemin	Chemin d'accès à l'entité dans l'interface utilisateur.

Pour afficher les dépendances d'une règle, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Règles**.
   La vue Règle s'affiche.

3. Dans le panneau **Liste de règles**, cliquez sur  > Dépendances
. La boîte de dialogue Dépendances des règles s'affiche.



Exporter une règle ou un groupe de règles

Conditions préalables

Assurez-vous que vous disposez de règles dans le groupe de règles.

Pour exporter une règle, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
L'onglet Gérer s'affiche.
2. Dans le panneau **Liste de règles**, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle et cliquez sur  > **Exporter** dans la barre d'outils Règle.
   - Cliquez sur  > **Exporter**.

   Une boîte de dialogue d'exportation spécifique au navigateur peut s'afficher, vous permettant d'ouvrir ou d'enregistrer le fichier. Vous pouvez exporter plusieurs règles à la fois. Pour sélectionner plusieurs règles, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les règles à exporter.

Remarque : Pour exporter plusieurs règles, il est nécessaire d'exporter des groupes de règles.

Pour exporter un groupe de règles, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
L'onglet Gérer s'affiche.

2. Dans le panneau **Groupes de règles**, sélectionnez le groupe contenant les règles à exporter. Vous pouvez exporter plusieurs groupes de règles à la fois. Pour sélectionner plusieurs groupes de règles, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les groupes de règles à exporter.
3. Cliquez sur  > **Exporter**.
   Une boîte de dialogue d'exportation spécifique au navigateur peut s'afficher, vous permettant d'ouvrir ou d'enregistrer le fichier.

Gérer un rapport

Contrôle d'accès pour un rapport ou un groupe de rapports

Cette section couvre les autorisations d'accès dont l'utilisateur bénéficie selon son rôle, pour gérer un rapport ou un groupe de rapports. Le Reporting fournit un contrôle d'accès au niveau du rapport et du groupe de rapports. L'utilisateur disposant de l'ensemble d'autorisations approprié peut uniquement effectuer les tâches du module Reporting. Le contrôle d'accès est géré par l'administrateur à partir de l'onglet **ADMIN > Sécurité > Rôles**.

Lorsqu'il crée des utilisateurs et des rôles d'utilisateur, l'administrateur doit s'assurer que les rôles créés pour les tâches spécifiques ont accès à toutes les autorisations supérieures dans la hiérarchie de rôles.

Les rapports et groupes de rapports peuvent être liés à un ensemble spécifique de rôles d'utilisateur. Ainsi, lorsqu'un utilisateur se connecte à NetWitness Suite, il peut afficher les rapports associés aux privilèges d'accès du rôle d'utilisateur spécifique. Les utilisateurs dont le rôle d'utilisateur dispose de l'autorisation d'accès en Lecture et écriture peuvent définir des rapports. En outre, l'accès aux rapports peut être restreint aux seuls utilisateurs disposant de l'autorisation d'accès en Lecture seule.

Remarque : Vous devez avoir l'autorisation de Lecture seule sur un groupe pour afficher les rapports de ce groupe.

Au niveau du rapport, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness Suite :

- Lecture et écriture
- Lecture seule
- Aucun accès

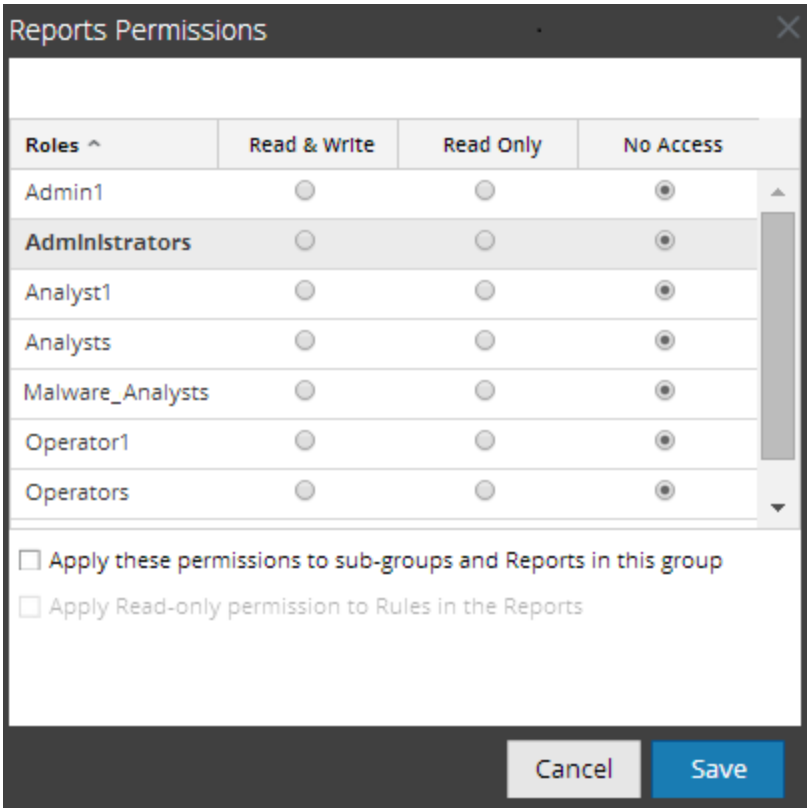
Supposons que vous souhaitiez que les NetWitness Suite aient accès à tous les rapports d'un groupe de rapports, vous pourriez alors définir l'autorisation **Lecture et écriture** au niveau du groupe de rapports. Et si vous ne souhaitez pas que le rôle **Opérateur** ait accès à un ensemble spécifique de rapports dans un groupe de rapports, vous pouvez définir l'autorisation **Aucun accès** au niveau du groupe de rapports.

L'autorisation n'est configurée que pour le groupe de rapports, et non les rapports, les règles ou les sous-groupes dans le groupe de rapports.

Contrôle d'accès pour un groupe de rapports

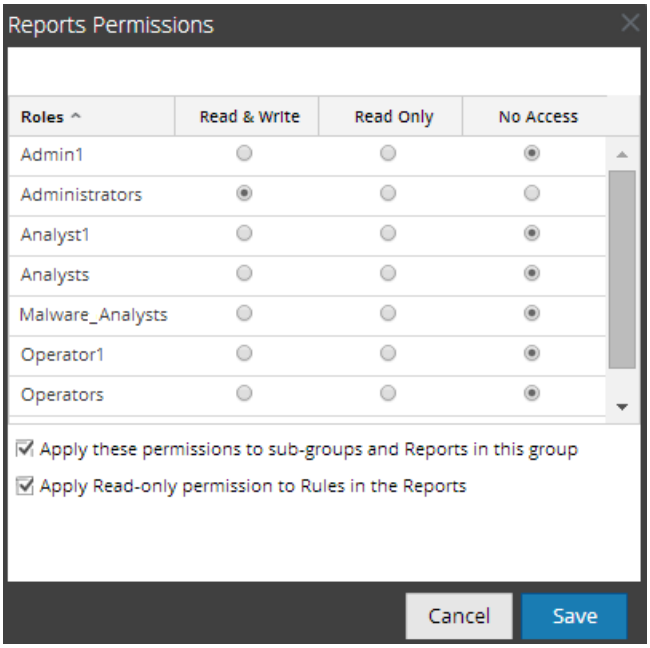
Lorsque vous souhaitez modifier les autorisations du groupe de rapports, vous devez sélectionner un groupe de rapports et définir les autorisations d'accès à l'aide du panneau Autorisations des rapports.

Avant d'appliquer les autorisations des groupes de rapports, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « Aucun accès », sauf pour les administrateurs, comme l'indique la figure.



Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez définir cela au niveau du groupe de rapports, comme le montre la figure. Supposons que vous souhaitiez que les administrateurs aient accès à tous les rapports d'un groupe de rapports, vous pouvez définir l'autorisation **Lecture et écriture** dans le panneau Autorisations des groupes de rapports.

Vous pouvez également appliquer des autorisations à des sous-groupes et rapports dans le groupe, mais aussi appliquer des autorisations en lecture seule aux règles dans les rapports en cochant les cases appropriées, comme l'indique la figure.



Ces trois scénarios sont expliqués brièvement :

- Scénario 1 : Autorisations appliquées au groupe de rapports, au sous-groupe et au rapport en fonction du rôle d'utilisateur.
- Scénario 2 : Autorisations appliquées au sous-groupe et au rapport dans le groupe.
- Scénario 3 : Autorisation de lecture seule appliquée aux règles du rapport.

	Rôle (Analyste)	Autorisations appliquées au groupe de rapports, au sous-groupe et au rapport en fonction du rôle d'utilisateur	Autorisations appliquées au sous-groupe et au rapport dans le groupe	Autorisation (Lecture seule) appliquée aux règles du rapport
Groupe	Lecture et écriture	**Lecture et écriture**	**Lecture et écriture**	Lecture et écriture
Sous-groupe	Lecture	**Lecture**	**Lecture et écriture - Héritée**	Lecture et écriture
Rapport	Lecture	**Lecture**	**Lecture et écriture - Héritée**	Lecture et écriture
Règles	Lecture	**Lecture**	Lecture	**Lecture**

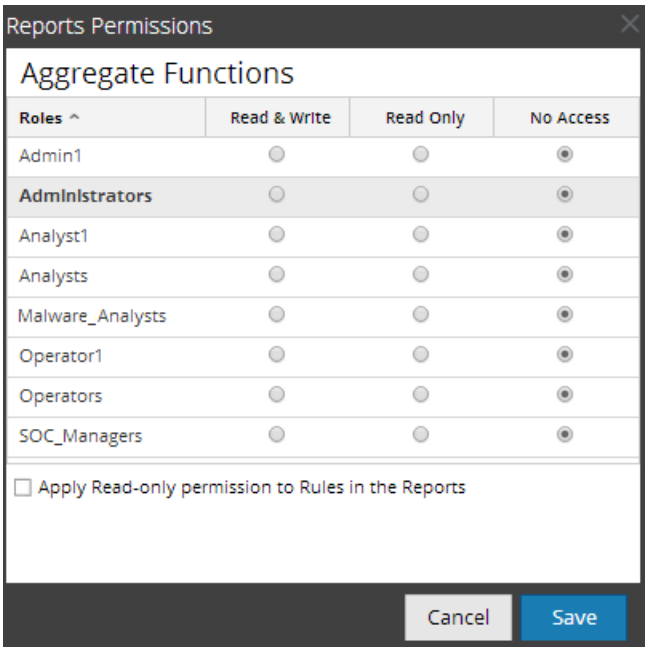
Il sera attribué au groupe de rapports le rôle d'un **Analyste de sécurité** et les autorisations sont définies en **Lecture et écriture** du groupe de rapports.

Pour le scénario 1, chacun des niveaux a un ensemble d'autorisations en fonction du rôle d'utilisateur. Pour le scénario 2, les autorisations au niveau du groupe de rapports (Lecture et écriture) sont héritées par le sous-groupe et les rapports dans le groupe. Pour le scénario 3, l'autorisation de lecture est définie pour les règles, sauf que l'ensemble d'autorisations pour les règles ne peut pas être supérieur aux autorisations définies pour le groupe de rapports.

Contrôle d'accès pour un rapport

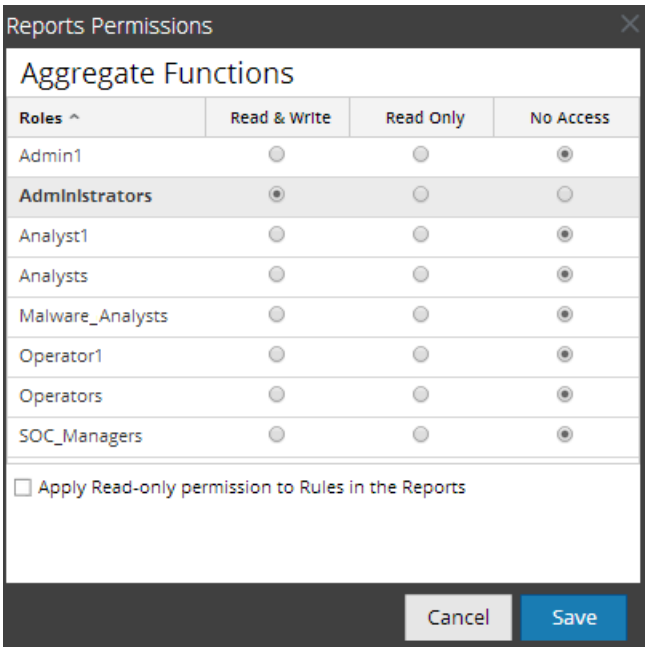
Lorsque vous souhaitez modifier les autorisations d'un rapport, vous devez sélectionner un rapport et définir ses autorisations d'accès à l'aide du panneau Autorisations des rapports.

Avant d'appliquer les autorisations des rapports, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « Aucun accès » et la case est décochée, comme l'indique la figure.



Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez définir cela au niveau du rapport, comme le montre la figure. Supposons que vous souhaitiez que les **administrateurs** aient accès à un rapport spécifique, vous pouvez définir l'autorisation **Lecture et écriture** dans le panneau Autorisations de rapport.

Vous pouvez appliquer l'autorisation de lecture seule aux règles des rapports en cochant la case, comme indiqué dans la figure.



Ces deux scénarios sont expliqués brièvement :

- Scénario 1 : Autorisations appliquées au groupe de rapports, au sous-groupe, au rapport et aux règles.
- Scénario 2 : Autorisation de lecture seule appliquée aux règles du rapport.

	Rôle (Analystes)	Autorisations appliquées au groupe de rapports, au sous-groupe, au rapport et aux règles en fonction du rôle d'utilisateur	Autorisation (Lecture seule) appliquée aux règles du rapport
Groupe	Lecture et écriture	**Lecture et écriture**	Lecture et écriture
Sous-groupe	Lecture	**Lecture**	Lecture et écriture
Rapport	Lecture	**Lecture**	Lecture et écriture
Règles	Lecture	**Lecture**	**Lecture**

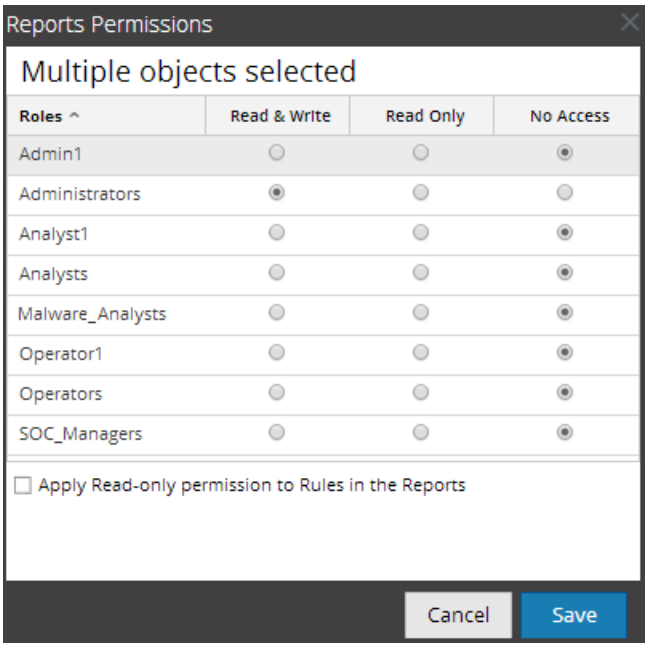
Il sera attribué au rapport le rôle d'un **Analyste de sécurité** et les autorisations sont définies en **Lecture et écriture** des rapports.

Pour le scénario 1, chacun des niveaux a un ensemble d'autorisations en fonction du rôle d'utilisateur. Pour le scénario 2, l'autorisation de lecture est définie pour les règles, sauf que l'ensemble d'autorisations pour les règles ne peut pas être supérieur à l'autorisation définie pour les rapports.

Remarque : Si l'autorisation pour les règles est supérieure à l'autorisation pour les rapports, alors l'autorisation est appliquée. Par exemple, si vous définissez les autorisations pour le Groupe de rapports sur **Aucun accès**, et que vous spécifiez l'option *Appliquer l'autorisation de lecture seule aux règles des rapports*, l'autorisation de lecture seule n'est pas définie pour les règles.

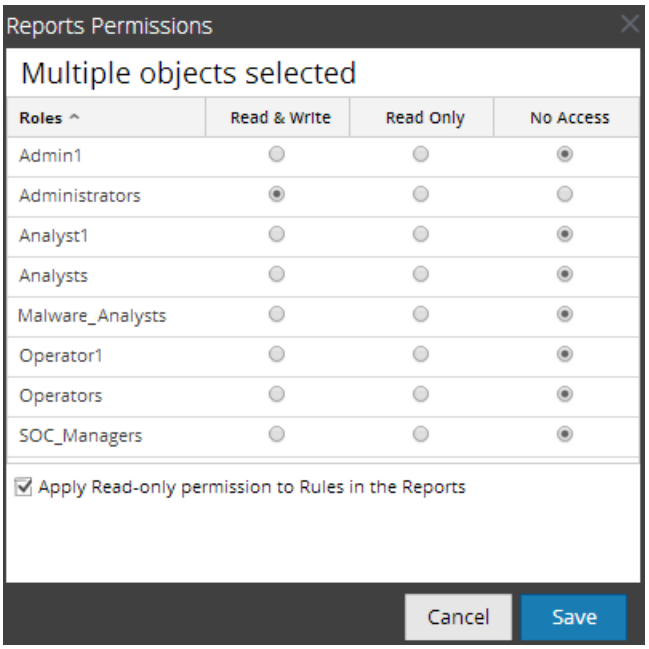
Contrôle d'accès pour un rapport lorsque plusieurs rapports sont sélectionnés

Lorsque vous souhaitez modifier les autorisations de modification de plusieurs rapports, vous pouvez sélectionner plusieurs rapports simultanément et paramétrer leurs autorisations d'accès dans le panneau Autorisations de rapport. L'autorisation d'accès que vous choisissez s'applique à tous les rapports.



Contrôle d'accès pour un rapport lorsque plusieurs rapports dotés de plusieurs règles sont sélectionnés

Si vous souhaitez modifier les autorisations lorsque plusieurs rapports dotés de plusieurs règles sont sélectionnés, vous devez cocher la case dans le panneau Autorisations des rapports, comme l'indique la figure. Si l'autorisation attribuée aux règles est inférieure à l'autorisation des rapports, l'autorisation d'accès en lecture seule s'applique à toutes les règles des rapports sélectionnés.

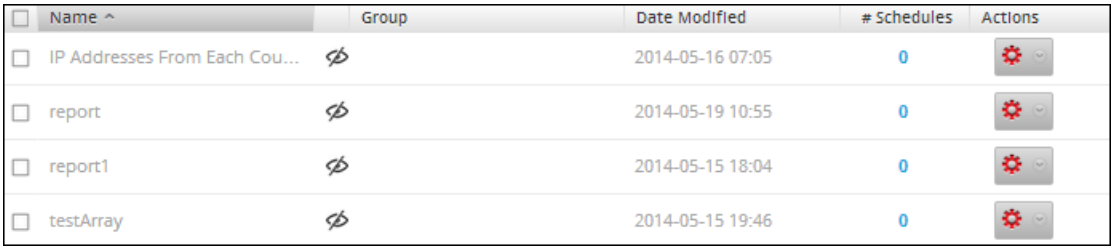


Se connecter en tant qu'utilisateur spécifique et afficher les détails d'accès

Lorsque vous vous connectez à l'interface utilisateur de NetWitness Suite en tant qu'utilisateur avec une autorisation de lecture seule, tous les rapports sont annotés du symbole 🕮. Lorsque vous cliquez sur ce symbole, la légende « Lecture seule » s'affiche dans le panneau Liste de rapports.

Lorsque vous vous connectez à l'interface utilisateur de NetWitness Suite en tant qu'utilisateur ne détenant pas l'autorisation d'accès en lecture et écriture à un rapport, tous les rapports sont marqués du symbole ( ) et ils sont grisés dans le panneau Liste des rapports.

La figure suivante montre le panneau Liste des rapports d'un utilisateur connecté avec l'autorisation d'accès en lecture/écriture minimale.



Remarque : Si un utilisateur (autre que le superutilisateur) crée un rapport, le superutilisateur ne pourra pas accéder à ce rapport.

Liste tabulaire

Le tableau suivant répertorie les différentes colonnes du panneau Autorisations des rapports :

Colonne	Description
Rôles	Rôle de l'utilisateur connecté dans l'interface utilisateur de NetWitness Suite.
Lecture et écriture	L'utilisateur peut accéder, afficher, modifier, importer, exporter et supprimer un rapport dans la vue Rapports. Il peut également modifier l'autorisation du rapport.
Lecture seule	L'utilisateur peut uniquement accéder au rapport et l'afficher dans la vue Rapports.
Aucun accès	L'utilisateur ne peut pas accéder au rapport pour lequel cette autorisation est définie, ou l'afficher.
Appliquer ces autorisations aux sous-groupes et rapports dans ce groupe	Cochez cette case pour appliquer les autorisations sélectionnées au groupe de rapports, aux sous-groupes dans le groupe et aux rapports dans le groupe. **Remarque :** Cette case à cocher n'apparaît que lorsque vous définissez les autorisations d'accès pour un groupe de rapports.
Appliquer l'autorisation de lecture seule aux règles des rapports	Cochez la case pour appliquer automatiquement les autorisations aux règles des rapports.

Définir un contrôle d'accès pour un rapport

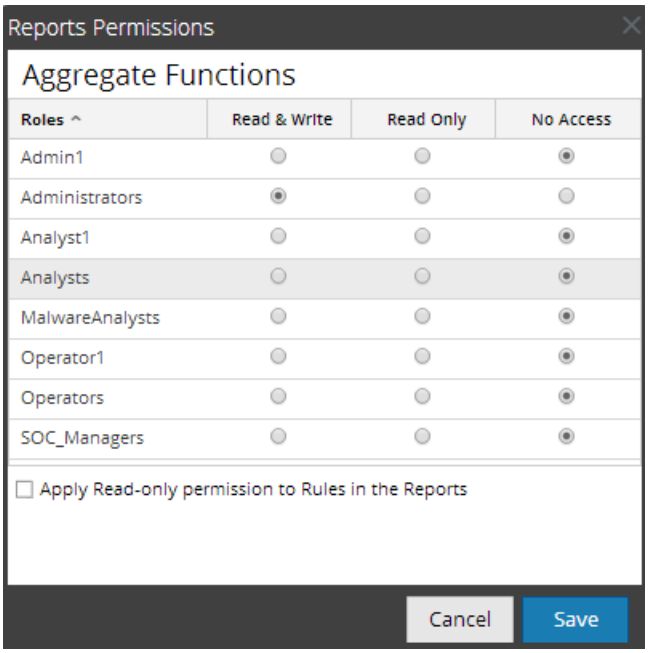
Conditions préalables

Veillez à disposer d'une autorisation d'accès minimale en lecture et écriture pour définir les autorisations d'accès d'un rapport.

Pour définir les autorisations d'accès à un rapport, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.

2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport.
4. Cliquez sur > **Autorisations**.
   La boîte de dialogue Autorisations des rapports s'affiche.



5. En fonction du rôle d'utilisateur, sélectionnez les boutons appropriés.
6. (Facultatif) Pour accorder les autorisations d'accès en lecture aux règles des rapports, activez la case à cocher.

Remarque : En activant la case à cocher, toutes les règles dépendantes ont une autorisation d'accès en LECTURE, à condition que les autorisations du rapport soient supérieures aux autorisations des règles.

6. Cliquez sur **Enregistrer**.
   Un message de confirmation s'affiche indiquant que les autorisations ont été définies pour le rapport sélectionné.

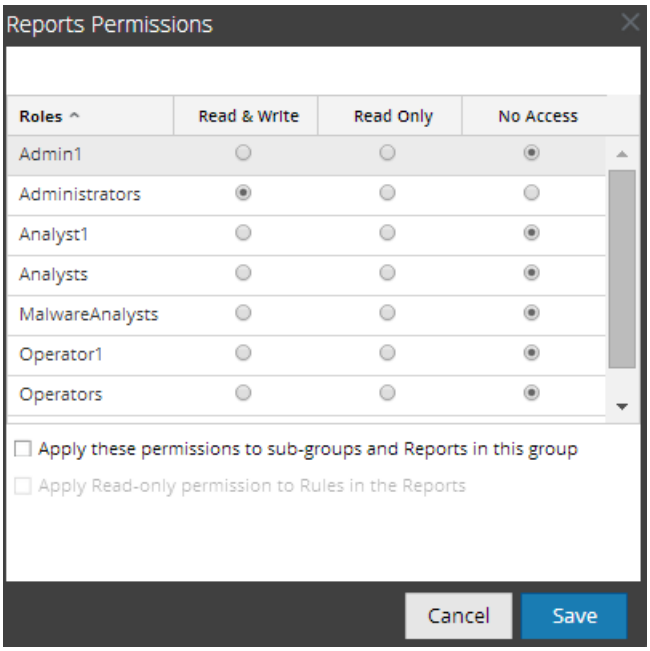
Définir un contrôle d'accès pour un groupe de rapports

Conditions préalables

Veillez à disposer d'une autorisation d'accès minimale en lecture et écriture pour définir les autorisations d'accès d'un groupe de rapports.

Pour définir les autorisations d'accès à un groupe de rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Groupes de rapports**, sélectionnez ou cliquez avec le bouton droit sur un groupe de rapports.
4. Cliquez sur  > Autorisations
   . La boîte de dialogue Autorisations des rapports s'affiche.



4. En fonction du rôle d'utilisateur, sélectionnez les boutons appropriés.
5. (Facultatif) Activez la case à cocher appropriée pour appliquer les autorisations sélectionnées aux sous-groupes et aux rapports du groupe.
6. (Facultatif) Activez la case à cocher appropriée pour fournir une autorisation d'accès en lecture aux règles dans les rapports.

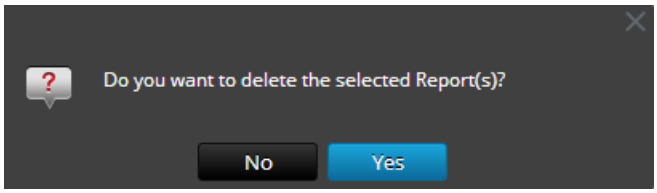
Remarque : En activant la case à cocher, toutes les règles dépendantes ont une autorisation d'accès en LECTURE, à condition que les autorisations du rapport soient supérieures aux autorisations des règles.

7. Cliquez sur **Enregistrer**.
   Un message de confirmation de la définition de l'autorisation pour le groupe de rapports sélectionné s'affiche.

Supprimer un rapport ou un groupe de rapports

Pour supprimer des rapports dans un groupe ou sous-groupe dans le panneau Liste des rapports :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :
   - Sélectionnez les rapports, puis cliquez sur .
   - Cliquez sur > **Supprimer**.
     Une boîte de dialogue de confirmation s'affiche.



4. Cliquez sur **Oui** pour supprimer le rapport.
   Un message de confirmation indiquant que la suppression du rapport s'est déroulée correctement s'affiche et le rapport sélectionné est supprimé du panneau Liste des rapports.

Supprimer un groupe de rapports

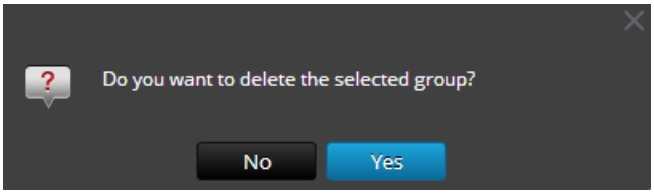
Conditions préalables

Veillez à ce qu'aucun rapport ne soit associé au groupe de rapports.

Pour supprimer des groupes de rapports dans le dossier par défaut ou des sous-groupes dans un groupe de rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.

3. Dans le panneau **Groupes de rapports**, sélectionnez le groupe de rapports et cliquez sur .
   Une boîte de dialogue de confirmation s'affiche.



4. Cliquez sur **Oui** pour supprimer le groupe.
   Un message de confirmation indiquant que la suppression du groupe s'est déroulée correctement s'affiche et le groupe sélectionné est supprimé du panneau Groupes de rapports.

Dupliquer un rapport

Vous pouvez dupliquer un rapport afin de prévoir plusieurs planifications de rapport et planifier le même rapport. Le rapport dupliqué s'affiche dans le panneau Liste des rapports avec les suffixes. Par exemple, Rapport (1).

Généralement, l'option de duplication est utilisée dans deux cas :

- Vous souhaitez créer une copie du rapport afin de déplacer le même rapport dans un autre groupe.
- Vous souhaitez conserver la plupart des paramètres de configuration d'un objet et en modifier quelques-uns.
  Par exemple, si une règle comporte une requête complexe ou si plusieurs règles sont présentes dans un rapport, il est beaucoup plus approprié d'utiliser l'option de duplication.

Pour dupliquer un rapport existant, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport que vous souhaitez dupliquer, puis cliquez sur .
   Le rapport est enregistré et ajouté à la liste des rapports.

Vous pouvez déplacer le rapport dupliqué dans un autre groupe.

Modifier un rapport

Pour modifier des rapports dans un groupe ou un sous-groupe dans le panneau Liste des rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :
   - Sélectionnez un rapport et cliquez sur  .
   - Cliquez sur  > **Modifier**.

   L'onglet de la vue Élaborer le rapport s'affiche.

4. Modifiez le texte et ajoutez d'autres règles au rapport (si nécessaire).
5. Cliquez sur **Enregistrer**.
   Un message de confirmation de l'enregistrement du rapport s'affiche.

Actualiser un groupe de rapports ou une liste de rapports

Vous pouvez actualiser un groupe de rapports ou des rapports afin d'afficher la réorganisation des groupes ou des rapports.

Pour actualiser un groupe de rapports ou des rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.

La vue Rapport s'affiche.

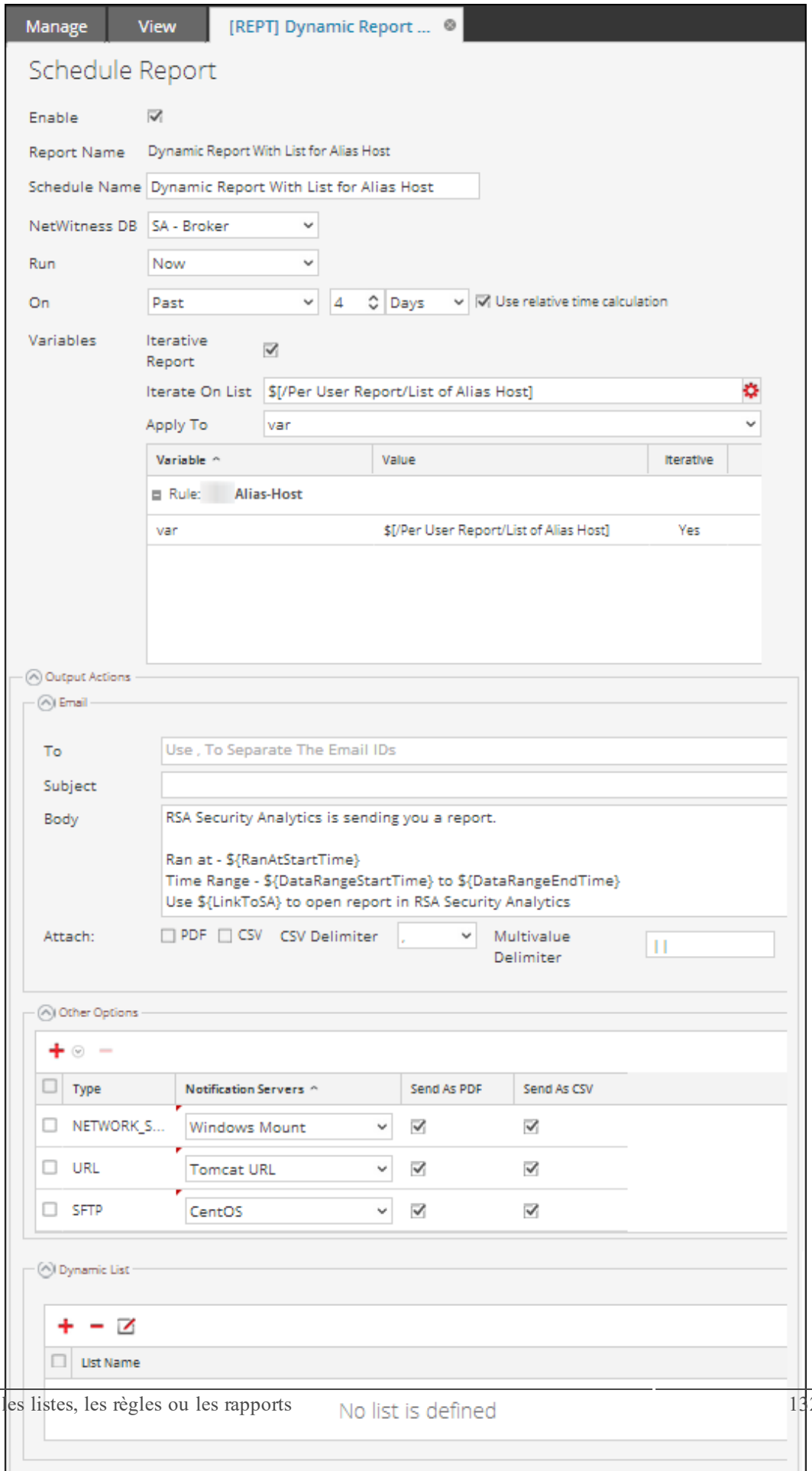
3. Pour déplacer le groupe ou les rapports vers un nouvel emplacement, procédez comme suit :
   - Dans le panneau **Groupes de rapports**, faites glisser le groupe.
   - Dans le panneau **Liste des rapports**, faites glisser les rapports dans le groupe voulu dans le panneau Groupes de rapports.
     Le groupe de rapports ou les rapports sont déplacés vers le nouvel emplacement.
4. Pour actualiser une liste de groupes ou de rapports, procédez comme suit :
   - Dans le panneau **Groupe des rapports**, cliquez sur.
     Le groupe des rapports est actualisé.
   - Dans le panneau **Liste des rapports**, cliquez sur .
     La liste des rapports est actualisée.

Modifier un rapport planifié

Pour modifier un rapport planifié à partir du panneau Liste des rapports planifiés, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport et cliquez sur > **Afficher les rapports programmés**.
   L'onglet Afficher les rapports programmés s'affiche.
4. Dans le panneau **Liste des rapports planifiés**, exécutez l'une des opérations suivantes :
   - Sélectionnez un rapport, puis cliquez sur .
   - Sélectionnez un rapport, puis cliquez sur > **Modifier le planning**.

L'onglet Planifier un rapport s'affiche.


Manage
View
[REPT] Dynamic Report ...
Schedule Report
Enable
Report Name
Dynamic Report With List for Alias Host
Schedule Name
Dynamic Report With List for Alias Host
NetWitness DB
SA - Broker
Run
Now
On
Past
4
Days
Use relative time calculation
Variables
Iterative Report
Iterate On List
$[/Per User Report/List of Alias Host]
Apply To
var
Variable
Value
Iterative
Rule:
Alias-Host
var
$[/Per User Report/List of Alias Host]
Yes
Output Actions
Email
To
Use , To Separate The Email IDs
Subject
Body
RSA Security Analytics is sending you a report.
Ran at - ${RanAtStartTime}
Time Range - ${DataRangeStartTime} to ${DataRangeEndTime}
Use ${LinkToSA} to open report in RSA Security Analytics
Attach:
PDF
CSV
CSV Delimiter
Multivalue Delimiter
Other Options
Type
Notification Servers
Send As PDF
Send As CSV
NETWORK_S...
Windows Mount
URL
Tomcat URL
SFTP
CentOS
Dynamic List
List Name
No list is defined

5. Sous l'onglet Planifier un rapports, effectuez les tâches suivantes :
   a. Dans le champ **Nom de planning**, saisissez le nom de la configuration de planification de rapport.
   b. Pour exécuter les rapports selon le planning, cochez la case **Activer**.
   c. Dans le champ **Source de données**, sélectionnez la source de données.

   Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubrique « Configurer les autorisations d'accès aux sources de données » dans le *Guide de configuration de Reporting Engine*.

6. (Facultatif) Dans la liste déroulante **Pool de ressource Warehouse**, sélectionnez le pool ou la file d'attente pour le rapport.

   Remarque : La liste déroulante **Pool de ressource Warehouse** s'affiche uniquement si la règle Warehouse est sélectionnée. Si aucun pool ni aucune file d'attente ne sont définis pour le Reporting Engine, ce champ est désactivé.

7. Dans le champ **Exécuter** , sélectionnez le type de planification d'exécution. (Par exemple, Maintenant ou Toutes les heures).
8. Sélectionnez la période pour exécuter la requête d'après la durée absolue ou cochez la case **Utiliser le calcul de temps relatif** pour exécuter la requête basée sur la durée relative.
9. (Facultatif) Dans le panneau Actions de sortie, effectuez les opérations suivantes :
   i. Saisissez l'adresse e-mail et l'objet.
   ii. Modifiez le corps de message du rapport.
   iii. Sélectionnez le format de la pièce jointe.
   iv. Saisissez une valeur pour les séparateurs de plusieurs valeurs et CSV.
10. (Facultatif) Dans le champ Autres options, procédez comme suit :
    i. Cliquez sur  > **SFTP** ou **URL** ou **Partage réseau**. D'après l'option sélectionnée, une ligne est ajoutée dans le champ Autres options.
    ii. Sélectionnez les options appropriées pour envoyer le rapport au format PDF ou CSV au partage SFTP, URL ou réseau configuré.
11. (Facultatif) Pour ajouter une liste dans le panneau Liste dynamique, voir la section « Générer une liste à partir du rapport planifié » dans Créer et planifier un rapport.

12. (Facultatif) Pour choisir un autre logo dans le panneau Logo, voir la section Gérer et sélectionner un logo de rapport.

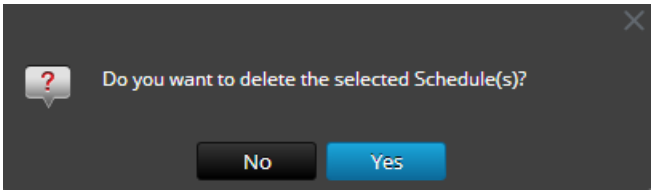
    Remarque : Si vous ne spécifiez pas de logo, le logo RSA par défaut est utilisé.

13. Cliquez sur **Planifier**.
    Le rapport planifié s'exécute comme prévu et fournit les sorties configurées.

Supprimer un rapport planifié

Pour supprimer un rapport planifié dans le panneau Liste des rapports planifiés, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans la barre d'outils **Rapport**, cliquez sur **Afficher tous les plannings**.
   La vue Rapports planifiés s'affiche.
4. Dans le panneau **Liste des rapports planifiés**, sélectionnez le rapport.
5. Cliquez sur  >**Supprimer le planning**.
   Une boîte de dialogue de confirmation s'affiche.



6. Cliquez sur **Oui** pour supprimer le rapport planifié.
   Un message de confirmation indiquant que la suppression du rapport planifié s'est déroulée correctement s'affiche et le planning sélectionné est supprimé du panneau Liste des rapports planifiés.

Exporter un rapport

Vous pouvez exporter les rapports sélectionnés vers un fichier externe qui peut être importé ultérieurement vers un autre environnement NetWitness Suite.

Conditions préalables

Veillez à disposer de rapports dans le groupe de rapports.

Pour exporter les rapports sélectionnés dans le panneau Groupes de rapports vers un fichier externe, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :
   - Sélectionnez un rapport, puis cliquez sur  > **Exporter**.
   - Cliquez sur  > **Exporter**.

   Vous pouvez exporter plusieurs rapports à la fois. Pour sélectionner plusieurs rapports, activez la case à cocher du rapport à exporter. Le fichier exporté est enregistré sur le disque local au format archivé.

Ouvrez des fichiers CSV contenant des caractères Unicode dans MS Excel

Pour ouvrir des fichiers CSV téléchargés contenant des caractères Unicode dans MS Excel, procédez comme suit :

1. Téléchargez et enregistrez le fichier CSV.
2. Ouvrez Microsoft Excel et accédez à l'onglet **Données**.
3. Cliquez sur l'élément de menu **À partir de texte**, recherchez le fichier CSV que vous avez téléchargé, puis cliquez sur **Importer**.
   L'assistant Importation de texte s'affiche.
4. Sélectionnez le type de données **Délimité** ou **Largeur fixe** dans la case d'option **Type de données d'origine**.
5. Cliquez sur la zone de liste déroulante **Origine du fichier** et sélectionnez **65001 : Unicode (UTF-8)**, puis cliquez sur **Suivant**.
6. Sélectionnez le délimiteur utilisé dans le fichier que vous avez importé, puis cliquez sur **Suivant**.
7. Sélectionnez le format de données pour chaque colonne de données à importer, puis cliquez sur **Terminer**.
   La sortie correcte s'affiche dans une feuille MS Excel.

Exporter un groupe de rapports

Vous pouvez exporter le groupe de rapports sélectionné vers un fichier externe qui peut être importé ultérieurement vers un autre environnement NetWitness Suite.

Conditions préalables

Veillez à disposer de rapports dans le groupe de rapports.

Pour exporter les groupes de rapports sélectionnés dans le panneau Groupes de rapports vers un fichier externe, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Groupes de rapports**, sélectionnez un groupe de rapports et choisissez l'une des options suivantes :
   - **Exporter** - Cette sélection exporte un rapport dans un fichier .zip.
   - **Exporter en tant que texte** - Cette sélection exporte tout le contenu de Reporting Engine dans un fichier .zip qui contient les données au format texte.

   Vous pouvez exporter plusieurs groupes de rapports à la fois. Pour sélectionner plusieurs groupes de rapports, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les groupes de rapports à exporter. Le fichier exporté est enregistré sur le disque local.

Importer un rapport ou un groupe de rapports

Vous pouvez importer des groupes contenant des sous-groupes et des rapports d'autres instances de NetWitness Suite vers le panneau Groupes de rapports. Les rapports doivent figurer dans un fichier binaire valide qui a été exporté d'une autre instance de NetWitness Suite.
Lors du processus d'importation, sélectionnez le fichier binaire, puis spécifiez si les rapports existants avec le même nom doivent être remplacés ou non par les rapports du fichier d'importation binaire.

- Si vous optez pour le remplacement, tous les règles, listes et rapports dupliqués seront remplacés par le contenu du fichier d'importation binaire.
- Si vous ne choisissez pas le remplacement alors que le dossier cible contient une règle, une liste ou un rapport dupliqué, l'importation échoue et affiche un message concernant les rapports dupliqués.

Vous ne pouvez pas importer des rapports vers un groupe de rapports spécifique. Les fichiers importés sont stockés dans le dossier racine **Tout**.

Conditions préalables

Vous possédez les rapports ou groupes de rapports exportés à partir d'autres instances de NetWitness Suite.

Pour importer des groupes contenant des sous-groupes et des rapports d'autres instances de NetWitness Suite vers le panneau Groupes de rapports, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Groupes de rapports**, sélectionnez un dossier pour importer le fichier.
4. Exécutez l'une des opérations suivantes :
   - Dans le panneau **Groupes de rapports**, cliquez sur  > **Importer** pour importer un groupe.
   - Dans la barre d'outils **Rapport**, cliquez sur  > **Importer** pour importer un rapport.
     La boîte de dialogue Importer le rapport s'affiche. Vous pouvez importer plusieurs rapports et groupes de rapports à la fois. Pour sélectionner plusieurs rapports ou groupes de rapports, appuyez et maintenez la touche CTRL enfoncée et sélectionnez les rapports ou groupes de rapports à importer.
5. Cliquez sur **Parcourir** pour sélectionner le fichier binaire.
   NetWitness Suite fournit une vue Système de fichiers sur les fichiers.
6. Recherchez le fichier binaire, puis cliquez sur **Ouvrir**.
   Le fichier est alors ajouté dans la liste Importer le rapport.
7. (Facultatif) Pour écraser toutes les règles existantes dans la bibliothèque par une règle possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case **Règle**. Si vous ne sélectionnez pas l'option Remplacer et qu'une règle identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
8. (Facultatif) Pour écraser toutes les listes existantes dans la bibliothèque par une liste possédant un nom identique dans le fichier binaire, cochez la case **Liste**. Si vous ne sélectionnez pas l'option Remplacer et qu'une liste identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
9. (Facultatif) Pour écraser tous les rapports existants dans la bibliothèque par un rapport possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case

Rapport. Si vous ne sélectionnez pas l'option Remplacer et qu'un rapport identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.

10. Cliquez sur **Importer** pour importer le fichier binaire.

Activer ou désactiver un rapport planifié

Pour activer ou désactiver un rapport planifié dans le panneau Liste des rapports planifiés, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport et cliquez sur  > **Afficher les rapports programmés**.
   La vue Rapports planifiés s'affiche.
4. Sélectionnez un rapport planifié dans le panneau Liste des rapports planifiés.
5. Cliquez sur  > **Activer**.
   Le rapport passe à l'état « En cours d'exécution » si le rapport est planifié pour s'exécuter immédiatement.
6. Cliquez sur  > **Désactiver**.
   L'état du rapport passe à l'état « Inactif ».

Démarrer ou arrêter un rapport planifié

Pour démarrer ou arrêter un rapport planifié, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport et cliquez sur  > **Afficher les rapports programmés**.
   La vue Afficher les rapports programmés s'affiche.

4. Sélectionnez un rapport planifié dans le panneau Liste des rapports planifiés.
5. Cliquez sur  > **Démarrer**.

   Le rapport passe à l'état « En cours d'exécution » si le rapport est planifié pour s'exécuter immédiatement.
6. Cliquez sur  > **Arrêter**.

   L'état du rapport passe à « Terminé ».

Afficher l'historique d'exécution d'un rapport planifié

Vous pouvez afficher l'historique d'exécution d'un rapport planifié. Vous pouvez afficher l'historique d'un rapport planifié exécuté. Vous pouvez afficher l'historique en fonction des critères suivants :

- Nombre de plannings antérieurs exécutés
- Date de début et date de fin composant la période.

Vous pouvez afficher des informations détaillées telles que le nombre d'exécutions du rapport planifié, la durée d'exécution (en secondes) et l'état d'exécution. Vous pouvez également afficher le rapport généré en plein écran.

Pour afficher l'historique d'exécution d'un rapport planifié, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.

   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :
   - Cliquez sur  > **Afficher les rapports programmés**.
   - Cliquez sur la colonne **#Schedules**.

     L'onglet de la vue Planifier un rapports affiche l'état de chaque rapport planifié.
4. Exécutez l'une des opérations suivantes :
   - Sélectionnez un rapport planifié et cliquez sur  > **Historique d'exécution**.
   - Sélectionnez un rapport planifié et cliquez sur  .

     La vue Historique d'exécution s'affiche.

Remarque : Par défaut, vous pouvez afficher 10 historiques d'exécution d'un rapport planifié. L'historique d'exécution affiché dépend de la configuration de la conservation de l'historique des rapports définie sous l'onglet **Général** de **ADMIN > Services > vue Config de Reporting Engine**.
Par exemple, si vous définissez la configuration de la conservation de l'historique des rapports à 100 jours, les données affichées dans la vue Historique d'exécution correspondent au détail de l'historique d'exécution des 100 derniers jours, à partir de la date actuelle.

5. Dans le champ **Obtenir l'historique par :**, sélectionnez le type d'historiques à extraire. (Par exemple, Derniers/Dernières ou Plage (spécifique))
6. Dans le champ **Nombre**, saisissez le nombre d'exécutions à afficher.
7. Cliquez sur **Afficher l'historique**.
   L'historique d'exécution du rapport planifié s'affiche.

Gérer et sélectionner un logo de rapport

Conditions préalables

Assurez-vous de définir le service Reporting Engine avant de gérer un logo.

Gérer des logos de rapport

Pour gérer les logos, procédez comme suit :

1. Sélectionnez **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Dans le panneau **Liste des services**, sélectionnez un service Reporting Engine et cliquez sur **Vue** > **Config**.
   La vue Configuration des services s'affiche.
3. Sélectionnez l'onglet **Gérer les logos**.
   Tous les logos disponibles s'affichent.

Ajouter un logo

Pour ajouter un logo par défaut, procédez comme suit :

1. Sous l'onglet **Gérer les logos**, cliquez sur  .
   Un navigateur de fichiers s'ouvre pour vous permettre de choisir le fichier sur le disque local.

2. Sélectionnez le logo et cliquez sur **Sélectionner**.

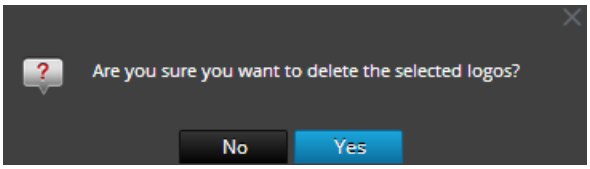
   Le logo sélectionné est ajouté à la section Gérer les logos.

Supprimer un logo

Pour supprimer un logo, procédez comme suit :

1. Sous l'onglet **Gérer les logos**, exécutez l'une des opérations suivantes :
   - Sélectionnez le logo et cliquez sur .
   - Appuyez sur Ctrl+clic pour sélectionner plusieurs logos, puis cliquez sur .

   Une boîte de dialogue de confirmation s'affiche.



2. Pour supprimer le logo, cliquez sur **Oui**.

   Le logo sélectionné est supprimé de la section Gérer les logos.

Définir un logo par défaut

Pour définir un logo par défaut, procédez comme suit :

Sous l'onglet **Gérer les logos**, sélectionnez un logo et cliquez sur Set default.

Le logo sélectionné est défini comme valeur par défaut pour le service RE.

Sélectionner un logo

Pour sélectionner un logo par défaut, procédez comme suit :

1. Sélectionnez **ADMIN** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Cliquez sur **Rapports**.

   La vue Rapport s'affiche.

3. Dans le panneau **Liste des rapports**, sélectionnez un rapport.

4. Cliquez sur > **Afficher les rapports programmés**.

   L'onglet de la vue Afficher les rapports programmés s'affiche.

5. Sélectionnez un rapport planifié et cliquez sur > **Modifier le planning**.

   L'onglet de la vue Planifier un rapport s'affiche.

6. Dans le panneau Logo, cliquez sur **Modifier le logo**.

La boîte de dialogue Modifier un logo s'affiche.

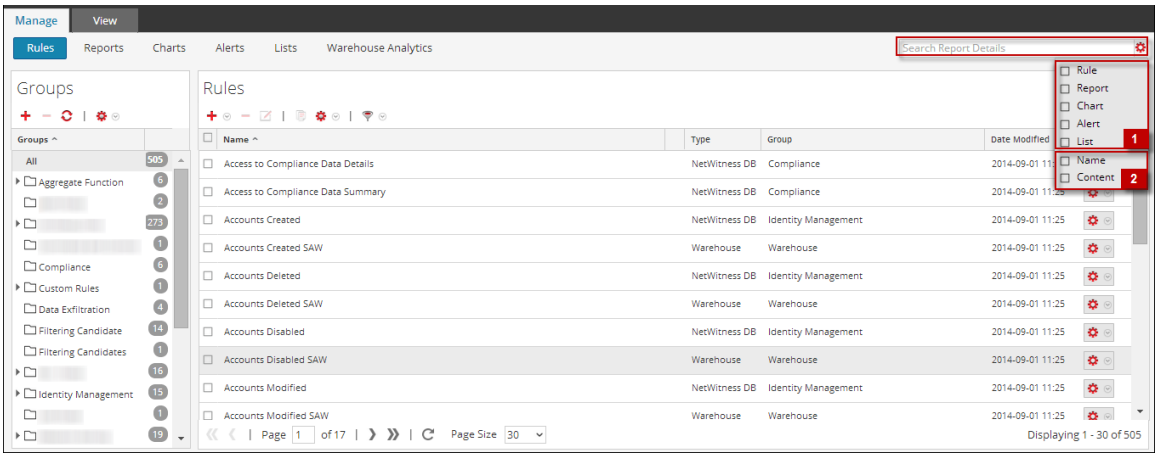
7. Exécutez l'une des opérations suivantes :
   - Cliquez sur **Télécharger le nouveau logo** pour télécharger un autre logo.
   - Sélectionnez un logo dans la liste.
8. Cliquez sur **Sélectionner**.
   Le logo sélectionné est disponible dans le panneau Logo.

Rechercher des détails sur le reporting

Cette section fournit des instructions sur l'exécution d'une recherche par mot-clé d'un nom et de contenu pour chacun des composants Reporting. Vous pouvez effectuer une recherche par mot clé sur le nom et le contenu de chacun des composants Reporting (Règle/Rapport/Graphique/Alerte/Liste) dans l'interface utilisateur de Reporting.

Remarque : Vous ne pouvez pas effectuer de recherche en fonction des dates et des valeurs numériques.

La figure suivante montre les paramètres de recherche disponibles dans le module Reporting :



La éléments suivants sont les paramètres de recherche disponibles dans l'interface utilisateur de Reporting :

1. Recherche d'entités (règle, rapport, graphique, alerte, liste).
2. Recherchez les entités basées sur le nom ou le contenu.

Remarque : Les recherches ne sont pas sensibles à la casse. Par exemple, Terminé est équivalent à terminé.

Conditions préalables

Dans le module Reporting, vous pouvez effectuer une recherche par mot clé basée sur le nom et le contenu (définition). Dans ce contexte, le contenu implique la définition de chacun des composants Reporting. Par exemple, la valeur définie dans le panneau règle, rapport, planning de rapport, graphique et alerte. Vous pouvez hiérarchiser votre recherche en sélectionnant un ou tous les composants : Règle, Rapport, Graphique, Alerte ou Liste.

Remarque : Vous ne pouvez pas effectuer de recherche sur la base des valeurs de la liste et sur le chemin de la liste stockée dans le panneau de définition du planning.

Par exemple, pour rechercher le nom de la règle (ExpertRule), vous devez sélectionner **Règle, nom et contenu** dans le menu déroulant **Options de filtrage** pour afficher tous les noms des règles qui correspondent à la recherche. De même, vous pouvez rechercher une définition de rapport, graphique, alerte, ou liste.

Effectuez les étapes suivantes pour rechercher les détails de reporting de l'onglet Gérer :

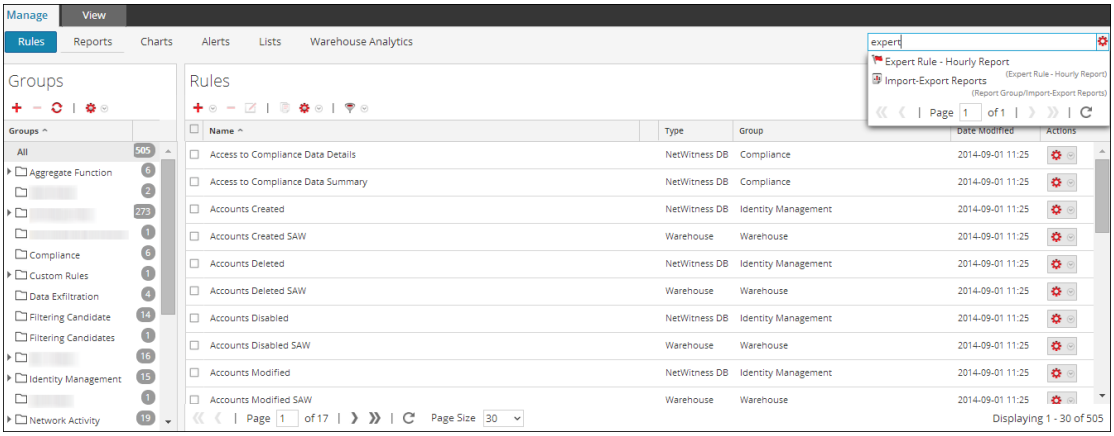
1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet **Gérer** s'affiche.

2. Cliquez sur  , puis sélectionnez les critères de recherche appropriés.

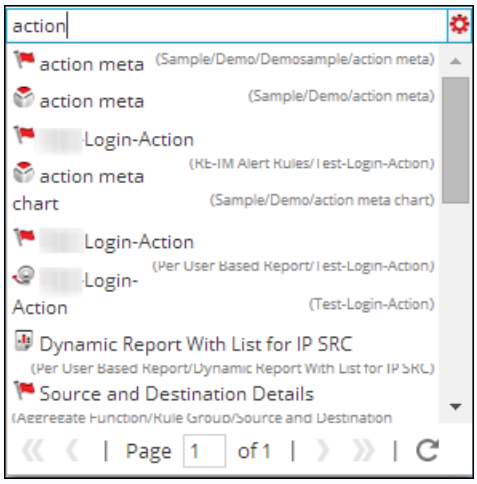
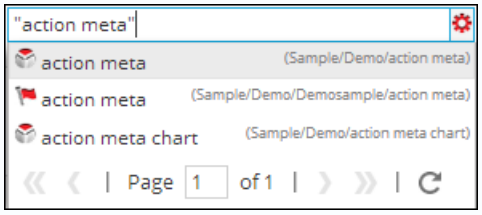
3. Dans le champ **Recherche** , saisissez le texte à rechercher.

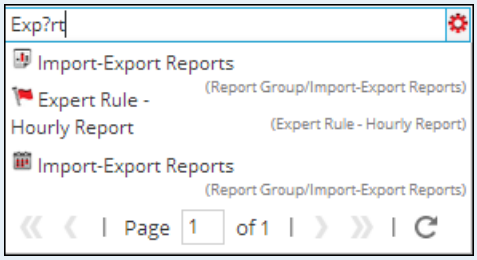
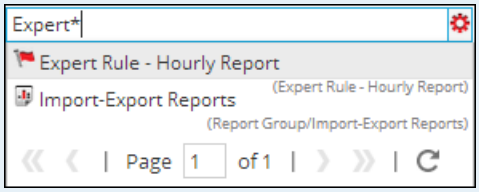
   La liste déroulante de recherche s'affiche :

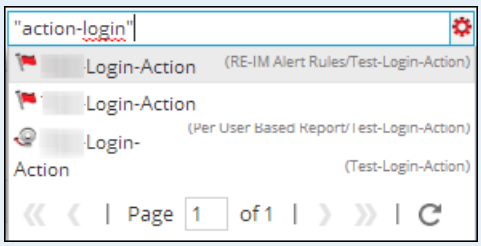


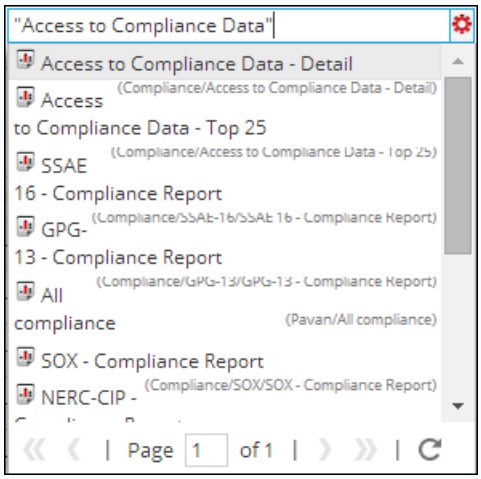
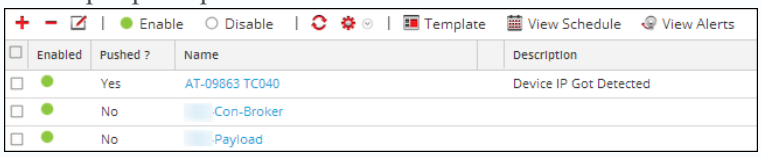
Syntaxe de recherche et types de recherches différents

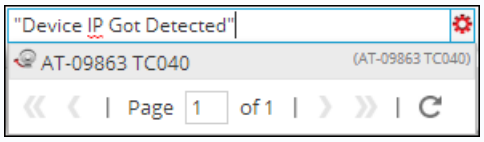
Le tableau suivant explique la syntaxe de recherche et les recherches possibles qui peuvent être effectuées sur l'interface utilisateur de Reporting.

Types de recherche	Description
Recherche basée sur des termes ou une phrase	**Recherche basée sur des termes** : Pour rechercher un mot comme « action » ou « méta », vous devez saisir le mot dans la zone de recherche. La figure suivante indique le résultat de la recherche pour le texte **action**.  **Recherche basée sur une phrase :** Une phrase est un groupe de mots entourés par des guillemets doubles comme "action méta". Pour rechercher une phrase, vous devez la placer entre des guillemets doubles dans la zone de recherche. La figure suivante indique le résultat de la recherche pour la phrase "action méta". 

Types de recherche	Description
Recherche de caractère générique (recherche simple / multiple / de caractère spécial) Le point d'interrogation **?** est utilisé pour effectuer une recherche simple de caractère générique et l'astérisque « * » est utilisé pour effectuer une recherche de caractère générique multiple.	**Recherche de caractère unique :** La recherche de caractère générique simple cherche des termes qui correspondent au caractère simple remplacé. Par exemple, pour rechercher « Expert » ou « Export », vous pouvez utiliser la syntaxe de recherche : Exp?rt La figure suivante indique le résultat de la recherche pour le caractère générique **Exp?rt**.  **Recherche de caractère multiple :** La recherche de caractère générique multiple cherche 0 ou plusieurs caractères. Par exemple, pour rechercher Expert, ou Experts, vous pouvez utiliser la syntaxe de recherche : Expert* La figure suivante indique le résultat de la recherche pour le caractère générique multiple **Expert***. 

Types de recherche	Description
	Recherche de caractère spécial : Certains signes de ponctuation et caractères spéciaux sont ignorés lors de la recherche (@#$%^&*(){}"~=+-[]\?|!:,.). Par exemple, une recherche pour action-login sera interprétée lors de la recherche comme "action" "login". Si des règles existent avec le nom "action-login" et "action@login" et si la chaîne de recherche est "action login", le résultat de la recherche va renvoyer les deux règles. 

Types de recherche	Description
Recherche basée sur le nom ou le contenu	**Recherche basée sur le nom :** Lorsque vous souhaitez effectuer une recherche en fonction du nom d'un rapport, sélectionnez **Rapport** et la zone **Nom** dans le menu déroulant des options de filtrage. Par exemple, pour rechercher le nom du rapport « Rapport avec plusieurs règles », vous pouvez utiliser la syntaxe de recherche : "Accès aux données de conformité" **Remarque :** Lorsque vous recherchez un rapport, cela implique que vous pouvez rechercher les plannings des rapports également. Le résultat de la recherche renvoie le rapport contenant le nom spécifique.  **Recherche basée sur le contenu :** Lorsque vous souhaitez rechercher le contenu dans une alerte, par exemple la description de l'alerte, sélectionnez **Alerte** et la zone **Contenu** dans le menu déroulant des options de filtrage. Par exemple, pour rechercher la description de l'alerte « IP de périphérique détectée », vous pouvez utiliser la syntaxe de recherche : "IP de périphérique détectée"  La recherche va renvoyer le résultat ayant le contenu

Types de recherche	Description
	spécifique. 

Dépannage

Cette rubrique donne des instructions de dépannage pour les problèmes rencontrés lors de l'utilisation du module Reporting dans NetWitness Suite.

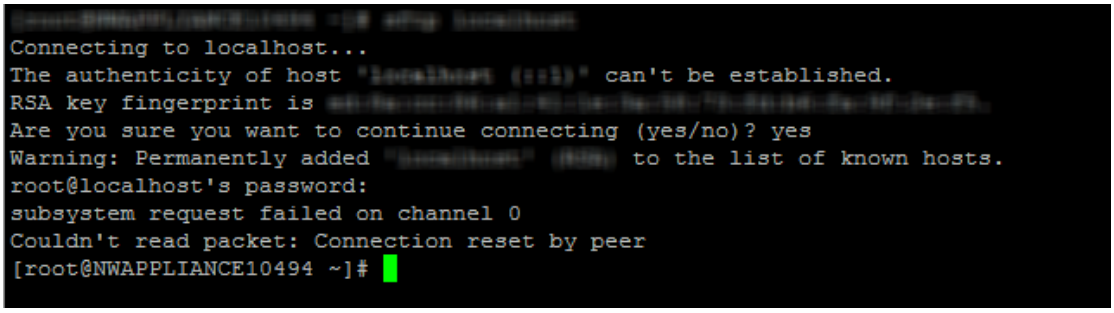
Problèmes de dépannage avant la configuration du serveur SFTP

Procédure

Si vous rencontrez des problèmes avec le serveur SFTP Linux configuré, procédez comme suit :

1. Si l'opération de résultat de rapport du serveur SFTP configuré échoue, vous devez activer SSH sur le serveur SFTP et tentez de vous connecter localement pour vérifier que le serveur SFTP fonctionne bien.

   Connectez-vous au serveur SFTP :

2. Si la connexion locale échoue, ouvrez le fichier **sshd_config> vi /etc/ssh/sshd_config.**
3. Vérifiez l'entrée suivante :

   ```
   # override default of no subsystems
   Subsystem sftp /usr/libexec/openssh/sftp-server
   ```

4. Si cette entrée n'existe pas, ajoutez les deux lignes mentionnées à l'étape 3 au bas du fichier et **enregistrez-le**.
5. Redémarrez le service avec **SSH > service sshd restart**.
6. Essayez maintenant de vous reconnecter à SFTP.
7. Vérifiez que le port SFTP n'est pas bloqué par le pare-feu de l'appliance serveur SA. Mettez à jour les règles de table IP pour autoriser le port sftp.

Définitions :

Parser strict : un parser strict (non obsolète) exige que la syntaxe de la requête soit saisie correctement.
Pour toutes les méta de type texte, utilisez des guillemets ; par exemple, username = ‘user1’.
Pour toutes les adresses IP, les adresses Ethernet et les méta de type numérique, n'utilisez pas de guillemets ; par exemple, service = 80 &&
ip.src = 192.168.1.1.
Pour les méta de type date et heure,
si le format de date et heure est 'AAAA-MM-JJ HH:MM:SS’, utilisez des guillemets.
Si le format de la date et de l'heure est 1448034064 (nombre de secondes depuis EPOCH (1er janvier 1970)), n'utilisez pas de guillemets.
Les requêtes de reporting seront analysées à l'aide de l'analyseur strict lorsque la valeur de configuration /sdk/config/query.parse est **stricte** dans les services NWDB Core.

Analyseur non strict : un analyseur non strict (obsolète) n'exige pas que la syntaxe de la requête soit saisie correctement, c'est-à-dire que les valeurs pour les méta de type texte et numérique peuvent être indiquées entre guillemets ou non, quel que soit le type de méta.

Par exemple, le nom d'utilisateur est une méta de type chaîne, donc ses valeurs peuvent être indiquées avec ou sans guillemets. Ainsi, les syntaxes suivantes sont toutes deux valides : username = user1 et username = user.

Les requêtes de reporting seront analysées à l'aide de l'analyseur non strict lorsque la valeur de configuration /sdk/config/query.parse est **obsolète** dans les services NWDB Core.

Remarque : La règle NWDB où la clause est correctement entre guillemets si la syntaxe possède des guillemets non valides. Par exemple, dans le cas d’une méta non valide ou manquant de séparateur, l’état et le message d’erreur sont mis à jour correctement.

Annexe

Cette rubrique fournit des informations détaillées sur les fonctions d’agrégation prises en charge, la syntaxe des règles, la syntaxe des requêtes de règles avancées dans Reporting et le planificateur de tâches pour Warehouse Reporting.

Syntaxe de la règle

Cette rubrique décrit la syntaxe des différentes règles prises en charge par Reporting Engine.

Syntaxe des règles NWDB

La règle NWDB est une des syntaxes de règle prises en charge dans Reporting Engine. Pour améliorer le délai d'exécution de vos entités de reporting, reportez-vous à la section « Directives de reporting » dans Présentation du Reporting.

Une règle est une fonction qui manipule l'ensemble de résultats afin de rendre la sortie d'un rapport plus explicite ou d'ajouter de nouvelles fonctionnalités à une règle autre que l'interrogation des données et leur affichage. Toute combinaison de ces actions de règle peut être utilisée pour créer des représentations uniques et intéressantes des informations collectées par NetWitness Suite.

Le Reporting Engine prend en charge les catégories suivantes de syntaxes de règles de sources NWDB :

- Clause **select**
  - Règle non agrégée
  - Règle agrégée
- **alias**
- Clause **where**
- Opérateurs de clause **where**
- Clause **then**
- Champ **Limite**
- Actions de règle
- Opérateurs dans les règles

Clause select

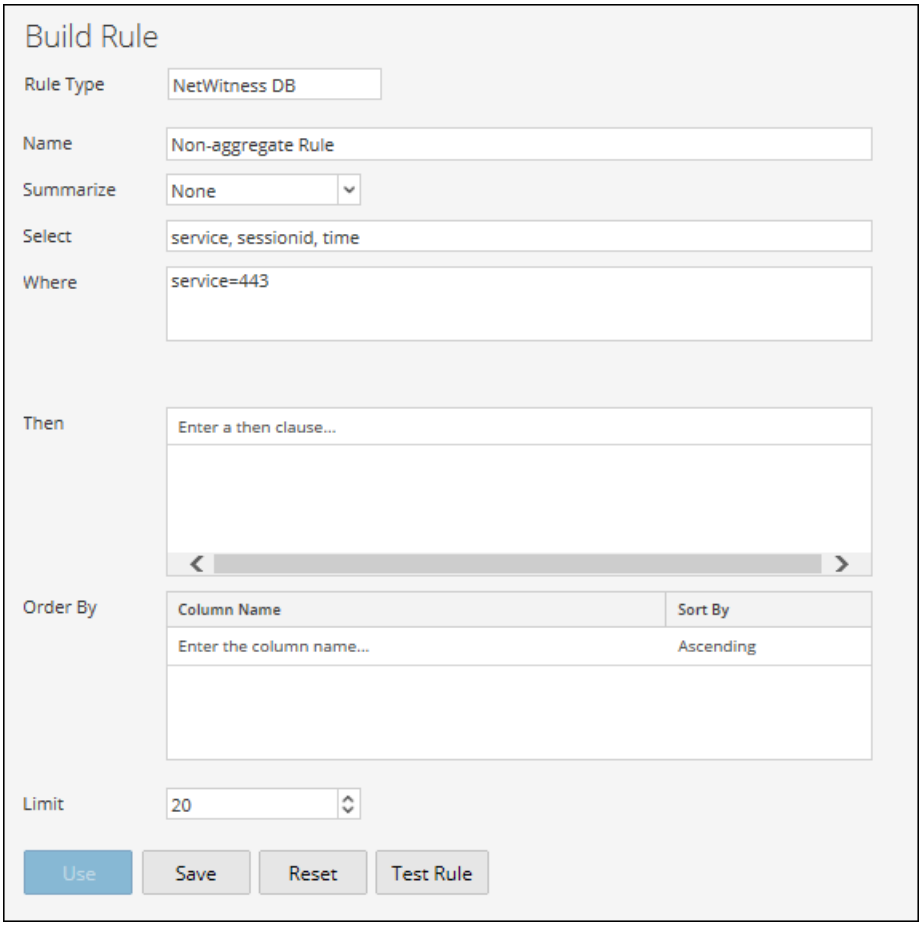
La clause select est une liste de valeurs séparées par une virgule. Par exemple : select sessionid,time,service.

Il existe deux types de clause select pour la règle NWDB :

- Règle non agrégée
- Règle agrégée

Règle non agrégée

Pour définir une règle sans regroupement, choisissez Aucun dans le champ Résumé. Dans une règle non agrégée, vous pouvez sélectionner n'importe quel nombre de métadonnées dans la clause *select*. Par exemple, select service, sessionid, time.

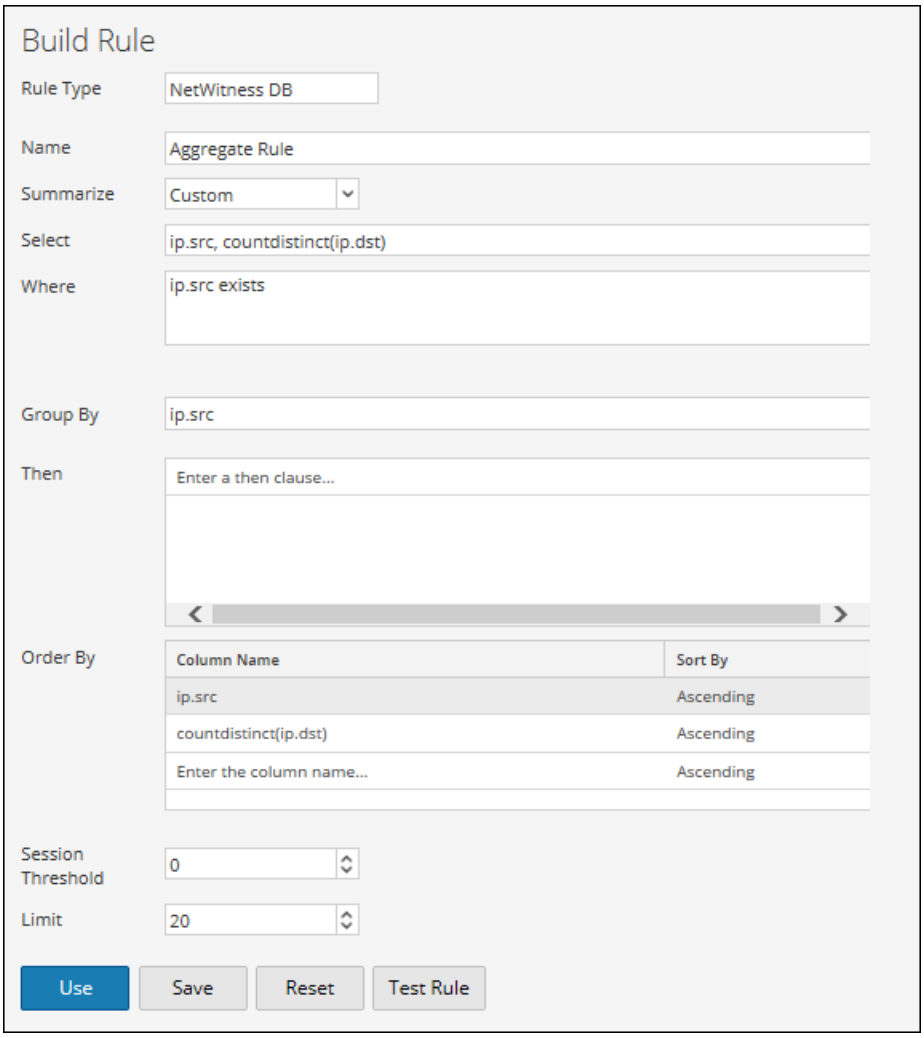


Règle agrégée

Pour effectuer une requête sur une métadonnée spécifique et sa valeur agrégée associée, vous devez utiliser la règle agrégée. Pour obtenir une règle agrégée, vous devez choisir l'une des trois métadonnées (Décompte d'événements, Nombre de paquets et Taille des sessions) ou choisir Personnaliser dans le champ **Résumé** pour inclure une fonction agrégée dans la clause *select*. Par exemple, select ip.src, sum (ip.dst). Lorsque l'option Règle d'agrégation personnalisée est activée, les champs suivants sont renseignés dans l'interface utilisateur :

- Regrouper par
- Réorganiser par
- Seuil de session

La figure suivante illustre la vue Élaborer une règle pour la règle agrégée.



Deux types de valeurs agrégées peuvent être interrogés :

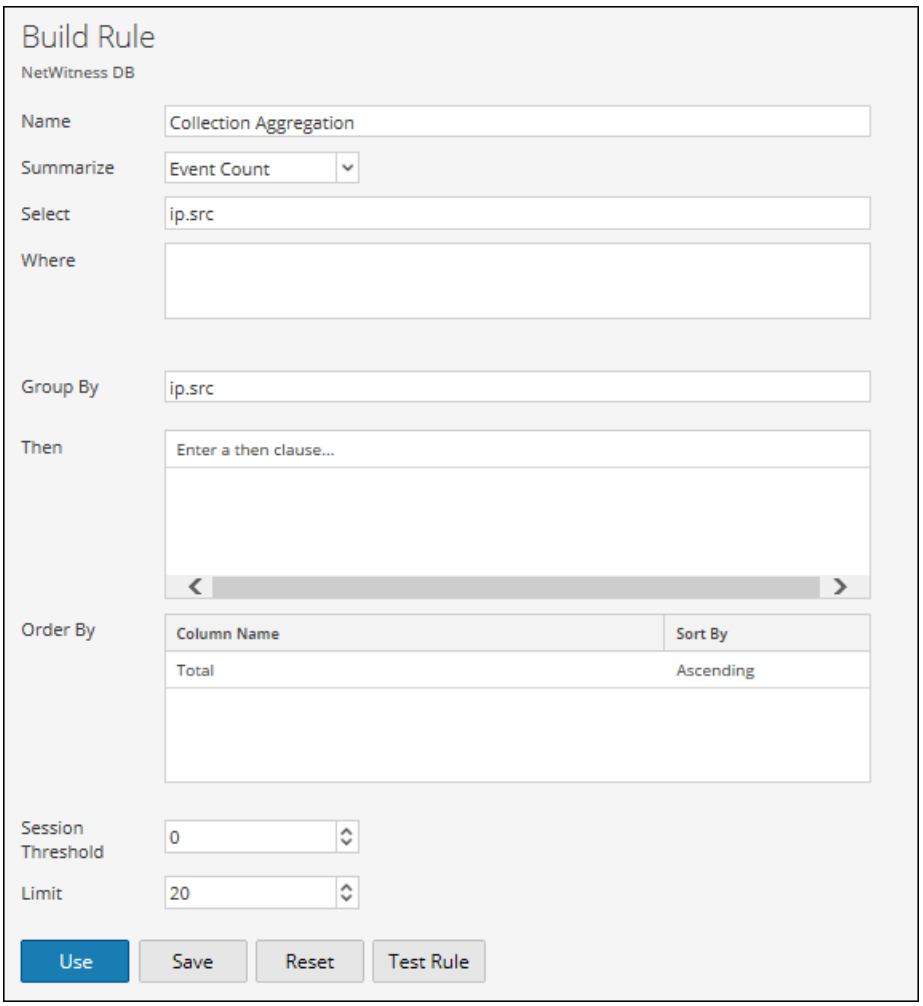
- Agrégation de collection
- Agrégation des métadonnées

Agrégation de collection

Avec l'agrégation de collection, vous pouvez obtenir des agrégats relatifs aux événements, à la session ou aux paquets. Les valeurs suivantes peuvent être interrogées dans une agrégation de collection :

- **Décompte d'événements** : Nombre total d'événements.
- **Nombre de paquets** : Nombre total de paquets.
- **Taille des sessions** : Taille totale de la session.

Ces options sont répertoriées dans le champ Résumé et peuvent être sélectionnées dans une règle.
Par exemple, choisissez un agrégat de collection (Décompte d'événements, Nombre de paquets ou Taille des sessions) dans le champ Personnalisé.



Agrégation des métadonnées

Avec l'agrégation des métadonnées, vous pouvez obtenir des agrégats de métavaleurs. Les fonctions suivantes sont les fonctions d'agrégation de métadonnées prises en charge :

- sum(meta)
- count(meta)
- countdistinct(meta)
- min(meta)
- max(meta)

- avg(meta)
- first(meta)
- last(meta)
- len(meta)
- distinct(meta)

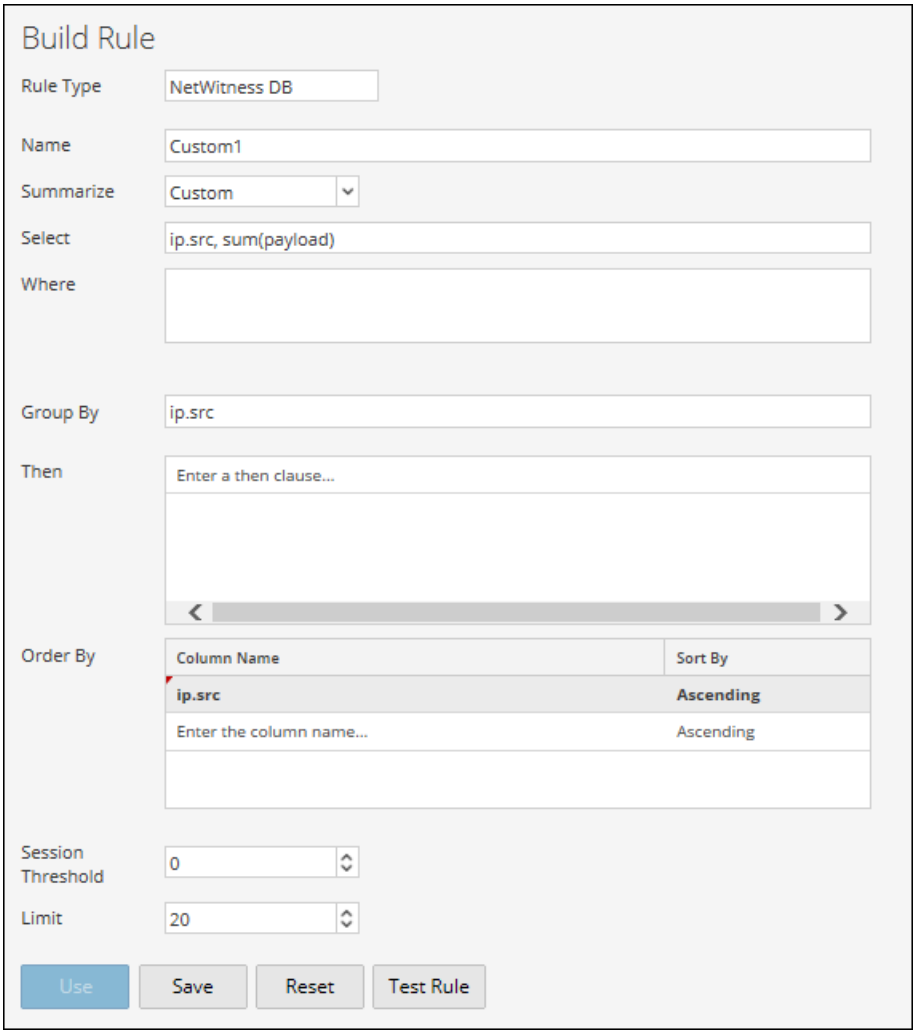
Fonctions d'agrégation méta prises en charge

Le service NWDB prend en charge les fonctions et syntaxes d'agrégation suivantes dans cette version.

Syntaxe	Fonction
sum (<meta>)	Somme de toutes les métavaleurs. Par exemple, si vous fournissez le champ sum(payload) dans la clause select, l'ensemble de résultats est la somme de la taille de la charge utile. **Remarque :** Le champ de métadonnées choisi pour la fonction agrégée sum doit être de type numérique.
count (<meta>)	Nombre total de champs de métadonnées qui serait renvoyé. Par exemple, si vous fournissez le champ countdistinct(ip.dst) dans la clause select, l'ensemble de résultats est le nombre de fois qu'une valeur ip.dst est renvoyée.
countdistinct (<meta>)	Nombre total de champs de métadonnées distincts qui serait renvoyé. Par exemple, si vous fournissez le champ countdistinct(ip.dst) dans la clause select, l'ensemble de résultats est le nombre de fois qu'une valeur ip.dst distincte est renvoyée.
min (<meta>)	Valeur minimale de toutes les métavaleurs. Par exemple, si vous fournissez le champ min(payload) dans la clause select, l'ensemble de résultats est la valeur minimale de la taille de la charge utile.
max (<meta>)	Valeur maximale de toutes les métavaleurs. Par exemple, si vous fournissez le champ max(payload) dans la clause select, l'ensemble de résultats est la valeur maximale de la taille de la charge utile.

Syntaxe	Fonction
avg (<meta>)	Moyenne de toutes les métavaleurs. Par exemple, si vous fournissez le champ avg(payload) dans la clause select, l'ensemble de résultats est la moyenne de la taille de la charge utile. **Remarque :** Le champ de métadonnée choisi pour la fonction agrégée avg doit être de type numérique.
first (<meta>)	Première occurrence de la valeur des métadonnées. Par exemple, si vous fournissez le champ first(ip.src) dans la clause select, l'ensemble de résultats est la première occurrence d'ip.src pour ce groupe.
last (<meta>)	Dernière occurrence de la valeur des métadonnées. Par exemple, si vous fournissez le champ last(ip.src) dans la clause select, l'ensemble de résultats est la dernière occurrence d'ip.src pour ce groupe.
len(<meta>)	Convertit toutes les valeurs de champ en longueur UInt32 plutôt que de retourner la valeur réelle. Cette longueur est le nombre d'octets permettant de stocker la valeur réelle, non la longueur de la structure stockée dans la métabase de données. Par exemple, la valeur méta « NetWitness » renvoie une longueur égale à 10. Tous les champs IPv4, comme ip.src, renvoie 4 octets.
distinct (<meta>)	Valeurs distinctes de la métadonnée. Par exemple, si vous fournissez le champ distinct(ip.src) dans la clause select, l'ensemble de résultats est le champ entier ip.src pour ce groupe.

Vous devez sélectionner Personnaliser dans le champ Résumé et fournir les métadonnées et les fonctions d'agrégation de métadonnées dans la clause select.



Remarque : Les fonctions d'agrégation de métadonnées ne sont pas utilisables dans une clause WHERE et les actions de règle comme min_threshold/max_threshold peuvent être utilisées pour filtrer les fonctions d'agrégation. Il est conseillé d'utiliser une clause WHERE plus affinée pour obtenir une meilleure performance de règle avec Group By .

Requête d'agrégation pour plusieurs métadonnées

Pour exécuter une requête d'agrégation pour plusieurs métadonnées, procédez comme suit :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer est mis en évidence, et la vue **Règles** s'affiche

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

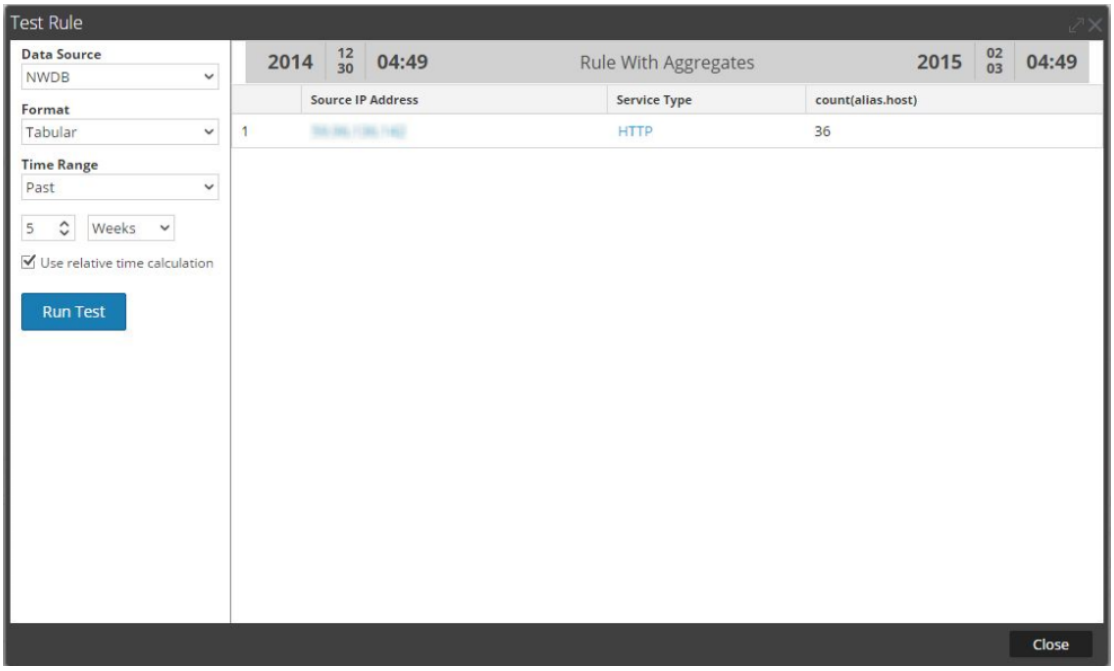
   Par exemple, saisissez les métadonnées suivantes dans les champs mis en évidence -ci-après :

SELECT: ip.src, service, count(alias.host)
ALIAS: Adresse IP source, type de service, count(alias.host)
WHERE: ip.src = 59.96.136.142

Remarque : Dans le champ alias, vous pouvez saisir un nom pour les colonnes utilisées dans la clause select. Si vous ne spécifiez pas d'alias pour l'un des champs dans la clause select, alors la description par défaut sera utilisée. Par exemple, si la clause select a Field1, Field2, Field3, Field4 et que l'alias a uniquement Field1, Field3, Field4, alors une description par défaut est utilisée pour Field2.

3. Cliquez sur le bouton **Tester la règle** au bas de l'écran.

   La page Tester la règle s'affiche.



Résumé

Résumé détermine le type de résumé ou d'agrégation correspondant à la règle.

Nom	Valeur de configuration
Résumé	Pour interroger les métadonnées sans regroupement personnalisé, sélectionnez : • **Aucun** : les données sont alors regroupées par session. Pour obtenir des agrégats liés à une collection (sessions/événements/paquets), sélectionnez l'une des options suivantes : • **Nombred'événements** : Nombre total d'événements. • **Nombre de paquets** : Nombre total de paquets. • **Taille des sessions** : Taille totale de la session. Pour obtenir des agrégats basés sur des métadonnées, sélectionnez : • **Personnaliser** : Cela indique que la fonction d'agrégation de métadonnées attendue est définie dans la clause select de la règle.

Réorganiser par

Trier par détermine le mode de tri de l'ensemble de résultats.

Nom	Valeur de configuration
Nom de colonne	**Nom de la colonne** correspond au nom des colonnes à utiliser pour trier les résultats. Par défaut, la valeur est vide. Lorsque vous cliquez sur une colonne, la valeur est remplie d'après le champ Résumé. • Pour Aucun et Personnaliser, la valeur est remplie en fonction des entrées du champ Select. Vous pouvez sélectionner dans cette liste ou ajouter un nom personnalisé. • Pour Décompte d'événements, Nombre de paquets et Taille des sessions, les valeurs acceptées sont Total et Valeur. • Total : le tri est effectué par valeur agrégée • Valeur : le tri est effectué par groupe et par métadonnée
Trier par	**Trier par** détermine l'ordre dans lequel vous souhaitez trier les résultats. Les valeurs sont les suivantes : • Ordre croissant • Ordre décroissant

Seuil de session

Le seuil de session est le paramètre d'optimisation qui permet de rechercher chaque valeur unique possible
de la métadonnée sélectionnée dans les sessions correspondantes. Le seuil est un nombre entier compris entre 0 (par défaut) et 2147483647. Le seuil 0 analyse toutes les sessions correspondantes.

Remarque : Si vous fournissez une valeur non nulle (une valeur supérieure à zéro), les résultats agrégés sont inexacts. Cette valeur ne peut être utilisée que si vous êtes intéressé par les valeurs uniques au lieu des valeurs agrégées.

Clause where prise en charge

Syntaxe	Description
where <champ1> [<opérateur-champ>] < valeur1>,<valeur2>,<valeur3-valeur4> <opérateur-logique> <champ2>,etc.	La clause where est une liste de valeurs et plages de champ séparées par des virgules qui est utilisée par la fonction NwValues. Dans la clause where, les valeurs de chaînes doivent être placées entre apostrophes. Par exemple, where username = 'admin' && service = 22.
where <champ1> [<champ-opérateur>] <Liste1>	Vous pouvez utiliser une liste dans la clause where pour exécuter un rapport sur plusieurs valeurs. Par exemple, where ip.src exists && alias.host exists && alias.host contains $[Rapports utilisateur/Liste alias hôte]. Lorsque vous utilisez la liste, vous devez la spécifier en utilisant le format $[<chemin>/<Nom de la liste>].

Dans la clause where, assurez-vous que la syntaxe est correcte en fonction du type de métadonnées.
Par exemple,
pour toutes les métadonnées de type texte, utilisez des guillemets : par exemple, username = ‘user1'.
Pour toutes les adresses IP, les adresses Ethernet et les méta de type numérique, n'utilisez pas de guillemets ; par exemple, service = 80 && ip.src = 192.168.1.1.
Pour les méta de type date et heure, si le format de date et heure est 'AAAA-MM-JJ HH:MM:SS‘, utilisez des guillemets.
Si le format de la date et de l'heure est 1448034064 (nombre de secondes depuis EPOCH (1er janvier 1970)), n'utilisez pas de guillemets.

Remarque : Si une liste est utilisée dans la règle, assurez-vous que les valeurs de la liste sont mises ou non entre guillemets, selon le type de métadonnées utilisé. Si vous activez la case à cocher **Des guillemets seront insérés pour toutes les valeurs** sur la page de définition de liste (pour plus d'informations, reportez-vous à la section Créer des listes ou des groupes de listes dans Configurer une règle), toutes les valeurs de liste sont mises entre guillemets.

Opérateurs pris en charge dans la clause where

Syntaxe	Description
=	Renvoie les résultats pour lesquels le champ est égal à une valeur fournie. Par exemple, tcp.dstport = 21-25,110 renvoie une session avec les ports de destination TCP 21, 22, 23, 24, 25 ou 110.
!=	Renvoie les résultats pour les champs qui ne correspondent pas aux valeurs spécifiées. Par exemple, eth.type !=0x0800 renvoie les sessions en dehors de la plage hexadécimale (valeur décimale de 2048), c'est-à-dire tous les protocoles autres qu'IP.
begins	Recherche une valeur au début d'un texte ou d'un champ binaire.
contient	Recherche une correspondance partielle dans un texte ou une valeur binaire.
ends	Recherche une valeur à la fin d'un texte ou d'un champ binaire.
exists	Si la valeur de champ existe, quelle qu'elle soit, l'opération renvoie la valeur true.
!exists	Si la valeur de champ n'existe pas, l'opération renvoie la valeur true.
length	Évalue la longueur du champ. Par exemple, username length 20-u renvoie un nom d'utilisateur qui contient 20 caractères ou plus.
regex	Effectue une recherche des expressions régulières dans du texte ou des valeurs binaires.
not	L'opérateur not est utilisé pour annuler une clause ou une condition. Par exemple, (not(user.dst ends "$")) n'affichera pas les valeurs pour la destination de l'utilisateur.

Clause then prise en charge

Syntaxe	Description
then <action de règle>	La clause then contient une action de règle qui manipule l'ensemble de résultats original d'une règle afin de rendre la sortie du rapport plus concrète oui d'ajouter d'autres fonctionnalités que l'interrogation des données et leur affichage. Par exemple, dedup (nom de fichier).

Champ Limite

Ce champ indique la limite à appliquer à la requête lors de l'extraction des données de la base de données. Si l'ensemble des résultats est trié par nombre d'événements, nombre de paquets ou taille de session, la limite représentera les premières (ou dernières) valeurs N à renvoyer. Si l'ensemble de résultats n'est pas trié, les premières valeurs N sont renvoyées.

Actions de règle

La syntaxe de règle de source de données NWDB prend en charge les actions de règle suivantes :

- dedup
- filter_on
- filter_out
- lookup_and_add
- max_threshold
- min_threshold
- regex
- sum_count
- sum_values
- show_whats_new

dedup (string field)

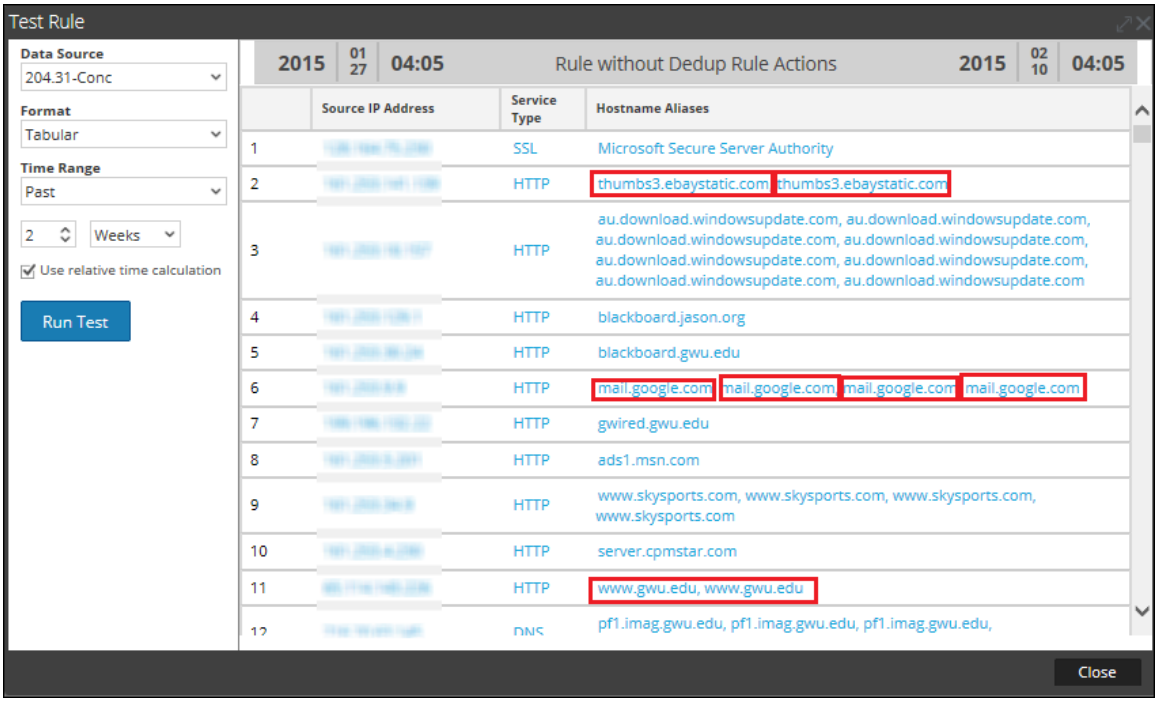
dedup supprime les entrées en double dans un ensemble de résultats non trié et n'affiche que les données pertinentes. L'action de règle dedup supprime les entrées en double d'un champ spécifique du rapport afin que seule la première occurrence de cette valeur soit répertoriée dans le rapport.

Remarque : L'action de règle dedup ne peut pas être utilisée avec une règle agrégée.

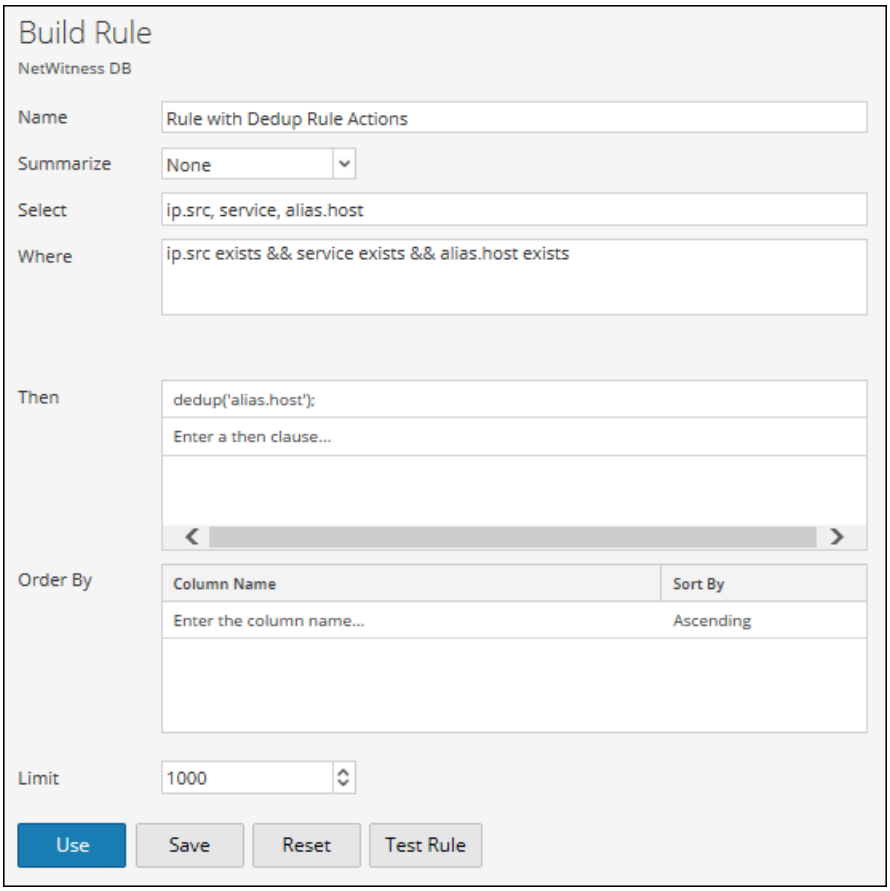
Par exemple, les métadonnées générées par une session individuelle sont souvent répétitives, notamment pour les sessions contenant de nombreuses recherches DNS ou les sessions Web qui accèdent souvent au même hôte pour utiliser diverses ressources (javascript, css, etc.). Pour supprimer les entrées en double de l'hôte, vous pouvez utiliser l'action de règle dedup.

Exemple :

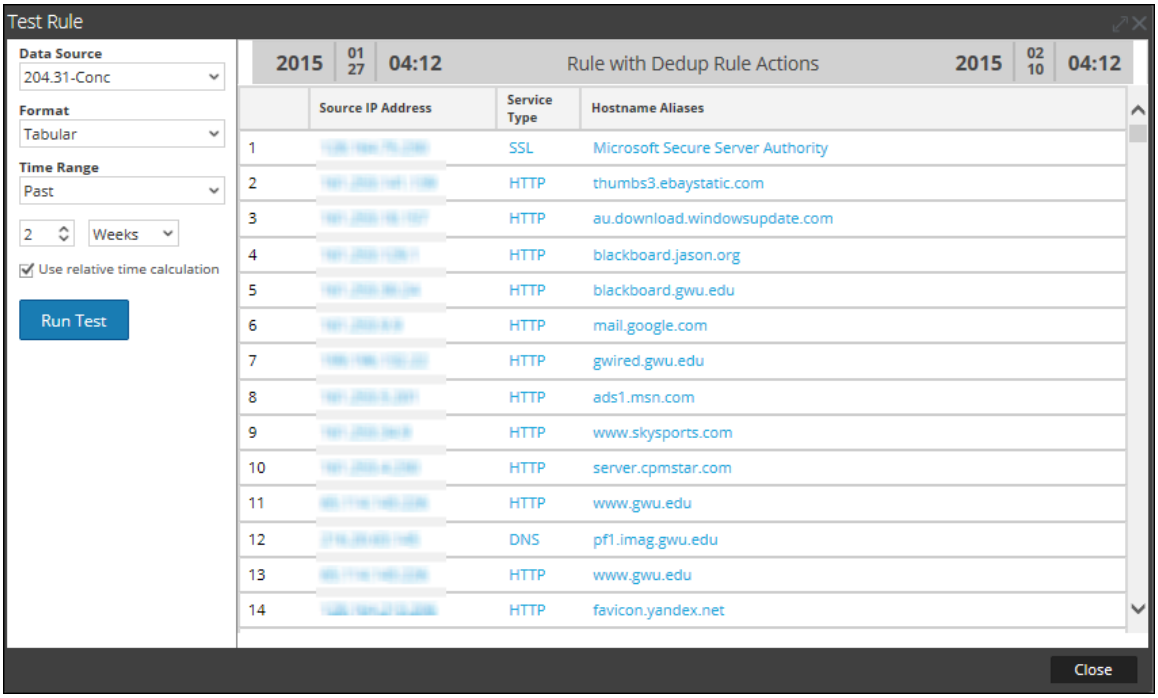
L'exemple suivant est un ensemble de résultats volumineux qui peut être tronqué en supprimant les valeurs en double dans la même session.



La figure suivante illustre l'utilisation de l'action de règle dedup pour supprimer les entrées en double dans l'ensemble de résultats.



La valeur en double de chaque entrée de l'ensemble de résultats de la règle est réduite à une seule valeur.



filter_on (filtre de chaîne, champ de chaîne, paramètre booléen matchExact)

`filter_on` supprime les valeurs qui contiennent le critère `filter` de l'ensemble de résultats. Si l'ensemble de résultats contient plusieurs champs, vous devez sélectionner un champ spécifique auquel le filtre est appliqué. Pour ajouter d'autres résultats à un ensemble de résultats unique, incluez une fonction telle que lookup_and_add.

Le paramètre matchExact détermine si la correspondance est exacte ou partielle.

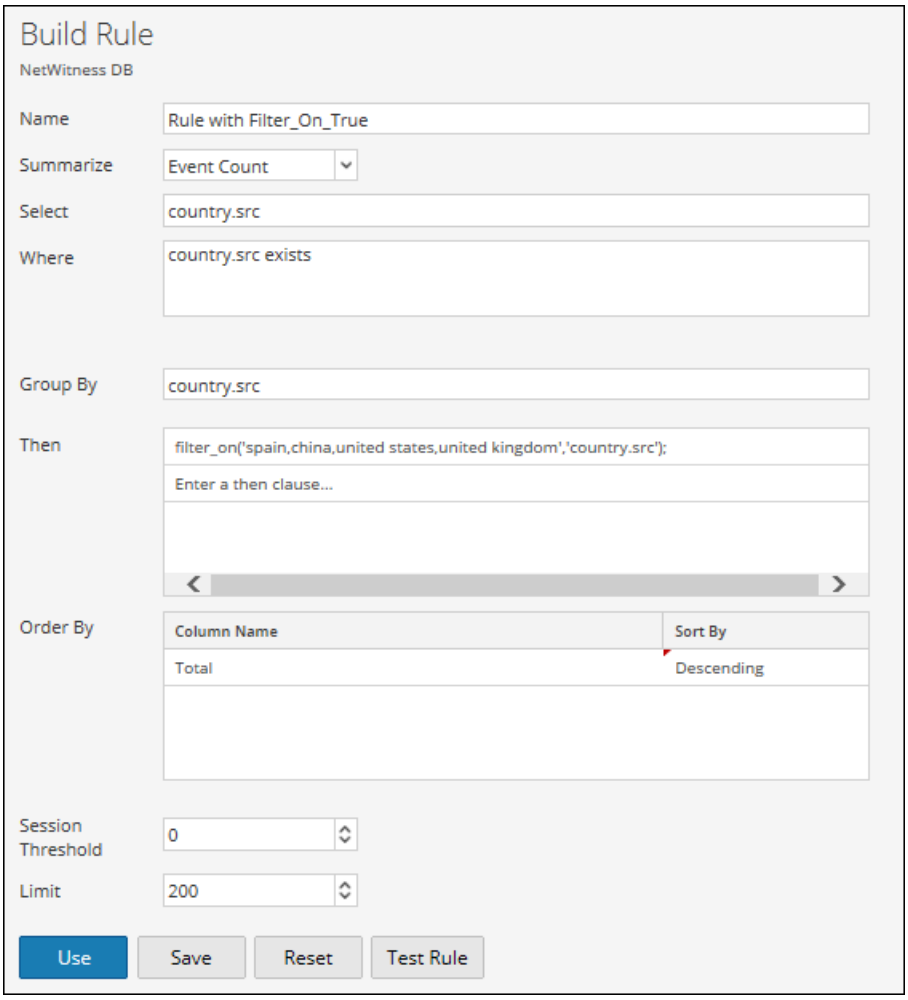
- Si matchExact est défini sur `false`,, toute valeur qui contient le texte de filtrage est considérée comme une occurrence.
- Si matchExact est défini sur `true`, seules les valeurs qui correspondent au texte de filtrage fourni sont incluses dans l'ensemble de résultats.

Remarque : Si le paramètre matchExact est spécifié, le comportement par défaut de l'action de règle est de correspondre exactement au texte spécifié dans le paramètre de filtrage. Pour spécifier que les résultats contenant le texte de filtrage doivent être conservés dans l'ensemble de résultats, les utilisateurs doivent définir le paramètre matchExact sur false.

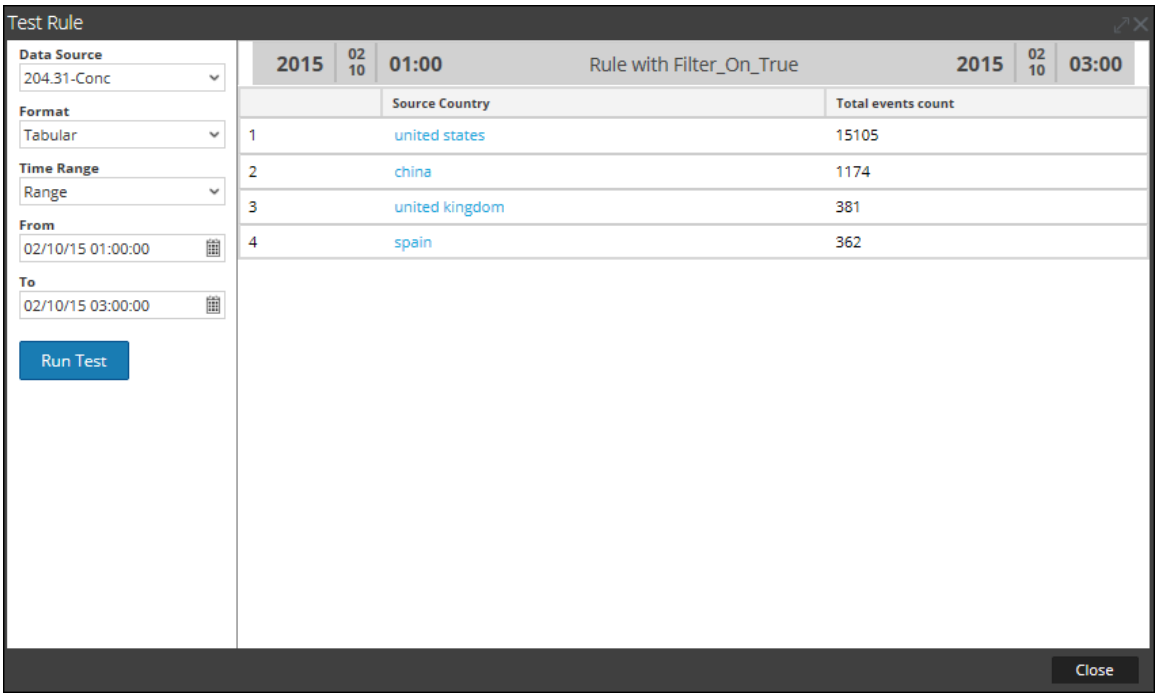
Exemple :

La figure ci-dessous présente la liste des pays et leur nombre d'événements.

La figure suivante illustre une action de règle filter_on, destinée à exclure tous les pays, sauf l'Espagne, la Chine, les États-Unis et le Royaume-Uni, de l'ensemble de résultats.



La figure suivante affiche le résultat de l'action de règle filter_on.



Une autre méthode d'exclusion d'entrées de l'ensemble de résultats est de créer une liste de variables à exclure. Par exemple, vous pouvez créer une liste contenant les valeurs Royaume-Uni, France et Allemagne. Vous pouvez utiliser cette liste dans l'action de règle pour obtenir le même ensemble de résultats. Par exemple, si vous créez une liste appelée COUNTRY_LIST, vous pouvez utiliser cette liste comme suit :

```
filter_on ('$COUNTRY_LIST', 'country.src', 'false');
```

```
filter_out (string filter, string field)
```

```
filter_out (string filter, string field, bool matchExact)
```

filter_out supprime les valeurs qui contiennent les critères *filter* de l'ensemble de résultats. Si l'ensemble de résultats contient plusieurs champs, vous devez sélectionner un champ spécifique auquel le filtre est appliqué (par exemple, vous pouvez utiliser une fonction lookup_and_add pour ajouter des résultats à un seul ensemble de résultats).

Le paramètre matchExact détermine si la correspondance est exacte ou partielle.

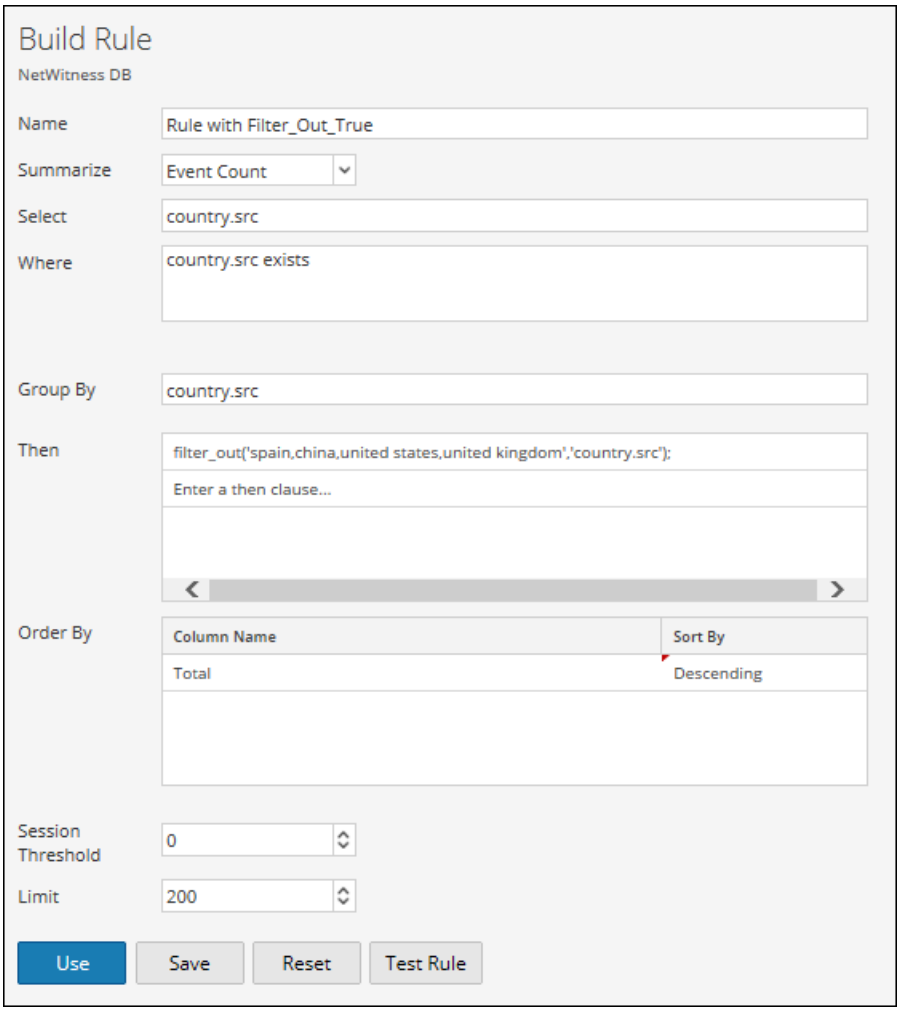
- Si matchExact est défini sur false, toute valeur qui contient le texte de filtrage est considérée comme une occurrence.
- Si matchExact est défini sur true, seules les valeurs qui correspondent au texte de filtrage fourni sont exclues de l'ensemble de résultats.

Remarque : Si le paramètre `matchExact` est spécifié, le comportement par défaut de l'action de règle est de correspondre exactement au texte spécifié dans le paramètre de filtrage. Pour spécifier que les résultats contenant le texte de filtrage doivent être supprimés de l'ensemble de résultats, les utilisateurs doivent définir le paramètre `matchExact` sur false.

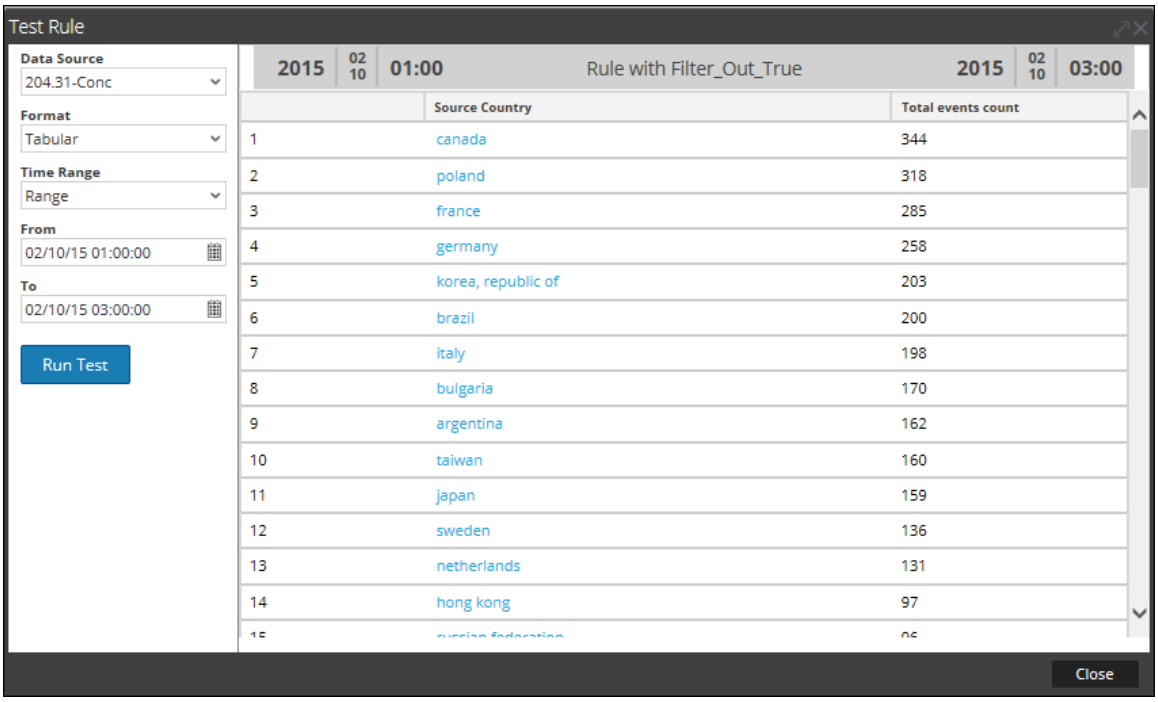
Exemple :

La figure ci-dessous présente la liste des pays et leur nombre d'événements.

La figure suivante illustre l'action de règle filter_out, destinée à supprimer le nombre d'événements pour l'Espagne, la Chine, les États-Unis et le Royaume-Uni de l'ensemble de résultats.



La figure suivante affiche le résultat de l'action de règle filter_out.




```
lookup_and_add (string select, string field)

lookup_and_add (string select, string field, int limit)

lookup_and_add (string select, string field, int limit, boolean inherit)

lookup_and_add (string select, string field, int limit, boolean inherit,
string extraWhere)

lookup_and_add(string select, string field, int limit, boolean inherit,
string extraWhere, boolean aggregate)
```

Cette action de règle itère sur une liste de valeurs dans un ensemble de résultats et recherche d'autres métadonnées pour continuer à décrire les relations entre les différents éléments d'un ensemble de résultats.

Remarque : L'action de règle lookup_and_add ne peut être utilisée qu'avec une règle agrégée.

Le premier paramètre ,select, désigne le type de métadonnées qui doivent être ajoutées aux éléments de l'ensemble de résultats. Le second paramètre, field, spécifie l'emplacement de l'ensemble de résultats auquel l'ajout doit être appliqué. Une limite doit également être appliquée pour éviter de charger l'ensemble de résultats avec un ensemble de résultats volumineux.

Par défaut, les requêtes suivantes émises vers le SDK hériteront de la clause where de la règle parent. Pour utiliser une clause where unique, vous pouvez spécifier une valeur booléenne dans le quatrième paramètre avec la valeur false, et vous pouvez spécifier une clause where différente dans le cinquième paramètre.

Remarque : Si vous utilisez une clause where unique dans votre requête, veillez à placer les arguments entre apostrophes (') et les valeurs de chaîne entre guillemets (").

Désormais, avec l'ajout de l'option Résumé **personnalisé** et de la fonction **Group By** , le résultat peut être obtenu même sans l'action de règle lookup_and_add. La nouvelle syntaxe de règle avec Regrouper par affiche le résultat dans une structure à plat et est donc supérieure à la syntaxe de règle précédente sans la fonctionnalité Regrouper par . Il est donc recommandé de modifier/mettre à jour manuellement les règles avec l'action de règle lookup_and_add et d'utiliser la clause Group By lorsqu'elle est applicable.

Remarque : L'action de règle Lookup_And_Add rule n'est prise en charge que si la clause select n'a qu'une seule fonction de métadonnées et d'agrégation.

Par exemple, consultez les scénarios ci-dessous : dans l'exemple **2a**, l'action de règle lookup_ and_add rule est utilisée. Au lieu d'utiliser l'action de règle lookup_and_add, le même résultat peut être obtenu en utilisant l'option Résumé **personnalisé** et la fonction **Regrouper par** . Voir l'exemple **2b** ci-dessous.

Cependant, l'action de règle lookup_and_add rule continue à être prise en charge par les règles NWDB dans les conditions suivantes :

- Toutes les versions de règles NWDB avec le résumé sous la forme Décompte d'événements, Nombre de paquets et Taille des sessions.
- Pour l'option Résumé personnalisé, la règle lookup_and_add rule ne doit avoir qu'un seul groupe par métadonnée avec une seule fonction d'agrégation, celle-ci devant être sum() ou count().

Remarque : Elle n'est pas prise en charge pour « Résumé-Aucun ».

Par exemple, l'action de règle lookup_and_add peut être utilisée pour les règles suivantes :

- select ip.src, sum(size) group by ip.src
- select ip.src, count(filename) group by ip.src

Elle ne peut pas être utilisée pour les règles suivantes :

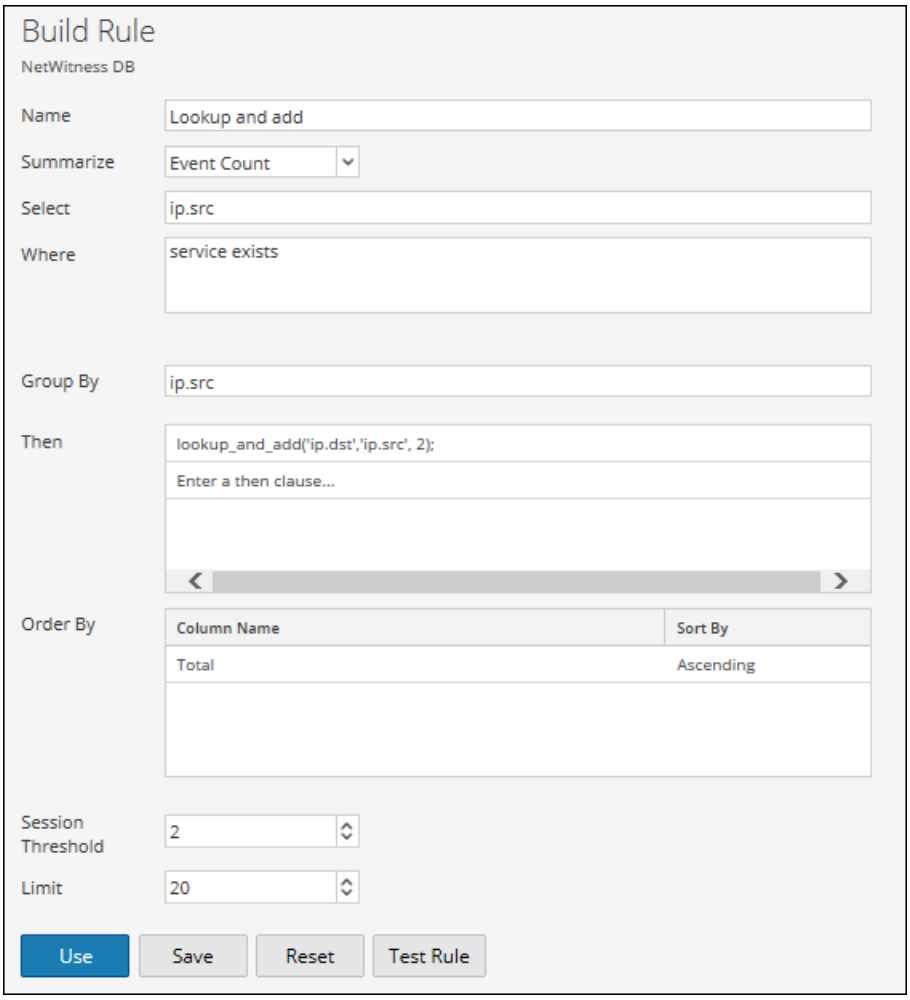
- select ip.src, sum(size),count(filename) group by ip.src
- select ip.src, sum(size),avg(size) group by ip.src
- select ip.src,ip.dst count(filename) group by ip.src,ip.dst

Exemples :

1. lookup_and_add('ip.dst','ip.src', 2);

Cette action de règle itèrerait chaque ip.src dans l'ensemble de résultats initial et rechercherait les deux premières adresses IP de destination avec chaque ip.src.

La figure ci-dessous présente la définition de règle.

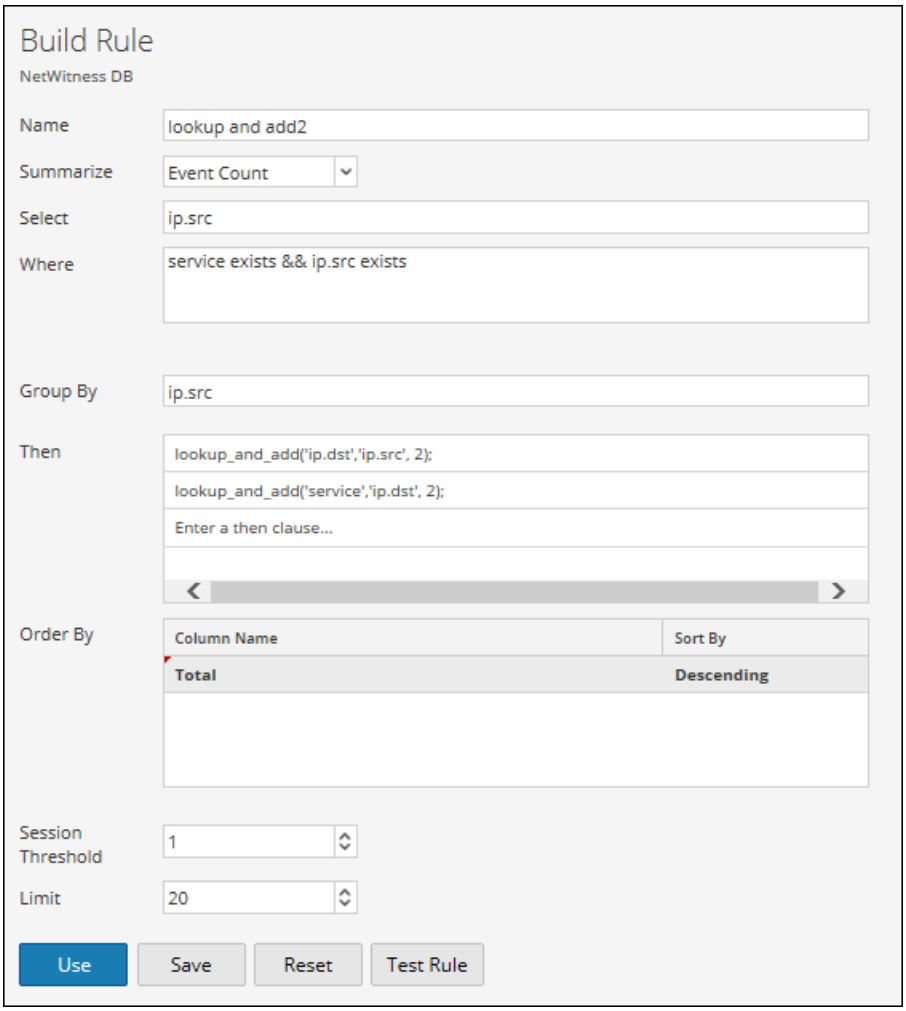


La figure ci-dessous présente l'ensemble de résultats contenant les adresses IP source et les deux principales adresses IP de destination avec chaque ip.src.

2a. lookup_and_add('ip.dst','ip.src', 2); lookup_and_add('service','ip.src', 3);

Cette action de règle itèrerait chaque ip.src dans l'ensemble de résultats initial et rechercherait les deux premières adresses IP de destination avec chaque ip.src et les trois ports principaux utilisés par chaque ip.src.

La figure ci-dessous présente la définition de règle.



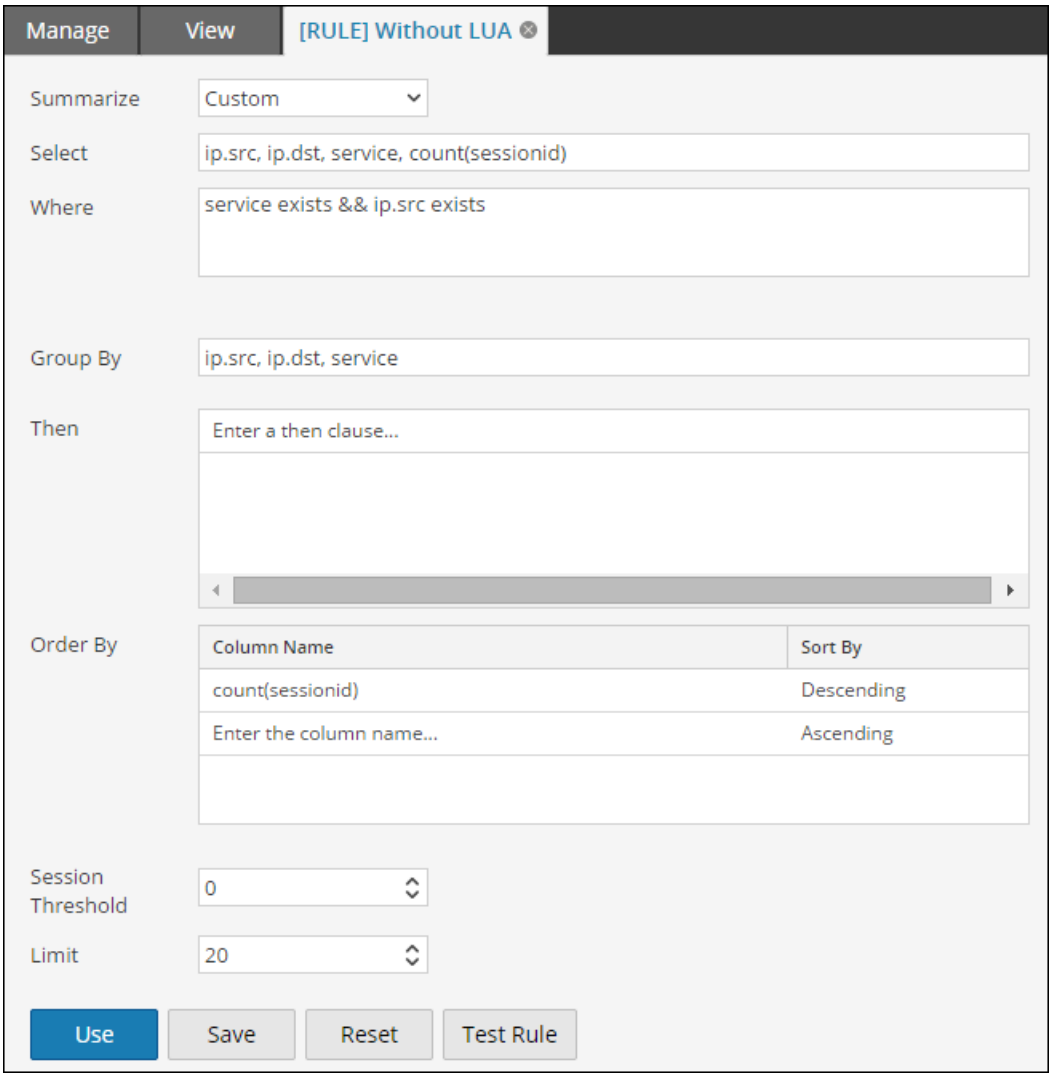
La figure ci-dessous présente l'ensemble de résultats contenant les adresses IP source et les deux principales adresses IP de destination avec chaque ip.src et les trois principaux ports utilisés par chaque ip.src.

Vous pouvez rendre la requête aussi complexe que vous le souhaitez en sélectionnant différents champs dans l'ensemble de résultats et en effectuant des ajouts à différentes parties. Par exemple, vous voudrez peut-être connaître les fichiers que chaque IP source avait utilisés. Cependant, comme la règle parent a une clause WHERE service = 6667, et que le comportement par défaut de cette action de règle est d'effectuer un ajout à la clause WHERE initiale, il s'avère nécessaire de remplacer la clause WHERE parente. La meilleure façon de comprendre ce concept est de consulter l'action de règle lookup_and_add call lookup_and_add ('ip.dst','ip.src',2) précédente. La requête effective envoyée au serveur est SELECT ip.dst WHERE service = 6667 &&ip.src = 206.42.199.194. Pour forcer la clause WHERE à remplacer la partie service = 6667 de la clause WHERE (héritée de la règle parente), l'utilisateur peut spécifier un quatrième paramètre false, comme indiqué dans l'exemple 3.

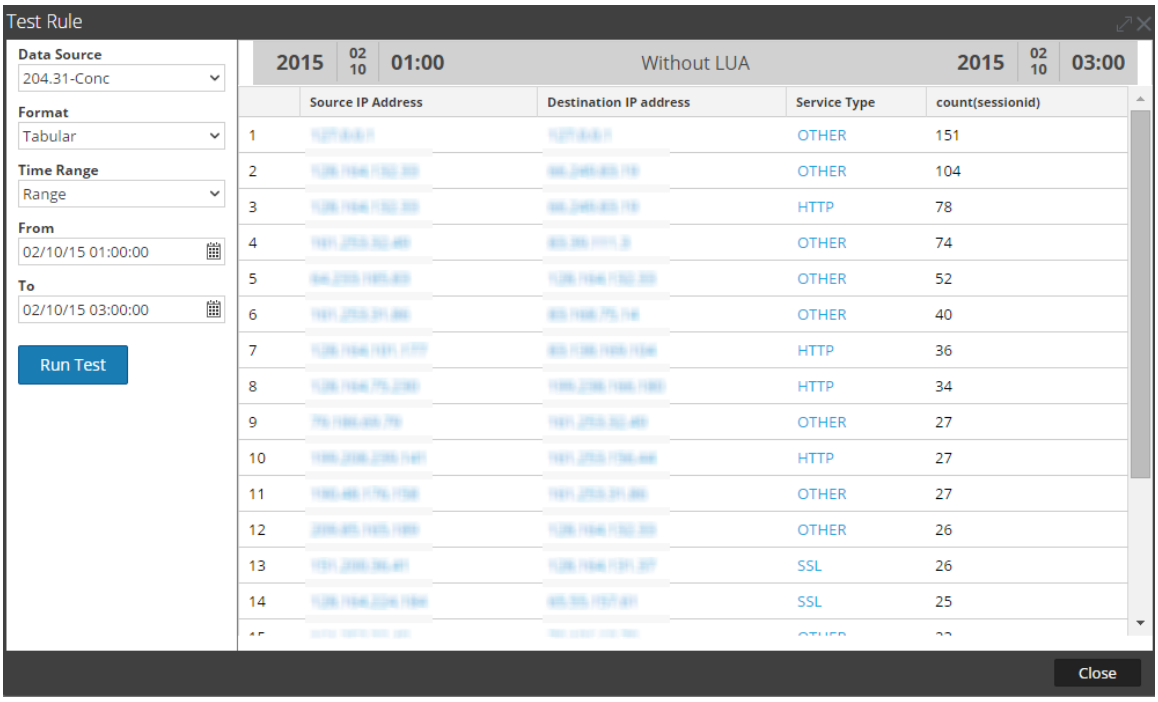
2b. Règle Without Lookup_and_add

Cette règle utilise l'option Résumé personnalisé et la fonction Regrouper par pour trier les résultats.

La figure ci-dessous présente la définition de règle.



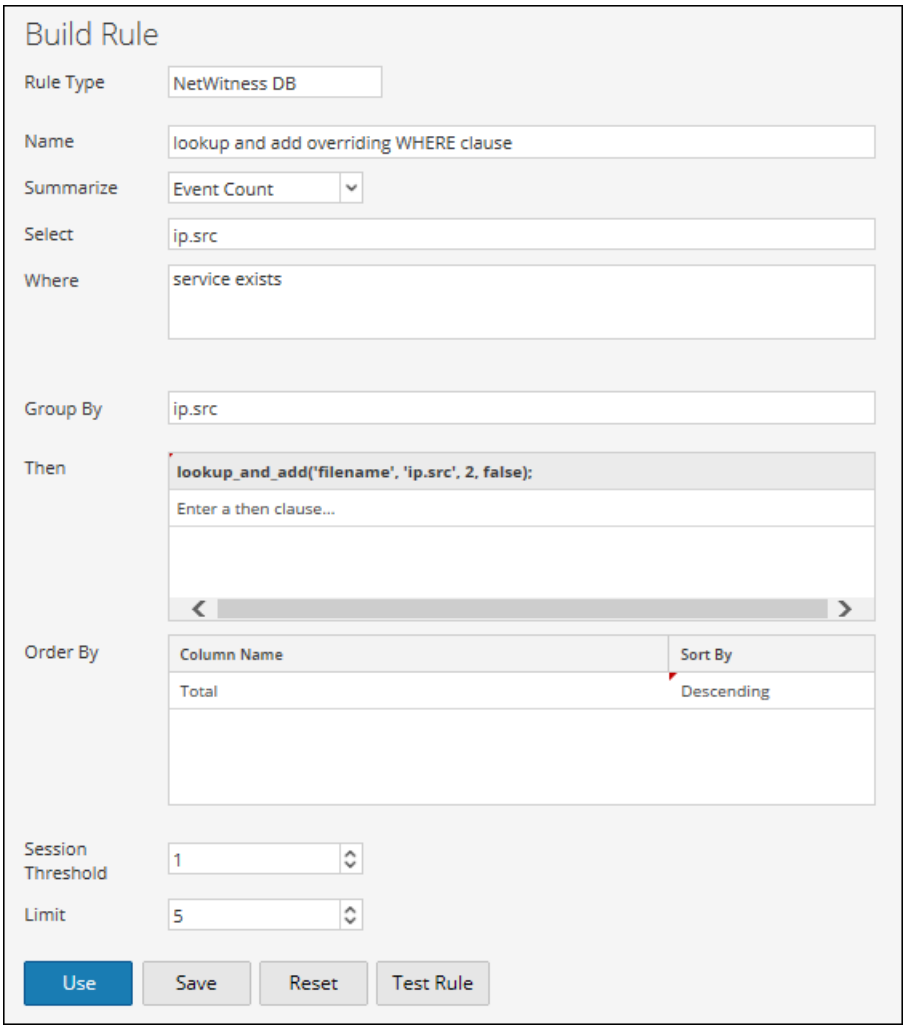
La figure ci-dessous présente l'ensemble de résultats contenant les adresses IP source et les deux principales adresses IP de destination avec chaque ip.src et les trois principaux ports utilisés par chaque ip.src.



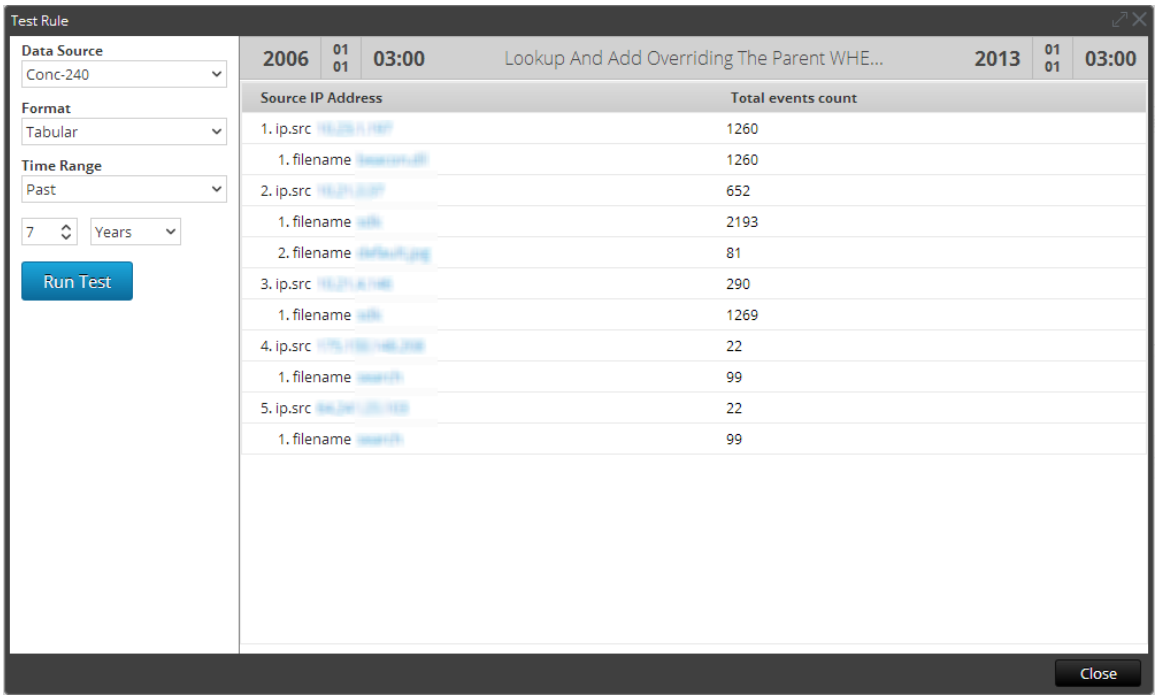
3. lookup_and_add('filename', 'ip.src', 2, false);

Cet appel émet une requête vers le serveur similaire à `SELECT filename WHERE ip.src = 90.0.0.142` au lieu de `SELECT filename WHERE service = 6667' && ip.src = 90.0.0.142`, car vous avez spécifié l'action de règle de sorte que la clause `WHERE` initiale de la règle parent soit ignorée.

La figure ci-dessous présente la définition de règle.



La figure ci-dessous présente l'ensemble de résultats.

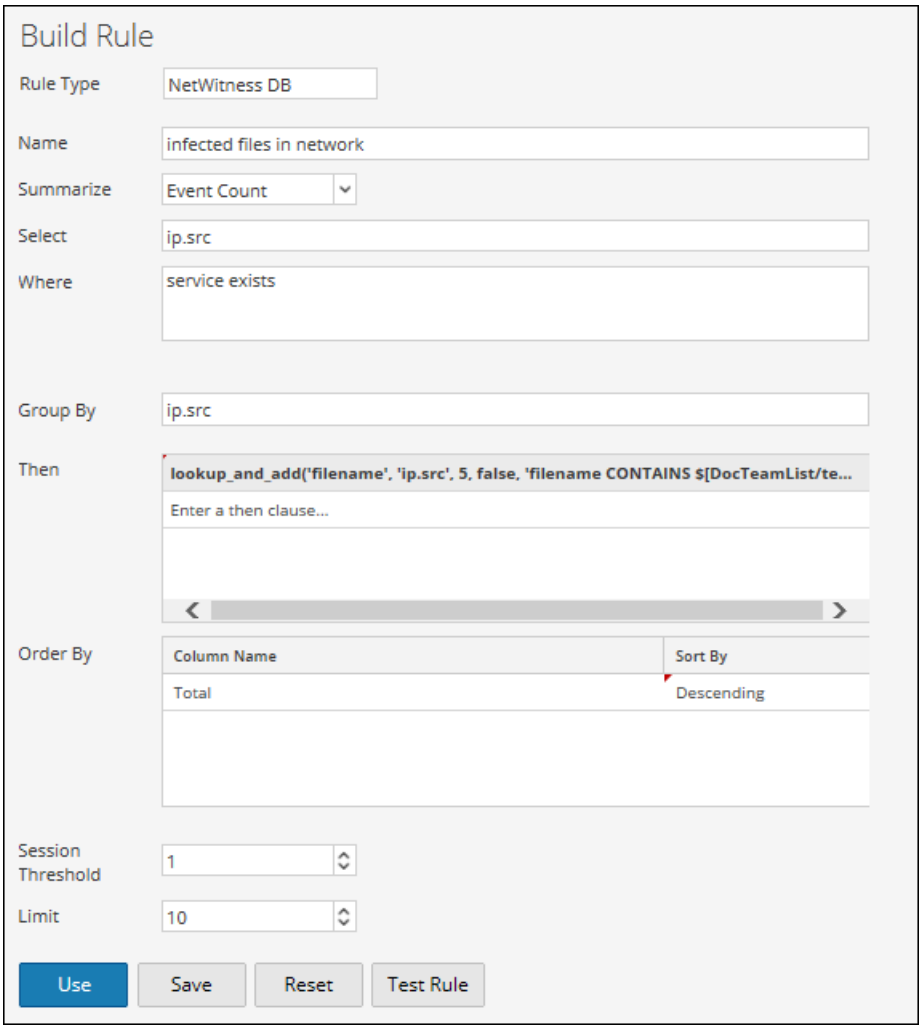


Si la liste test se trouve dans un groupe nommé netwitness, vous pouvez accéder à cette liste avec la syntaxe suivante.

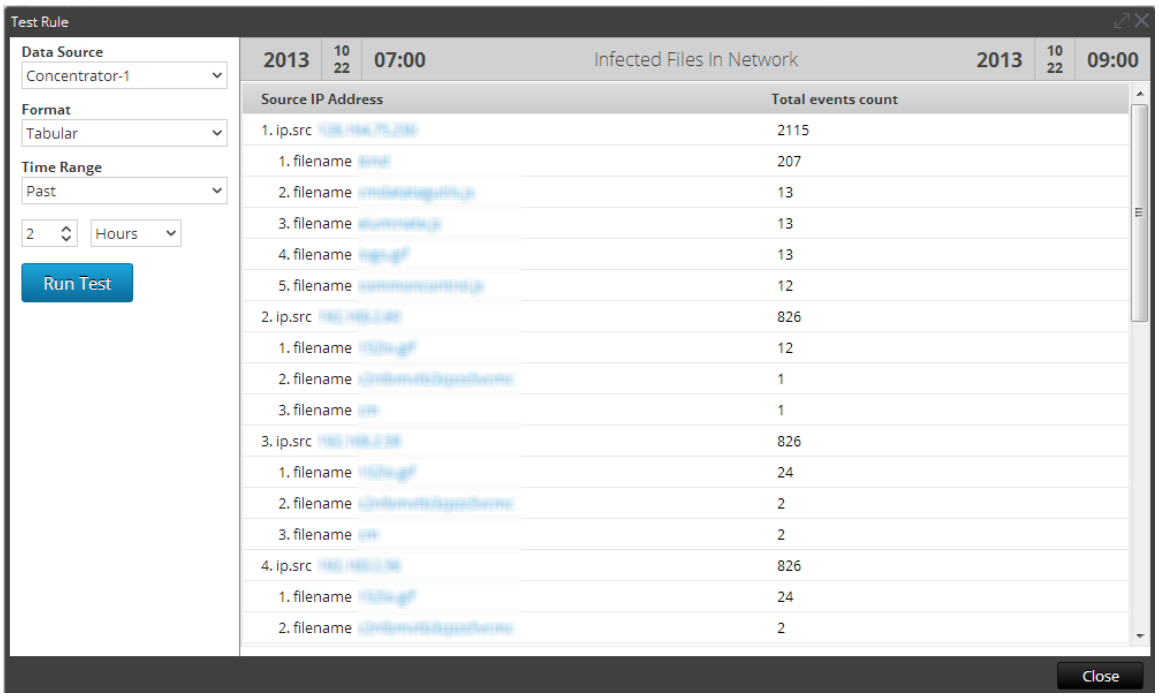
Vous pouvez même limiter encore ces résultats ajoutés pour n'inclure que les noms de fichier avec l'extension .gif en utilisant le cinquième paramètre dans l'action de règle. Le cinquième paramètre vous permet de spécifier des critères de clause WHERE supplémentaires. Les fichiers avec l'extension .gif seront stockés dans la liste **test** dans un groupe nommé **DocTeamList**. Cette liste est accessible avec la syntaxe suivante : threat.source = $[DocTeamList/test]
Cela peut être référencé dans le paramètre de clause where supplémentaire de la manière suivante :

4. lookup_and_add('filename', 'ip.src', 5, false, 'filename CONTAINS $[DocTeamList/test]');

La figure ci-dessous présente la définition de règle.



La figure ci-dessous présente l'ensemble de résultats.

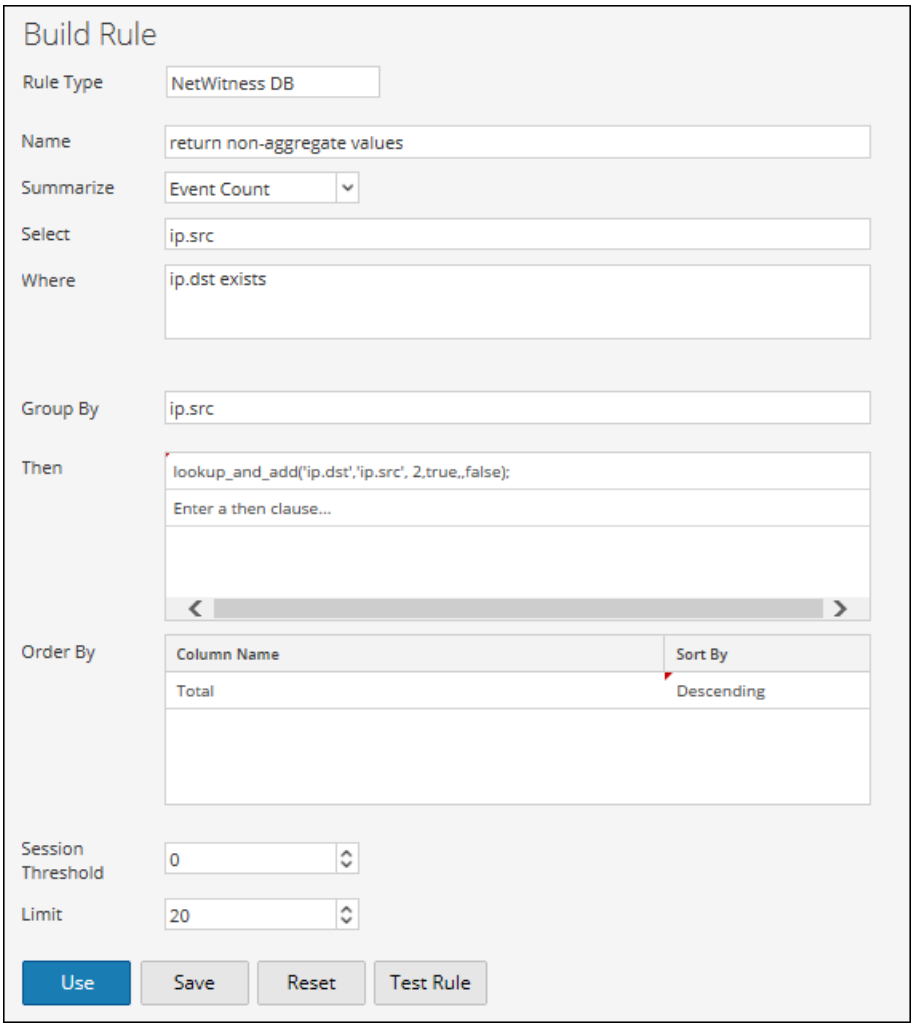


5. lookup_and_add('ip.dst','ip.src', 2,true,,false);

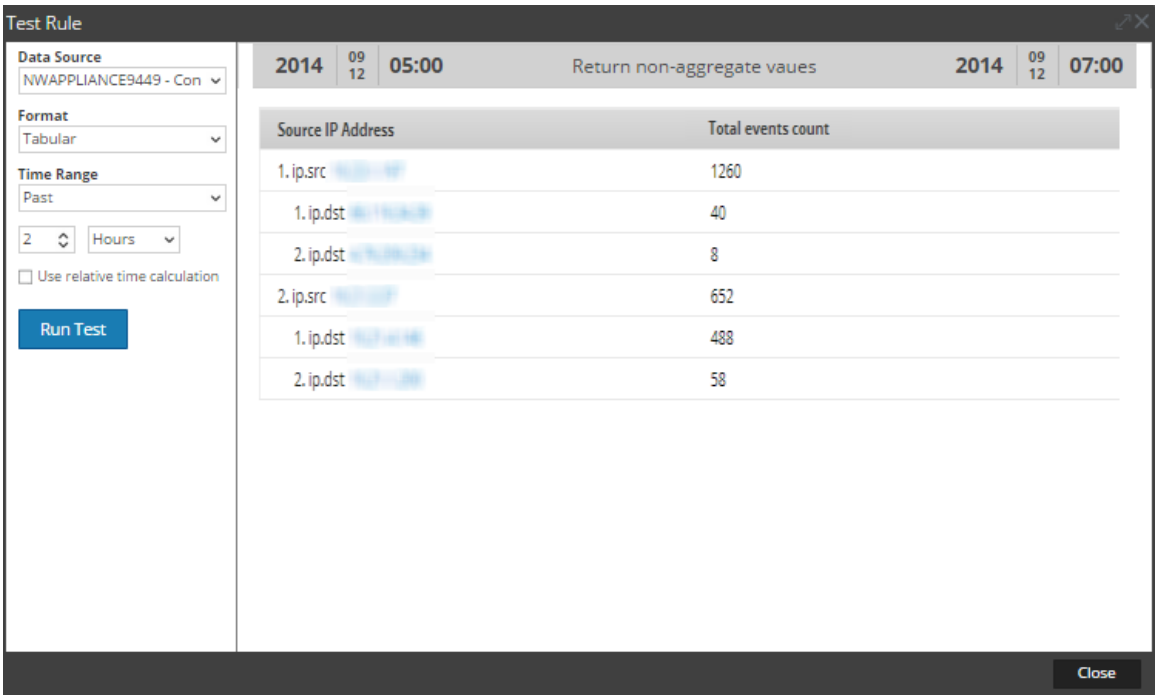
Cette action de règle itèrerait chaque ip.src dans l'ensemble de résultats initial et rechercherait les deux premières adresses IP de destination avec chaque ip.src. Le paramètre aggregate est défini sur false. Cela implique que les agrégats seront ignorés concernant les valeurs de recherche et donc que les requêtes de recherche seront exécutées plus rapidement.

Remarque :
La valeur par défaut du paramètre aggregate est true. Lorsque le paramètre aggregate est défini sur false, Reporting Engine transmet threshold=1, Sort by='value' et Order=Ascending à NWDB pour accélérer l'exécution des requêtes de recherche.
. Vous devez définir le paramètre aggregate sur false, lorsque la règle contient des fonctions agrégées ou qu'elle est exécutée sur une plage d'heures étendue. La règle peut ainsi s'exécuter plus rapidement.

La figure ci-dessous présente la définition de règle.



La figure ci-dessous présente l'ensemble de résultats.




```
max_threshold (string quantity)
```

```
max_threshold (string quantity, string field)
```

max_threshold supprime de l'ensemble de résultats les résultats comportant une quantité supérieure à la quantité seuil maximale. La quantité peut être en termes de nombre ou de taille et est relative aux options de tri de la règle parent. Cela signifie que si vous triez une règle par taille, l'action de règle s'attend à ce que vous spécifiiez le paramètre en octets (vous pouvez ajouter KB, MB, GB, TB au paramètre pour simplifier la conversion de taille).

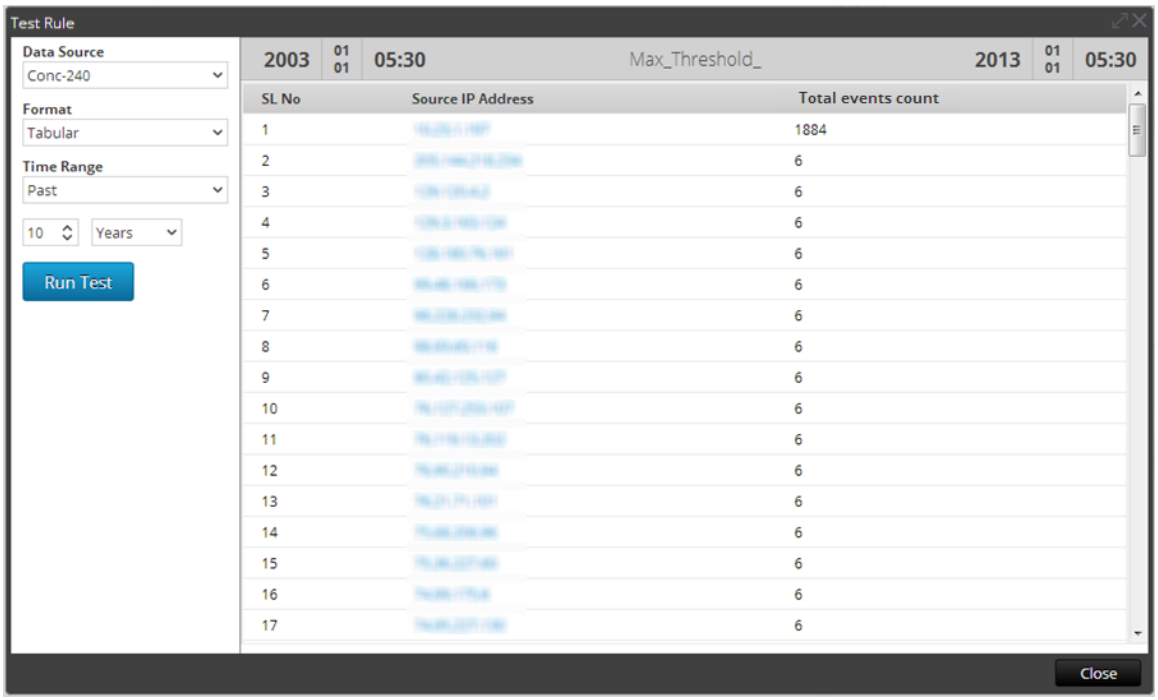
La règle max_threshold peut être également utilisée pour filtrer les valeurs en fonction des valeurs de la fonction agrégée. Utilisez la syntaxe basée sur le type de récapitulation employé dans la règle, comme indiqué ci-dessous :

- max_threshold(String quantity): Peut être utilisé pour filtrer les éléments Décompte d'événements, Nombre de paquets et Taille des sessions.
- max_threshold(String quantity, String field): Peut être utilisé pour filtrer les valeurs des agrégats Personnalisé ou de tous les métas.

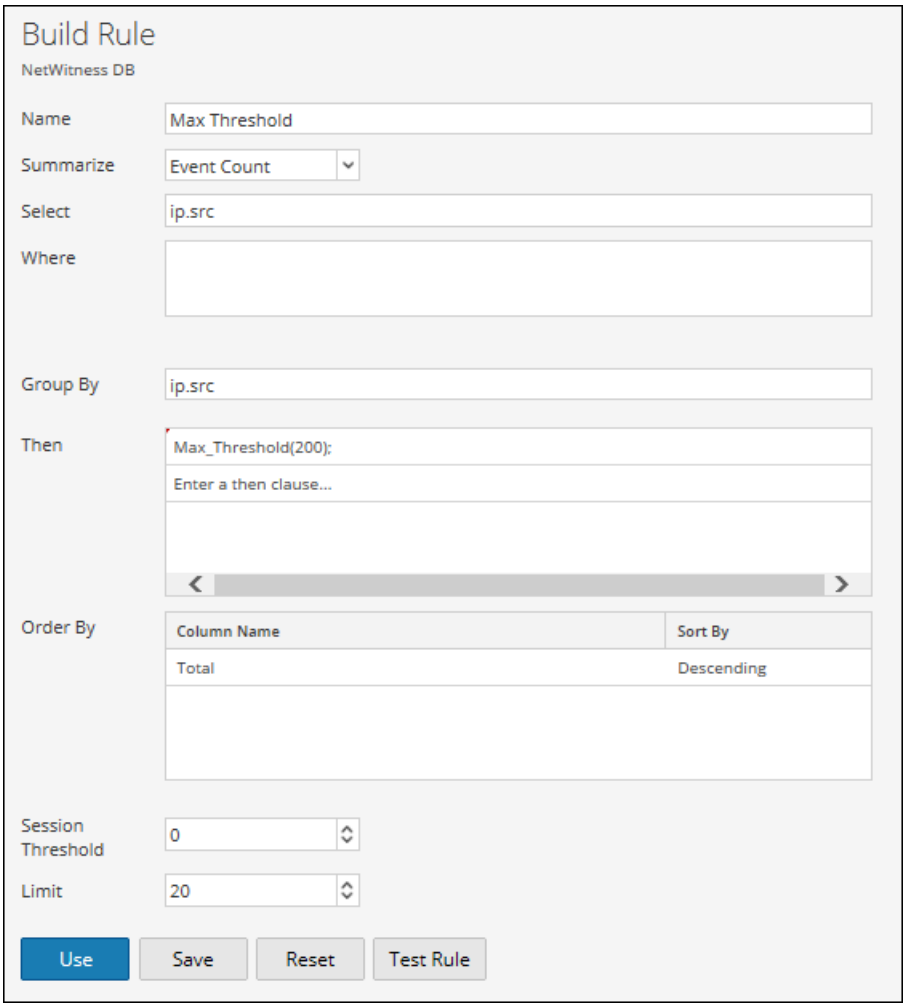
Exemples :

1. max_threshold(200);

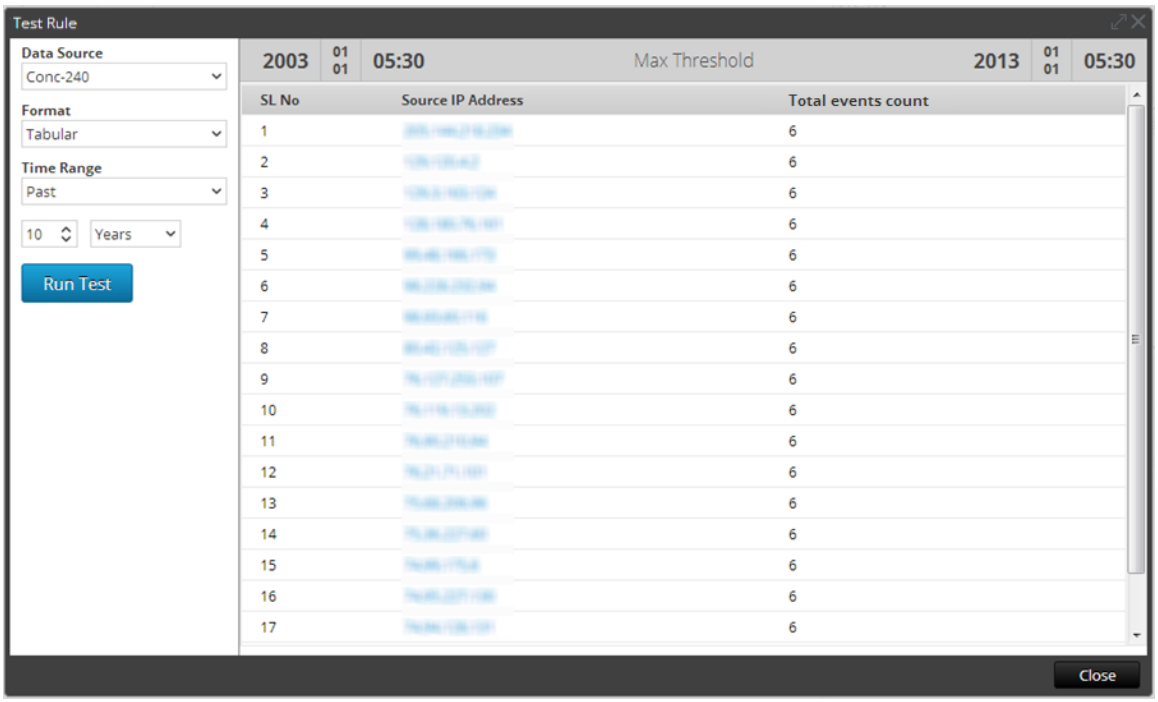
La figure ci-dessous illustre le résultat sans l'argument max_threshold. Les résultats de sortie contiennent des nombres d'événements supérieurs à 200.



La figure ci-dessous présente une action de règle max_threshold qui place une limite de 200 octets sur la sortie. Toute sortie contenant plus de 200 octets de données n'est pas répertoriée.

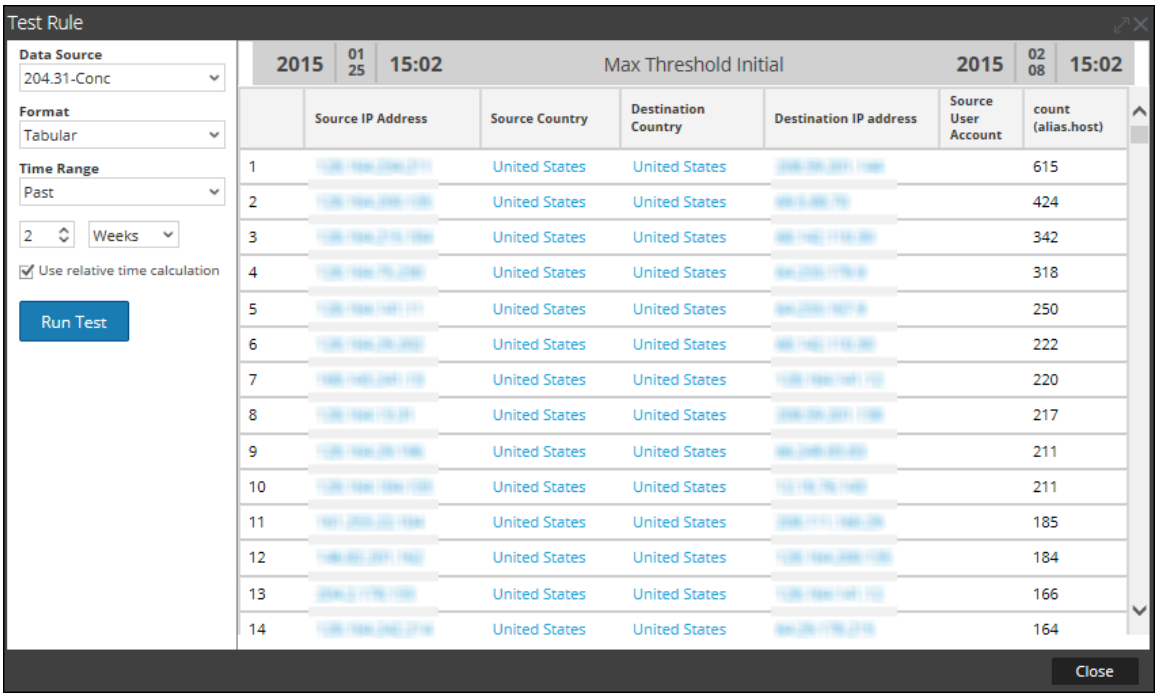


La figure suivante présente le résultat lorsque l'action de règle max_threshold est appliquée. Le résultat numéroté 1 dans la capture d'écran ci-dessus est supprimé du résultat.

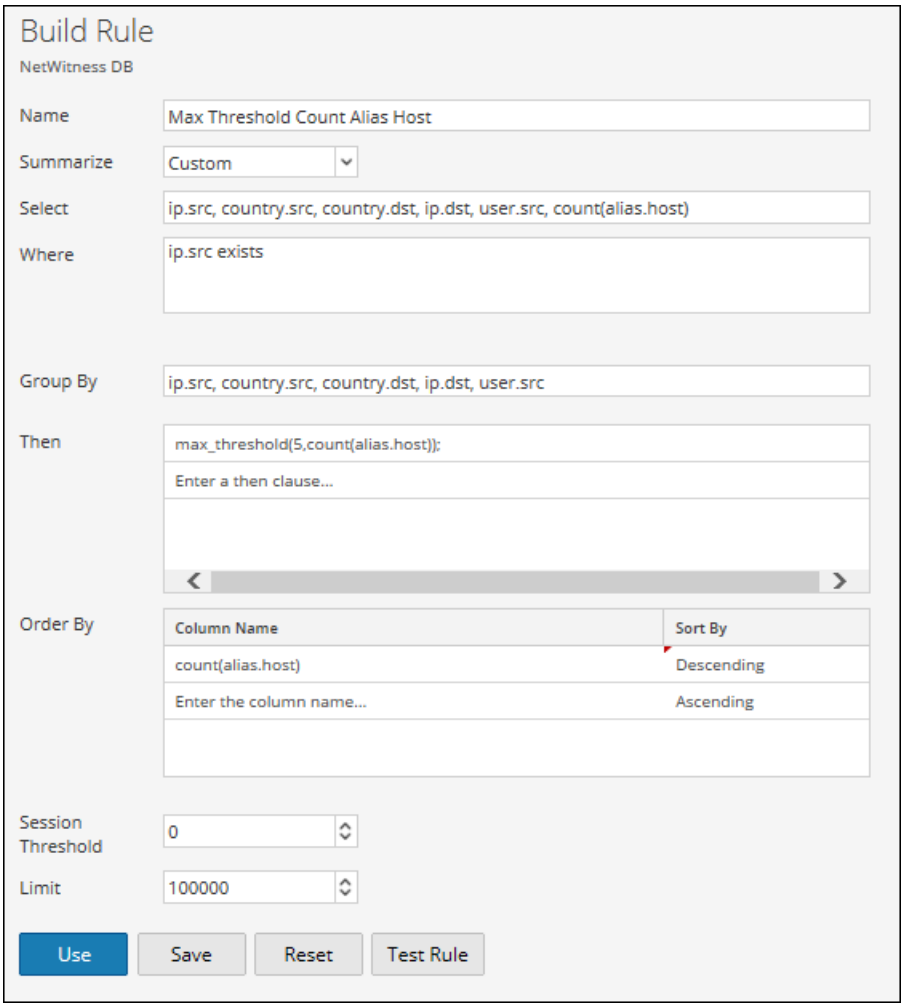


2. max_threshold(5,count(alias.host));

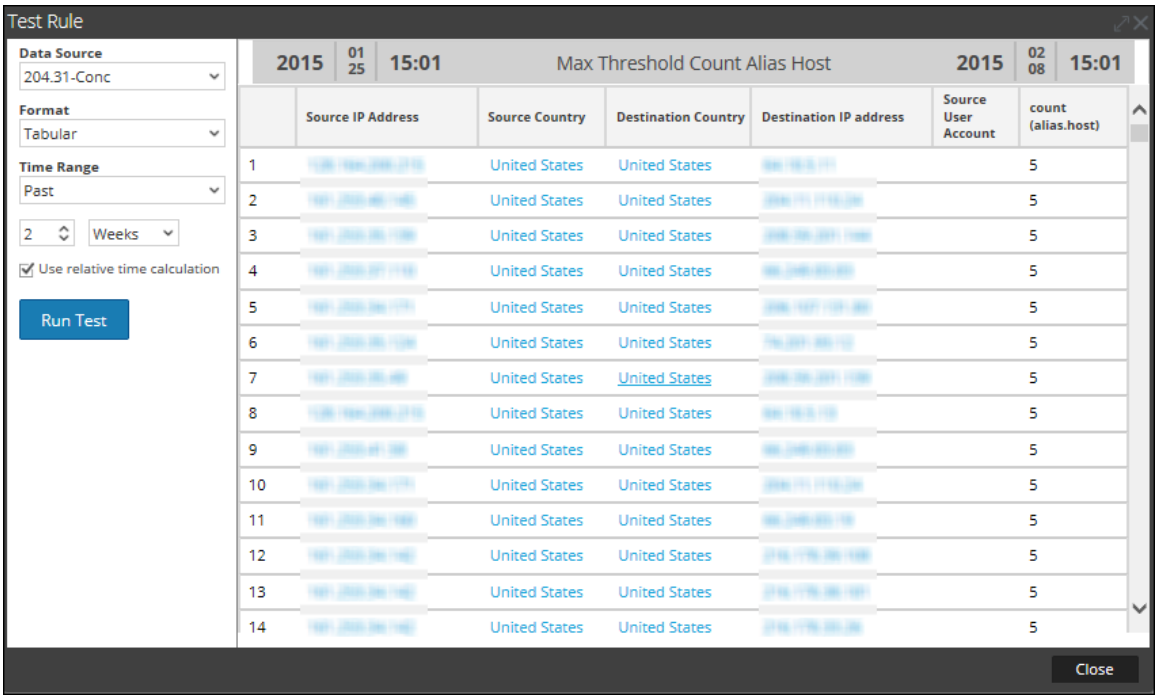
La figure ci-dessous illustre le résultat sans l'argument max_threshold. Les résultats de sortie contiennent un nombre de alias.host supérieur à 5.



La figure ci-dessous présente une action de règle max_threshold qui place une limite de 5 sur la sortie. Toute sortie comportant une valeur supérieure à 5 n'est pas répertoriée.



La figure ci-dessous présente le résultat lorsque l'action de règle max_threshold est appliquée. Toute sortie comportant une valeur supérieure à 5 est supprimée du résultat.



min_threshold (string quantity)

min_threshold supprime de l'ensemble de résultats les résultats comportant une quantité inférieure à la quantité seuil minimale. La quantité peut être en termes de nombre ou de taille et est relative aux options de tri de la règle parent. Cela signifie que si vous triez une règle par taille, l'action de règle s'attend à ce que vous spécifiiez le paramètre en octets (vous pouvez ajouter KB, MB, GB, TB au paramètre pour simplifier la conversion de taille).

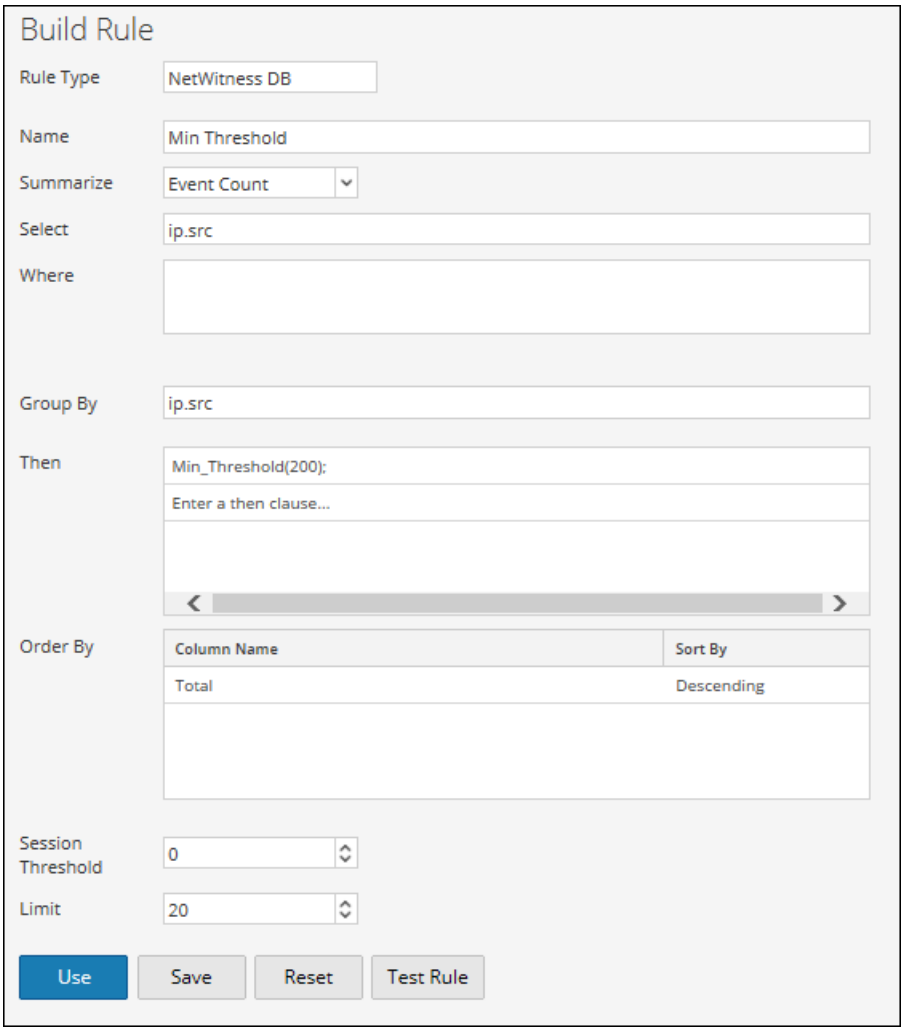
La règle min_threshold peut également être utilisée pour filtrer les valeurs en fonction des valeurs de la fonction agrégée. Utilisez la syntaxe basée sur le type de récapitulation employé dans la règle, comme indiqué ci-dessous :

- min_threshold(String quantity): Peut être utilisé pour filtrer les éléments Décompte d'événements, Nombre de paquets et Taille des sessions.
- min_threshold(String quantity, String field): Peut être utilisé pour filtrer les valeurs des agrégats Personnalisé ou de tous les métas.

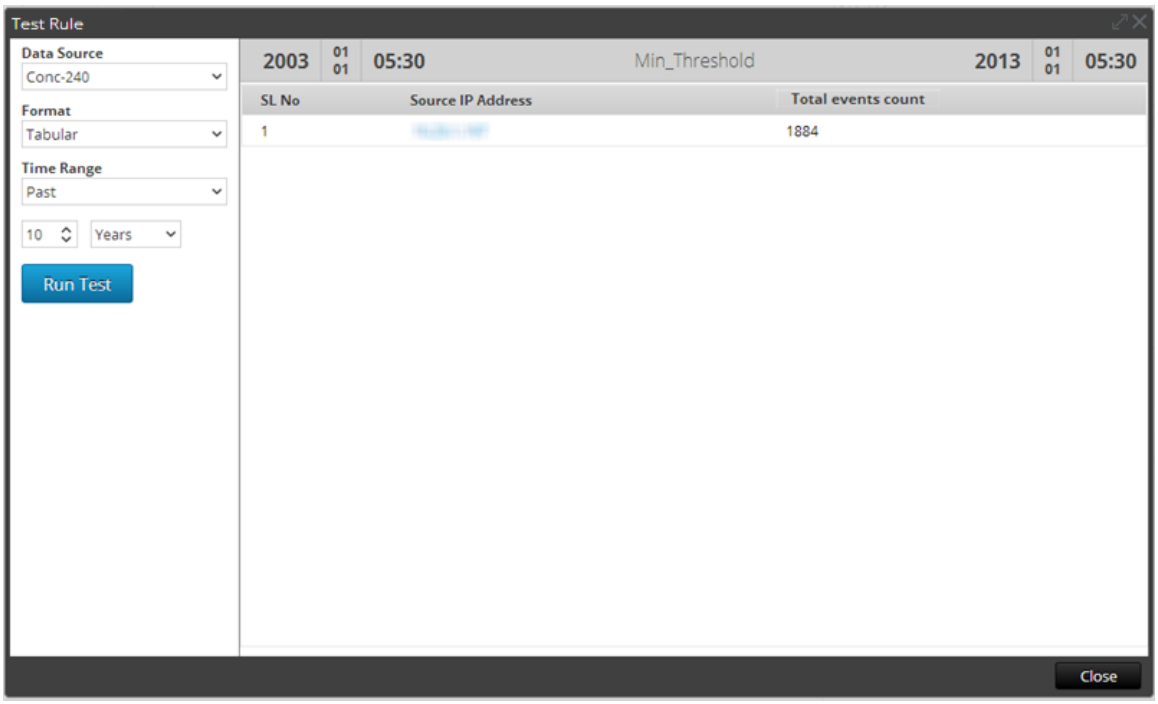
Exemples :

1. min_threshold(200);

La figure ci-dessous présente un exemple de requête min_threshold.



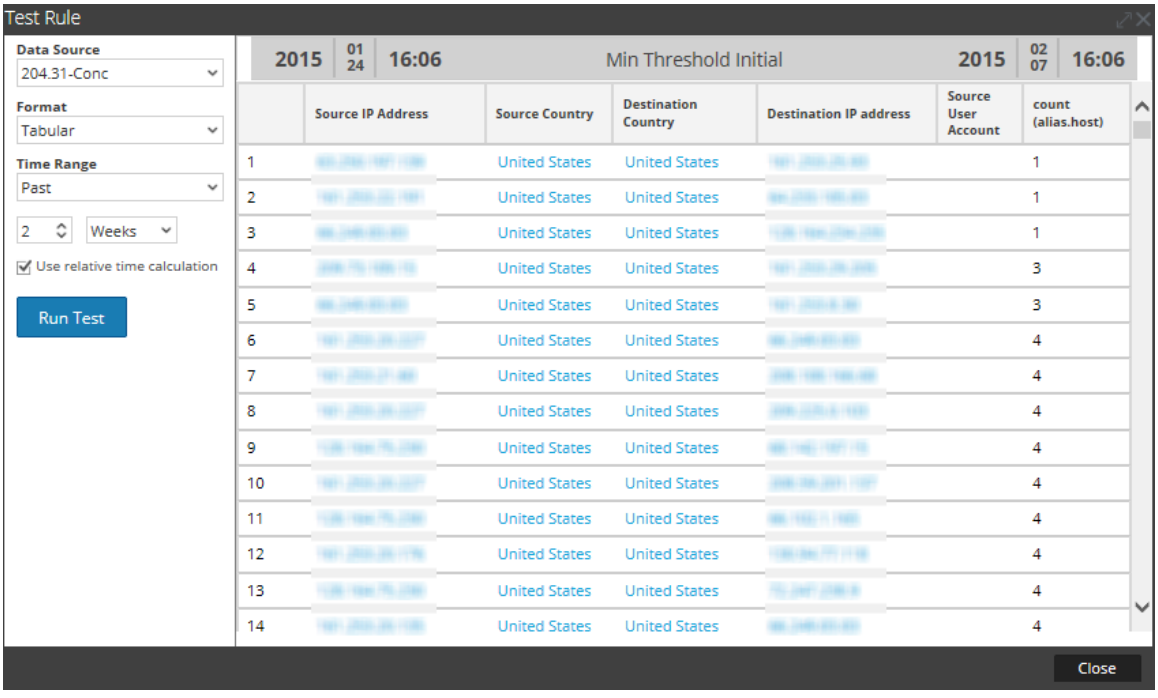
La figure ci-dessus place une limite de 200 octets sur la sortie. Toute sortie contenant moins de 200 octets de données n'est pas répertoriée. La sortie avec l'action de règle min_threshold est appliquée.



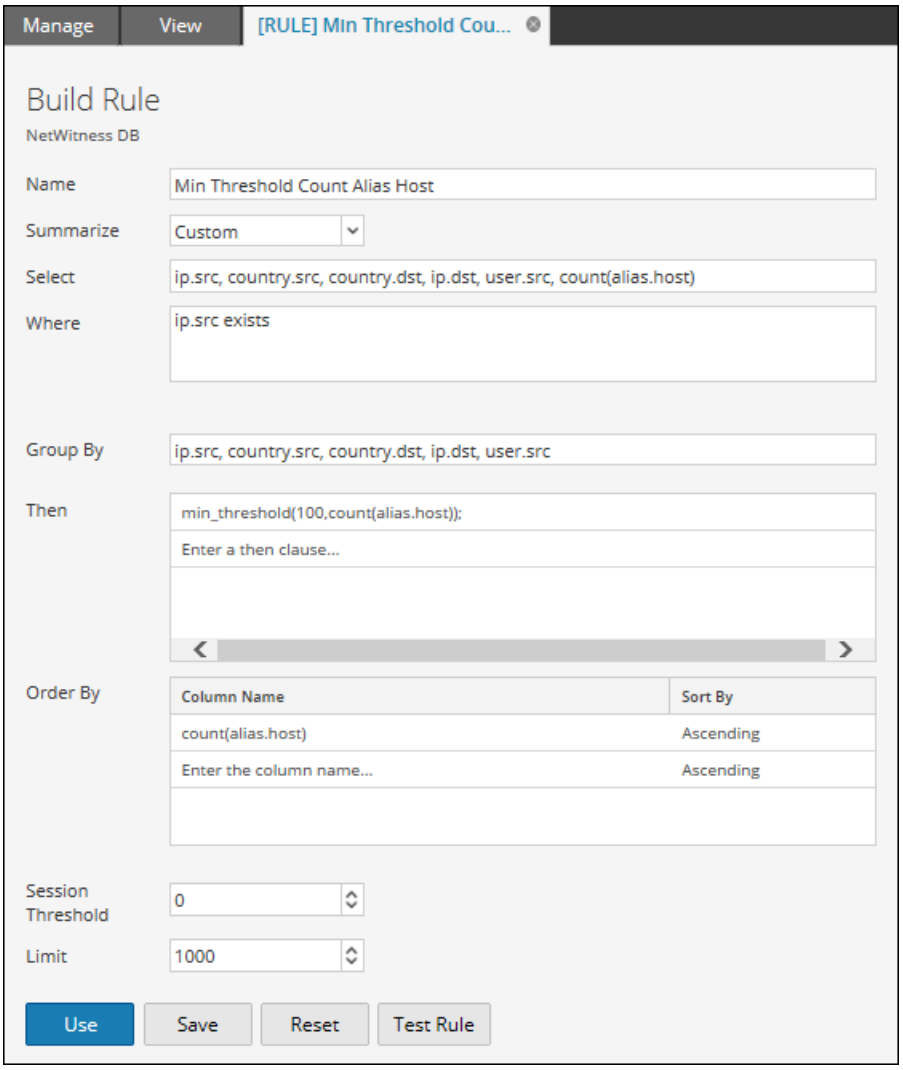
Comme l'indique la figure, toutes les valeurs sont supérieures à 200 octets.

2. min_threshold(100,count(alias.host));

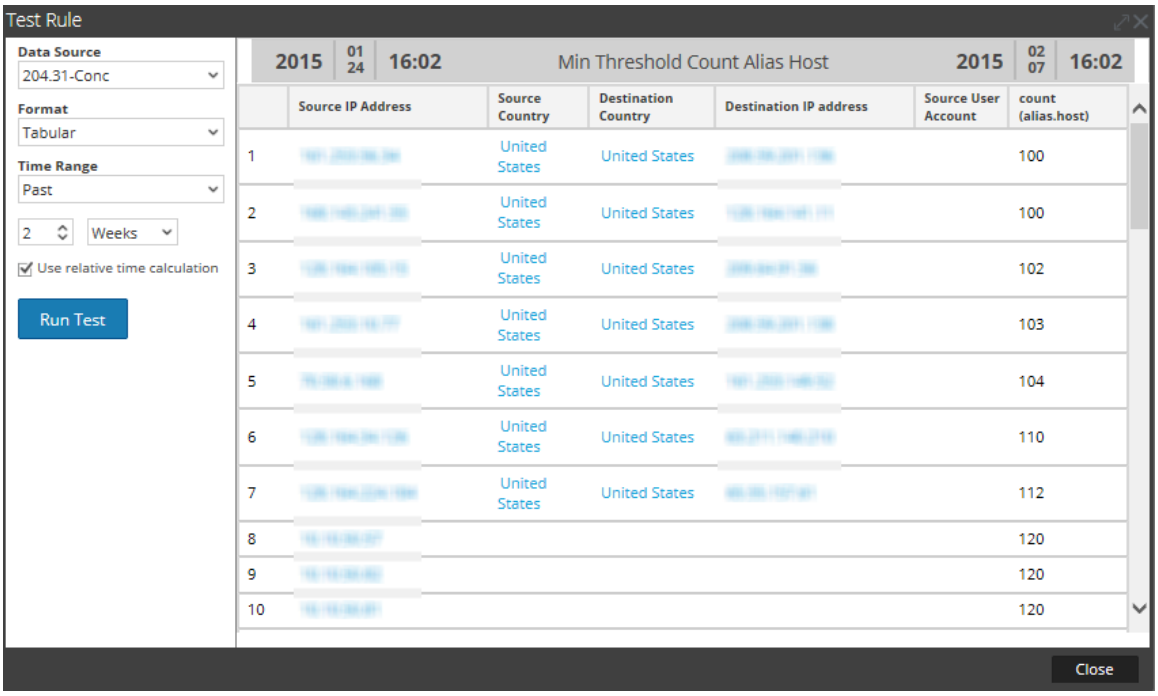
La figure ci-dessous illustre le résultat sans l'argument min_threshold. Les résultats de sortie comportent un nombre d'alias.host inférieur à 100.



La figure ci-dessous présente une action de règle min_threshold qui définit la limite minimale de 100 sur la sortie. Toute sortie comportant des données inférieures à 100 n'est pas répertoriée.



La figure ci-dessous présente le résultat lorsque l'action de règle min_threshold est appliquée. Toute sortie comportant des données inférieures à 100 est supprimée du résultat.



regex (string regex, string field)

L'action de règle regex applique une expression régulière à l'ensemble de résultats. Voici le format de l'action de règle regex :

regex(regular_expression, meta_name)

Où :

- regular_expression correspond à une expression régulière utilisée pour mettre en correspondance la valeur de la métadonnée.
- meta_name correspond au nom de la métadonnée ou du champ auquel l'action de règle regex doit être appliquée.

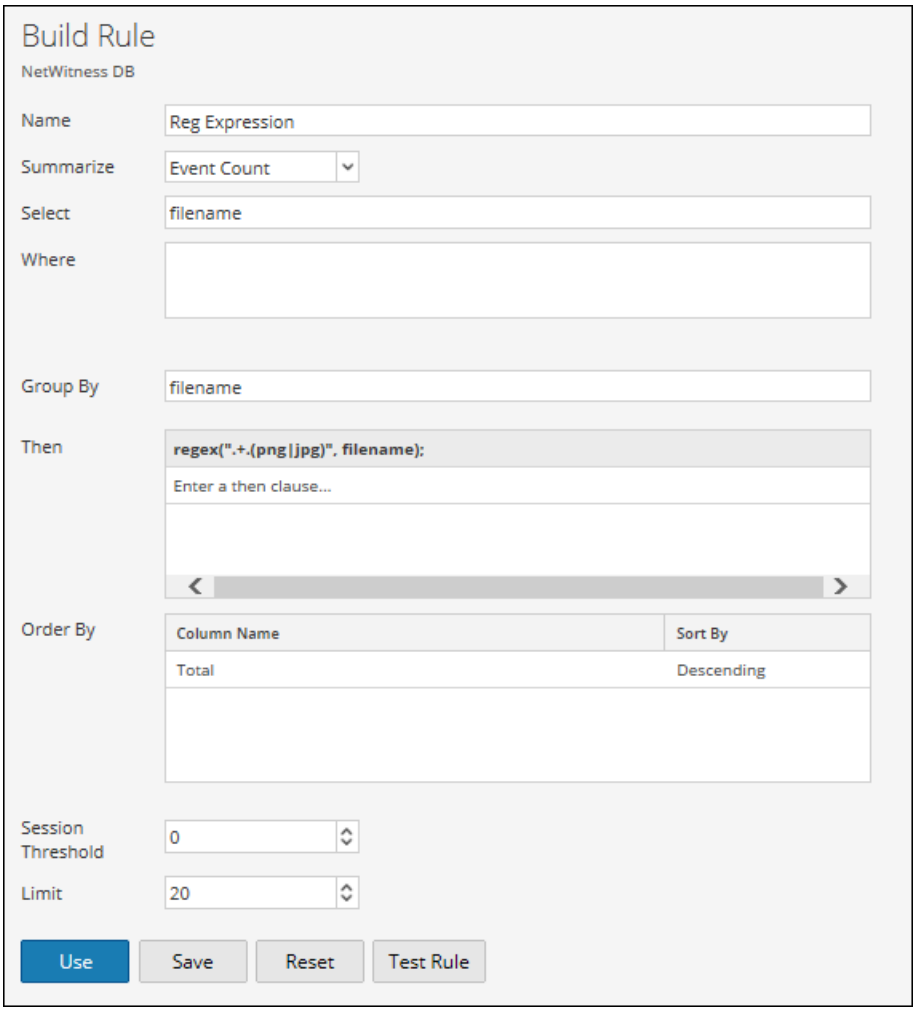
Pour consulter la liste complète des modèles regex pris en charge, reportez-vous à http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.

Exemple d'action de règle regex :

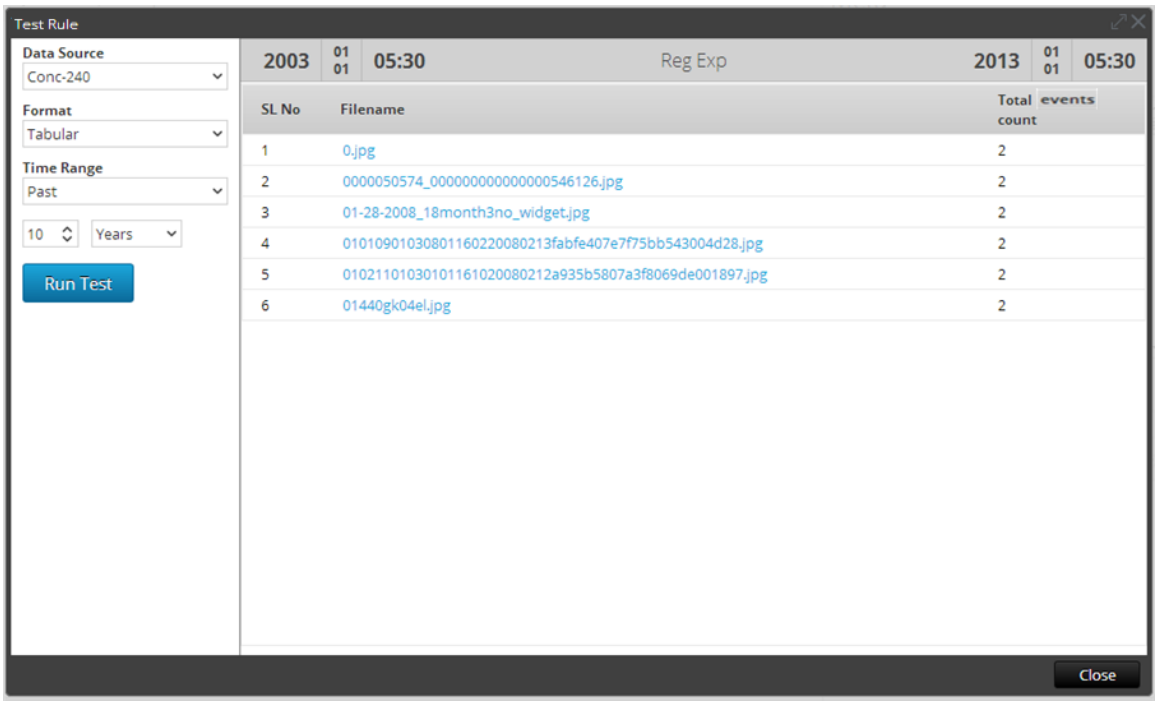
Pour répertorier les noms de fichier de tous les fichiers au format PNG et JPEG issus de différentes sessions, vous pouvez écrire une règle avec l'action de règle regex suivante :

regex(".+.(png|jpg)", filename);

La figure ci-dessous présente cette règle.



La sortie lorsque l'action de regex est appliquée est illustrée par la figure ci-dessous.

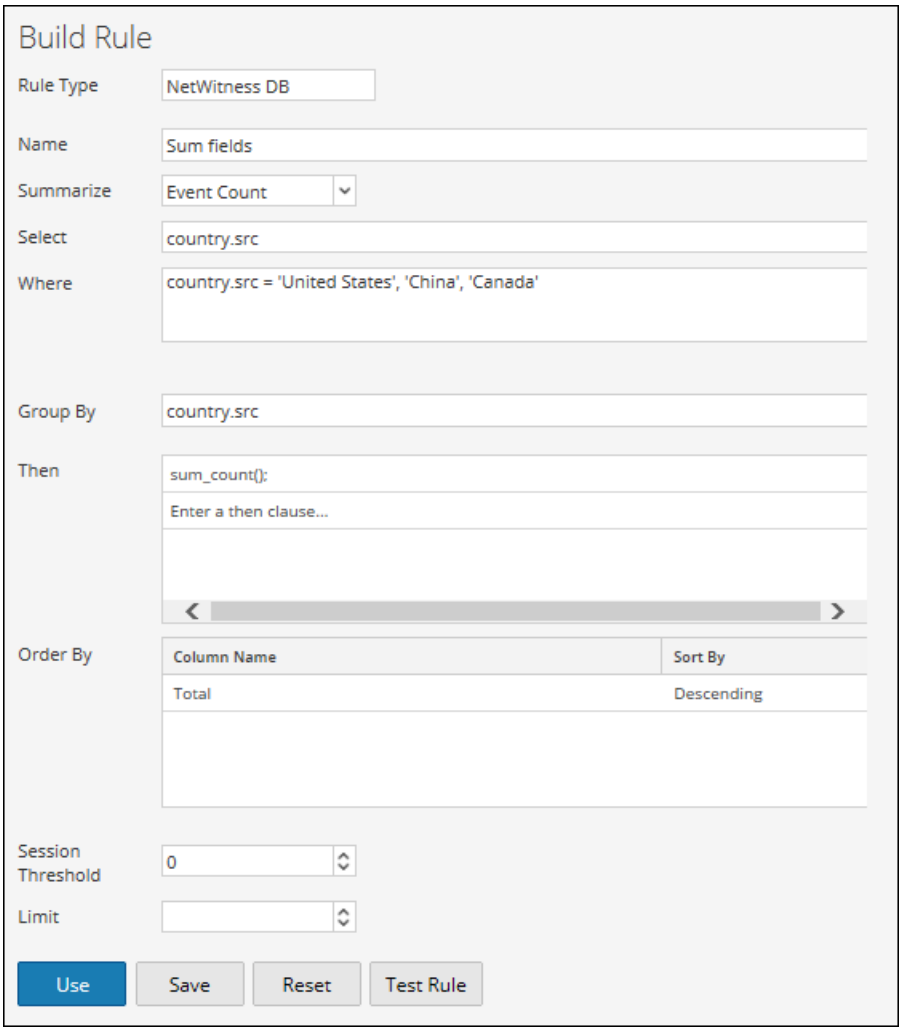


`sum_count()`

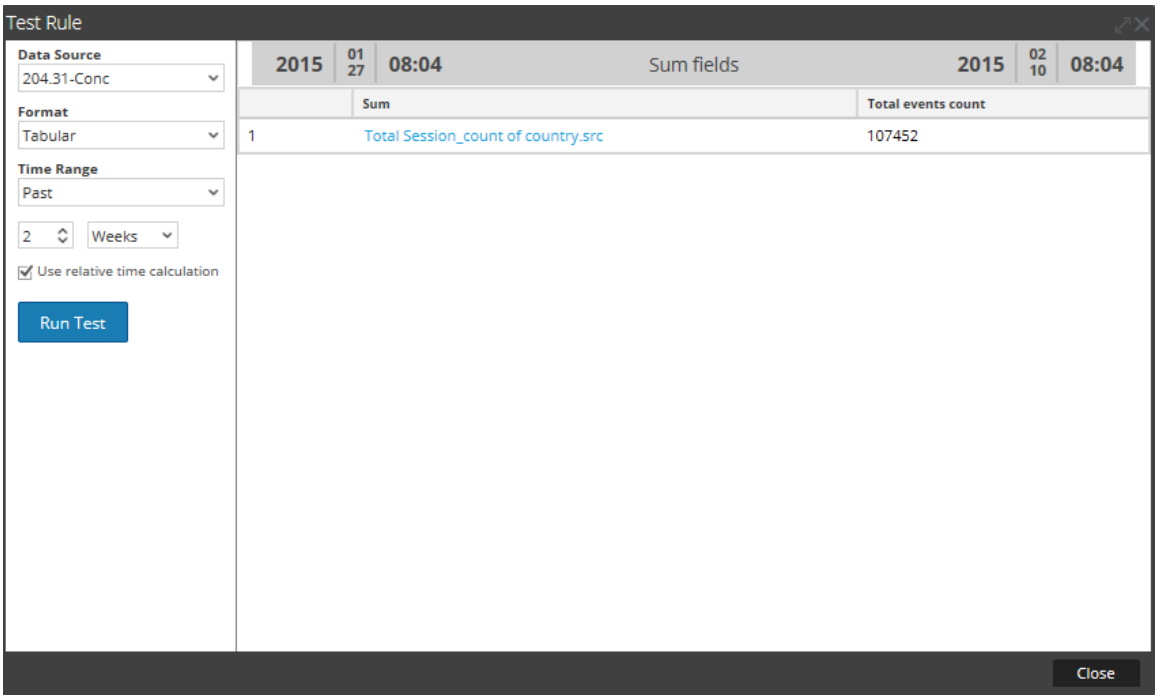
Additionne les quantifiants pour un ensemble de résultats donné. Par exemple, l'appel de l'action de règle sum_count() pour une règle triée par nombre d'événements additionne la taille de toutes les valeurs dans l'ensemble de résultats et affiche le total au lieu de l'ensemble de résultats.

Exemple :

La figure ci-dessous présente l'action de règle sum_count().



Avec l'action de règle sum_count(), la sortie indique la taille totale de tous les nombres d'événements.

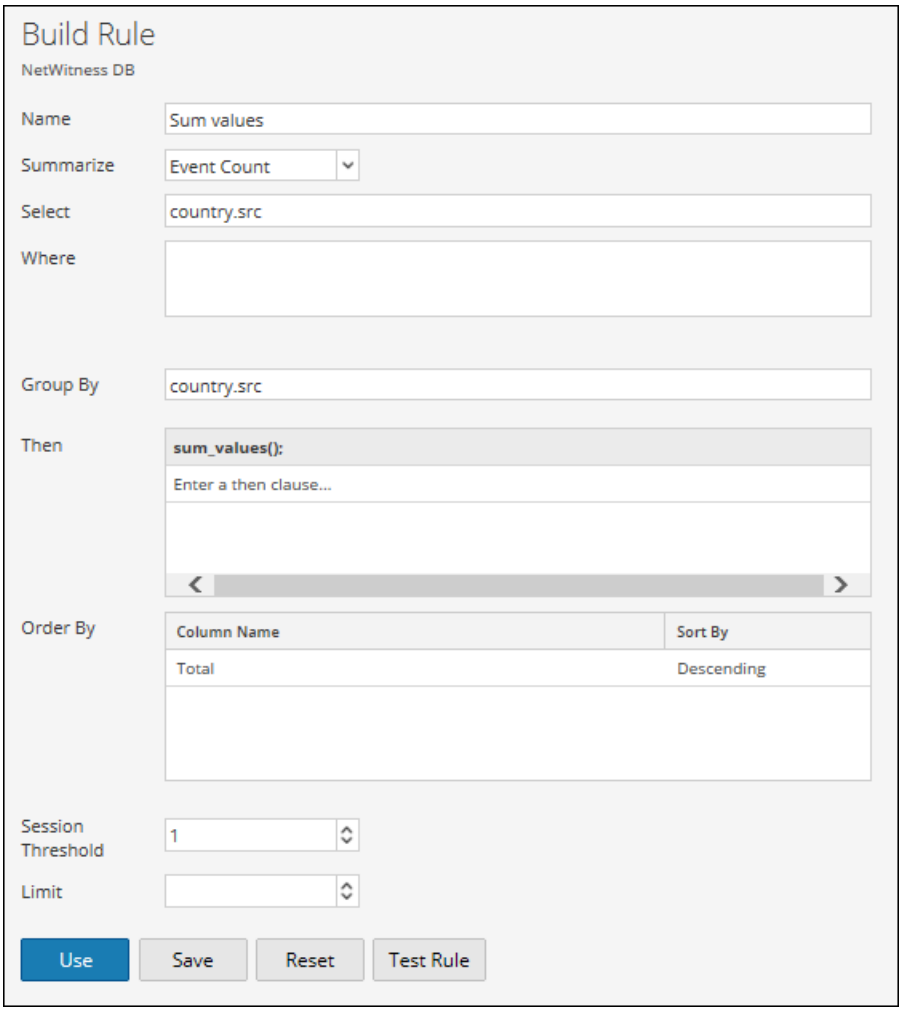


`sum_values()`

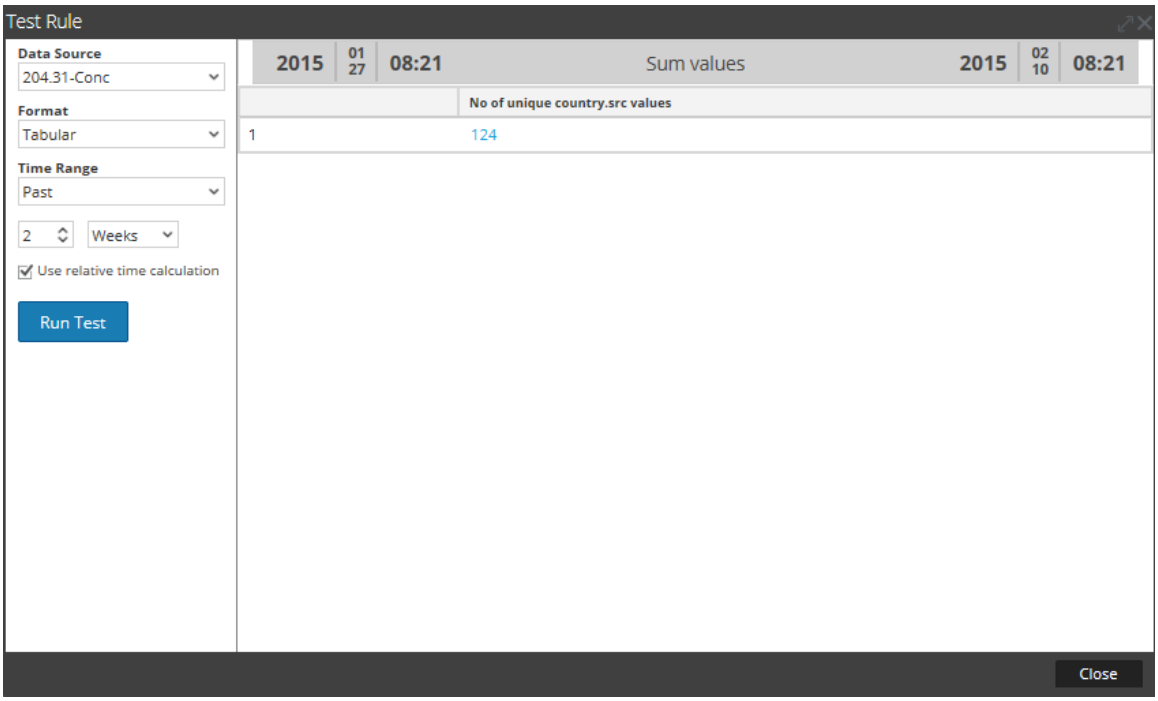
Additionne le nombre de valeurs pour un ensemble de résultats donné. Utilisez cette action pour afficher le nombre d'occurrences existant pour une règle donnée.

Exemple :

La figure ci-dessous présente l'action de règle sum_values().



La figure ci-dessous présente le résultat obtenu avec l'action de règle sum_values.



show_whats_new()

L'action de règle show_whats_new() prend un résultat dans un ensemble de résultats et exclut toute valeur disponible dans la base de données méta NetWitness avant la période du rapport en cours. Lorsqu'un rapport est exécuté, NetWitness Suite détermine l'ID de la première session dans la période du rapport. Si une valeur comprise dans un ensemble de résultats a un premier ID de session supérieur au premier ID de session de la période du rapport, elle n'était pas présente dans la base de données méta NetWitness avant le rapport en cours d'exécution et est donc nouvelle dans le système NetWitness par rapport à la période du rapport.

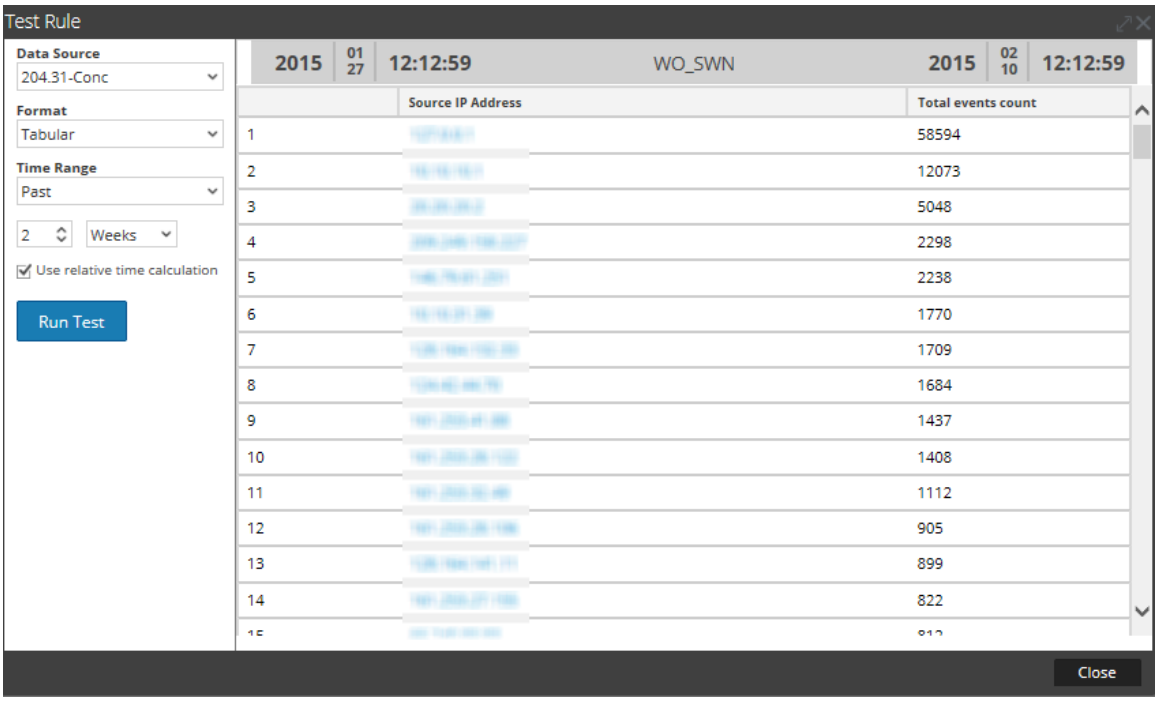
L'action de règle show_whats_new() est également prise en charge pour une règle d'agrégation personnalisée. Lorsque plusieurs métadonnées sont sélectionnées dans la règle personnalisée, la première métadonnée est prise en compte pour exclure les anciennes valeurs. Consultez l'exemple 2 ci-dessous pour comprendre comment cette action de règle est utilisée pour la règle d'agrégation personnalisée.

Remarque : L'action de règle show_whats_new() ne peut être utilisée qu'avec une règle d'agrégation.

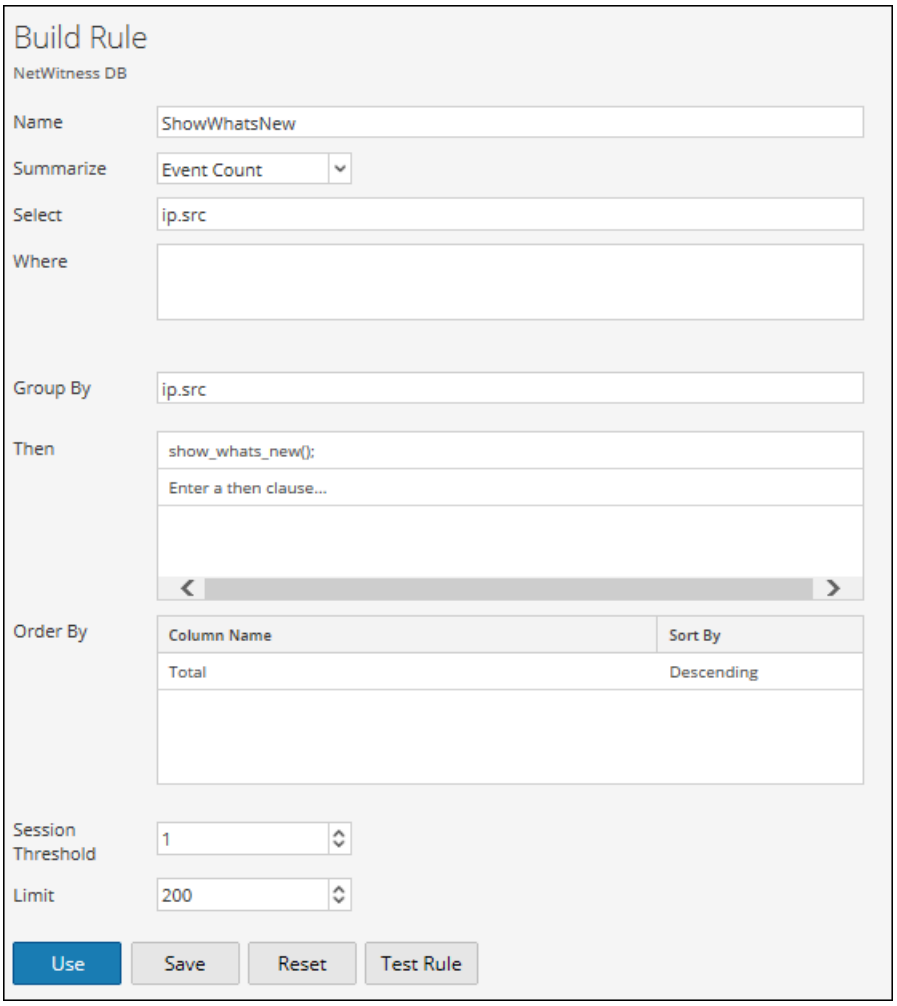
Exemples :

1. show_whats_new() pour règle d'agrégation avec Nombre d'événements

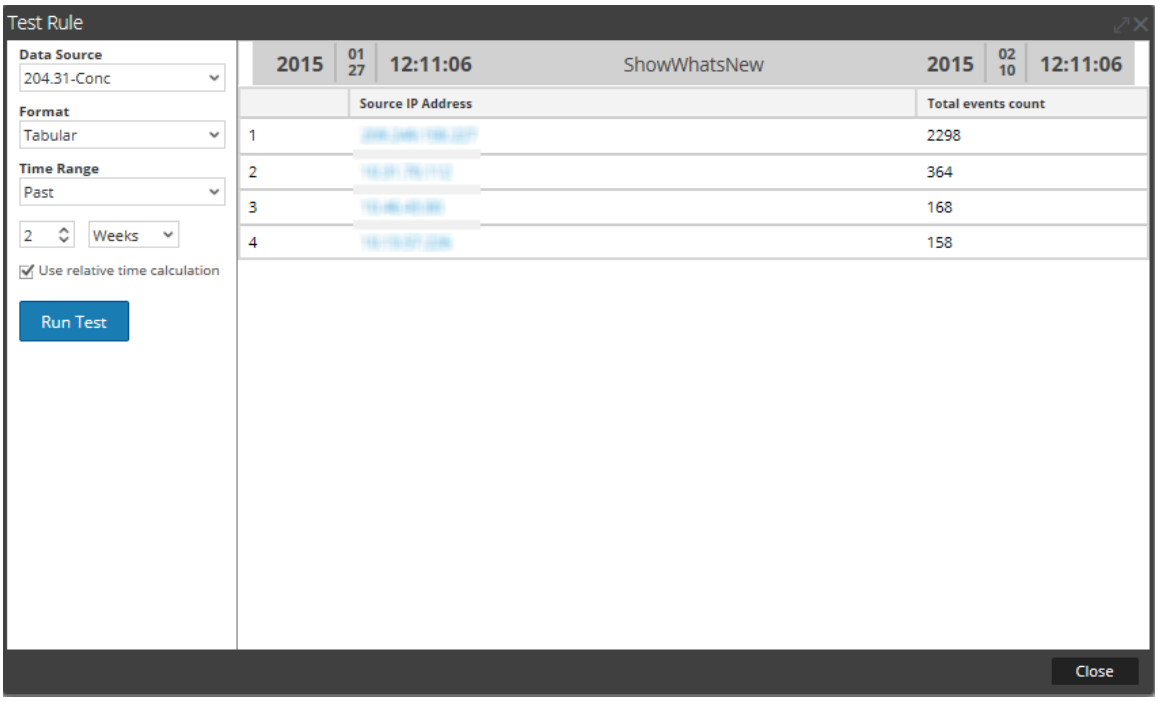
Dans l'exemple ci-dessous, toutes les adresses IP source disponibles pour les deux dernières semaines sont répertoriées.



La figure ci-dessous illustre l'utilisation de l'action de règle show_whats_new pour ne répertorier que les nouvelles entrées des deux dernières semaines.

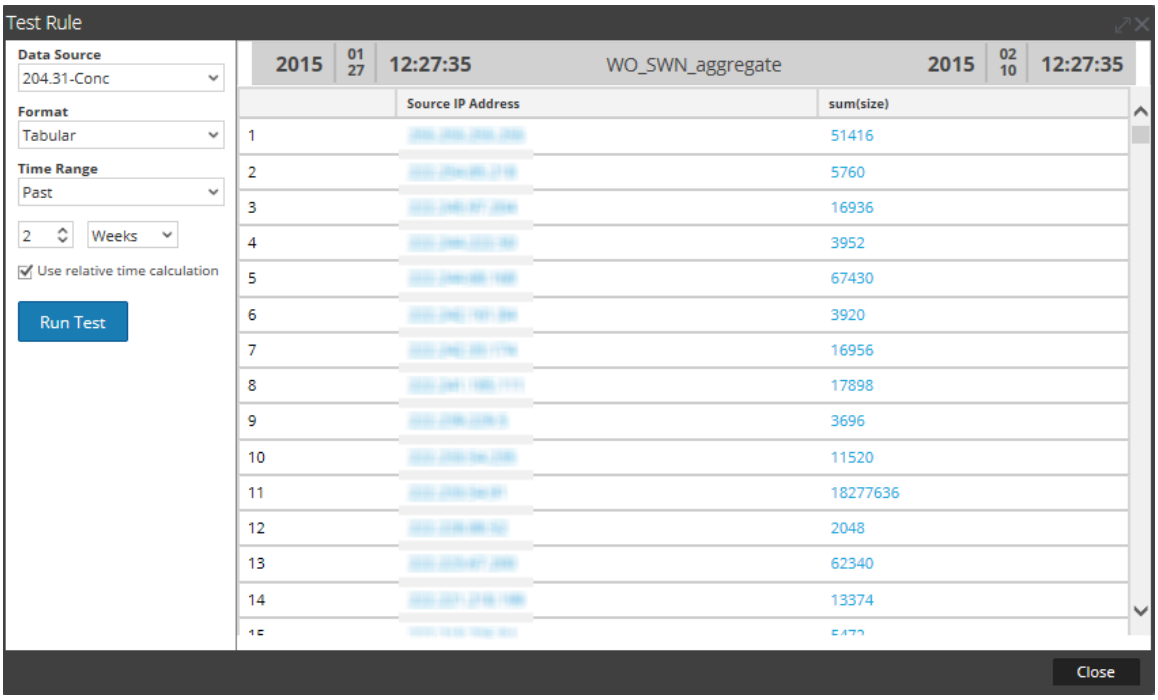


La figure ci-dessous répertorie les nouvelles entrées des deux dernières semaines.

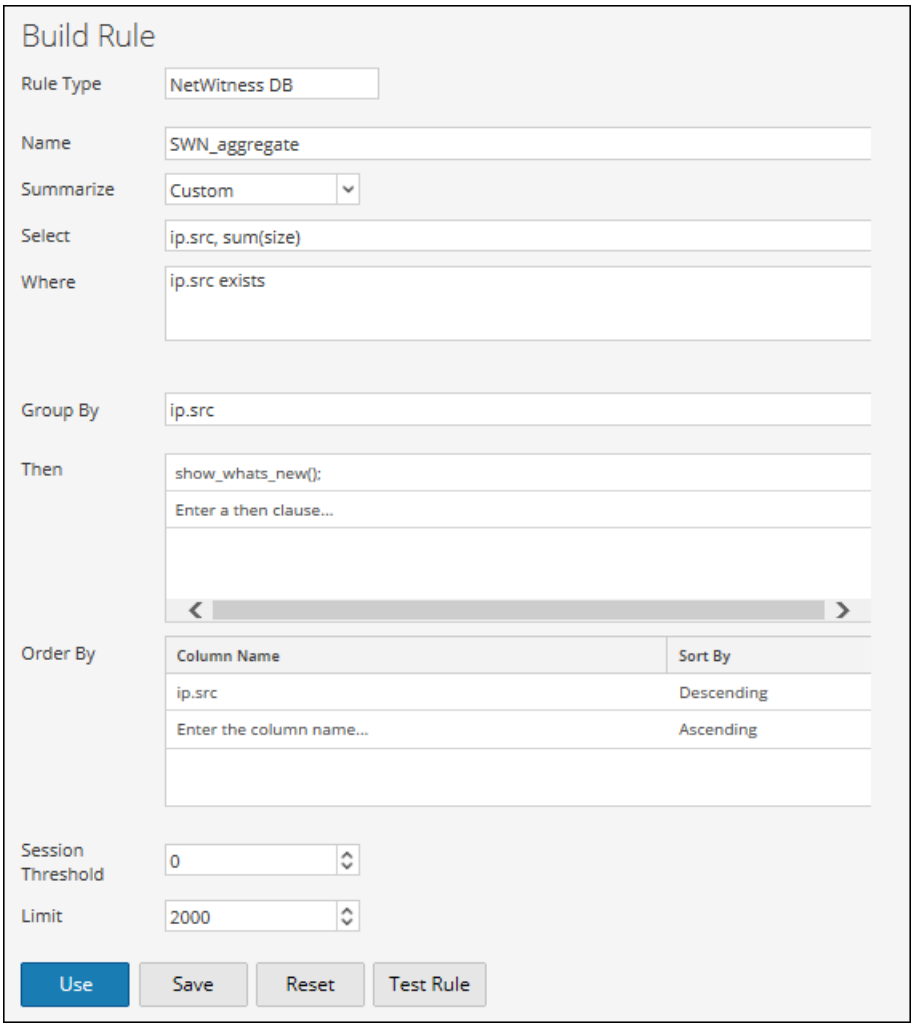


2. show_whats_new() pour la règle d'agrégation personnalisée

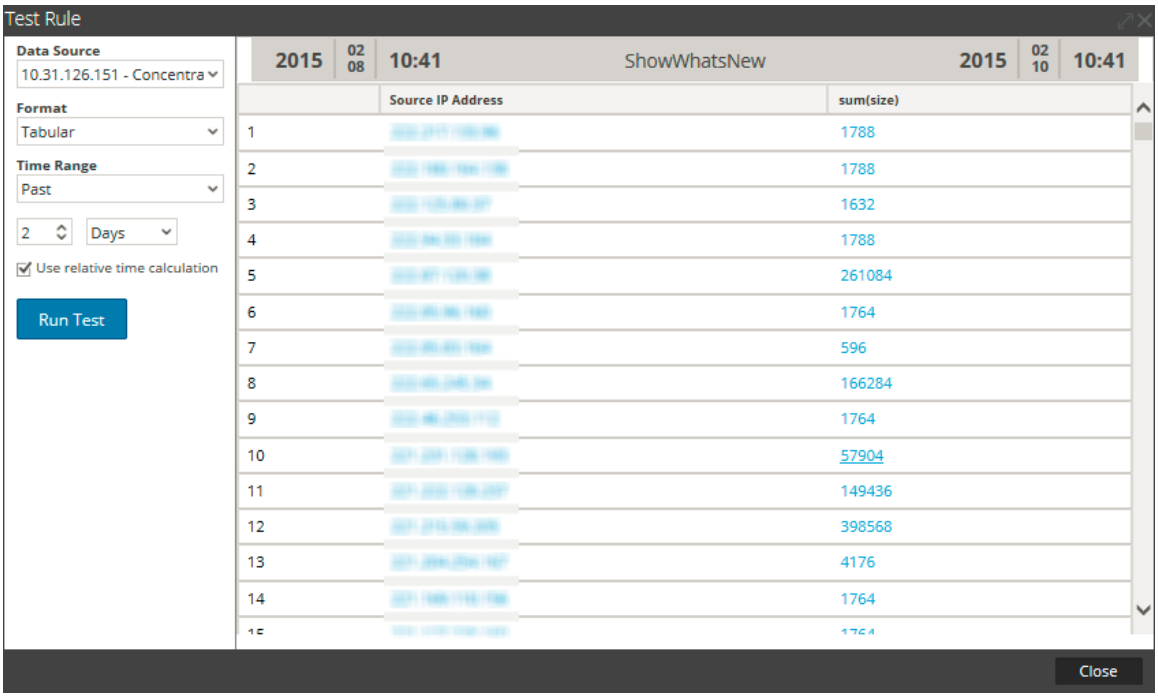
Dans l'exemple ci-dessous, toutes les adresses IP source disponibles pour les deux dernières semaines sont répertoriées.



La figure ci-dessous illustre l'utilisation de l'action de règle show_whats_new pour ne répertorier que les nouvelles entrées des deux dernières semaines.



La figure ci-dessous indique les nouvelles entrées d'Adresses IP source pour les deux dernières semaines.



Ce qui fait la force de cette fonctionnalité est que le moment d'exécution du rapport n'a pas d'importance pour identifier les valeurs qui sont nouvelles pour NetWitness. La restriction associée à cette fonctionnalité est que, si une réinitialisation des données se produit, vos données sont perdues. Cependant, il est facile d'établir les bases d'un système et d'en identifier les modifications et les nouveaux éléments sans exercer de contraintes importantes sur le système (en fonction de la taille de votre ensemble de résultats).

Opérateurs de règles pris en charge

La syntaxe de règle de source de données du Reporting Engine NWDB prend en charge un sous-ensemble d'opérateurs de règles pris en charge par NetWitness Suite.

Syntaxe	Description
*	Utilisez un astérisque (*) dans une règle comme seul opérateur pour sélectionner l'ensemble du trafic.
=	Opérateur Est égal à
!=	Opérateur Est différent de
&&	Opérateur ET logique
||	Opérateur OU logique

Syntaxe	Description
-u	Limite supérieure. Par exemple, **tcp.port = 40000-u** sélectionne tous les ports TCP au-dessus de 40000.
-l	Limite inférieure. Par exemple, **tcp.port = l-40000** sélectionne tous les ports TCP en dessous de 40000.
-	L'opérateur tiret (-) ne s'applique qu'aux valeurs numériques. Séparez les limites inférieure et supérieure par un tiret (-). Par exemple, **tcp.port = 25-443** sélectionne tous les ports TCP compris entre 25 et 443.

Exemples de requêtes prises en charge

Syntaxe de la règle de réponse

La syntaxe de règle prise en charge pour le service RÉPONDRE grâce aux descriptions et exemples de syntaxe prise en charge et non prise en charge. Dans cette version, il existe un nombre limité de syntaxes que vous pouvez utiliser pour élaborer des règles pour des rapports à l'aide du service RÉPONDRE.

Le Reporting Engine prend en charge les catégories suivantes de syntaxe de règle de Source de données RÉPONDRE :

- Clause **select**
  - Règle non agrégée
  - Règle agrégée
- **alias**
- Clause **where**
- Opérateurs de clause **where**
- Regrouper par
- Réorganiser par
- Champ **Limite**

Remarque : Liste n'est pas pris en charge dans les règles de source de données de réponse.

Clause select

La clause select est une liste de valeurs séparées par des virgules. Par exemple : select alert.severity, alert.name, count(*).

Il existe deux types de clause select pour la règle RÉPONDRE :

- Règle non agrégée
- Règle agrégée

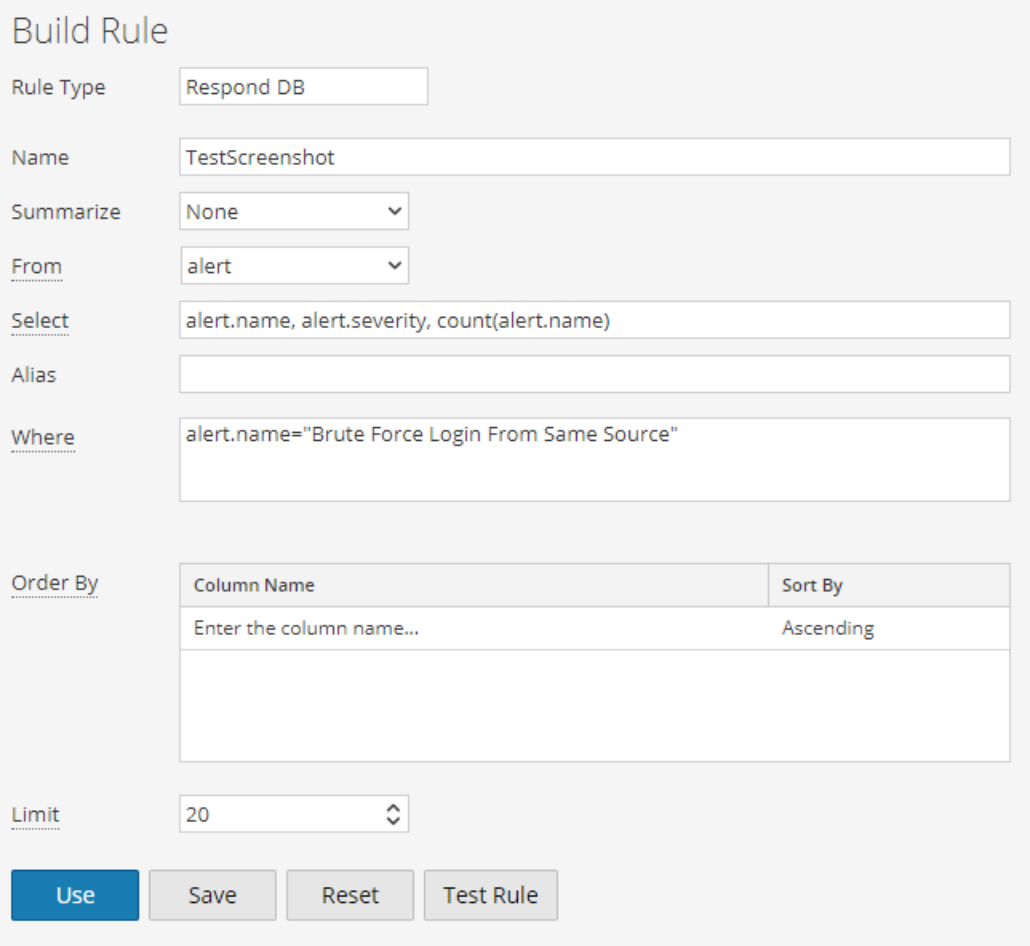
Règle non agrégée

Pour définir une règle sans regroupement, choisissez Aucun dans le champ Résumé. Dans une règle non agrégée, vous pouvez sélectionner n'importe quel nombre de métadonnées dans la clause *select*. Par exemple, select alert.severity, alert.name.

Règle agrégée

Pour effectuer une requête sur une métadonnée spécifique et sa valeur agrégée associée, vous devez utiliser la règle agrégée. Pour obtenir une règle agrégée, vous devez choisir Personnaliser dans le champ **Résumé** pour inclure une fonction agrégée dans la clause *select*. Par exemple, select alert.severity, alert.name, count(*).

La figure suivante illustre la vue Élaborer une règle pour la règle agrégée.



Fonctions d'agrégation prises en charge

Les règles du service RÉPONDRE prennent en charge les fonctions d'agrégation et la syntaxe.

- count
- max
- min
- sum
- avg

Remarque : Les fonctions d'agrégation doivent être ajoutées à la fin d'une clause select pour une requête d'agrégation. Par exemple, alert.name, alert.severity, sum(alert.numEvents). Par défaut, un maximum de résultats de 10 000 lignes est extrait et peut être configuré à l'aide de **rsa.response.query.QueryProperties**.

Exemples de syntaxe de la Clause select

Le tableau suivant fournit des exemples de syntaxe de la clause select.

Exemples	Descriptions
select *column1* , *column2* ,*column3*,...,*columnN*	Sélectionnez des métadonnées spécifiques à partir d'une source de données RÉPONDRE (vous devez séparer chaque colonne par une virgule).

Exemples de requêtes select prises en charge

select alert.name, alert.numEvents, count(alert.numEvents)

select alert.severity, avg(alert.severity)

select alert.timestamp, incidentCreated where alert.timestamp >= 1475658011

Résumé

Résumé détermine le type de résumé ou d'agrégation correspondant à la règle.

Nom	Valeur de configuration
Résumé	Pour interroger les métadonnées sans regroupement personnalisé, sélectionnez : • **Aucun** : Pour obtenir des agrégats basés sur des métadonnées, sélectionnez : • **Personnaliser** : Cela indique que la fonction d'agrégation de métadonnées attendue est définie dans la clause select de la règle.

Alias

Certains noms de métadonnées ne sont peut-être pas descriptifs ; dans ce cas, une description peut être ajoutée dans le champ alias pour faciliter la lecture des noms de colonne. Par exemple,
SELECT: alert.severity, alert.name, count(*)
ALIAS: Gravité de l'alerte, Nom de l'alerte

Dans le champ alias, vous pouvez saisir un nom pour les colonnes utilisées dans la clause select. Si vous ne spécifiez pas d'alias pour l'un des champs dans la clause select, alors la description par défaut sera utilisée. Par exemple, si la clause select a Field1, Field2, Field3, Field4 et que l'alias a uniquement Field1, Field3, Field4, alors une description par défaut est utilisée pour Field2.

Clause where

La clause where est une liste de valeurs et de plages de champ séparées par des virgules qui est utilisée par la fonction RÉPONDRE. Dans la clause where, les valeurs de chaînes doivent être placées entre apostrophes.

Exemples	Descriptions
alert.host summary =' (Primary) Link status "Down" on interface INTNAME.'	Pour les données de type TEXTE ou chaîne, placez la chaîne ou le texte entre des guillemets simples. S'il y a des caractères spéciaux comme les apostrophes dans les données, vous devez ajouter des guillemets simples ou doubles supplémentaires. Par exemple, alert.name = 'alertes principales de Cote d"Ivoire'.
alert.timestamp >= 1475658011	Pour la date et l'heure (colonnes de type données de date/horodatage), utilisez la syntaxe EPOCH.

Opérateurs pris en charge dans la clause where

Opérateur	Syntaxe
= (égal à)	*column1* = '*value*'
!= (différent de)	*column1* != '*value*'
>	*column1* > '*value*'
>=	*column1* >= '*value*'
<	*column1* < '*value*'
<=	*column1* <= '*value*'

Regrouper par

Syntaxe	Fonction
group by : alert.severity, alert.timestamp, incidentCreated **Remarque :** Le champ Regrouper par est activé pour les requêtes d'agrégation et n'est pas modifiable.	RÉPONDRE sélectionne les métadonnées pour le champ Regrouper par à partir de la clause Select sélectionnée automatiquement.

Réorganiser par

Réorganiser par détermine le mode de tri de l'ensemble des résultats et n'est pas sensible à la casse.

Nom	Valeur de configuration
Nom de colonne	Nom de la colonne correspond au nom des colonnes à utiliser pour trier les résultats. Par défaut, la liste est vide. Lorsque vous cliquez sur une colonne, la valeur est remplie d'après le champ Résumé. • order by alert.name asc • order by incidentCreated desc • order by count(numEvents) • order by status

Nom	Valeur de configuration
Trier par	Trier par détermine l'ordre dans lequel vous souhaitez trier les résultats, comme ascendant ou descendant. **Remarque :** Pour toutes les requêtes, il est obligatoire pour sélectionner le champ Classer par.

Champ Limite

Ce champ indique la limite à appliquer à la requête lors de l'extraction des données de la base de données. Si l'ensemble des résultats est trié par nombre
d'événements, nombre de paquets ou taille de session, la limite représentera les premières (ou dernières) valeurs N à renvoyer. Si l'ensemble de résultats n'est
pas trié, les premières valeurs N sont renvoyées.

Règles de syntaxe simples liées à une base de données Warehouse

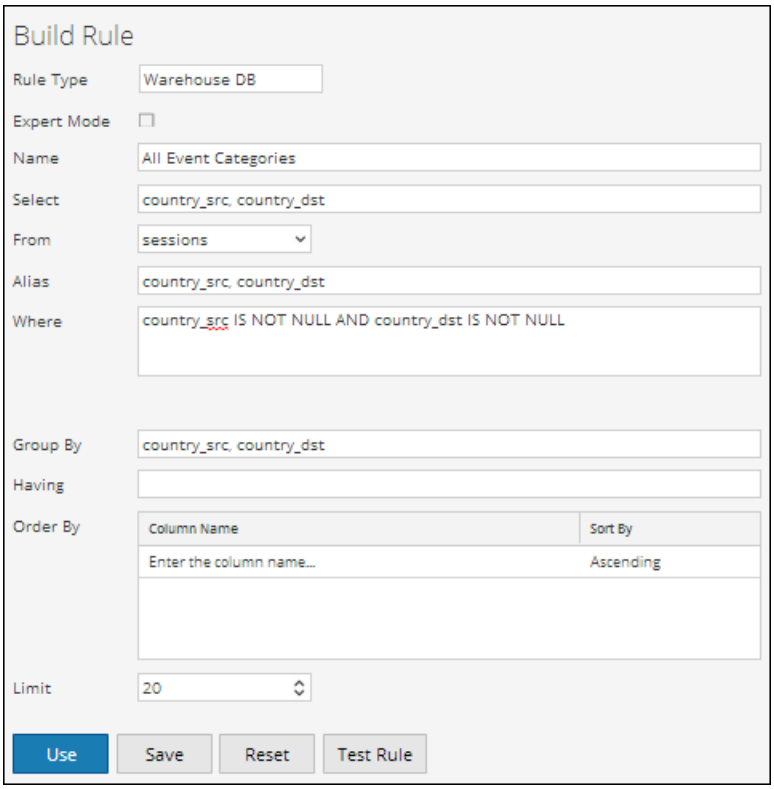
La rubrique explique la syntaxe et des exemples de requête des règles simples.

Les exemples suivants illustrent des règles simples en mode par défaut :

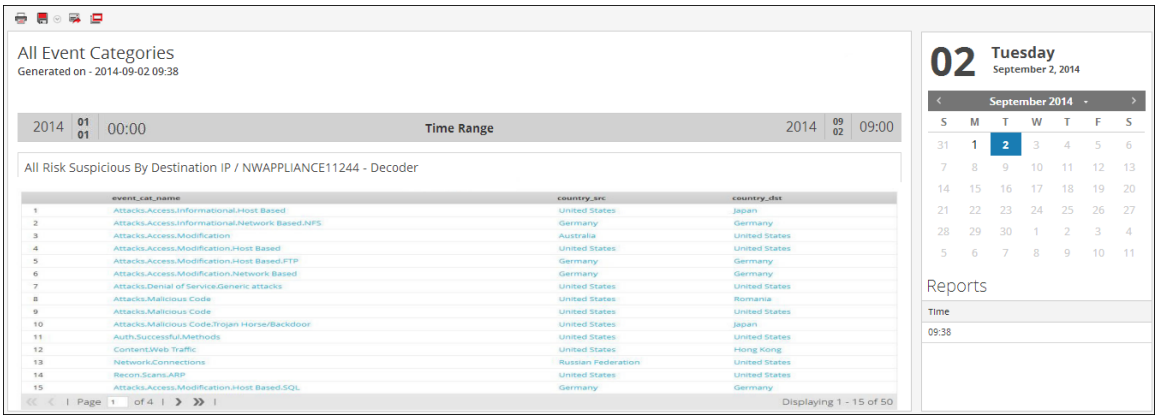
- Rapport sur toutes les catégories d'événements
- Rapport sur les catégories d'événements liés à des attaques
- Source: Rapport sur les catégories d'événements en Chine
- Rapport sur les catégories d'événements liés aux sources et destinations IP
- Rapport sur les catégories de menaces par heure
- Rapport sur les requêtes Array
- Rapport sur les requêtes de consignation brute

Rapport sur toutes les catégories d'événements

Cette règle extrait du tableau **sessions** toutes les catégories d'événements, le pays source et le pays de destination en définissant des noms d'alias (noms de colonnes temporaires) pour chacun des champs à extraire du tableau : **country_src** pour le pays source et **country_dst** pour le pays de destination.

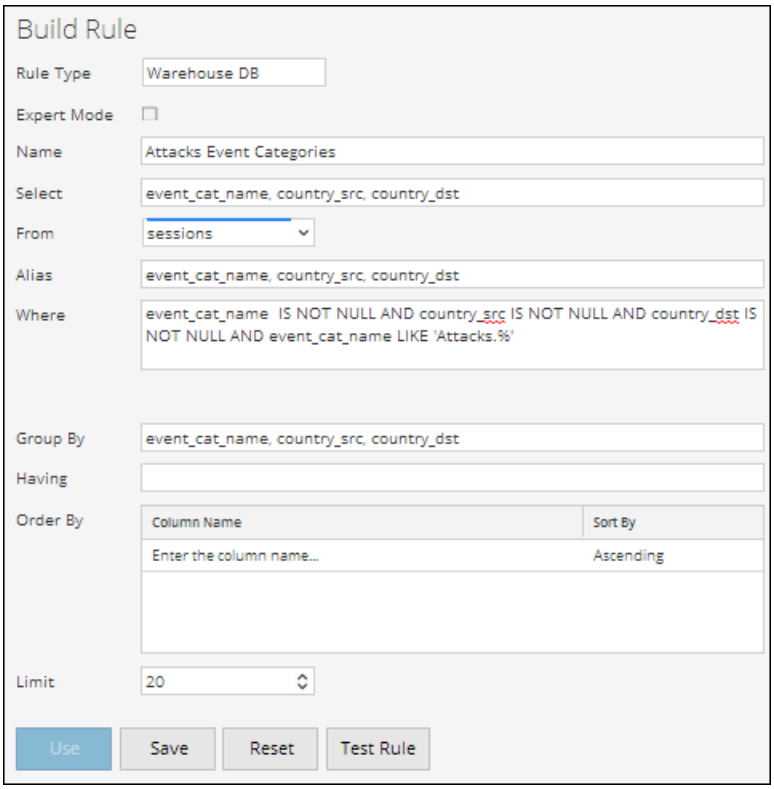


La figure suivante affiche l'ensemble des résultats de la règle Toutes les catégories d'événements.

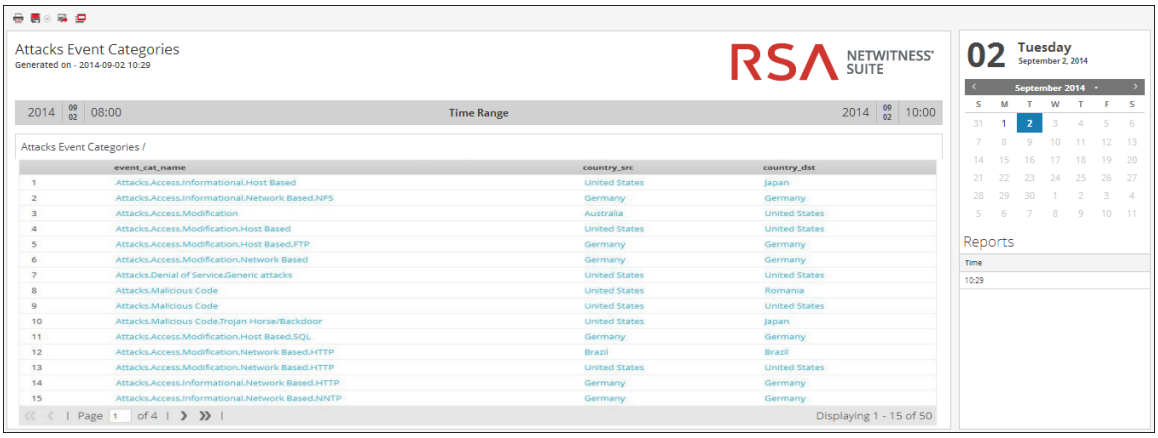


Rapport sur les catégories d'événements liés à des attaques

Cette règle extrait du tableau **sessions** les catégories d'événements, le pays source et le pays de destination en définissant des noms d'alias (noms de colonnes temporaires) pour chacun des champs à extraire du tableau et en sélectionnant uniquement les colonnes dont le nom de la catégorie d'événement contient « Attaques.% ».

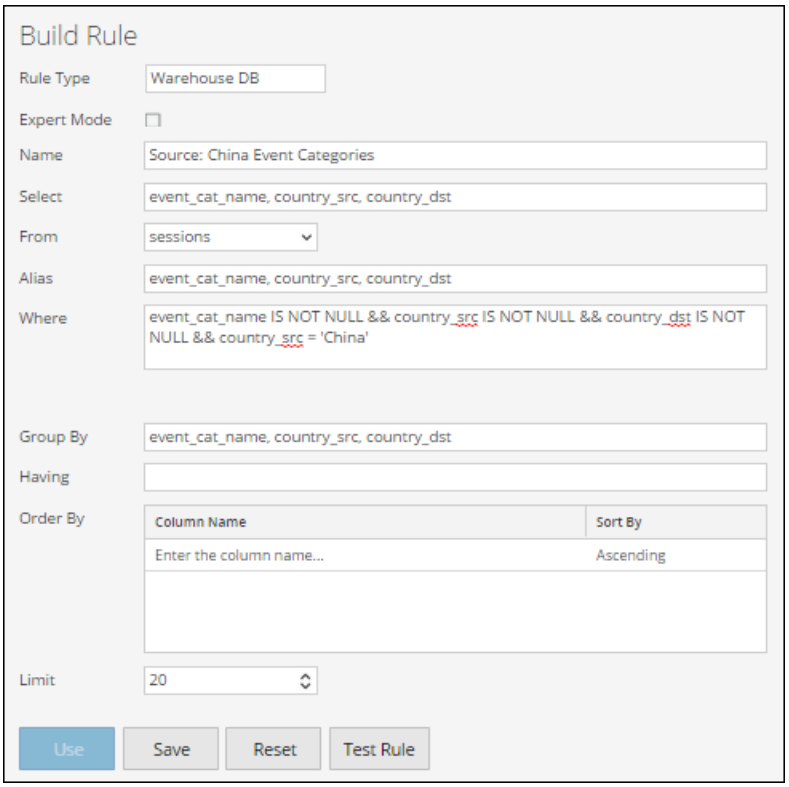


La figure suivante montre l'ensemble des résultats de la règle Catégories d'événements liés à des attaques.

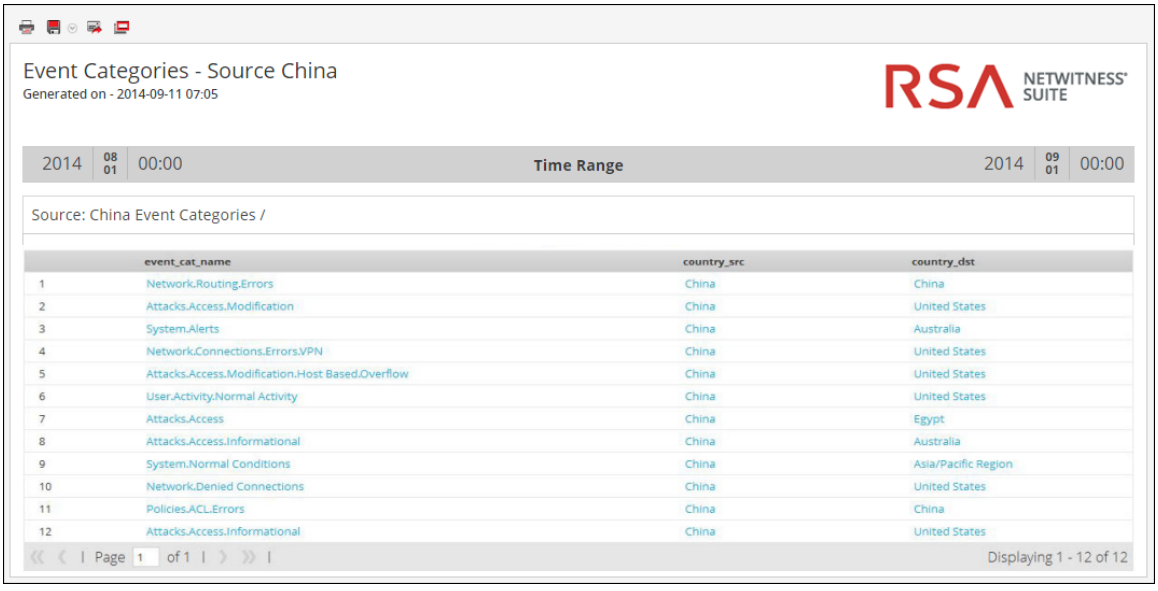


Source : Rapport sur les catégories d'événements en Chine

Cette règle extrait du tableau **sessions** les catégories d'événements, le pays source et le pays de destination en définissant des noms d'alias (noms de colonnes temporaires) pour chacun des champs à extraire du tableau et en sélectionnant uniquement les colonnes dont le pays source est « Chine ».

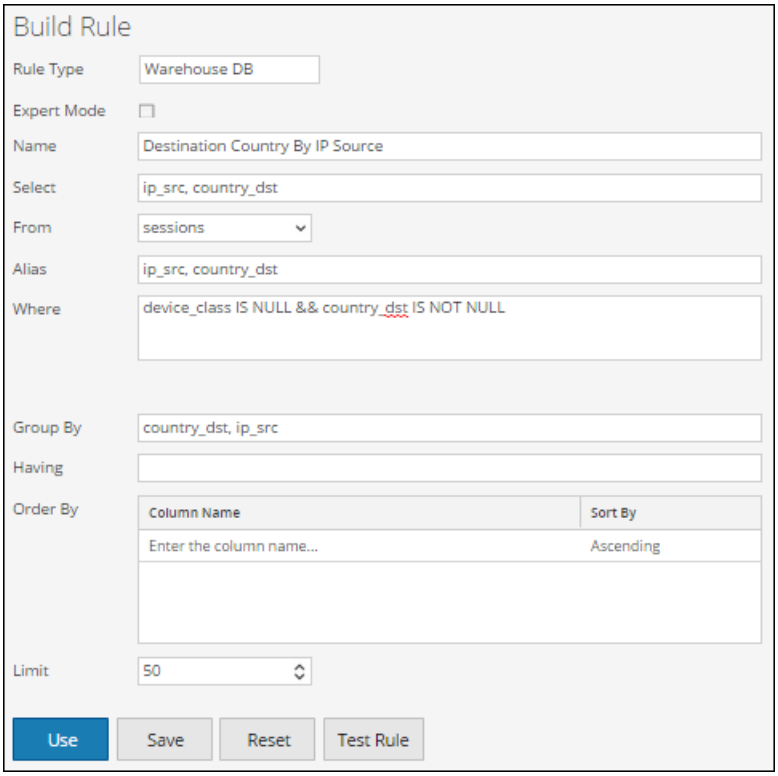


La figure ci-dessous montre l'ensemble des résultats de la source : Règle Catégories d'événements en Chine.

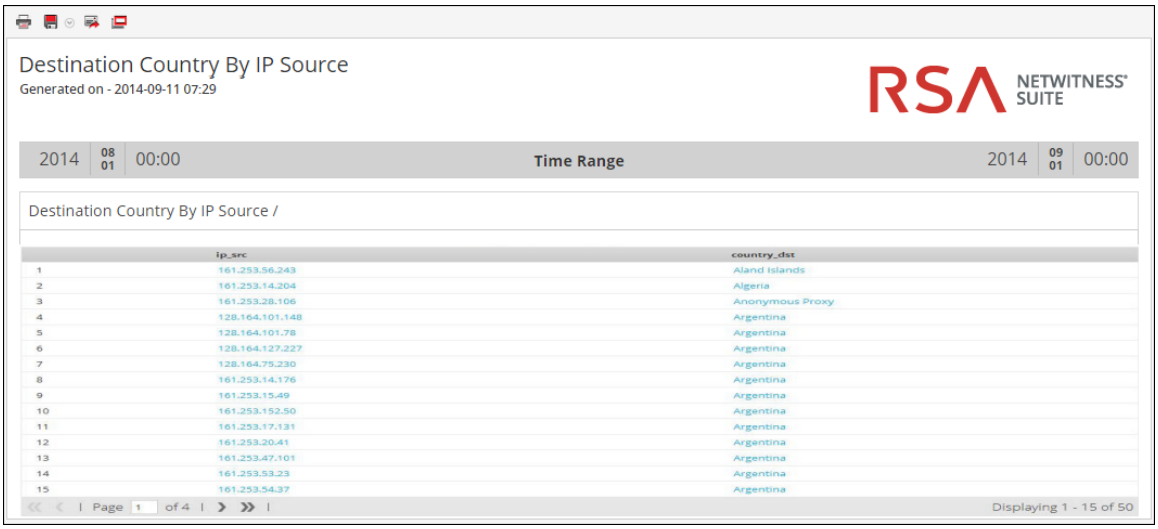


Rapport sur les catégories d'événements liés aux sources et destinations IP

Cette règle extrait du tableau **sessions** l'adresse IP des pays source et de destination en définissant des noms d'alias (noms de colonnes temporaires) pour chacun des champs à extraire du tableau et en sélectionnant uniquement les colonnes dont le pays de destination n'est PAS NUL.

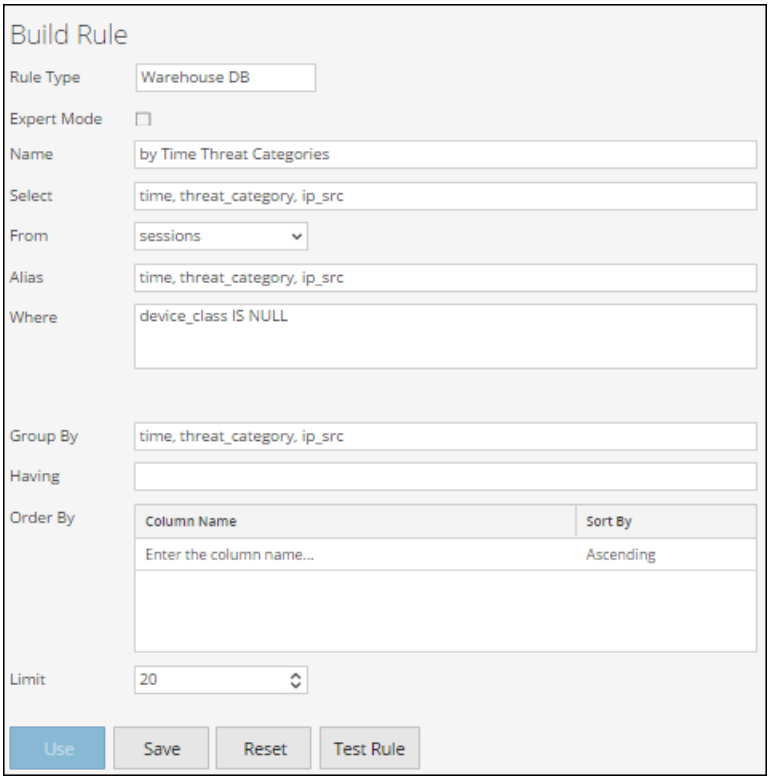


La figure suivante montre l'ensemble des résultats de la règle Catégories d'événements liés aux sources et destinations IP.



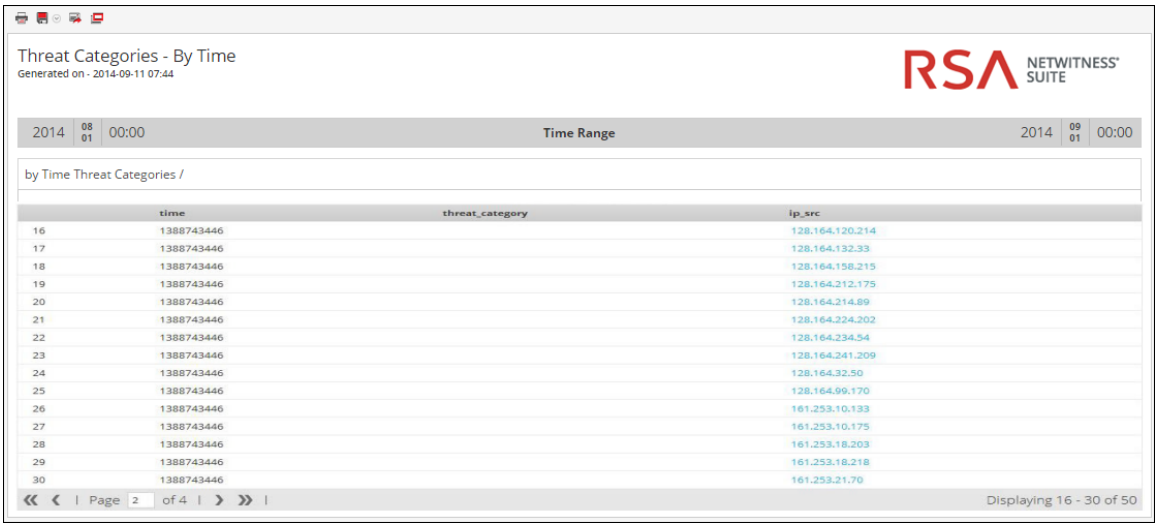
Rapport sur les catégories de menaces par heure

Cette règle extrait du tableau **sessions** les événements de la catégorie Menaces, l'heure à laquelle le log ou l'événement a été intégré à Log Decoder/Decoder, et les adresses IP source en définissant des noms d'alias (noms de colonnes temporaires) pour chacun des champs à extraire du tableau.



La figure suivante montre l'ensemble de résultats de la règle Catégories de menaces par heure. L'heure affichée dans le champ heure est le temps UNIX (par exemple, 1388743446).

Remarque : Dans la clause « Select », la syntaxe serait « UNIX time » pour une conversion au format d'heure UTC dans le rapport. Par exemple, vous pouvez utiliser l'outil de conversion d'heure Epoch pour convertir l'heure au format UNIX (1388743446) en UTC (Coordinated Universal Time) (1/3/2014 3:34:06 PM).



Threat Categories - By Time
Generated on - 2014-09-11 07:44

RSA NETWITNESS SUITE

2014 08 01 00:00 — Time Range — 2014 09 01 00:00

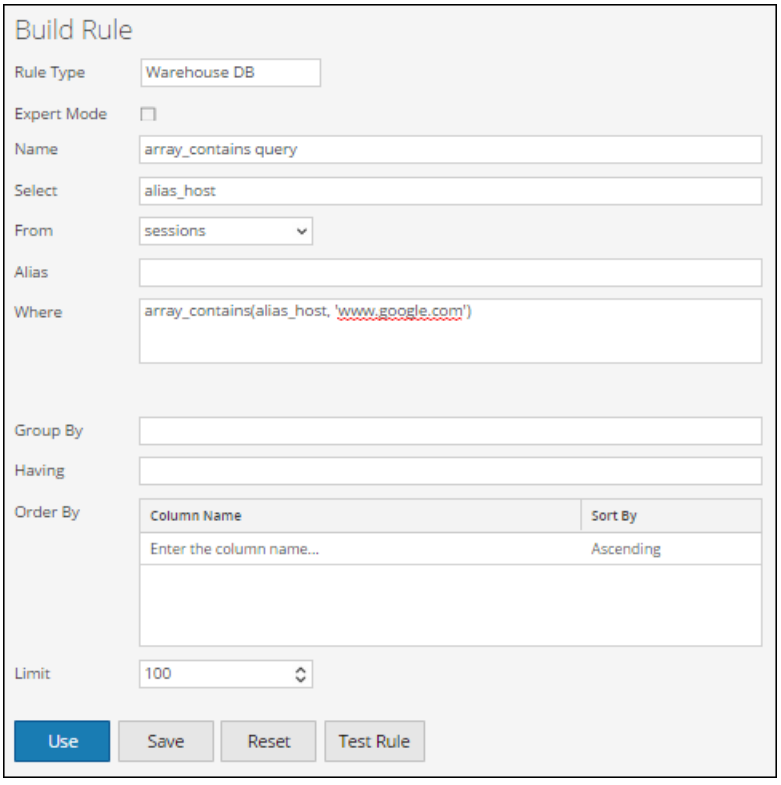
by Time Threat Categories /

	time	threat_category	ip_src
16	1388743446		128.164.120.214
17	1388743446		128.164.132.33
18	1388743446		128.164.158.215
19	1388743446		128.164.212.175
20	1388743446		128.164.214.89
21	1388743446		128.164.224.202
22	1388743446		128.164.234.54
23	1388743446		128.164.241.209
24	1388743446		128.164.32.50
25	1388743446		128.164.99.170
26	1388743446		161.253.10.133
27	1388743446		161.253.10.175
28	1388743446		161.253.18.203
29	1388743446		161.253.18.218
30	1388743446		161.253.21.70

« ‹ | Page 2 of 4 | › » | Displaying 16 - 30 of 50

Rapport sur les requêtes Array

Cette règle récupère un tableau d'alias de noms d'hôtes du tableau **Sessions** qui contient la valeur « www.google.com ».



Build Rule

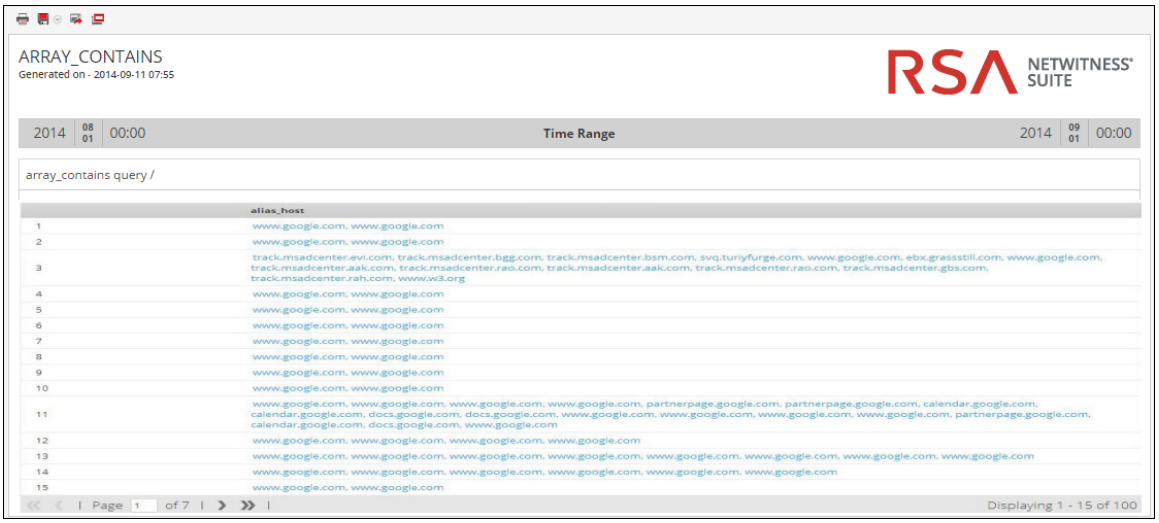
Rule Type: Warehouse DB
Expert Mode: ☐
Name: array_contains query
Select: alias_host
From: sessions
Alias:
Where: array_contains(alias_host, 'www.google.com')
Group By:
Having:
Order By:

Column Name	Sort By
Enter the column name...	Ascending

Limit: 100

Use | Save | Reset | Test Rule

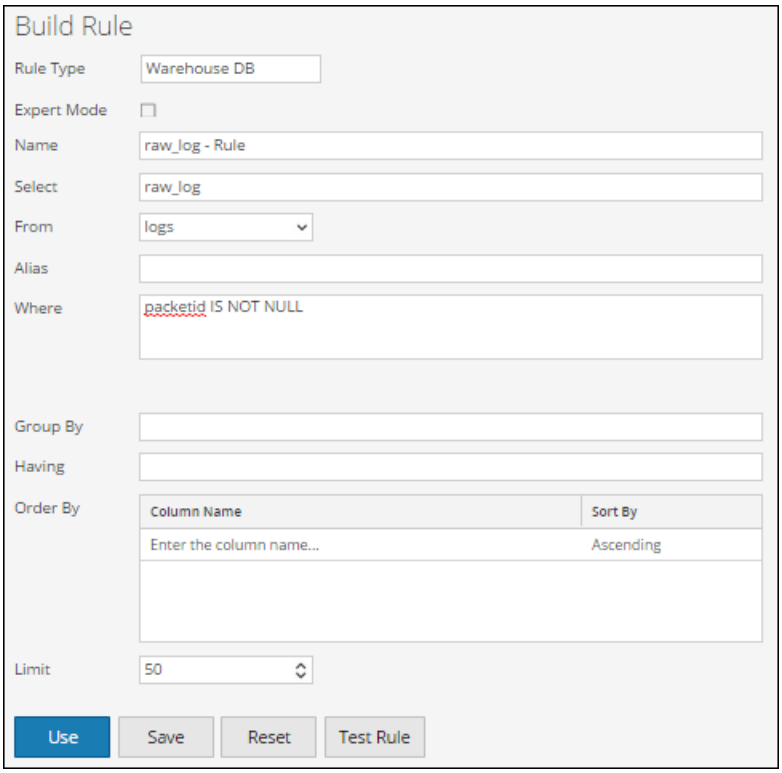
La figure suivante montre l'ensemble des résultats suite à l'interrogation du tableau Sessions.



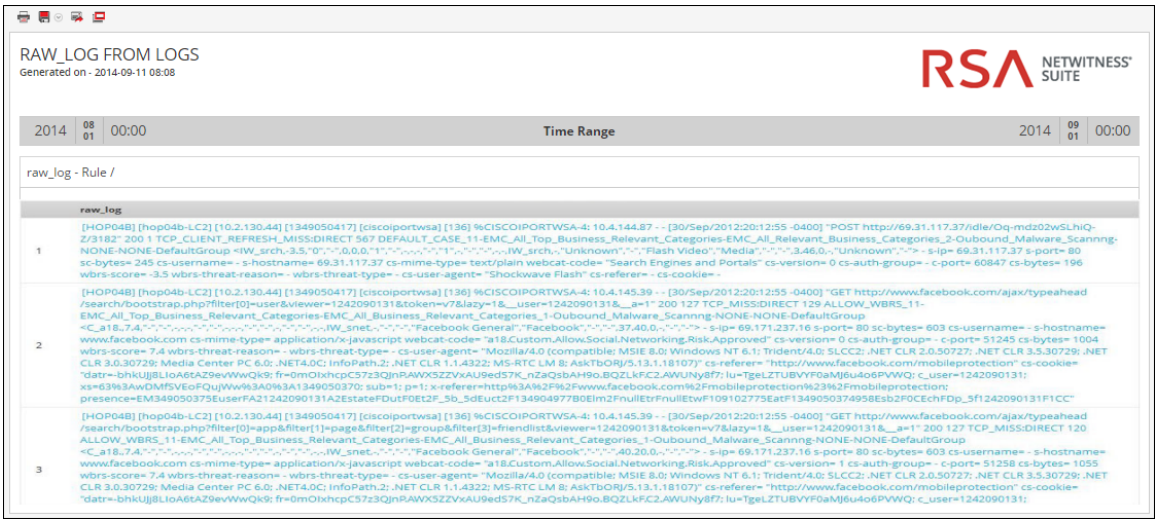
Rapport sur les requêtes de consignation brute

Les logs bruts peuvent être interrogés à partir du tableau des logs ou de sessions.

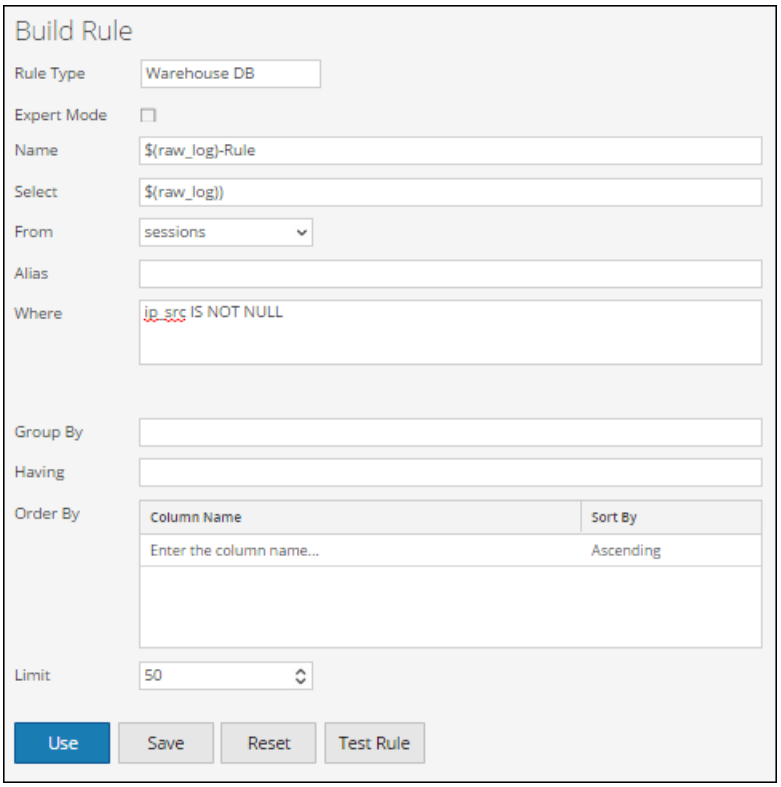
Cette règle utilise **raw_log** en tant que méta pour l'interrogation d'un log brut issu du tableau Logs dont l'ID de paquet n'est PAS NUL.



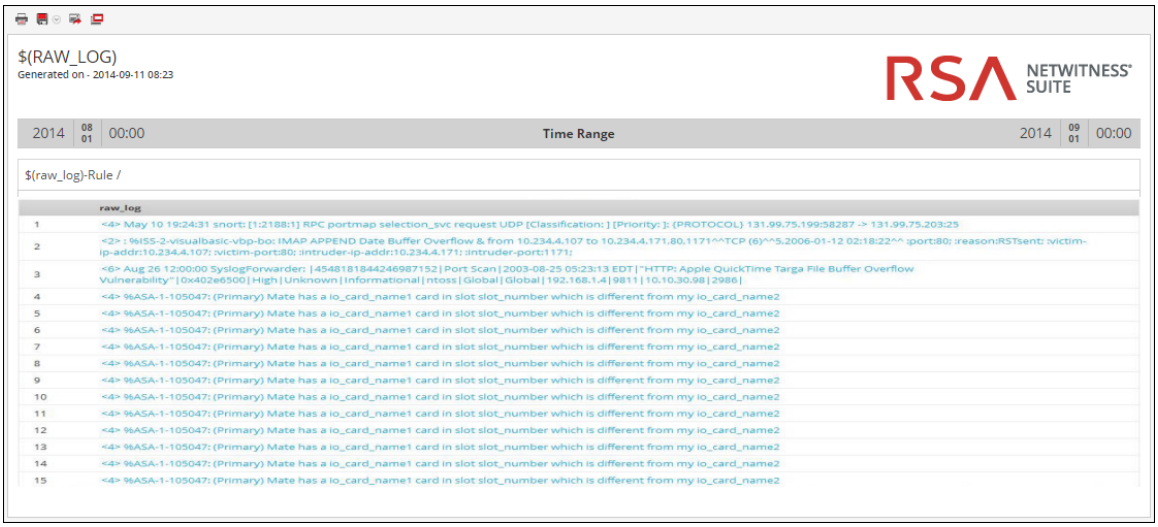
La figure suivante montre l'ensemble des résultats suite à l'interrogation des logs bruts issus du tableau Logs.



Cette règle utilise **${raw_log}** en tant que méta pour l'interrogation d'un log brut issu des sessions dont l'adresse IP source n'est PAS NULLE.



La figure suivante montre l'ensemble des résultats suite à l'interrogation des logs bruts issus du tableau Sessions.



$(RAW_LOG)
Generated on - 2014-09-11 08:23

RSA NETWITNESS SUITE

2014	08 01	00:00	Time Range	2014	09 01	00:00

$(raw_log)-Rule /

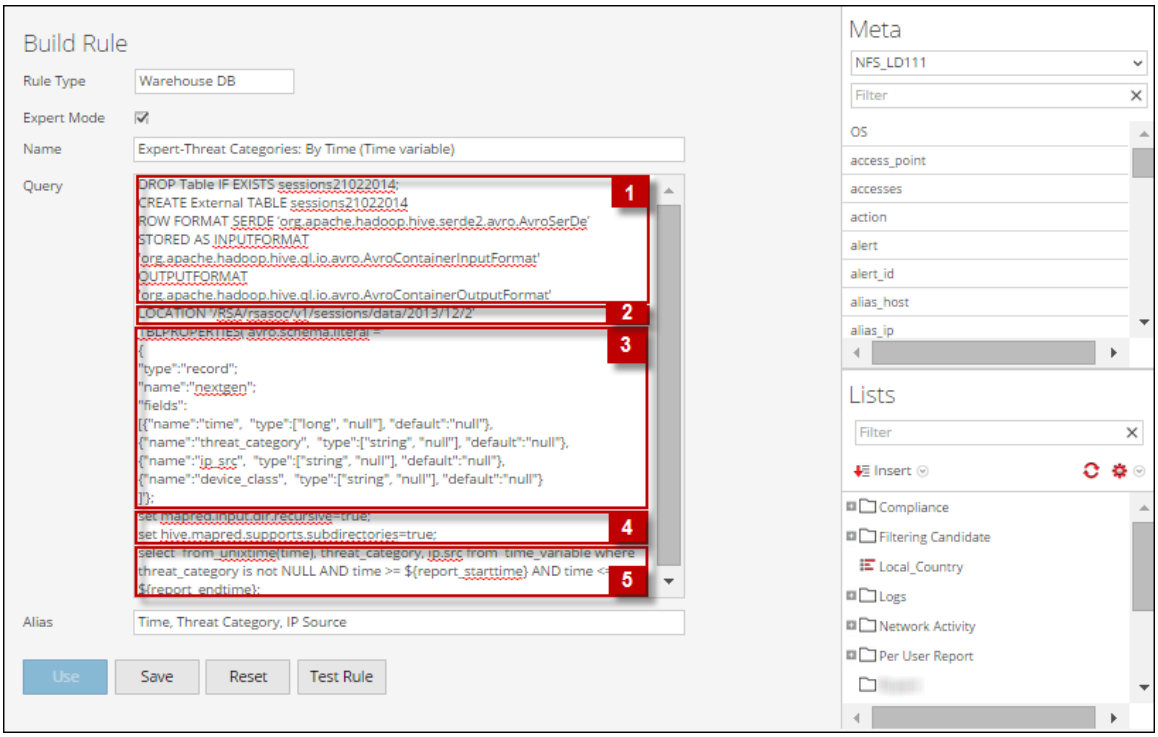
	raw_log
1	<4> May 10 19:24:31 snort: [1:2188:1] RPC portmap selection_svc request UDP [Classification:] [Priority:]: {PROTOCOL} 131.99.75.199:58287 -> 131.99.75.203:25
2	<2> : %ISS-2-visualbasic-vbp-bo: IMAP APPEND Date Buffer Overflow & from 10.234.4.107 to 10.234.4.171.80.1171^^TCP (6)^^5.2006-01-12 02:18:22^^ :port:80: :reason:RSTsent: :victim-ip-addr:10.234.4.107: :victim-port:80: :intruder-ip-addr:10.234.4.171: :intruder-port:1171:
3	<6> Aug 26 12:00:00 SyslogForwarder: |4548181844246987152|Port Scan|2003-08-25 05:23:13 EDT|"HTTP: Apple QuickTime Targa File Buffer Overflow Vulnerability"|0x402e6500|High|Unknown|Informational|ntoss|Global|Global|192.168.1.4|9811|10.10.30.98|2986|
4	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
5	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
6	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
7	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
8	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
9	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
10	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
11	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
12	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
13	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
14	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
15	<4> %ASA-1-105047: (Primary) Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2

Syntaxe des règles avancées liées à une base de données Warehouse

La rubrique explique la syntaxe et des exemples de requête des règles avancées.

Syntaxe générale d'une règle avancée

La figure suivante montre comment définir une requête avancée.



Voici un exemple de syntaxe pour une requête avancée :

```
DROP Table IF EXISTS sessions21022014;

CREATE External TABLE sessions21022014

ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'

STORED AS INPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2'

TBLPROPERTIES('avro.schema.literal'='
 {

"type":"record";
```

```
"name":"nextgen";
"fields":
 [
 {"name":"time",  "type":["long", "null"], "default":"null"},
{"name":"threat_category",  "type":["string", "null"],
"default":"null"},
{"name":"ip_src",  "type":["string", "null"], "default":"null"},
{"name":"device_class",  "type":["string", "null"], "default":"null"}
 ]
 '};
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

select `from_unixtime(time), threat_category, ip.src` from `time_variable` where `threat_category` is not `NULL` and `time >= ${report_starttime}` and `time <= ${report_endtime};`

Remarque : Reporting Engine traite une ligne commençant par <hyphen> <hyphen> comme un commentaire dans la règle Warehouse Expert.
Par exemple,

```
set mapred.input.dir.recursive=true;
-- This is an Expert comment
 set hive.mapred.supports.subdirectories=true;
```

La syntaxe générale d'une requête avancée est expliquée ci-dessous :

1. Déplacer et créer une table externe, puis formater la ligne :

   Tout d'abord, nous déplaçons la table si elle existe déjà, et nous créons une table externe **sessions21022014**

   ```
   DROP TABLE IF EXISTS sessions21022014
    CREATE EXTERNAL TABLE sessions21022014
   ```

   Remarque : Vous ne devez créer de table externe que si vous utilisez une autre table. Par exemple, si vous utilisez une autre table que **sessions21022014**, vous devez supprimer la table et créer une table externe.

Spécifiez ensuite le format de ligne comme interface Avro.SerDe pour indiquer à HIVE comment l'enregistrement doit être traité. Avro.SerDe vous permet de lire ou écrire des données Avro sous forme de tables HIVE et de les stocker sous forme de format d'entrée et de format de résultat.

```
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.Avro.SerDe'
 STORED AS INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat'
```

2. Spécifiez l'emplacement HDFS :
   Ensuite, vous devez spécifier l'emplacement HDFS '/RSA/rsasoc/v1/sessions/data/2013/12/2' à partir duquel les données sont interrogées avant d'exécuter les instructions HIVE. Le paramètre d'emplacement indique les données à extraire en fonction de l'entrée de date indiquée. Il s'agit d'un paramètre variable. Vous pouvez extraire des valeurs en fonction de la date saisie.
3. Définir le schéma de la table :
   Troisièmement, vous définissez le schéma de la table en définissant les colonnes avec un type de données spécifique et la valeur par défaut est 'null'.

```
TBLPROPERTIES('avro.schema.literal'='
 {"type":"record";
 "name":"nextgen";
 "fields":
 [
 {"name":"ip_src",  "type":["string", "null"], "default":"null"}
 ]
 '};
```

4. Importer les données à partir du répertoire contenant les sous-répertoires :
   Ensuite, vous devez activer HIVE afin qu'il analyse de manière récursive tous les sous-répertoires et qu'il extraie toutes les données à partir de tous les sous-répertoires.

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
```

5. Extraire les données à partir de la table HIVE :
   Lorsque vous avez exécuté toutes les instructions ci-dessus, vous pouvez envoyer une requête à la base de données avec la clause **select** dans une requête HIVE pour extraire les données de la table HIVE.

Les exemples suivants illustrent des règles avancées en mode expert :

- Rapport horaire, quotidien, hebdomadaire et mensuel
- Partition de table basée sur le rapport d'emplacement
- Joindre les logs et sessions en fonction du rapport unique_id
- Rapport de liste
- Rapport paramétré
- Table partitionnée comportant différents emplacements
- Partitionnement automatisé avec la fonction personnalisée (à partir de la version 10.5.1)

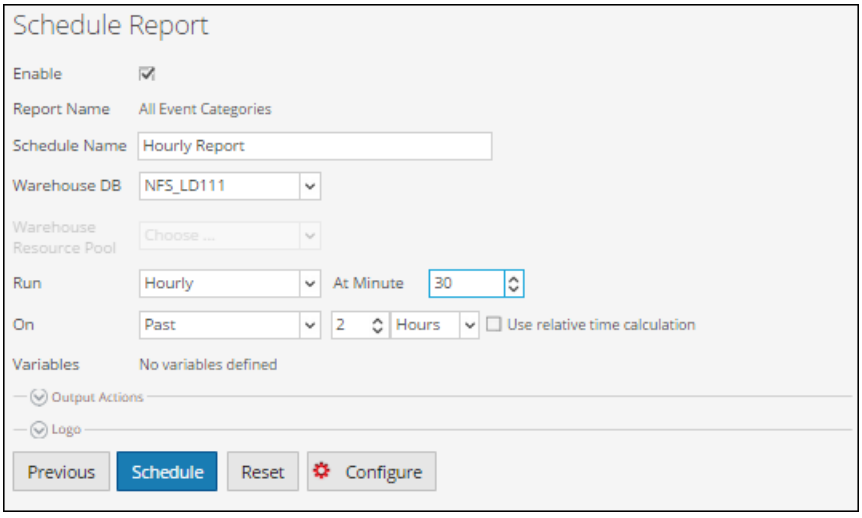
Rapport horaire, quotidien, hebdomadaire et mensuel

Dans ces exemples de règles, vous pouvez créer différents rapports pour le 2 décembre 2013 (comme dans la figure ci-dessous). La variable de date dans l'instruction LOCATION peut être modifiée, selon laquelle vous pouvez créer un rapport horaire, quotidien, hebdomadaire et mensuel.

Rapport horaire

Dans cet exemple de règle, vous pouvez créer un rapport horaire pour le 2 décembre 2013. L'instruction LOCATION peut être modifiée pour générer un rapport horaire.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12/2' - la date saisie (2013/12/2) indique l'année/le mois/le jour. Toutes les données du 2 décembre 2013 sont récupérées à l'aide de l'instruction « location ».

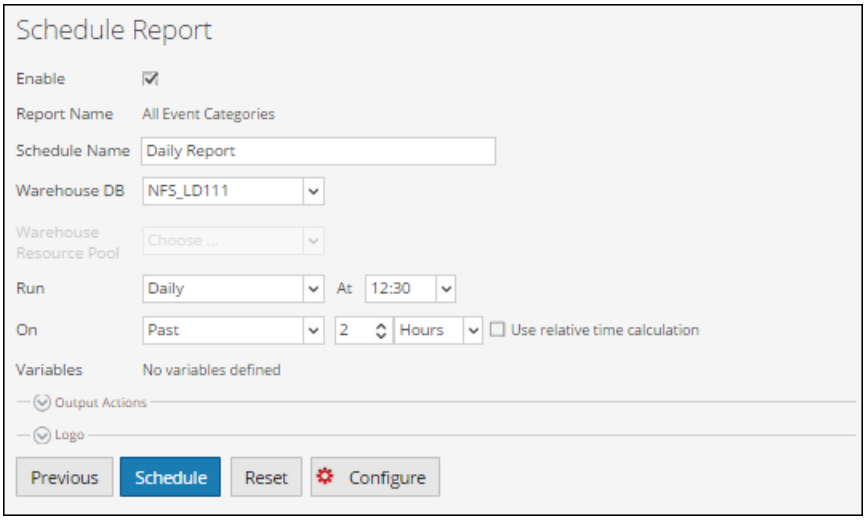


L'ensemble des résultats de cette requête sera présenté dans un rapport horaire.

Rapport quotidien

Dans cet exemple de règle, vous pouvez créer un rapport quotidien pour décembre 2013. L'instruction LOCATION peut être modifiée pour générer un rapport quotidien.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - la date saisie (2013/12) indique l'année/le mois. Toutes les données de décembre 2013 sont récupérées à l'aide de l'instruction « location ».

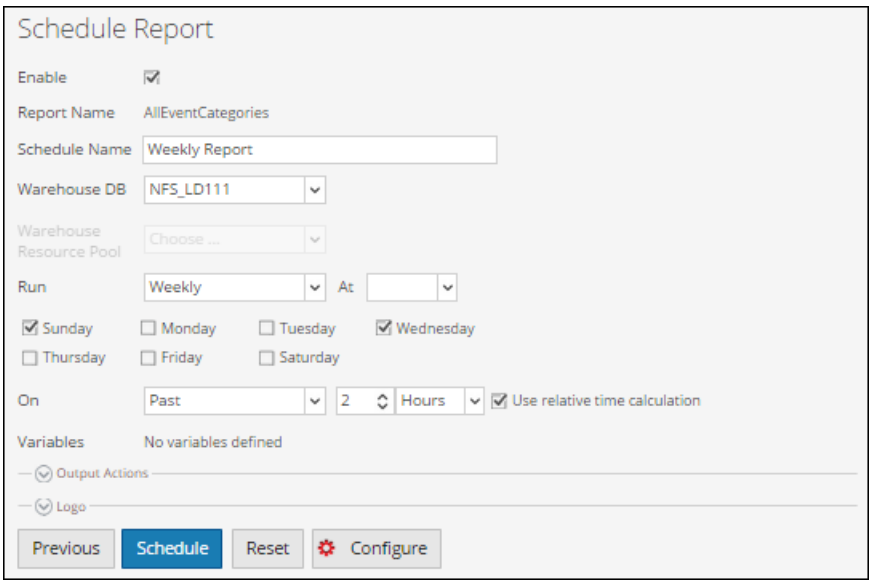


L'ensemble des résultats de cette requête sera présenté dans un rapport quotidien.

Rapport hebdomadaire

Dans cet exemple de règle, vous pouvez créer un rapport hebdomadaire pour décembre 2013. L'instruction LOCATION peut être modifiée pour générer un rapport hebdomadaire.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013/12' - la date saisie (2013/12) indique l'année/le mois. Toutes les données de décembre 2013 sont récupérées à l'aide de l'instruction « location ».

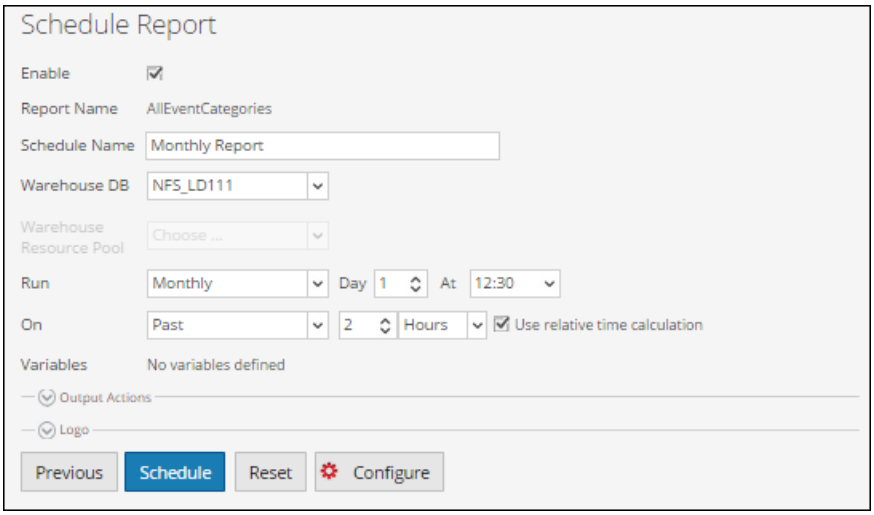


L'ensemble des résultats de cette requête sera présenté dans un rapport hebdomadaire.

Rapport mensuel

Dans cet exemple de règle, vous pouvez créer un rapport mensuel pour l'année 2013. L'instruction LOCATION peut être modifiée pour générer un rapport mensuel.

LOCATION '/RSA/rsasoc/v1/sessions/data/2013' - la date saisie (2013) indique l'année. Toutes les données de l'année 2013 sont récupérées à l'aide de l'instruction « location ».



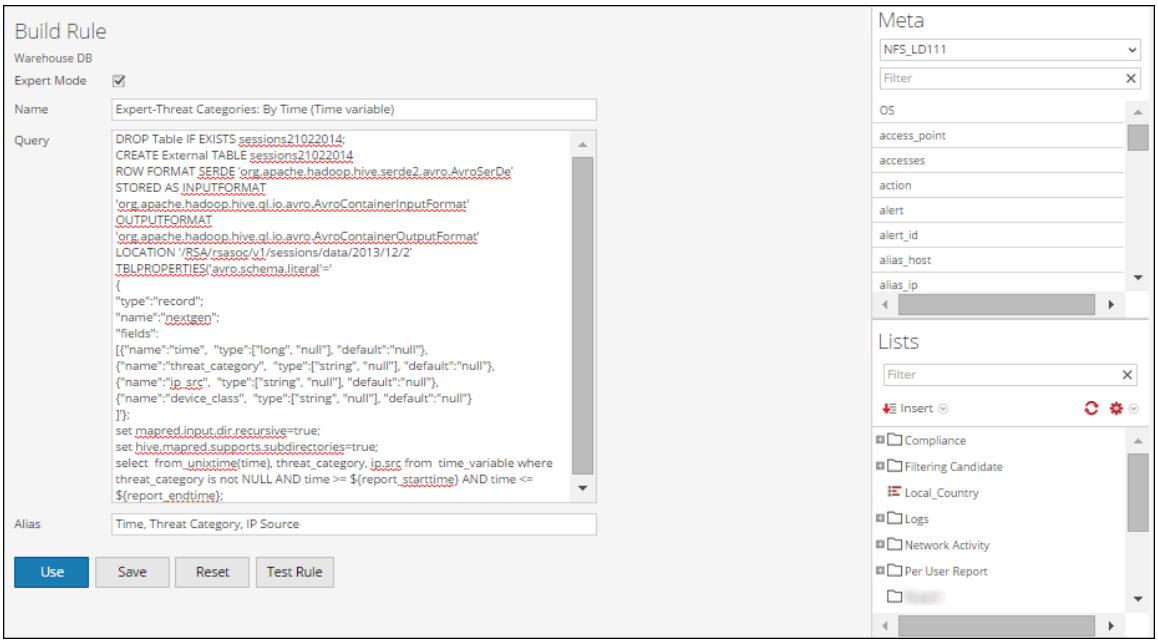
L'ensemble des résultats de cette requête sera présenté dans un rapport mensuel.

Pour plus d'informations sur la définition de LOCATION, consultez **Spécifier l'emplacement HDFS** dans la rubrique **Syntaxe générale d'une règle avancée**.

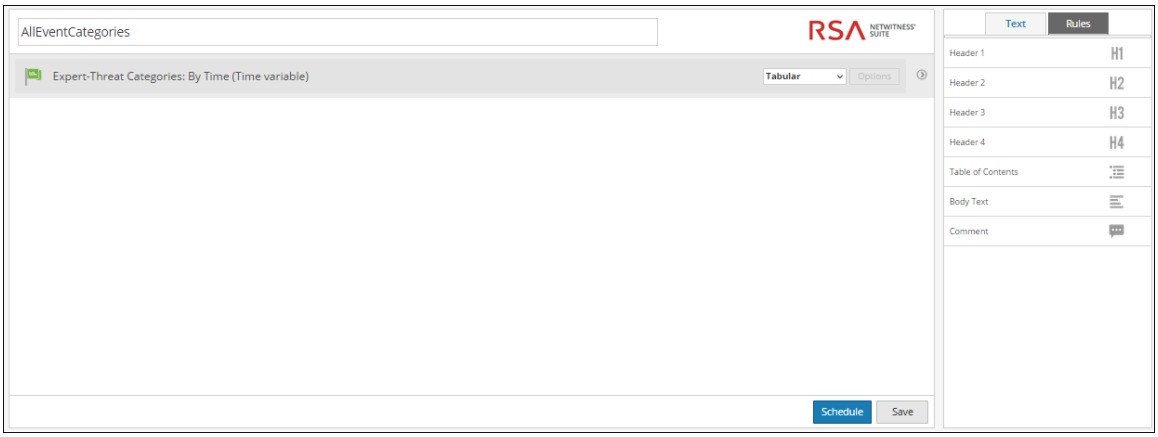
Vous devez réaliser les étapes suivantes dans l'ordre pour afficher l'ensemble de résultats d'une règle avancée :

1. Définir une règle avancée
2. Ajouter la règle avancée à un rapport
3. Planifier un rapport
4. Afficher un rapport planifié

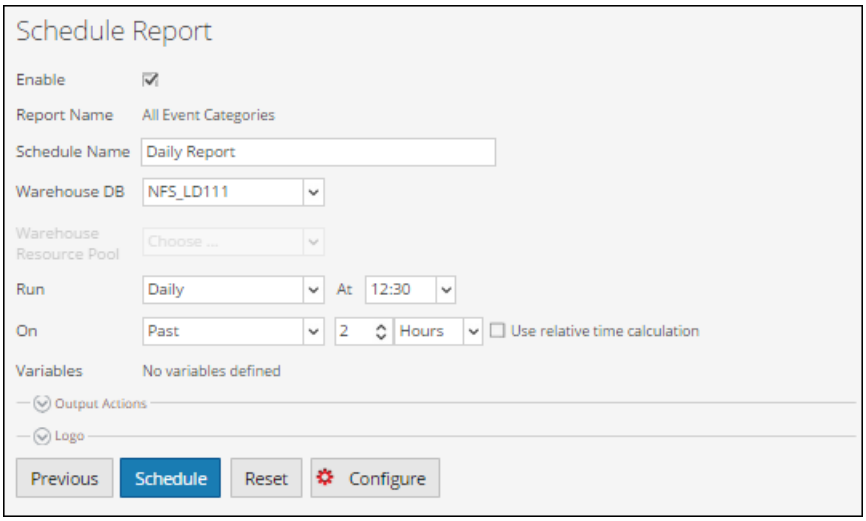
La figure suivante montre comment définir une règle avancée.



La figure suivante montre comment ajouter une règle avancée à un rapport (par exemple, **AllEventCategories**).



La figure suivante vous montre comment planifier un rapport quotidien.

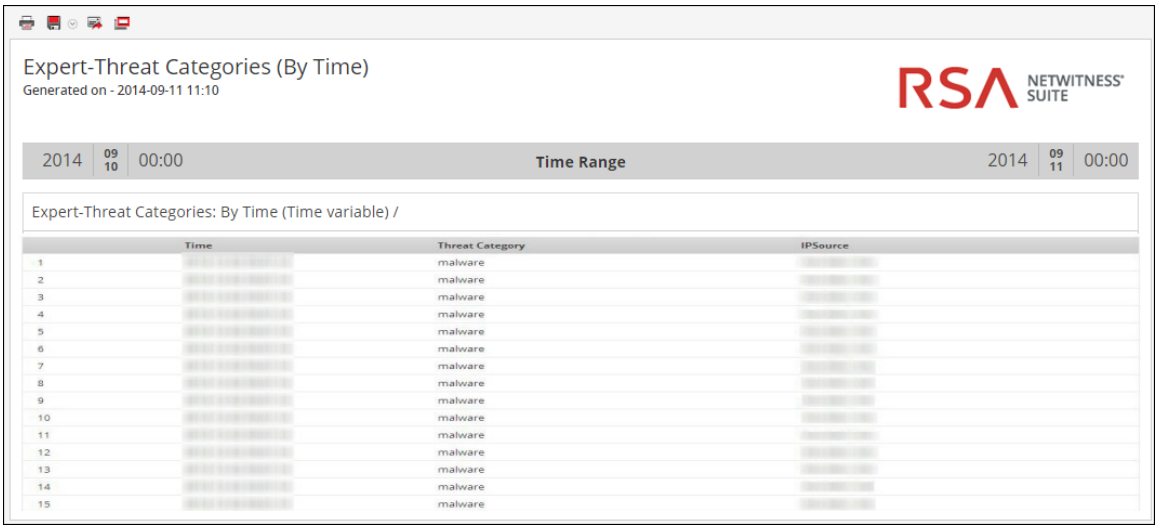


Si vous souhaitez générer un rapport pour une période spécifique, vous devez définir manuellement la période dans la requête à l'aide des deux variables suivantes :

```
${report_starttime} - The starting time of the range in seconds.
 ${report_endtime} - The ending time of the range in seconds.
```

Par exemple, `SELECT from_unixtime(time), threat_category, ip.src FROM time_variable WHERE threat_category is not NULL AND time >= ${report_starttime} AND time <= ${report_endtime};`

La figure suivante montre l'ensemble de résultats de la planification d'un rapport quotidien.

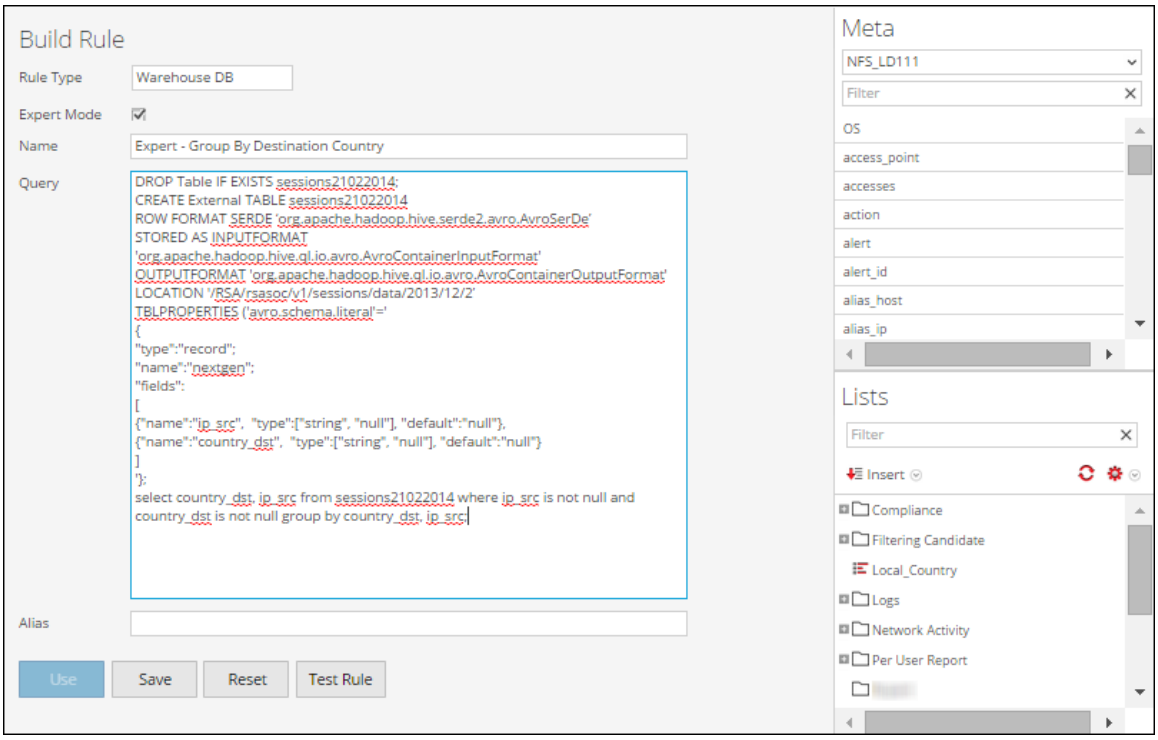


Partition de table basée sur le rapport d'emplacement

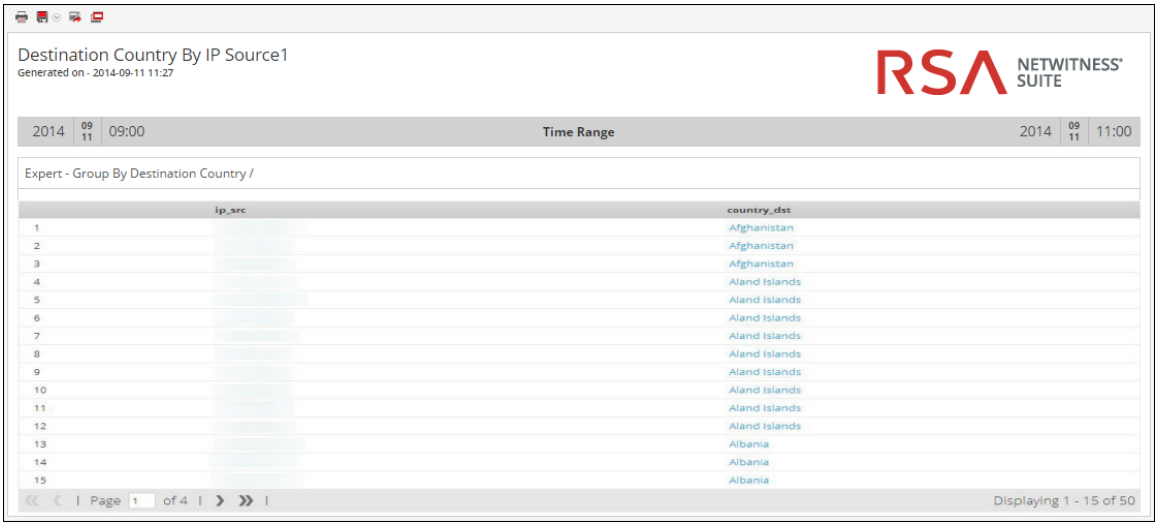
Dans cet exemple de règle, vous pouvez créer une partition de table basée sur l'emplacement. Chaque table peut disposer d'une ou de plusieurs clés de partition qui déterminent comment les données sont stockées. Par exemple, country_dst de type STRING et ip_src de type STRING. Chaque valeur unique des clés de partition définit une partition de la table.

Dans l'exemple fourni, nous exécutons une requête HIVE pour extraire le pays de destination et l'adresse IP de la source à partir de la table sessions05032014 et nous regroupons les résultats grâce à ces champs.

Cette règle fournit des informations sur la table créée, la ligne formatée, l'emplacement (chemin d'accès au répertoire) pour les fichiers de données avro dans Warehouse, et renvoie un ensemble de résultats en fonction de la requête HIVE pour indiquer que la requête a renvoyé un ensemble de résultats. Pour plus d'informations sur ces instructions, reportez-vous à la rubrique « Syntaxe générale d'une règle avancée ».



La figure suivante montre l'ensemble de résultats de la création d'une partition de table basée sur un rapport d'emplacement.

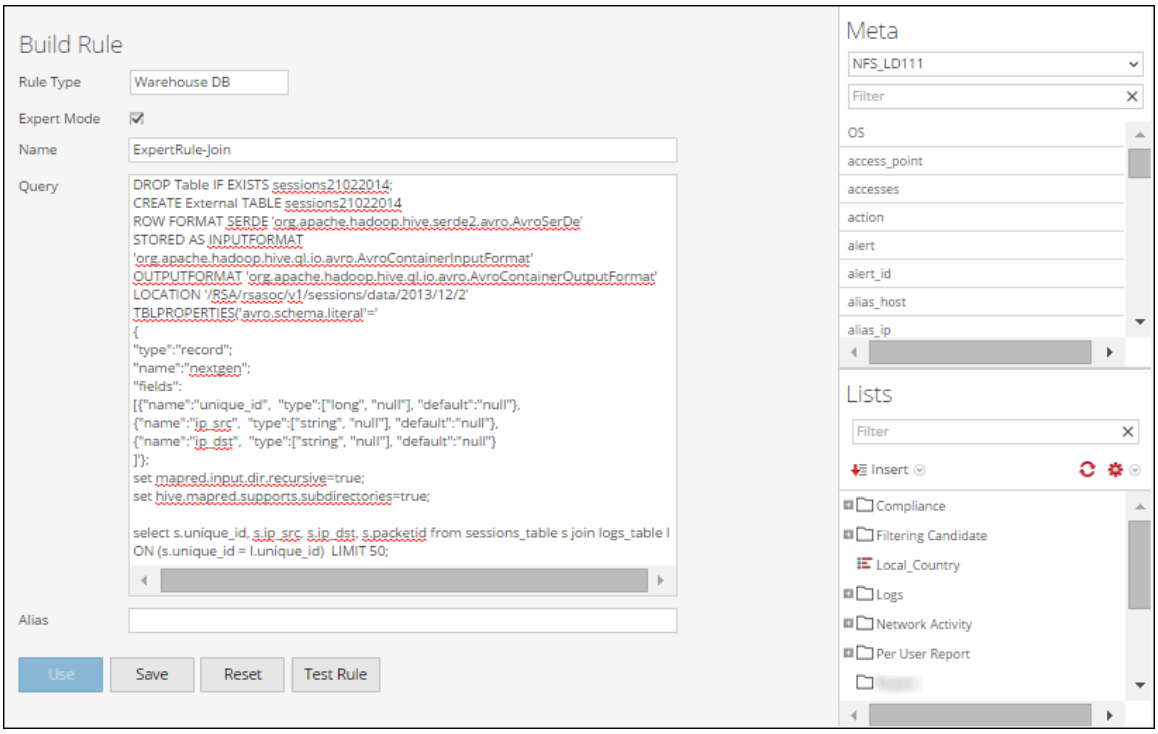


Joindre les logs et sessions en fonction du rapport unique_id

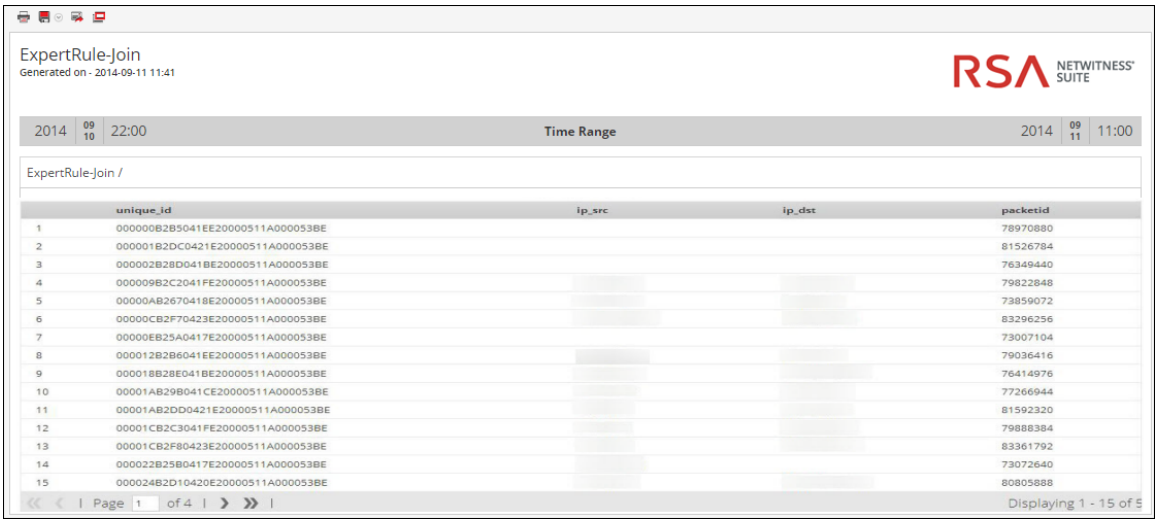
Dans cet exemple de règle, vous pouvez créer une règle pour joindre des tables de sessions et logs afin d'extraire unique_id, l'adresse IP de la source et de la destination, et l'ID de paquet basé sur unique_id.

Dans l'exemple fourni, nous exécutons une requête HIVE extraire certains champs de sessions_ table et logs_table en réalisant une jointure basée sur le champ « unique_id ».

Cette règle fournit des informations sur la table créée, la ligne formatée, l'emplacement (chemin d'accès au répertoire) pour les fichiers de données avro dans Warehouse, et renvoie un ensemble de résultats en fonction de la requête HIVE pour indiquer que la requête a renvoyé un ensemble de résultats. Pour plus d'informations sur ces instructions, reportez-vous à la rubrique **Syntaxe générale d'une règle avancée**.



La figure suivante montre l'ensemble de résultats de la jointure de tables de sessions et logs en fonction de unique_id.



ExpertRule-Join
Generated on - 2014-09-11 11:41

RSA NETWITNESS SUITE

2014 09 10 22:00 **Time Range** 2014 09 11 11:00

ExpertRule-Join /

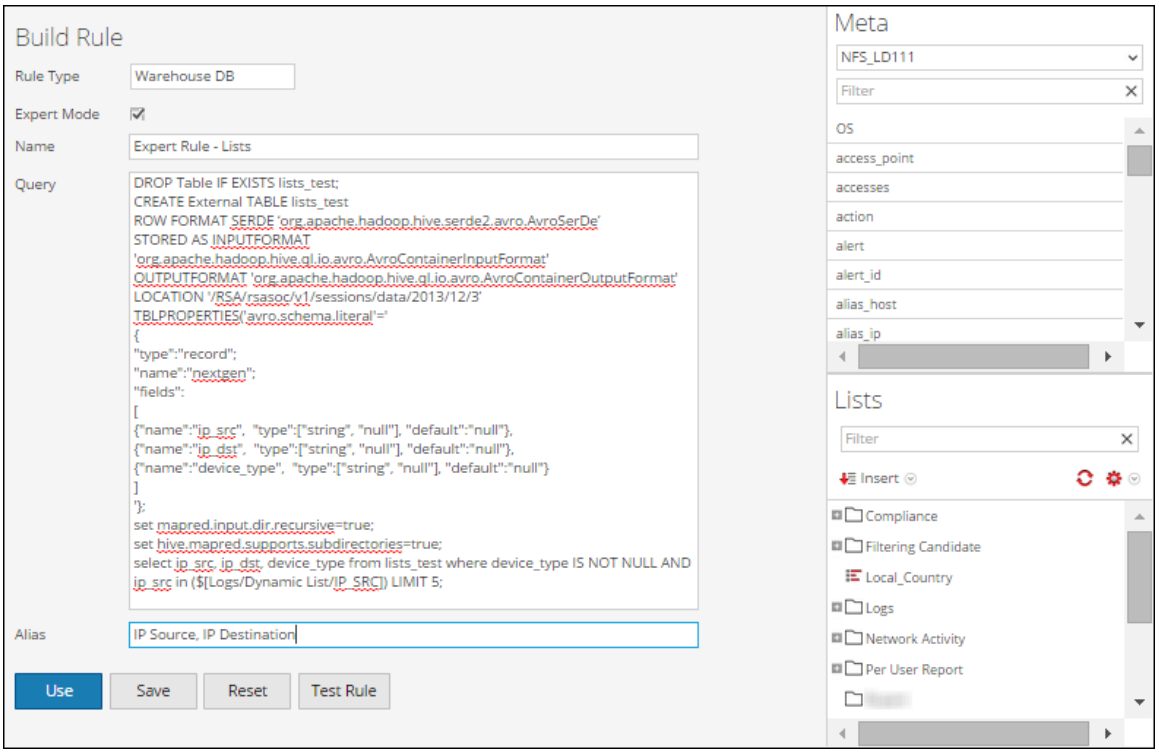
	unique_id	ip_src	ip_dst	packetid
1	000000B2B5041EE20000511A000053BE			78970880
2	000001B2DC0421E20000511A000053BE			81526784
3	000002B28D041BE20000511A000053BE			76349440
4	000009B2C2041FE20000511A000053BE			79822848
5	00000AB2670418E20000511A000053BE			73859072
6	00000CB2F70423E20000511A000053BE			83296256
7	00000EB25A0417E20000511A000053BE			73007104
8	000012B2B6041EE20000511A000053BE			79036416
9	000018B28E041BE20000511A000053BE			76414976
10	00001AB29B041CE20000511A000053BE			77266944
11	00001AB2DD0421E20000511A000053BE			81592320
12	00001CB2C3041FE20000511A000053BE			79888384
13	00001CB2F80423E20000511A000053BE			83361792
14	000022B25B0417E20000511A000053BE			73072640
15	000024B2D10420E20000511A000053BE			80805888

Page 1 of 4 Displaying 1 - 15 of 5

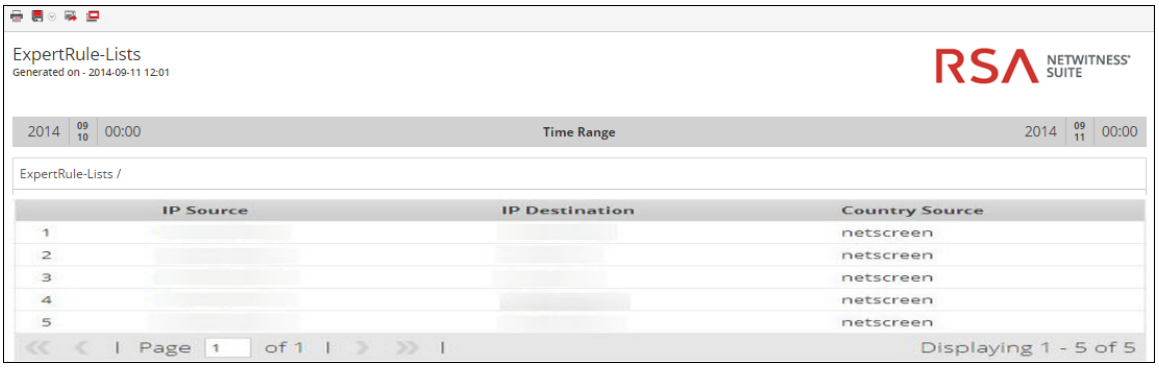
Rapport de liste

Dans cet exemple de règle, vous pouvez créer un rapport de liste pour extraire l'adresse IP de la source et de la destination, et le type de périphérique à partir de la table **lists_test** où le type de périphérique n'est pas nul et l'adresse IP de la source est extraite à partir de la liste d'événement adéquate.

Cette règle fournit des informations sur la table créée, la ligne formatée, l'emplacement (chemin d'accès au répertoire) pour les fichiers de données avro dans Warehouse, et renvoie un ensemble de résultats en fonction de la requête HIVE pour indiquer que la requête a renvoyé un ensemble de résultats. Pour plus d'informations sur ces instructions, reportez-vous à la rubrique **Syntaxe générale d'une règle avancée**.



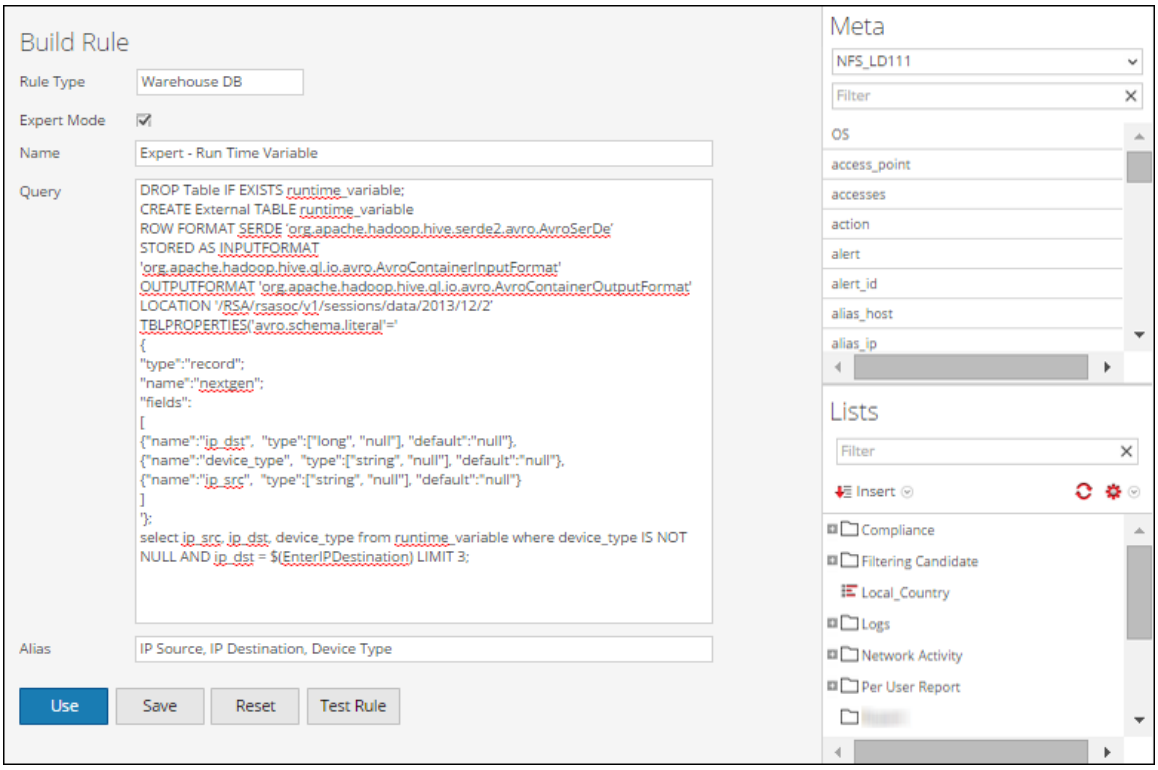
La figure suivante montre l'ensemble de résultats de l'exécution d'un rapport de liste.



Rapport paramétré

Dans cette règle d'exemple, vous pouvez créer une règle pour extraire les adresses IP de la source et de la destination, et le type de périphérique à partir de la table **runtime_variable** en fonction de la variable d'exécution `${EnterIPDestination}`. Lors de l'exécution, il vous est demandé de saisir une valeur pour l'adresse IP de l'ip_dst de destination. Selon la valeur saisie, l'ensemble de résultats s'affiche.

Cette règle fournit des informations sur la table créée, la ligne formatée, l'emplacement (chemin d'accès au répertoire) pour les fichiers de données avro dans Warehouse, et renvoie un ensemble de résultats en fonction de la requête HIVE pour indiquer que la requête a renvoyé un ensemble de résultats. Pour plus d'informations sur ces instructions, reportez-vous à la rubrique **Syntaxe générale d'une règle avancée**.



La figure suivante montre l'ensemble de résultats de l'exécution d'un rapport paramétré.

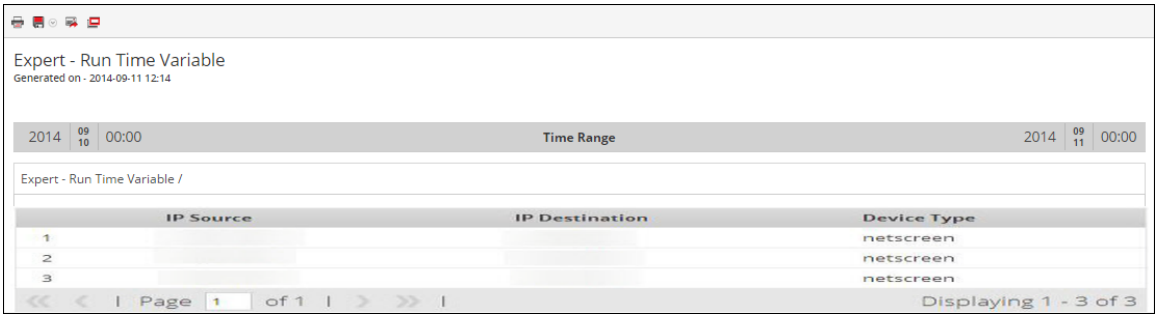


Table partitionnée comportant différents emplacements

Le texte suivant est un exemple de table partitionnée comportant différents emplacements :

```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;
 CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
 "name": "my_record", "type": "record",
 "fields": [
 {"name":"sessionid", "type":["null", "long"], "default" :
```

```
null},
 {"name":"time", "type":["null", "long"], "default" : null}
 ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/9';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/12/';
 SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
${report_starttime} AND time
 <= ${report_endtime};
```

La table partitionnée comportant différents emplacements se présente tel qu'il est expliqué ci-dessous.

1. Activez HIVE afin qu'il analyse de manière récursive tous les sous-répertoires et qu'il lise toutes les données à partir des sous-répertoires.

   ```
   set mapred.input.dir.recursive=true;
    set hive.mapred.supports.subdirectories=true;
   ```

2. Déplacez et créez une table externe, puis formatez les lignes :

   ```
   DROP TABLE IF EXISTS AVRO_COUNT;
    CREATE EXTERNAL TABLE AVRO_COUNT
    PARTITIONED BY (partition_id int)
    ROW FORMAT SERDE
   'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
    WITH SERDEPROPERTIES (
    'avro.schema.literal'='{
    "name": "my_record", "type": "record",
    "fields": [
    {"name":"sessionid", "type":["null", "long"], "default" :
   null},
   ```

```
{"name":"time", "type":["null", "long"], "default" : null}
]}'
)
STORED AS
INPUTFORMAT
'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
OUTPUTFORMAT

'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputForma
t';
```

Remarque : Il est nécessaire de créer une table externe uniquement si vous utilisez une autre table. Par exemple, si vous utilisez une autre table qu'**AVRO_COUNT**, vous devez supprimer cette table et créer une table externe.

Remarque : Points à ne pas oublier lorsque vous créez une table :
- la suppression d'une table non externe provoque la suppression des données.
- la table est partitionnée sur une colonne unique, appelée partition_id, et il s'agit de la colonne standard pour Reporting Engine.
- la valeur par défaut d'une colonne est nulle, car le fichier AVRO ne peut-être pas contenir la colonne spécifiée.
- les noms de colonne doivent contenir des lettres minuscules, car HIVE n'est pas sensible à la casse mais AVRO l'est.
- vous devez spécifier **avro.schema.literal** dans *SERDEPROPERTIES*.

Pour plus d'informations sur la syntaxe de la règle, consultez *Apache HIVE*.

3. Ajoutez des partitions :

   Lorsque vous définissez une table, vous devez spécifier les emplacements HDFS depuis lesquels les données doivent être interrogées avant d'exécuter les instructions HIVE. Le paramètre location spécifie les données à extraire en fonction de la date spécifiée. Les données sont réparties entre différents emplacements ou répertoires du système HDFS. Pour chaque emplacement, vous devez ajouter une partition avec des valeurs spécifiques attribuées à la colonne de partition. Les emplacements peuvent être n'importe quel répertoire dans le système HDFS

```
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=0) LOCATION
'/rsasoc/v1/sessions/data/2015/07/22/8';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=1)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/9';
ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=2)
```

```
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/10/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=3)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/11/';
 ALTER TABLE AVRO_COUNT ADD PARTITION(partition_id=4)
LOCATION '/rsasoc/v1/sessions/data/2015/07/22/12/';
```

Remarque : HIVE lit chaque fichier présent à ces emplacements comme étant un fichier AVRO. Si ces emplacements comportent un fichier non AVRO, la requête peut échouer.

4. Exécutez la requête

   ```
   SELECT COUNT(*) as TOTAL FROM AVRO_COUNT WHERE time >=
   ${report_starttime} AND time
    <= ${report_endtime};
   ```

   Lorsqu'une table est créée, vous pouvez exécuter des requêtes spécifiques pour filtrer les données. Par exemple, après avoir créé la table, vous pouvez filtrer les données de la manière illustrée dans les exemples ci-dessous :

   Sessions avec une adresse IP source spécifique :

   ```
   SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
   AND time <= ${report_endtime}  AND ip_src = '127.0.0.1'
   ```

   Regrouper en fonction de la destination de l'utilisateur :

   ```
   SELECT * FROM AVRO_COUNT WHERE time >= ${report_starttime}
   AND time <= ${report_endtime}  GROUP BY usr_dst;
   ```

Partition automatisée avec la fonction custom

Dans la version 10.5.1, vous pouvez utiliser la fonction custom pour automatiser l'ajout de partitions à une table définie par l'utilisateur en mode expert.

Syntaxe générale

```
RE WH CUSTOM ADDPARTITIONS(table, namespace, rollup, [starttime,
endtime])
```

La table suivante décrit la syntaxe de la fonction custom :

Numéro de session	Name	Description
1	table	Nom de la table pour laquelle la partition a été ajoutée.
2	espace de nommage	namespace peut correspondre à des sessions ou des logs.
3	rollup	Cette valeur détermine le niveau du chemin de répertoire à inclure dans les partitions. La valeur correspondante peut être HOUR, DAY ou MINUTE. Si Warehouse Connector est configuré pour la valeur Day de rollup, la valeur HOUR génère des résultats ZERO. Le nombre de partitions et l'emplacement de chaque partition dépendent de la période utilisée pour exécuter la règle et de la valeur de rollup.
4	(Facultatif) starttime, endtime	Pour générer des partitions pour une période spécifique différente de celle mentionnée dans la règle, vous devez spécifier l'heure de début et l'heure de fin en **Secondes Epoch**. **Remarque :** Les expressions ne sont pas prises en charge pour l'heure de début et l'heure de fin.

La fonction custom est appelée lorsque Reporting Engine exécute la règle, soit pendant l'exécution de la règle test, soit pendant le rapport planifié. Lors de l'exécution d'une règle d'expert, chaque fois que Reporting Engine identifie la déclaration de fonction, il extrait les arguments
nécessaires, insère *n* nombre d'instructions HiveQL ADD PARTITION et les exécute sur le serveur Hive.

La structure des emplacements et des répertoires est déterminée par l'argument transmis dans la règle et la configuration de la source de données Hive
 dans Reporting Engine. Le nombre de partitions dépend de la mise à jour spécifiée et la plage horaire utilisée lors de l'exécution de la règle. Par exemple, avec la valeur de rollup définie sur HOUR et la période sur PAST 2 Days, Reporting Engine génère 48 partitions pour 48 heures alors que
, avec la valeur de rollup définie sur DAY, Reporting Engine crée deux partitions, une pour chaque jour.

La requête de partition est générée par le modèle de syntaxe, tel qu'il est défini dans l'attribut de configuration Hive AlterTableTemplate du Reporting Engine.

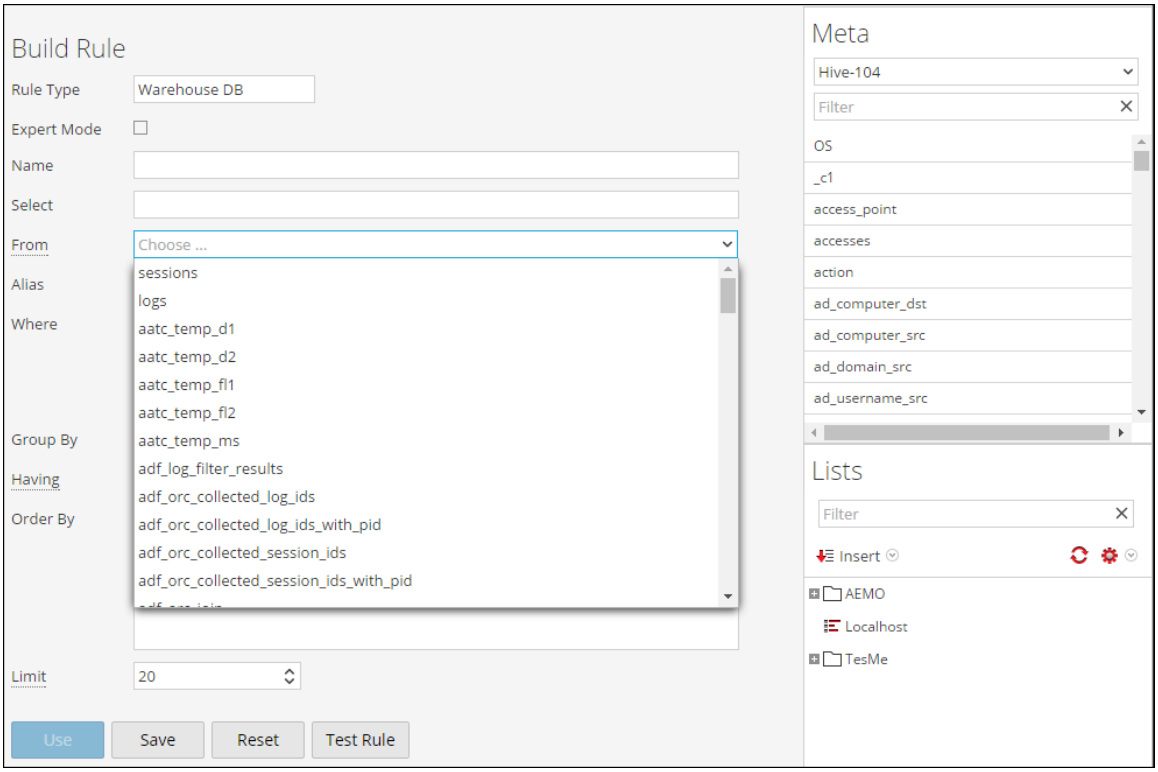
Remarque : Par défaut, cette fonction commence à ajouter des partitions à une table en numérotant les partitions de 0 à N-1. La table doit donc être partitionnée par colonne désignée par un seul nombre entier, appelé l'ID de partition.

Le texte suivant est un exemple de partition automatisée à l'aide de la fonction custom :

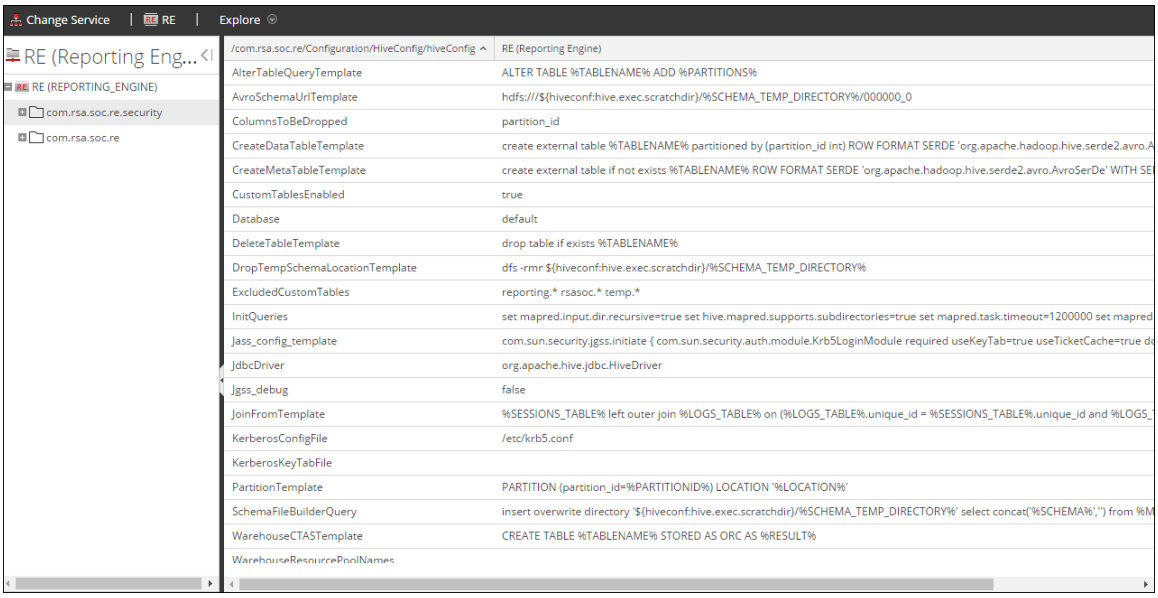
```
set mapred.input.dir.recursive=true;
 set hive.mapred.supports.subdirectories=true;
 DROP TABLE IF EXISTS AVRO_COUNT;

CREATE EXTERNAL TABLE AVRO_COUNT
 PARTITIONED BY (partition_id int)
 ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.avro.AvroSerDe'
 WITH SERDEPROPERTIES (
 'avro.schema.literal'='{
  "name": "my_record", "type": "record",
  "fields": [
  {"name":"sessionid", "type":["null", "long"], "default" :
null}
  ,{"name":"time", "type":[ "null" , "long"], "default" : null}
  ,{"name":"unique_id", "type":["null", "string"], "default" :
null}
  ]}'
 )
 STORED AS
 INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerInputFormat'
 OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.avro.AvroContainerOutputFormat';

RE_WH_CUSTOM_ADDPARTITIONS(AVRO_COUNT, 'sessions', 'DAY');
 SELECT COUNT(*) as TotalSessions FROM AVRO_COUNT
 WHERE time >= ${report_starttime} AND time <= ${report_
endtime};
```

Création d’un rapport de tables personnalisées

Dans 10.6.1, vous pouvez utiliser et créer des tables personnalisées sur le serveur Hive. Reporting Engine prend en charge les requêtes en cours d'exécution sur les tables définies par l'utilisateur et la possibilité de créer une nouvelle table à partir d'un résultat de la même règle. Lorsque cette fonction est activée dans l'interface utilisateur Générateur de règles Warehouse, l'utilisateur peut afficher la liste des tables personnalisées disponibles dans le serveur Hive.



Pour activer cette fonction, définissez **customTablesEnabled** à **TRUE** en accédant à **Reporting Engine -> Explorer -> Configuration de Hive**.



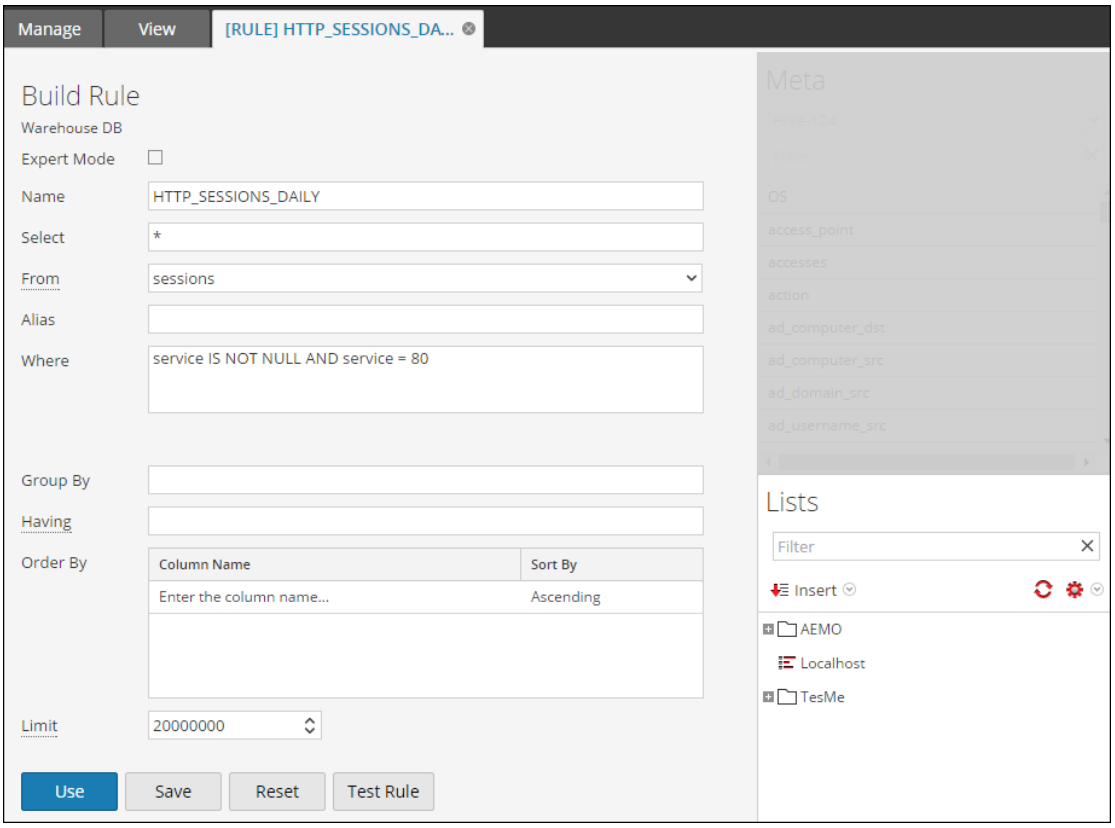
Création d'une table personnalisée à partir de règles standard

Pour planifier un rapport qui contient une seule règle SAW, une nouvelle entrée de texte avec un **Nom Warehouse CTA** est ajoutée. L'utilisateur peut désormais spécifier un nom de table personnalisée qui sera créé sur le résultat de la règle dans le rapport.

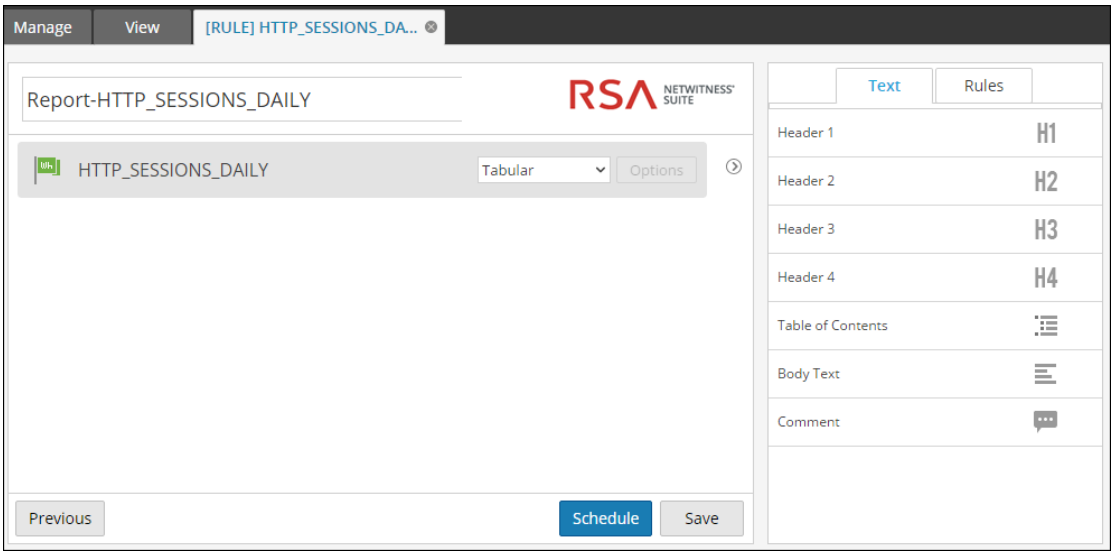
Remarque : Cette fonction est uniquement disponible si le rapport contient une seule règle SAW à la page Ordonnanceur. Dans le cas contraire, cette option est masquée.

Le processus pour utiliser la fonction est expliqué ci-dessous :

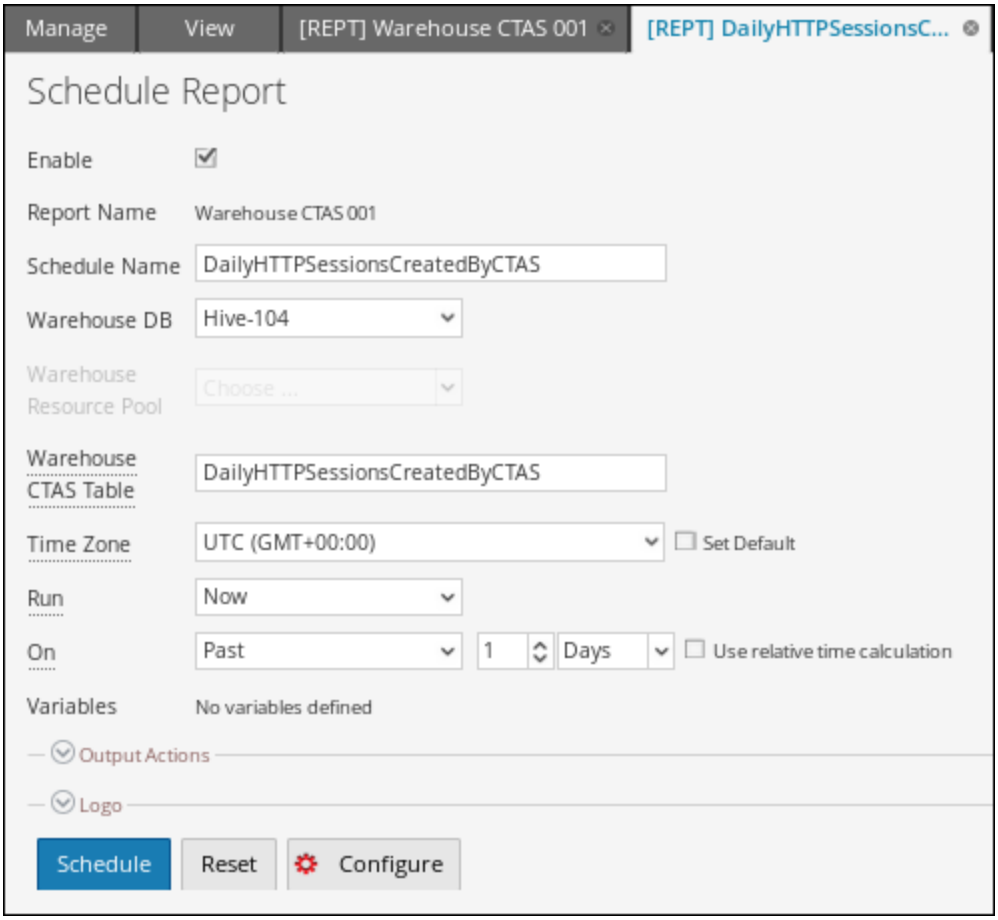
1. Créer une règle pour filtrer les données dans SAW.



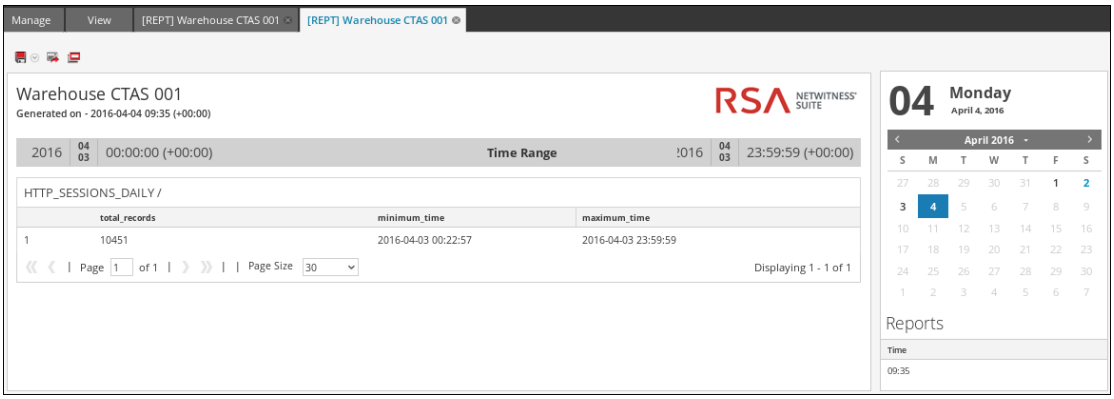
2. Créer un rapport avec la règle ci-dessus.



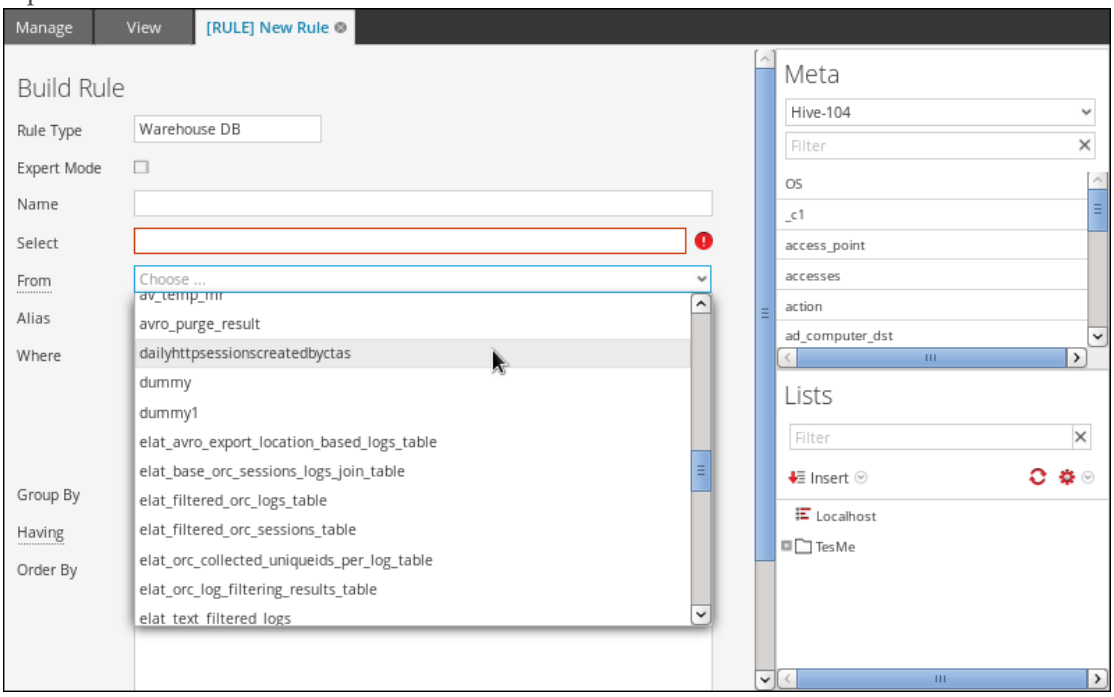
3. Créer un planning, puis saisissez le nom de la table CTAS.



4. Exécuter le rapport et le Reporting Engine crée le résumé des résultats ci-dessous pour le planning.



5. Sur le schéma suivant rafraîchir ou un redémarrer le Reporting Engine, la table CTAS est répertoriée.



Planificateur de tâches pour Warehouse Reporting

Un planificateur de tâches dans un cluster Hadhoop planifie les tâches, et alloue des ressources spécifiques à chaque tâche exécutée dans un cluster. Par défaut, le planificateur de tâches alloue un nombre égal de ressources à l'ensemble des tâches. Par exemple, si dix tâches sont exécutées, elles partageront les ressources du cluster de façon égale. Toutefois, vous pouvez configurer le planificateur de tâches pour contrôler l'exécution des tâches. Vous pouvez en effet faire en sorte qu'une tâche soit exécutée plus rapidement que d'autres en lui allouant davantage de ressources (pools ou files d'attente). Vous pouvez ainsi anticiper l'exécution de certains rapports avant les autres.

Fonctions

NetWitness Suite prend en charge deux planificateurs de tâches :

- Planificateur Fair (`org.apache.hadoop.mapred.FairScheduler`)
- Planificateur de capacité (`org.apache.hadoop.mapred.CapacityTaskScheduler`)

Planificateur Fair

Ce planificateur divise la capacité totale du cluster en pools logiques. Vous pouvez envoyer une tâche au pool de votre choix. Toutes les tâches envoyées à un pool partagent les ressources allouées à ce dernier uniquement. Lorsqu'un pool dispose de ressources, celles-ci sont attribuées à d'autres pool dans lesquels des tâches sont en cours d'exécution. Par exemple, un planificateur Fair dispose de 100 % des ressources dans deux pools, Pool A et Pool B. Ces deux pools se partagent la totalité des ressources à 40 et 60 %, respectivement. Si quatre tâches sont exécutées dans le Pool A, le planificateur alloue 10 % des ressources à chaque tâche. Lorsque ces quatre tâches sont terminées, les ressources libérées sont attribuées au Pool B.

Remarque : Vous pouvez configurer un pool pour qu'il exécute plusieurs tâches en parallèle.

Planificateur de capacité

Ce planificateur divise la capacité totale du cluster dans des files d'attente. Chaque file se voit allouer une partie préconfigurée de la capacité totale. Une tâche peut être envoyée à n'importe laquelle de ces files d'attente. Si plusieurs tâches sont envoyées à la même file d'attente, elles sont exécutées l'une à la suite de l'autre. Par exemple, il se peut que le planificateur de capacité dispose de 100 % des ressources et de trois files d'attente, Par défaut, Faible et Élevé qui se partagent la totalité des ressources à 20, 30 et 50%, respectivement. Si la file d'attente Par défaut comprend deux tâches, D1 et D2, que la file Faible en comporte trois L1, L2 et L3, et que la file Élevé en comporte quatre, H1, H2, H3 et H4, ces tâches sont exécutées dans leur file d'attente respectives l'une à la suite de l'autre. Si les tâches d'une file d'attente sont terminées, les ressources libérées ne sont pas réattribuées aux autres files d'attente.

Agrégats de requête

Cette rubrique décrit les fonctions d'agrégation prises en charge.

Fonctions d'agrégation prises en charge

Le tableau suivant présente les fonctions d'agrégation prises en charge.

Fonction d'agrégation	Description	Types de données d'entrée	Types de données de résultat
count	Renvoie le nombre de métavaleurs, y compris les valeurs dupliquées.	Numérique	Numérique
countdistinct	Renvoie le nombre total de valeurs Distinct ou uniques.	Numérique	Numérique
distinct	Renvoie toutes les valeurs uniques.	N'importe laquelle	N'importe laquelle
first	Renvoie la première occurrence de la valeur méta.	N'importe laquelle	Identique à l'entrée
last	Renvoie la dernière occurrence de la valeur méta.	N'importe laquelle	Identique à l'entrée
sum	Renvoie la somme de toutes les valeurs non nulles des clés méta dans un groupe.	Numérique	Numérique
avg (Average)	Renvoie la valeur moyenne de toutes les valeurs non nulles des clés méta au sein d'un groupe.	Numérique	Numérique
min (Minimum)	Renvoie le minimum de toutes les valeurs des clés méta de chaque groupe. Cette valeur se base sur le champ « order by ».	N'importe laquelle	N'importe laquelle

Fonction d'agrégation	Description	Types de données d'entrée	Types de données de résultat
max (Maximum)	Renvoie le maximum de toutes les valeurs des clés méta de chaque groupe. La valeur maximale est la valeur retournée par le champ « order by ».	N'importe laquelle	N'importe laquelle
length	Renvoie la longueur des valeurs de la clé méta. Elle est appelée « fonction scalaire » dans SQL.	N'importe laquelle	Numérique

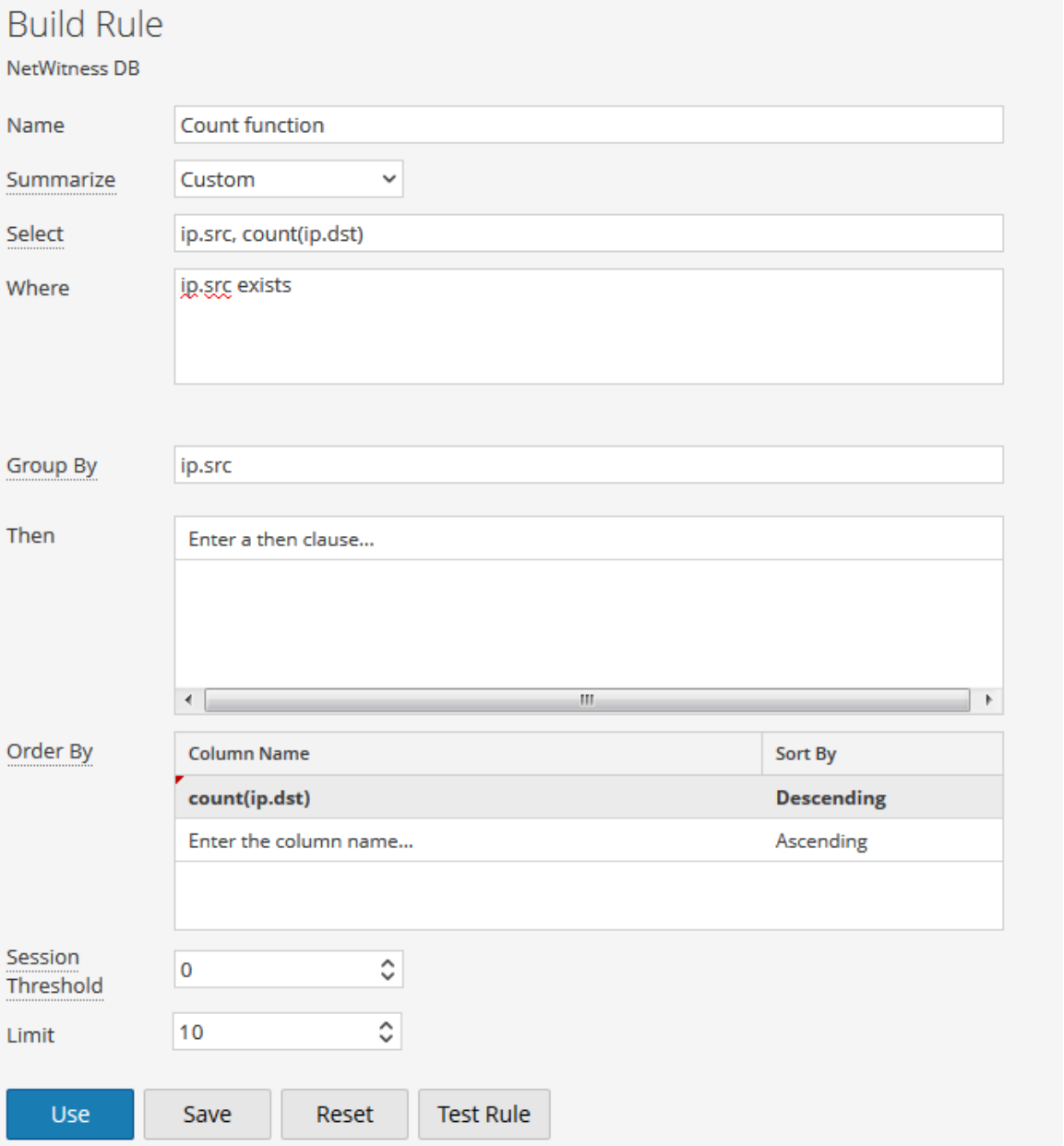
Exemples de requêtes et de résultats par fonction

Count

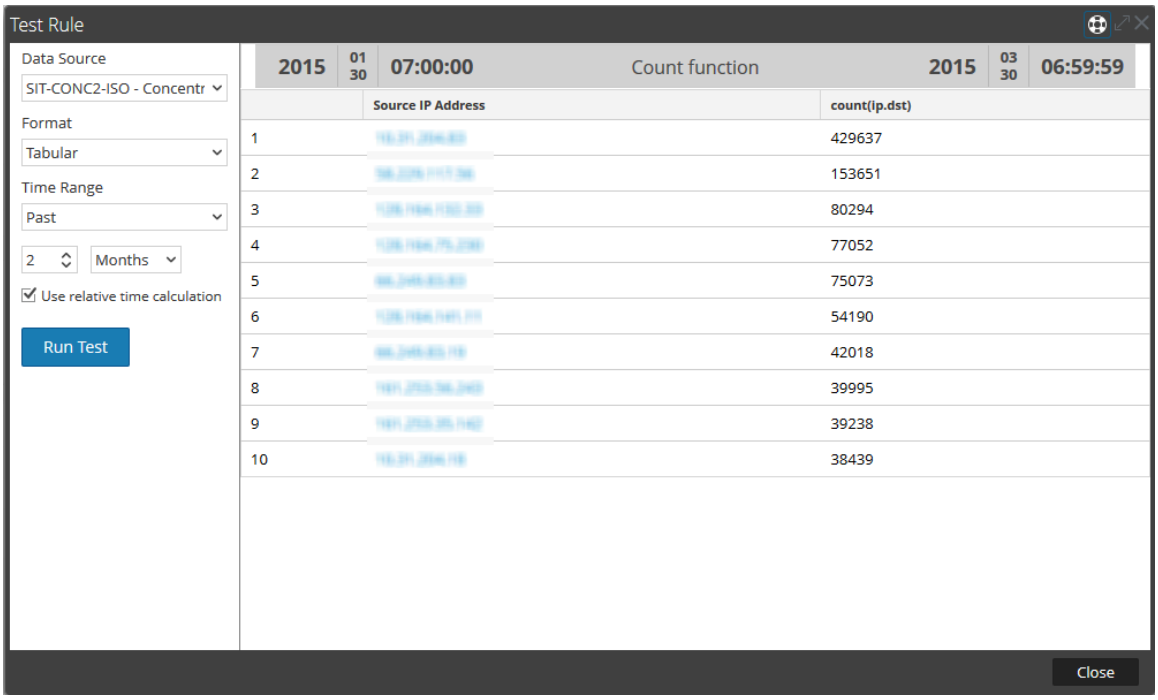
Cette fonction renvoie le nombre de valeurs pour une clé méta spécifiée. Elle exclut les valeurs nulles mais comprend les valeurs dupliquées.

Exemple

La figure suivante montre un exemple de requête pour la fonction « count » utilisée pour l'IP de destination et son IP source respective.



La figure suivante indique le résultat de la requête ci-dessus.



Ici, pour chaque ip.src (IP source) unique, la page renvoie le nombre total de valeurs ip.dst (IP de destination), y compris les valeurs dupliquées.

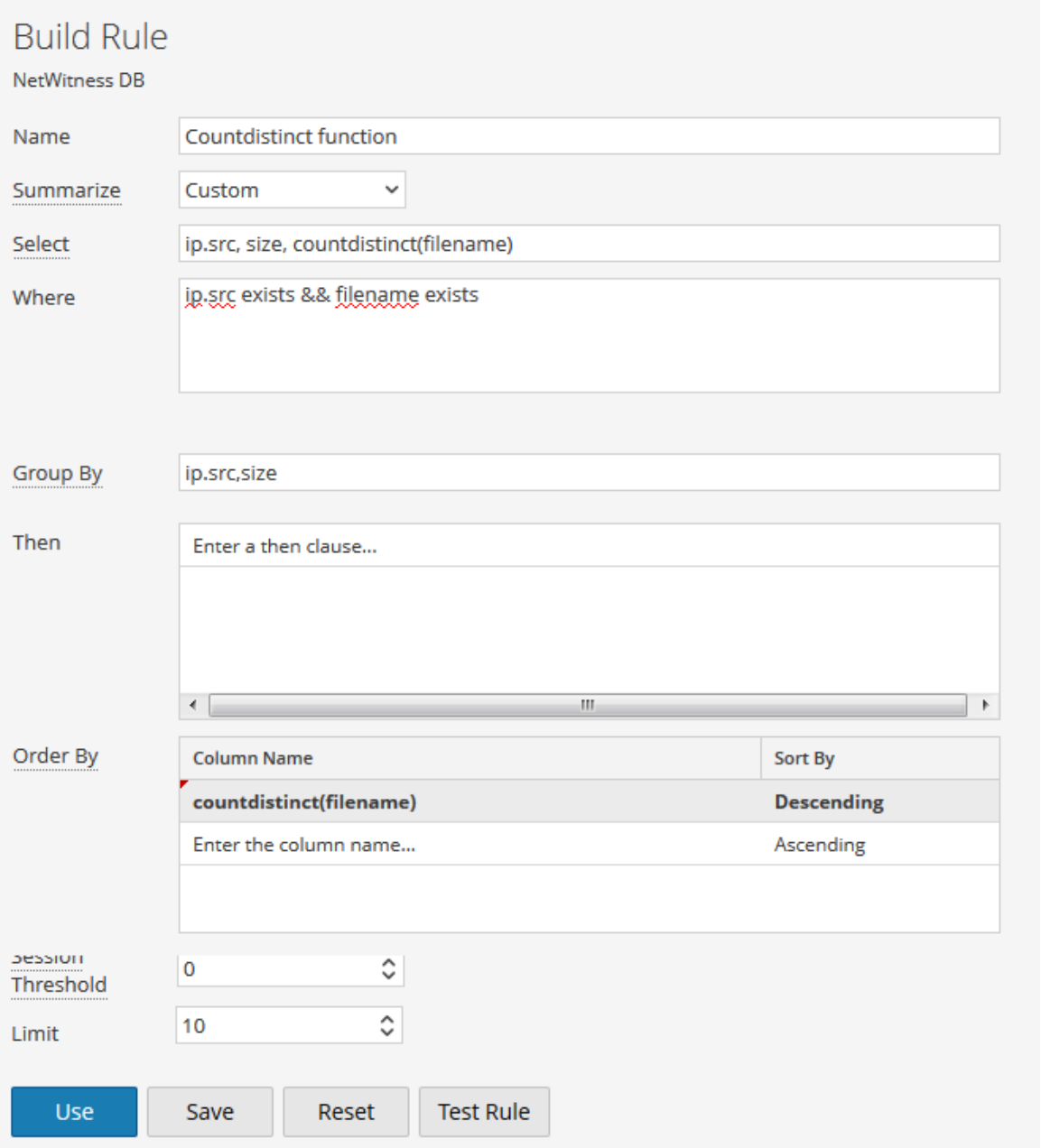
Remarque : Si votre version de RSA NetWitness Suite est actuellement la version 10.5 ou supérieure et que l'un des périphériques NetWitness Suite Core utilise la version 10.3 ou 10.4, il se peut que certaines des fonctions d'agrégation affichent des erreurs inattendues. Cependant, les fonctions d'agrégation comme sum() et count() sont prises en charge dans la version 10.4.

countdistinct

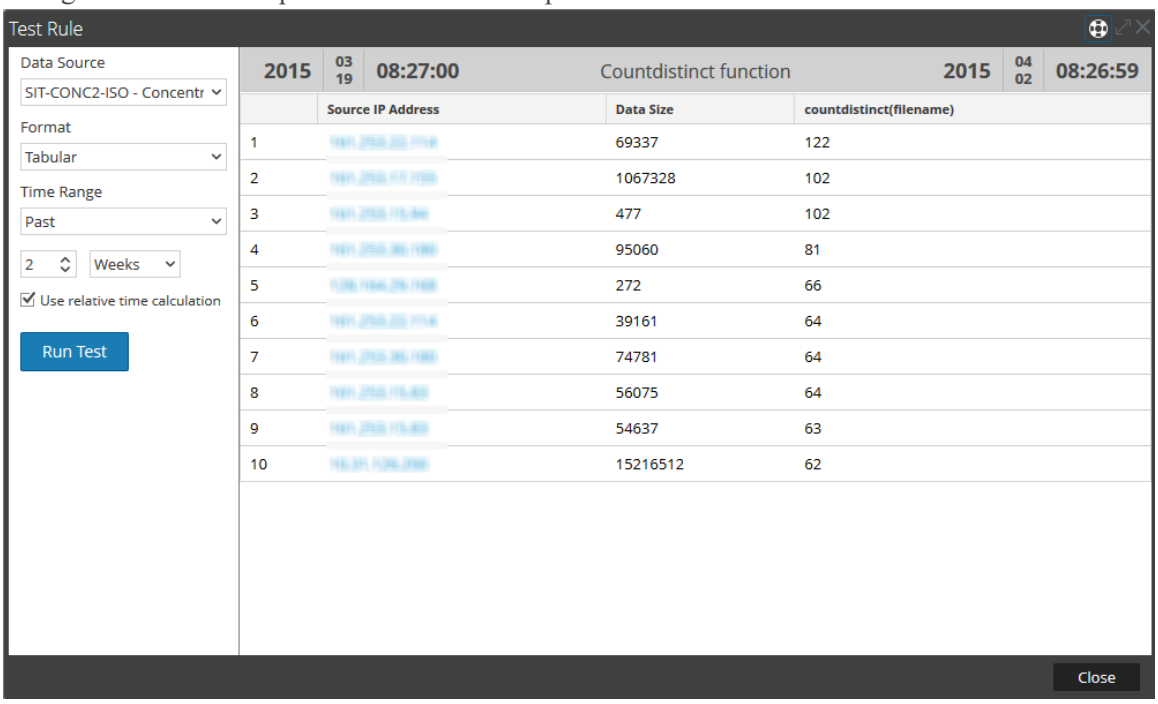
La fonction countdistinct renvoie le nombre de valeurs uniques ou Distinct pour la clé méta. En d'autres mots, la fonction countdistinct peut être utilisée pour récupérer un certain nombre de valeurs Distinct pour la clé méta spécifiée.

La figure suivante montre un exemple de requête où la fonction countdistinct est utilisée avec la source IP (ip.src) et la taille des données (size).

Exemple


Build Rule
NetWitness DB
Name
Countdistinct function
Summarize
Custom
Select
ip.src, size, countdistinct(filename)
Where
ip.src exists && filename exists
Group By
ip.src,size
Then
Enter a then clause...
Order By
Column Name
Sort By
countdistinct(filename)
Descending
Enter the column name...
Ascending
Threshold
0
Limit
10
Use
Save
Reset
Test Rule

La figure suivante indique le résultat de la requête ci-dessus.



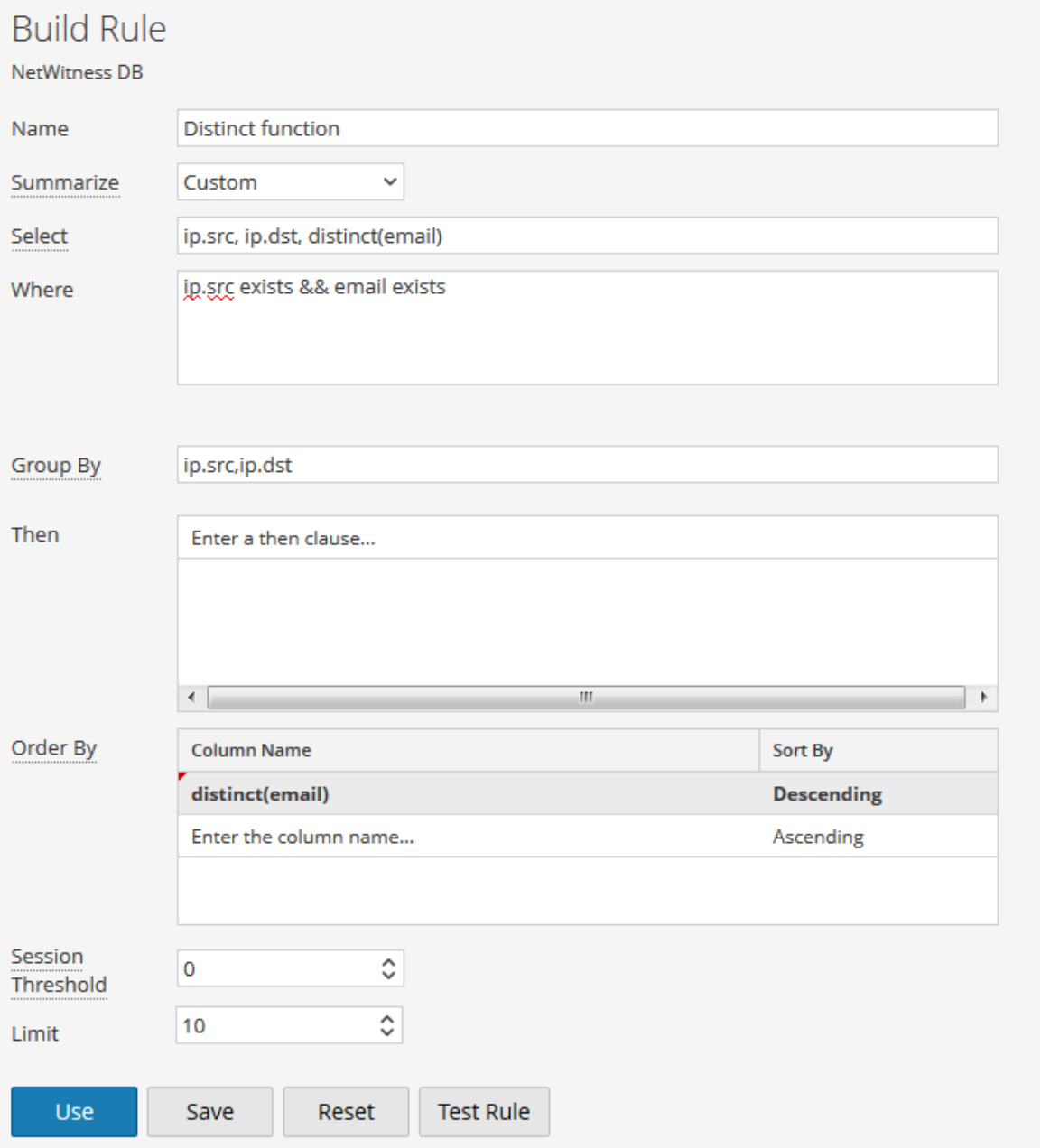
Ici, la page affiche la taille des données ainsi que le nombre total de noms de fichiers Distinct à partir de leurs sources IP respectives. À la différence de la fonction count, la fonction countdistinct exclut du résultat les valeurs dupliquées.

Distinct

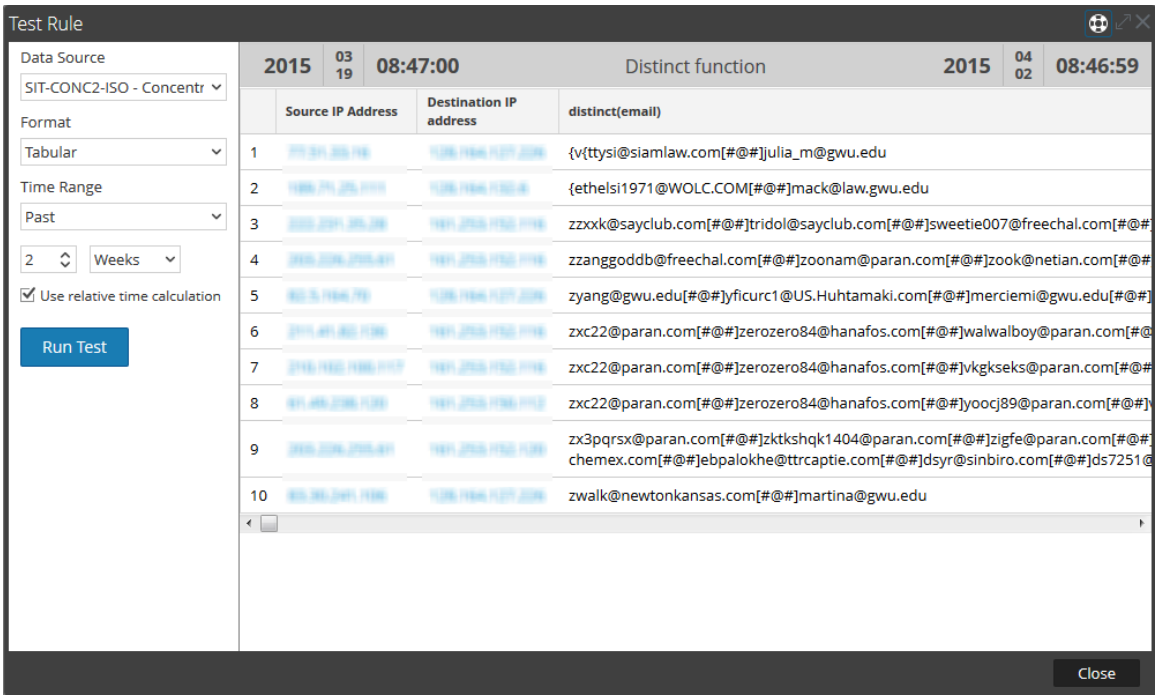
Cette fonction renvoie toutes les valeurs uniques ou Distinct de la clé méta.

Exemple

La figure suivante montre un exemple de requête pour la fonction Distinct utilisée pour récupérer les e-mails entre différentes IP source et IP de destination (ip.dst).



La figure suivante indique le résultat de la requête ci-dessus.



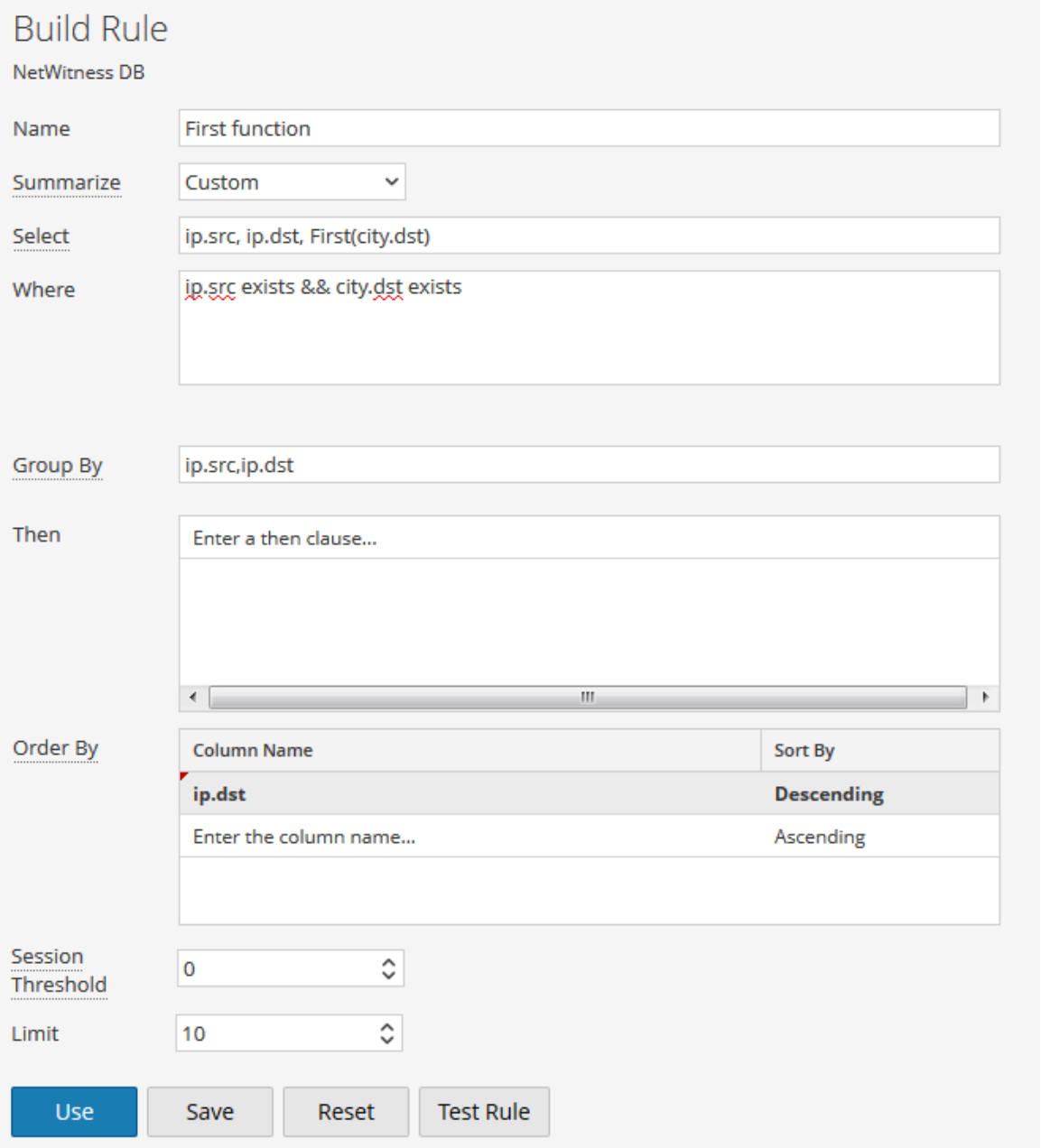
Ici, la page affiche la liste d'e-mails uniques qui ont été échangés entre les IP source et les IP de destination respectives.

Début

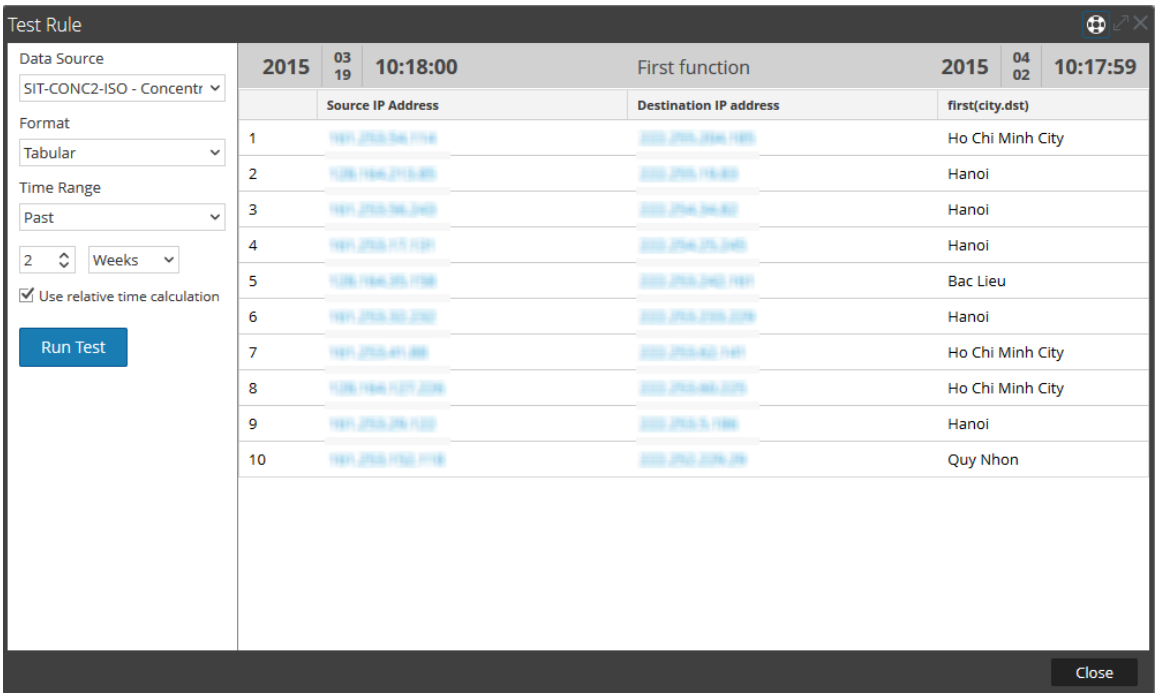
Cette fonction est utilisée pour récupérer la première valeur à partir d'une séquence ordonnée de valeurs pour une clé méta spécifiée.

Exemple

La figure suivante affiche un exemple de requête pour la première fonction utilisée pour récupérer le premier nom de ville de destination.



La figure suivante indique le résultat de la requête ci-dessus.



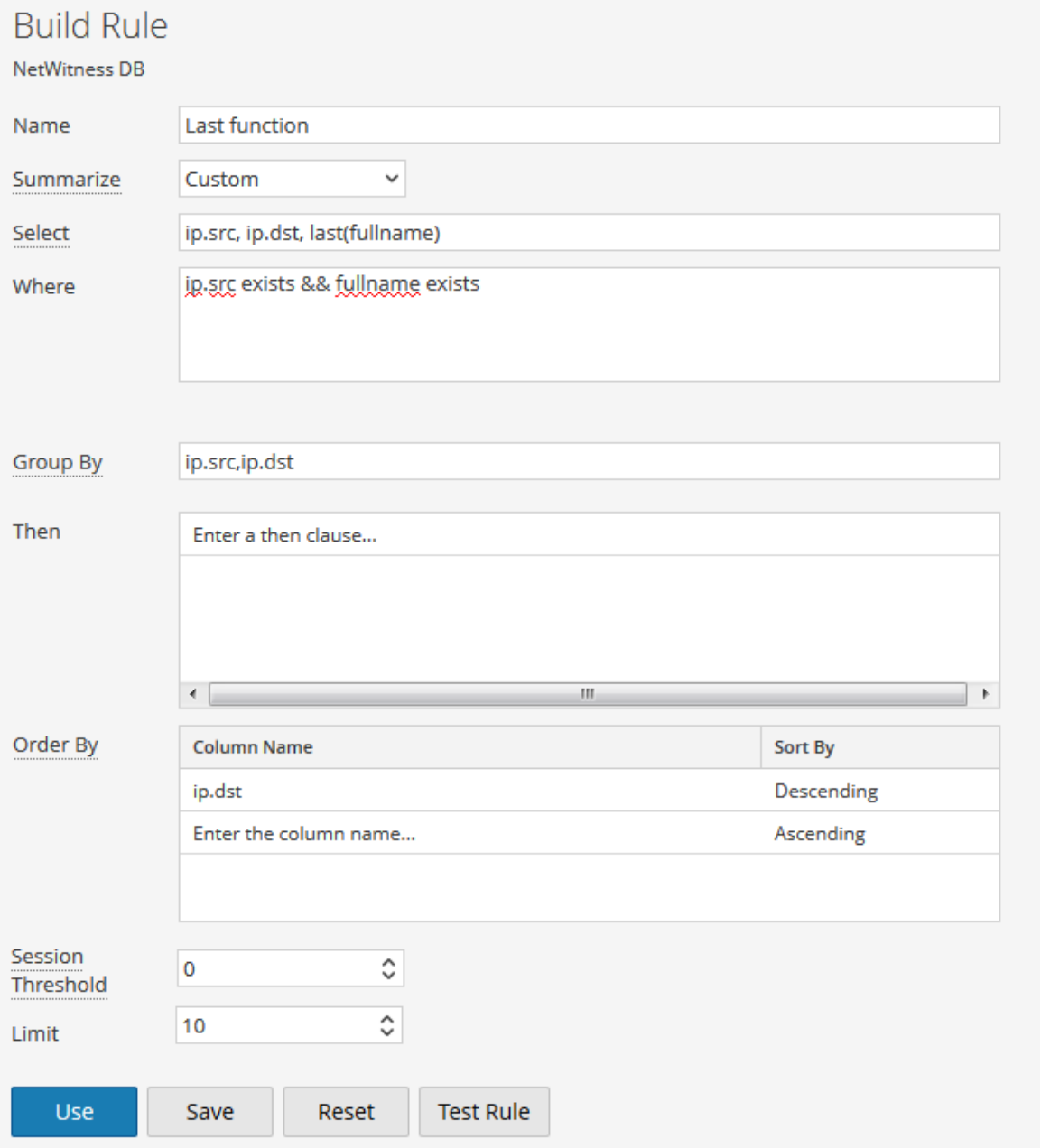
Ici, la page affiche la première ville de destination pour l'IP source et l'IP de destination correspondante. Vous pouvez utiliser la première fonction pour isoler une valeur particulière d'un résultat de la recherche.

Dernier

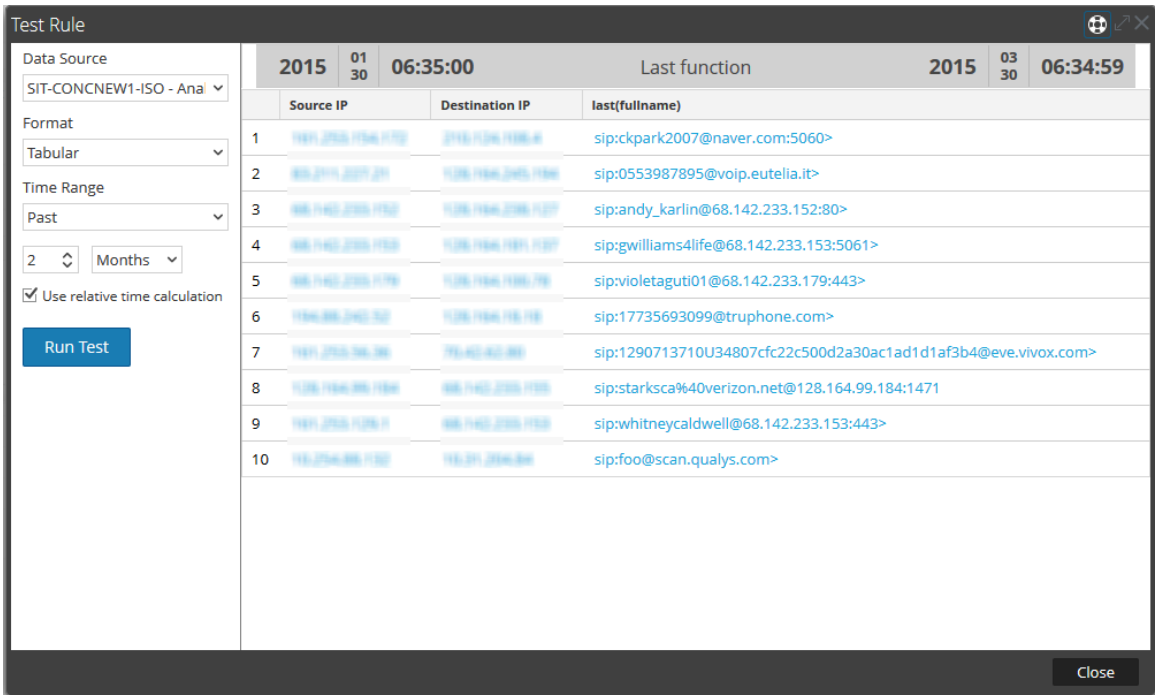
Cette fonction est utilisée pour récupérer la dernière valeur d'une séquence classée de valeurs pour une clé méta spécifique.

Exemple

La figure suivante montre un exemple de requête pour la dernière fonction utilisée pour récupérer le nom d'utilisateur le plus récent.



La figure suivante indique le résultat de la requête ci-dessus.



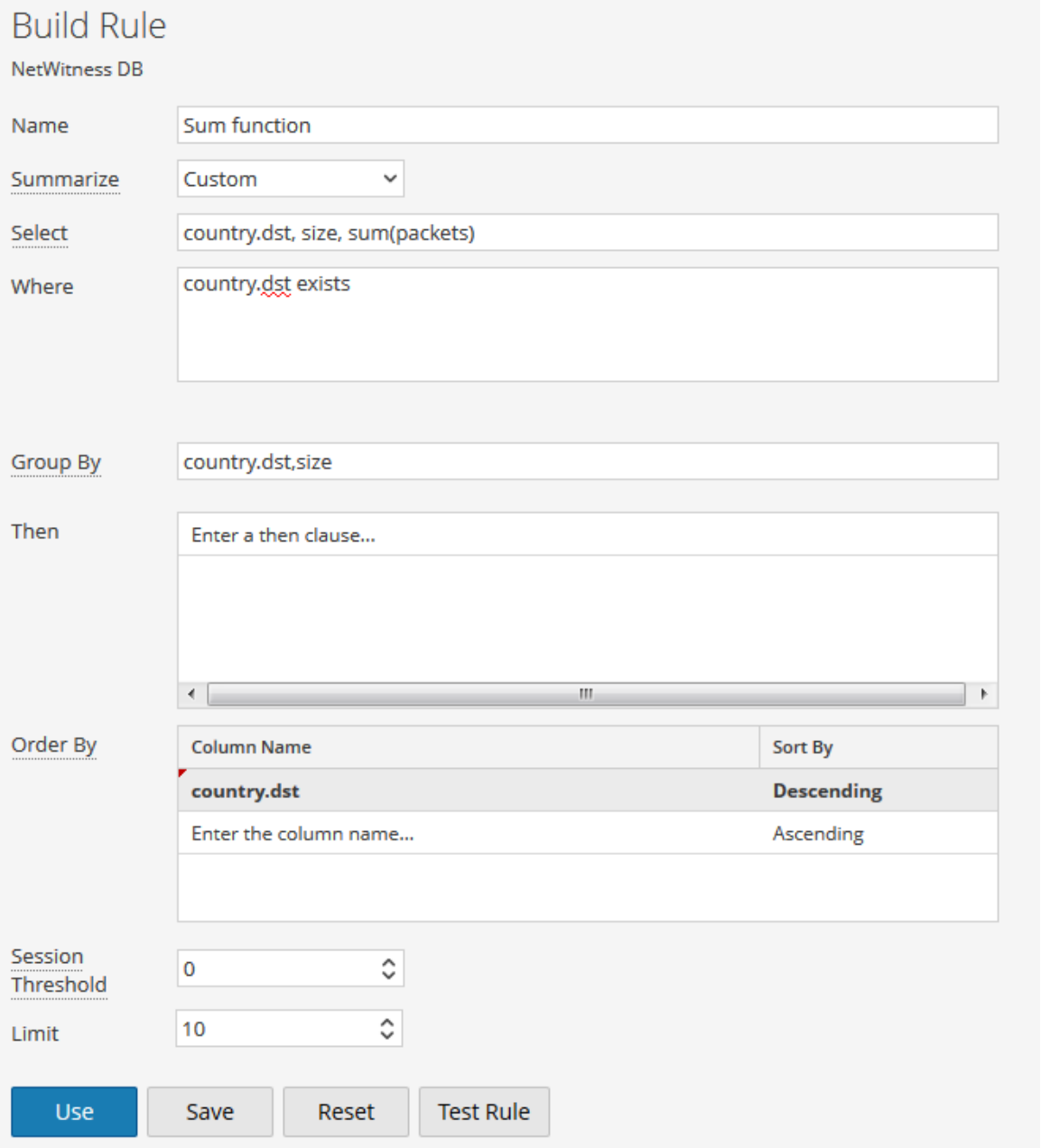
Ici, la page affiche la liste des noms d'utilisateurs les plus ou moins récents en entier, qui ont été échangés entre l'IP source et l'IP de destination.

Somme

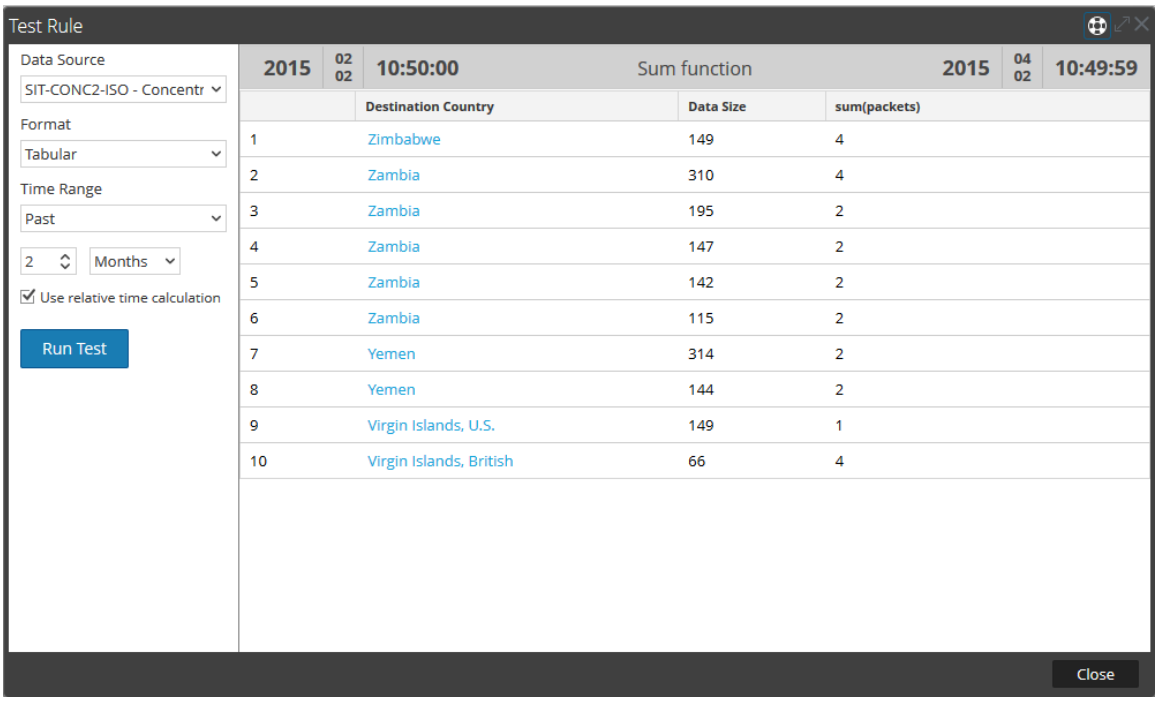
Cette fonction renvoie le total de valeurs non nulles de la clé méta au sein d'un groupe.

Exemple

La figure suivante montre la requête pour la fonction Sum utilisée pour les paquets.



La figure suivante indique le résultat de la requête ci-dessus.



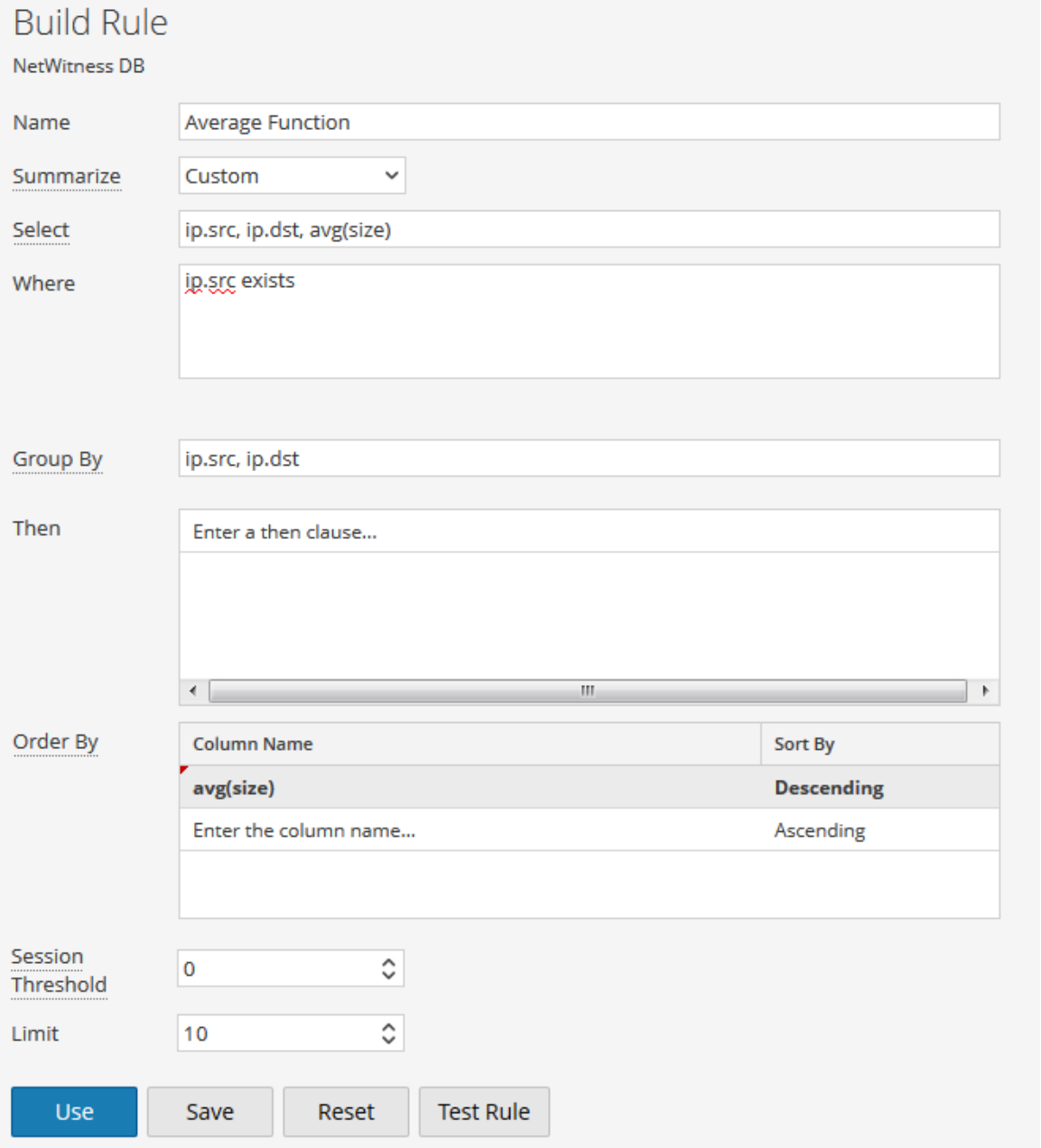
Ici la page affiche le total ou la somme des paquets ainsi que la taille des données pour leur pays de destination respectif.

Moy

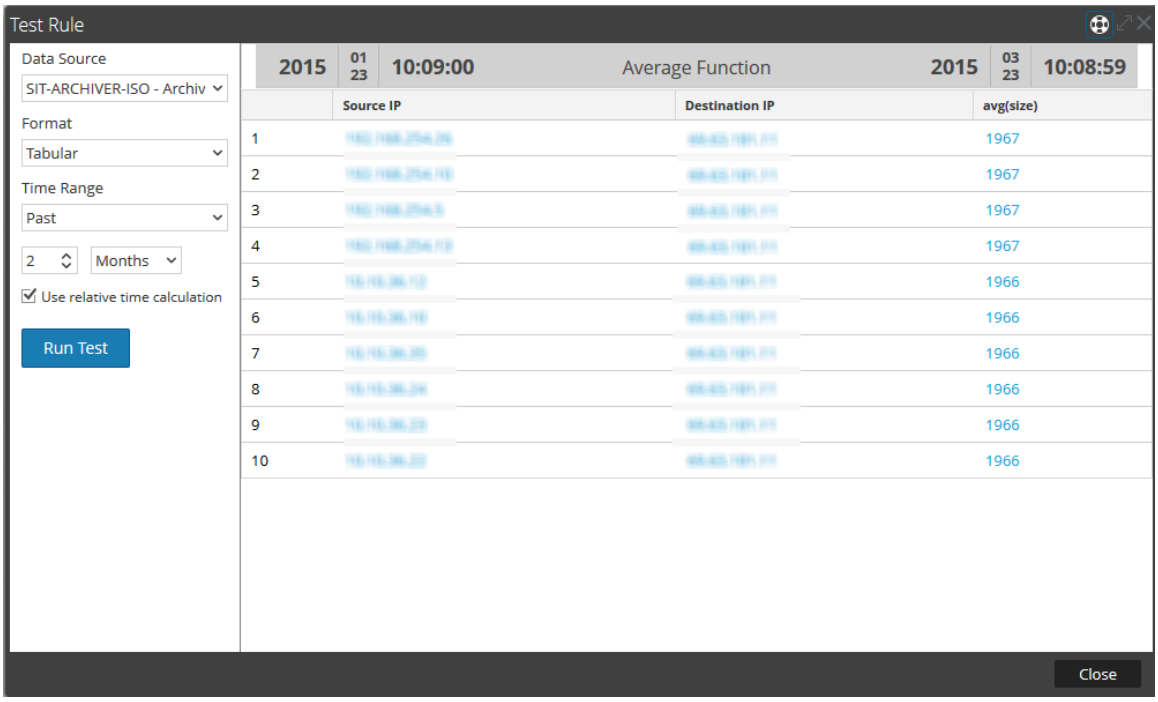
La fonction moyenne renvoie la moyenne des valeurs non nulles des méta au sein d'un groupe.

Exemple

La figure suivante montre un exemple de requête pour une taille de données moyenne transmise entre l'IP source et l'IP de destination.



La figure suivante indique le résultat de la requête ci-dessus.



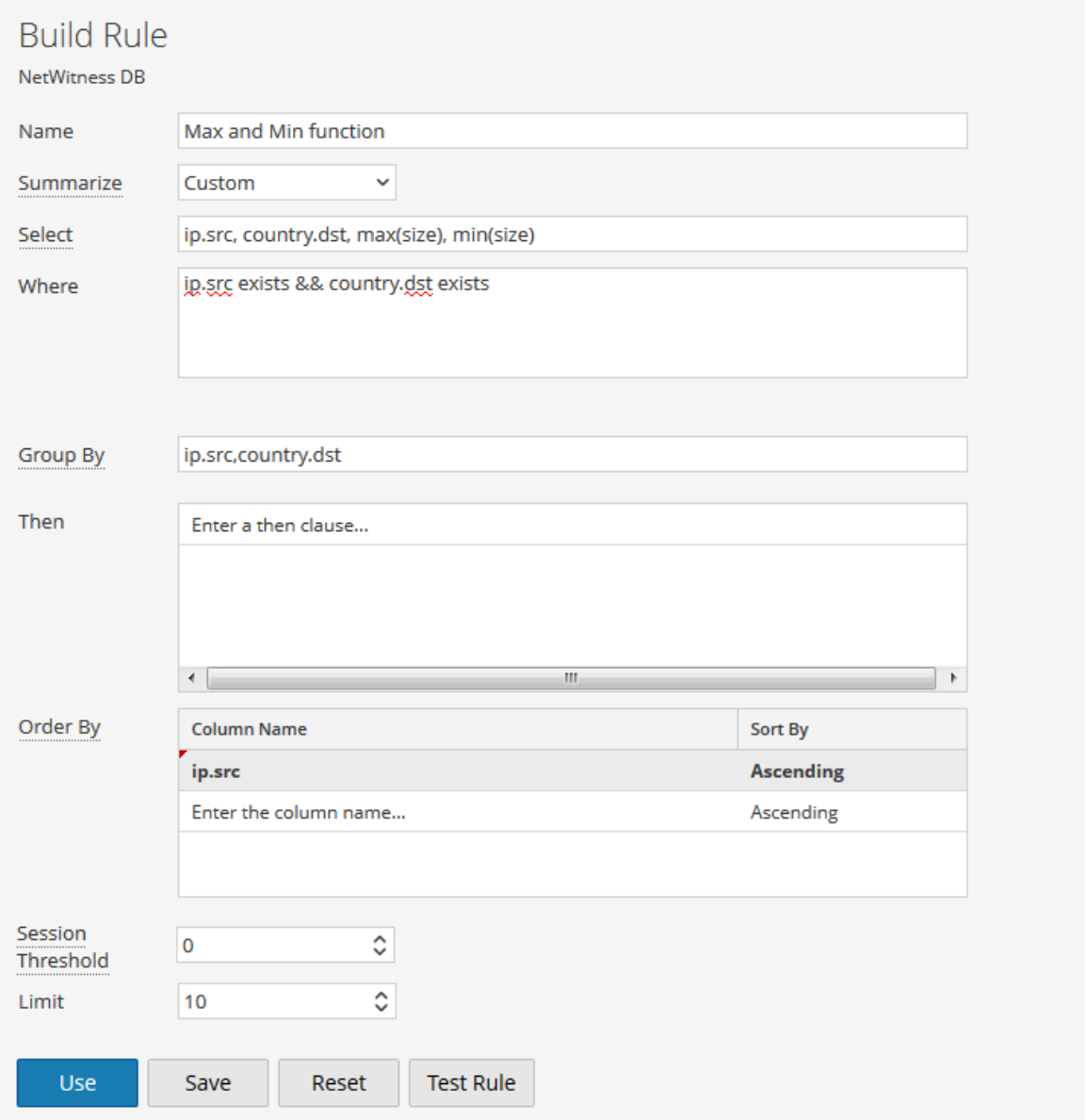
Ici, la page affiche la taille moyenne de données échangées entre l'IP source et l'IP de destination :

Max et Min

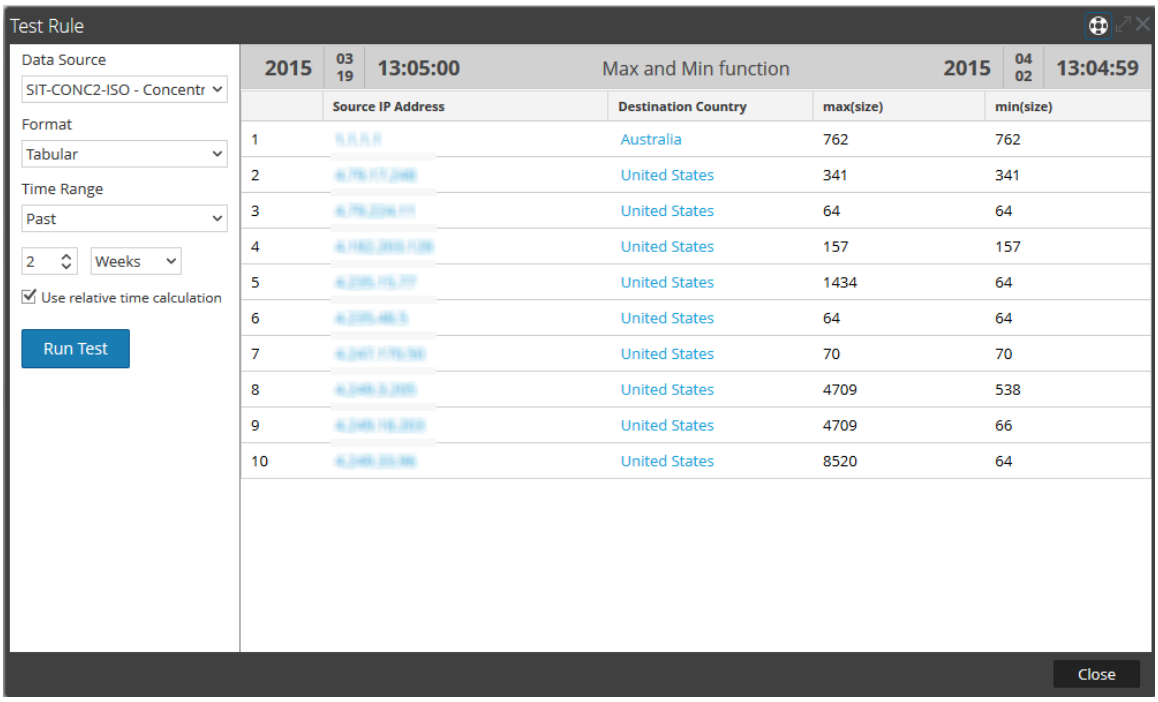
Les fonctions Max et Min donnent le maximum et le minimum pour les valeurs données d'une méta, respectivement.

La figure suivante montre un exemple de requête pour les fonctions max et min de différentes tailles de données, pour l'IP source et le pays de destination.

Exemple



La figure suivante indique le résultat de la requête ci-dessus.



Ici, la page affiche les colonnes max(size) et min(size), ainsi que la liste des IP source et des pays de destination. La colonne max(size) répertorie les tailles de données maximum alors que la colonne min(size) répertorie les tailles de données minimum qui ont été échangées.

Filtrer les résultats des méta-agrégats avec Max_threshold

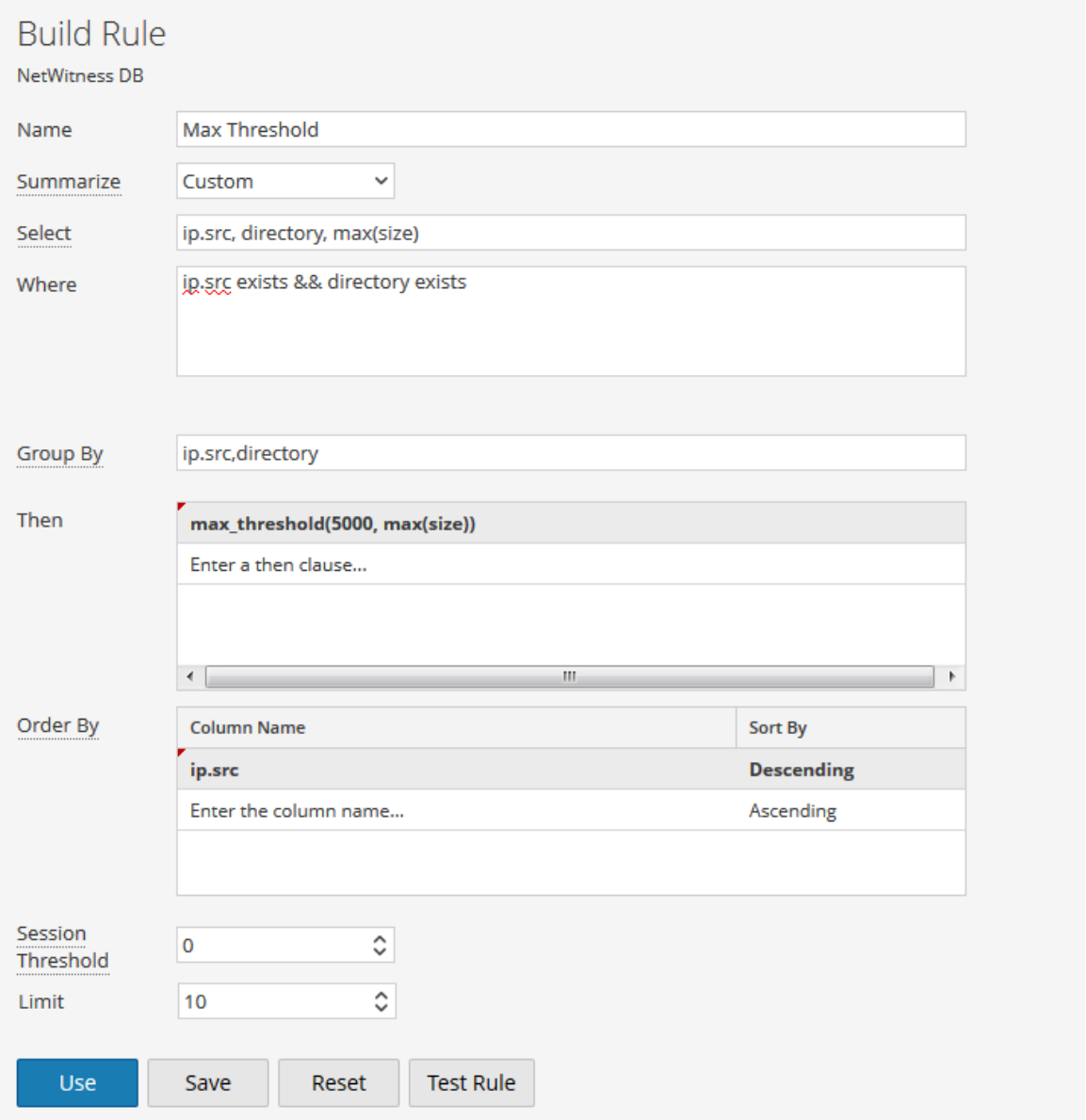
Vous pouvez filtrer encore davantage les résultats d'une fonction en utilisant l'action de règle de seuil.

Exemple

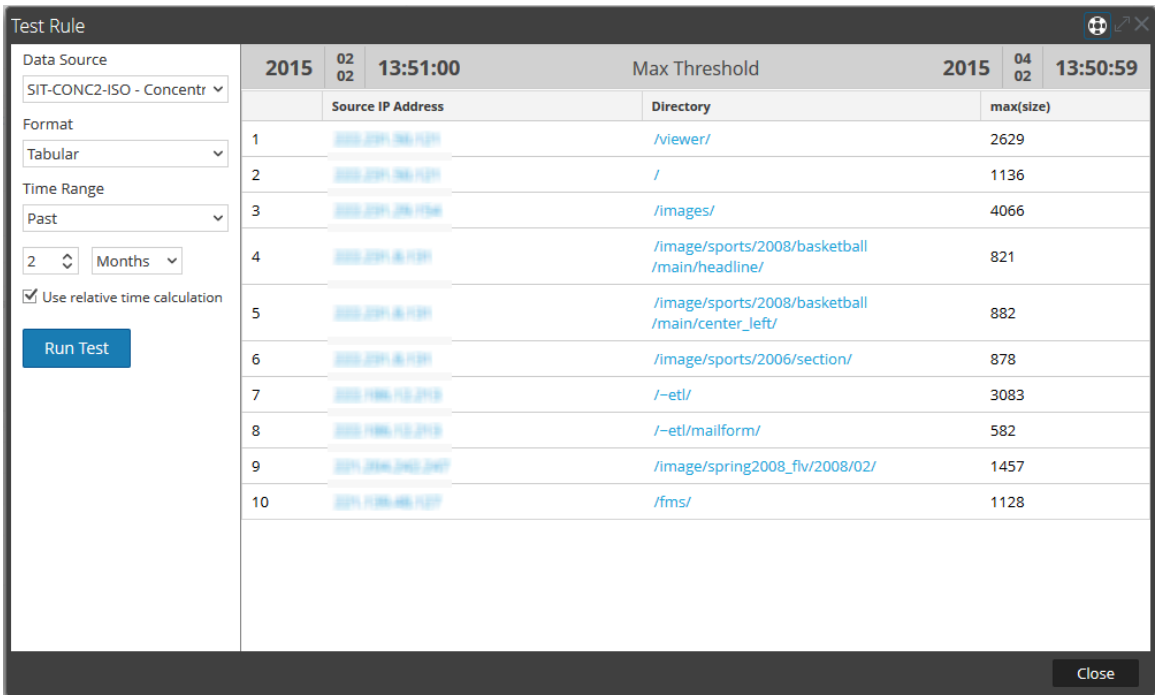
Voici un exemple de requête pour max_threshold utilisé avec la fonction Max dans le champ **Then** :

max_threshold(5000,max(size))

La figure suivante présente l'écran Élaborer une règle pour la requête ci-dessus.



Ici, max_threshold s'applique à la taille des données avec une limite supérieure de 5 000. La figure suivante indique le résultat.



Ici, la page de résultat affiche la colonne max(size), qui répertorie les tailles de données inférieures à 5 000, c'est-à-dire le seuil maximum dans la requête, ainsi que les sources IP correspondantes et leur répertoire respectif.

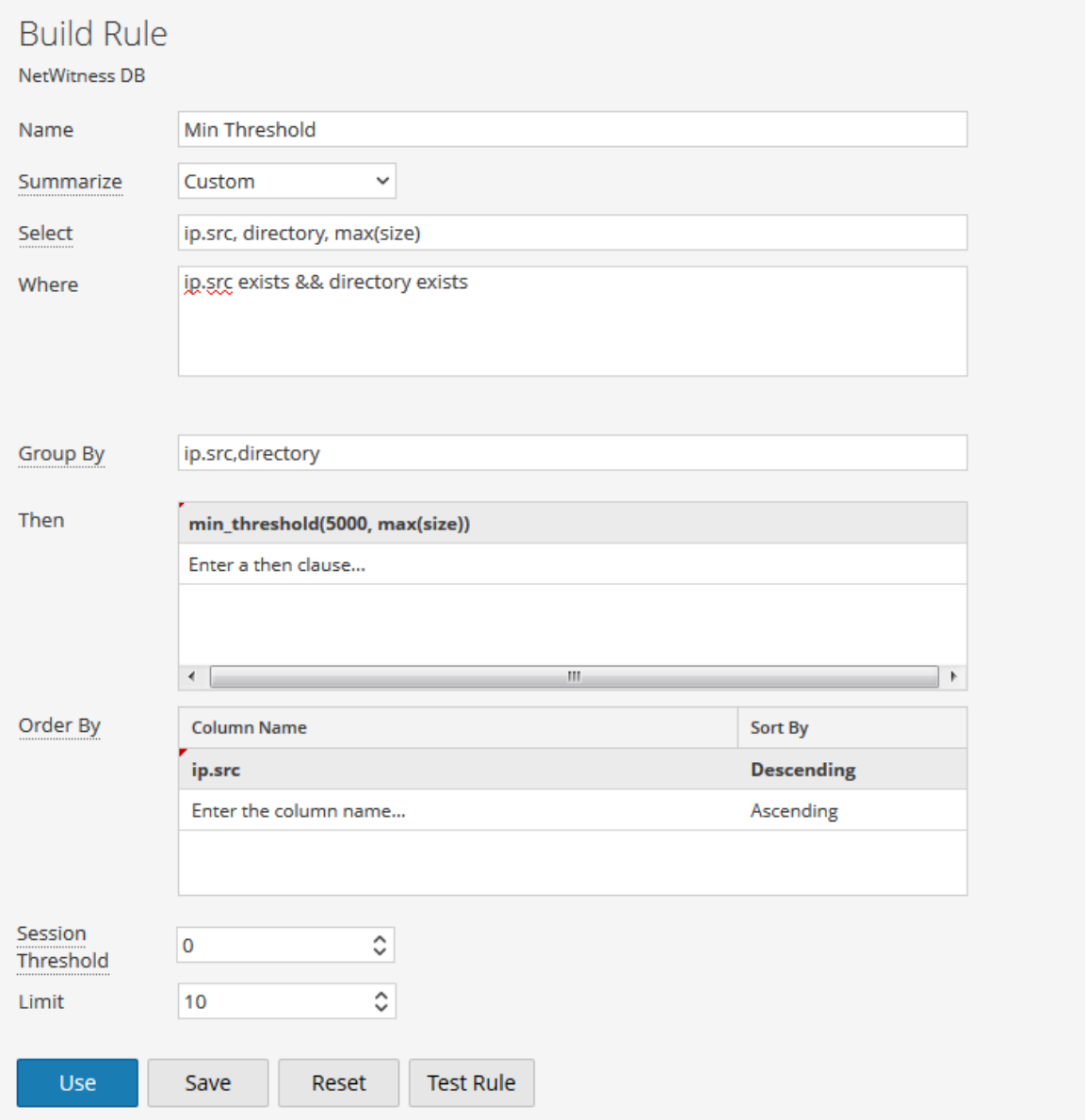
Filtrer les résultats des méta-agrégats avecMin_threshold

De la même façon, min_threshold est utilisé pour filtrer les résultats de n'importe quelle fonction. Un scénario similaire à max_threshold est utilisé pour expliquer cela.

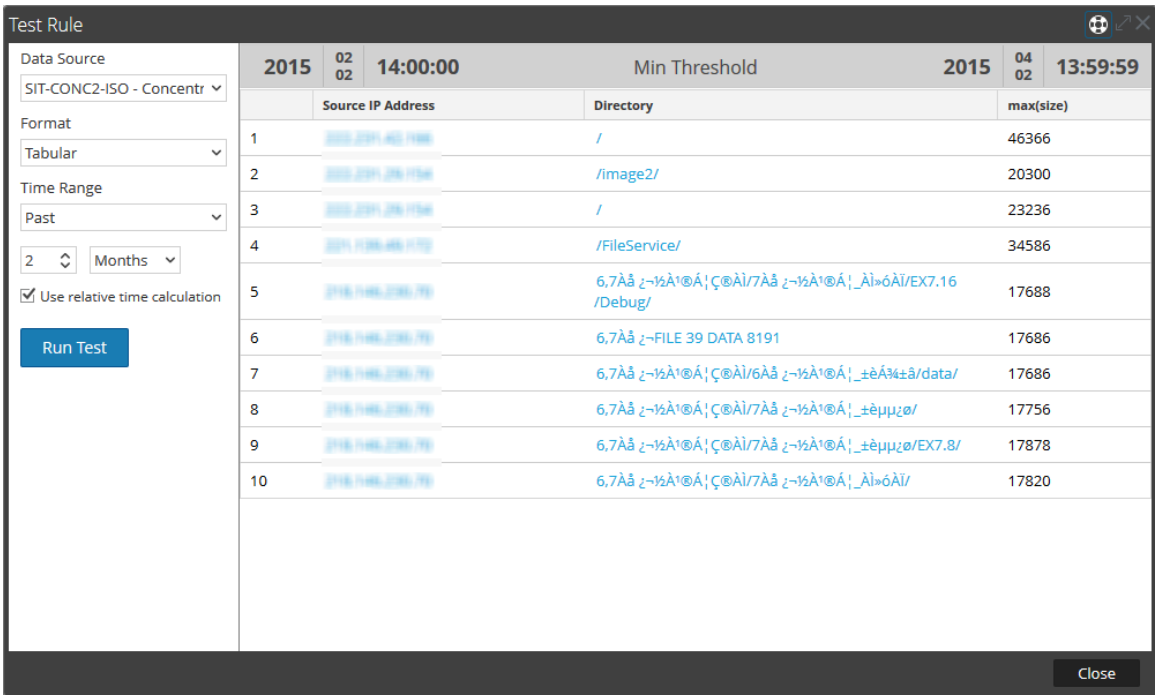
Exemple

Requête pour min_threshold utilisé avec la fonction Max dans le champ**Then** :
min_threshold(5000,max(size))

La figure suivante montre l'écran Élaborer une règle pour la requête ci-dessus.



Ici, min_threshold s'applique à la taille des données avec une limite inférieure de 5 000. La figure suivante indique le résultat.



Ici, la page de résultat affiche la colonne max(size), qui répertorie les tailles de données supérieures à 5 000, c'est-à-dire le seuil minimum dans la requête, ainsi que les sources IP correspondantes et leur répertoire respectif.

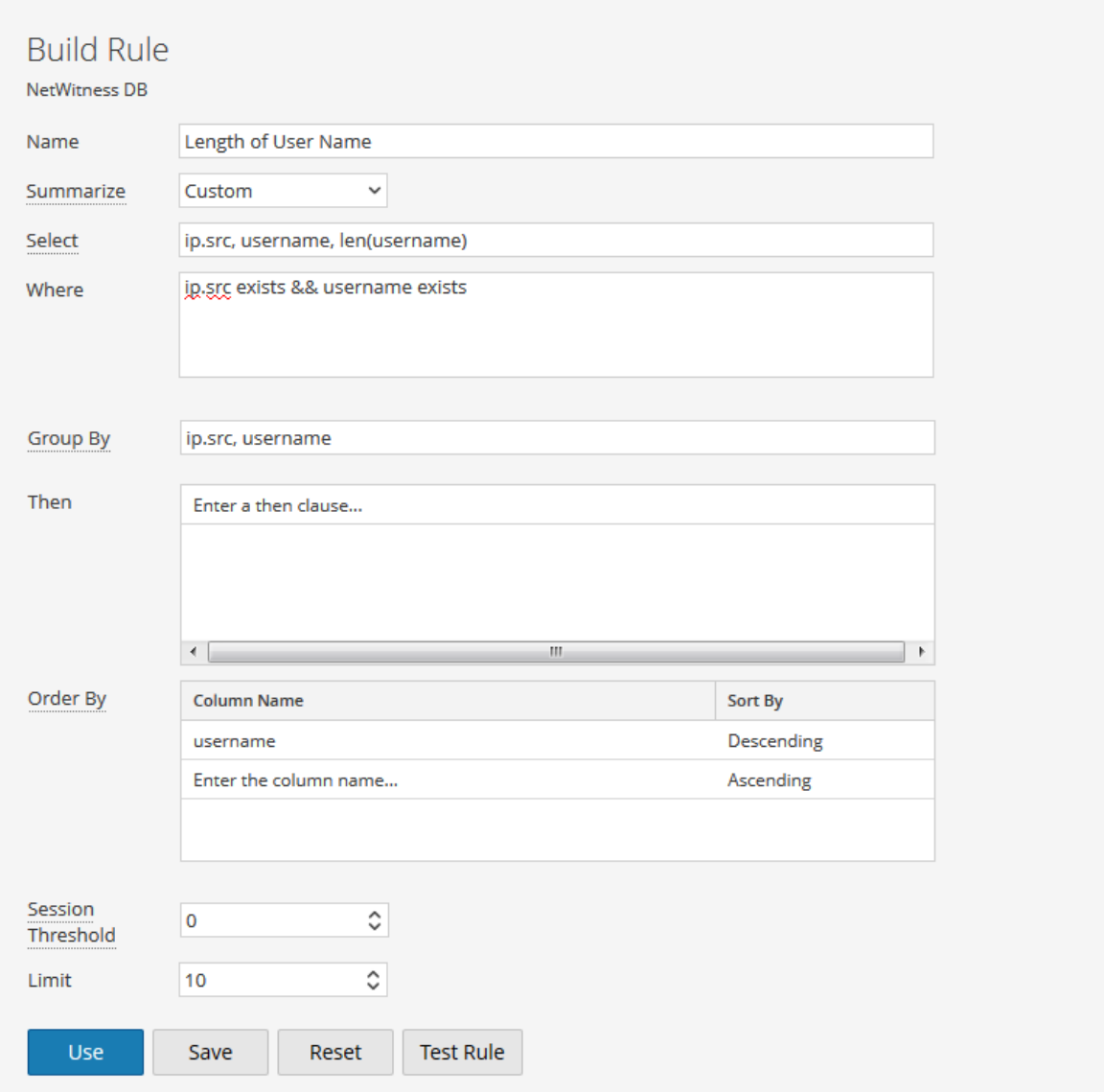
Remarque : Les actions de règles Max_threshold et Min_threshold sont communes à toutes les fonctions et peuvent être utilisées avec d'autres requêtes dans le champ **Then** pour récupérer leur résultat respectif.

Longueur

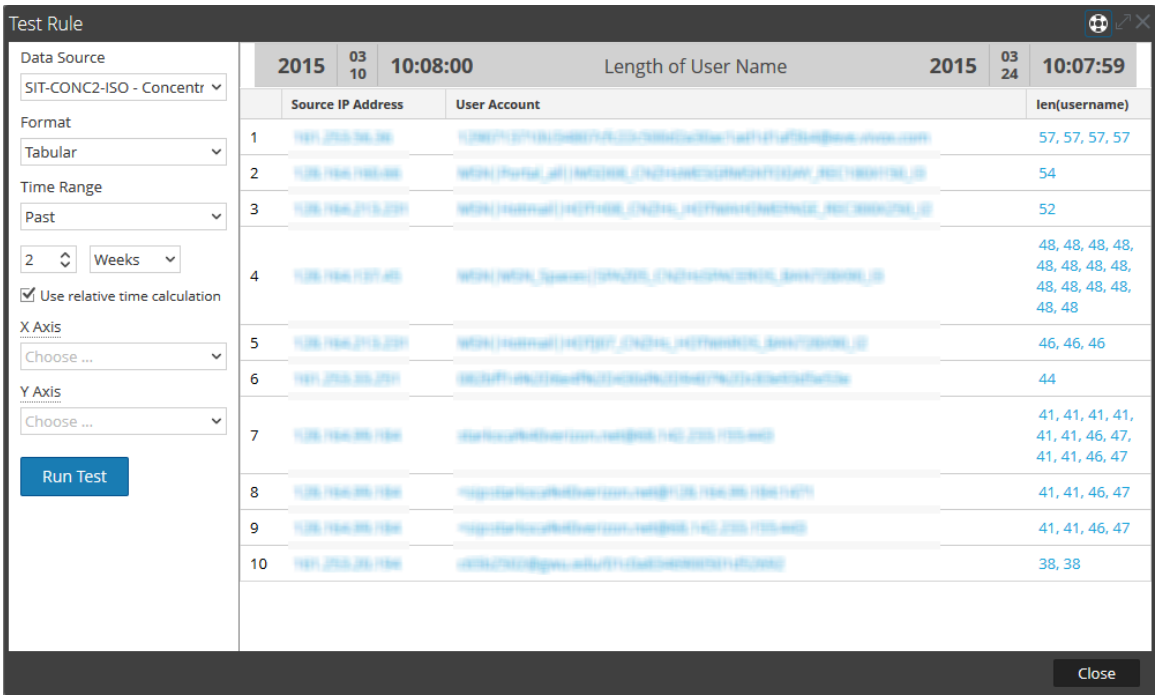
Cette fonction renvoie la longueur d'une métavaleur. En d'autres mots, la fonction Length renvoie le nombre d'octets utilisés pour stocker la valeur elle-même.
Par exemple, pour la valeur « Analytics », la longueur renvoyée est 9. De la même façon, pour IPv4 ip.src, la valeur renvoyée est 4 (ce qui représente 4 octets).

Exemple

La figure suivante montre un exemple de requête pour la fonction Length utilisée pour les noms d'utilisateur.



La figure suivante indique le résultat de la requête ci-dessus.



Ici, la page affiche la longueur des noms d'utilisateurs associés au compte utilisateur et leur IP source respective.

Informations complémentaires

Lorsque vous envoyez une requête sur des agrégats (par exemple, sum(size)) avec **Group By** sur une méta qui dispose de plusieurs valeurs dans une session, la session avec plusieurs valeurs est prise en compte dans le calcul d'agrégation pour chaque valeur de cette méta.

Exemple

Lorsque vous envoyez une requête pour la fonction d'agrégation Count avec Group By sur Alias.host, et si la colonne présente plusieurs valeurs dans une session, alors la session est comptée pour chaque occurrence, y compris les valeurs dupliquées.

Examinez le tableau suivant.

SessionID	Alias.host	Ip.src	Taille
1	host-a, host-b, host-a	a	10
2	host-b, host-c, host-a, host-c	c	20
3	host-b, host-c, host-d	b	30
4	host-c, host-a	a	40

Dans le tableau suivant, alias.host pour **host-a** et **host-c** présentent des valeurs dupliquées pour une session unique. Considérons la requête suivante :

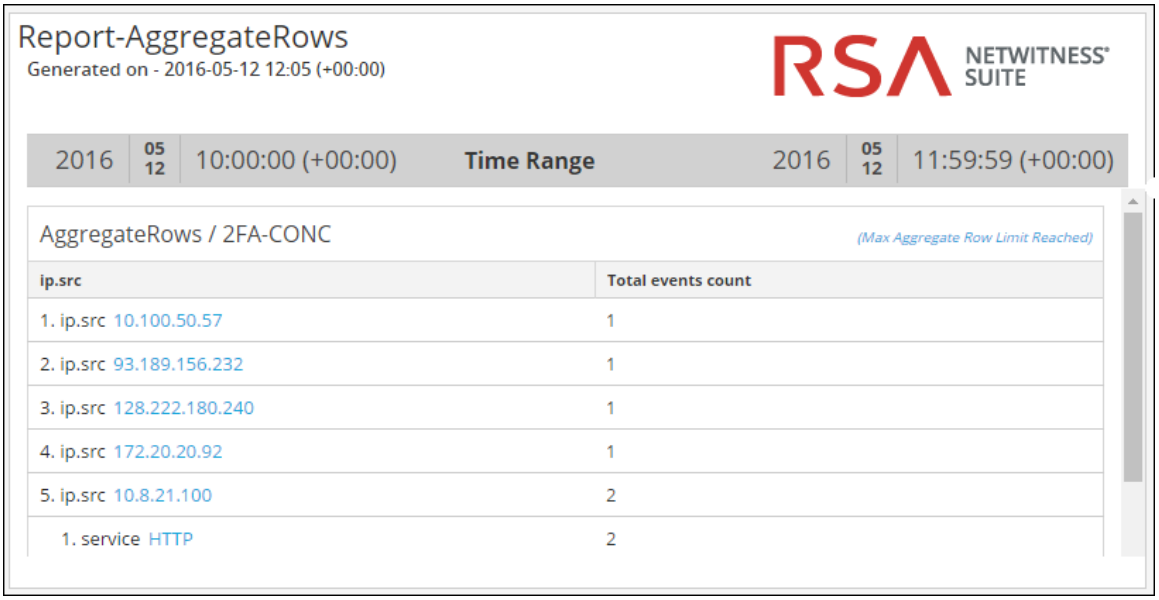
Sélectionnez : alias.host, count(ip.src), sum(size)
Grouper par : alias.host

Ici, **host-a** et **host-c** apparaissent dans 3 sessions et ils sont dupliqués dans deux sessions différentes. Toutefois, le résultat est le suivant.

Alias.host	count(Ip.src)	Sum (size)
host-a	4	80
host-b	3	60
host-c	4	110
host-d	1	30

Le tableau de résultat montre que le nombre de **host-a** et **host-c** est 4. C'est parce que pour chaque valeur alias.host, l'intégralité de la session est prise en compte. De la même façon, pour calculer sum (size), les mêmes sessions sont prises en compte pour chaque valeur alias.host.

Dans le résultat du rapport si le nombre de lignes atteint le **Nbre maximal de lignes agrégées NWDB** défini dans la configuration RE, alors un message **Limite maximale de lignes agrégées atteinte** s'affiche pour indiquer qu'il existe plus d'informations à afficher. La limite par défaut est 1 000 et vous pouvez modifier cette valeur selon vos besoins, dans la page Configuration de Reporting Engine.



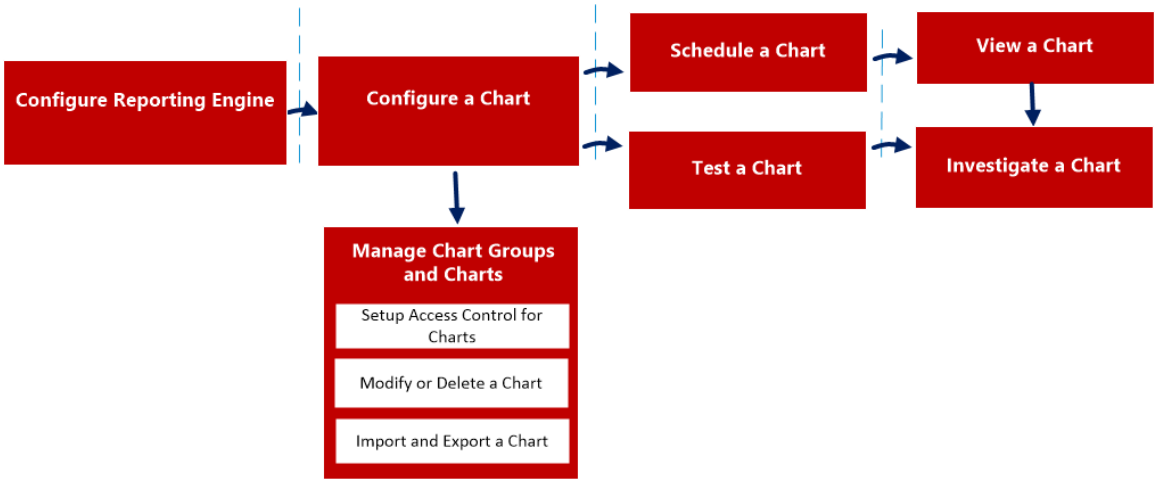
Configurer et générer un graphique

Un graphique est une visualisation graphique de données. Vous pouvez afficher différents types de graphiques, y compris plusieurs types de graphiques avec des courbes, lignes, barres et zones.

Toute règle NWDB présente dans le système Reporting Engine qui n'est pas triée par Aucun peut être utilisée pour créer instantanément un graphique. Pour plus d'informations sur « Comment créer une règle NWDB », reportez-vous à la rubrique Configurer une règle.

Le début du graphique peut être ajusté dans le panneau même de définition de graphique. Chaque fois qu'un graphique est exécuté, il stocke ses résultats de données localement dans le Reporting Engine afin d'être consulté dans la vue Tableau de bord ou Graphique sans impact sur les performances.

Voici une vue d'ensemble de tout le processus de configuration et de génération d'un graphique.



Pour configurer et générer un graphique, procédez comme suit :

1. Configurer le Reporting Engine
2. Configurer une règle NWDB
3. Configurer un graphique
4. Planifier un graphique
5. Afficher un graphique
6. Tester un graphique
7. Analyser un graphique
8. Gérer un groupe de graphiques et un graphique

Configurez Reporting Engine

Vous devez configurer le Reporting Engine avant de pouvoir configurer et générer un rapport. Vous devez également spécifier la source de données dans le Reporting Engine à partir de laquelle les données sont extraites. Pour plus d'informations sur la configuration d'un Reporting Engine, reportez-vous à la rubrique **Configurer le Reporting Engine** dans le *Guide de configuration de Reporting Engine*.

Configurer une règle NWDB

La règle NetWitness qui n'est pas triée par Aucun est utilisée pour créer un graphique. La base de données NetWitness extrait les métadonnées du Reporting Engine et fournit les métadonnées pour les règles. Ces règles sont un bloc de construction essentiel pour gérer un graphique.

Remarque : Si la règle contient les actions de règle lookup_and_add, sum_count ou sum_values, le graphique associé ne contiendra pas de données.

Configurer un graphique

Vous pouvez configurer un graphique à l'aide des règles NWDB.

Planifier un graphique

Lorsqu'un graphique est défini avec les composants requis, vous pouvez configurer ses propriétés d'exécution en planifiant un graphique. Ici, vous pouvez rapidement afficher, ajouter et modifier les détails du planning pour un graphique.

Afficher un graphique

Vous pouvez afficher les graphiques planifiés dans la vue Graphique.

Tester un graphique

Vous pouvez exécuter le test sur un graphique et afficher tous les détails du graphique en fonction de la période sélectionnée.

Contrôle d'accès pour un graphique

Le module Reporting fournit un contrôle d'accès au niveau du graphique. Seul l'utilisateur disposant de l'ensemble des autorisations approprié peut effectuer les tâches du module Reporting. Le contrôle d'accès est géré par l'administrateur à partir de l'onglet **Administration > Sécurité > Rôles**.

Lorsque vous créez des utilisateurs et des rôles d'utilisateur, assurez-vous que les rôles que vous créez pour des tâches spécifiques ont accès à toutes les autorisations nécessaires. Cela peut nécessiter des autorisations à plusieurs niveaux de la hiérarchie des rôles.

Les graphiques peuvent être liés à un ensemble spécifique de rôles d'utilisateur. Ainsi, lorsqu'un utilisateur se connecte à NetWitness, il peut afficher les graphiques associés aux privilèges d'accès du rôle d'utilisateur spécifique. Les utilisateurs dont le rôle d'utilisateur dispose de l'accès en « Lecture et écriture » peuvent définir des graphiques. En outre, l'accès aux graphiques peut être restreint aux seuls utilisateurs disposant de l'accès en « Lecture seule ».

Au niveau du graphique, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness :

- Lecture et écriture
- Lecture seule
- Aucun accès

Pour modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez la définir au niveau du graphique. Par exemple, pour que les **Administrateurs** aient accès à un graphique spécifique, vous pourriez alors définir l'autorisation « Lecture et écriture » dans la boîte de dialogue Autorisations des graphiques.

Vous pouvez appliquer l'autorisation en lecture seule aux règles des graphiques en cochant la case.

Deux scénarios qui décrivent comment définir un contrôle d'accès sont présentés ici :

- Scénario 1 : Autorisations appliquées au groupe de graphiques, au sous-groupe, au graphique et aux règles en fonction du rôle d'utilisateur.
- Scénario 2 : Autorisation de lecture seule appliquée aux règles du graphique.

	Rôle (Analyste)	Autorisations appliquées au groupe de graphiques, au sous-groupe, au graphique et aux règles en fonction du rôle d'utilisateur	Autorisations (lecture seule) appliquées aux règles du graphique.
Graphique	Lecture et écriture	Lecture et écriture	Lecture et écriture
Sous-groupe	Lecture	Lecture	Lecture et écriture
Graphique	Lecture	Lecture	Lecture et écriture
Règles	Lecture	Lecture	Lecture

Il sera attribué au graphique le rôle d'**Analyste de sécurité** et les autorisations sont définies en « Lecture et écriture » des graphiques.

Pour le scénario 1, chacun des niveaux a un ensemble d'autorisations en fonction du rôle d'utilisateur. Pour le scénario 2, l'autorisation de lecture est définie pour les règles, sauf que l'autorisation pour les règles ne peut pas être supérieure à l'autorisation définie pour les graphiques.

Remarque : Si l'autorisation des règles est supérieure à l'autorisation du graphique, l'autorisation n'est pas appliquée. Par exemple, si vous définissez les autorisations pour le Groupe de rapports sur **Aucun accès**, et que vous spécifiez l'option *Appliquer l'autorisation de lecture seule aux règles des rapports*, l'autorisation de lecture seule n'est pas définie pour les règles.

Contrôle d'accès pour un graphique lorsque plusieurs graphiques sont sélectionnés

Pour modifier les autorisations de plusieurs graphiques, vous devez sélectionner plusieurs graphiques simultanément et paramétrer leurs autorisations d'accès dans le panneau Autorisations des graphiques. L'autorisation d'accès que vous choisissez s'applique à tous les graphiques sélectionnés.

Contrôle d'accès à un graphique lorsque plusieurs graphiques dotés de plusieurs règles sont sélectionnés

Pour modifier les autorisations pour un rôle d'utilisateur spécifique lorsque plusieurs graphiques dotés de plusieurs règles sont sélectionnés, cochez la case dans le panneau Autorisations des graphiques.

Si l'autorisation attribuée aux règles est inférieure à l'autorisation des graphiques, l'autorisation d'accès en lecture seule s'applique à toutes les règles des graphiques sélectionnés.

Remarque : Si un utilisateur (autre que le superutilisateur) crée un graphique, le superutilisateur ne pourra pas accéder à ce rapport.

Contrôle d'accès pour un groupe de graphiques

Pour modifier les autorisations du groupe de graphiques, sélectionnez un groupe de graphiques et définissez ses autorisations d'accès à l'aide du panneau Autorisations des graphiques. Avant d'appliquer les autorisations des groupes de graphiques, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « Aucun accès ».

Pour modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, définissez l'autorisation au niveau du groupe de graphiques. Par exemple, pour que les administrateurs aient accès à tous les graphiques d'un groupe de graphiques, définissez l'autorisation « Lecture et écriture » dans le panneau Autorisations sur les groupes de graphiques.

Vous pouvez également appliquer des autorisations à des sous-groupes et graphiques dans le groupe, et appliquer des autorisations en lecture seule aux règles dans les graphiques en cochant les cases appropriées.

Trois scénarios qui décrivent comment définir un contrôle d'accès sont présentés ici :

- Scénario 1 : Autorisations appliquées aux groupes de graphiques, aux sous-groupes et aux graphiques en fonction des rôles d'utilisateur.
- Scénario 2 : Autorisations appliquées aux sous-groupes et aux graphiques dans le groupe
- Scénario 3 : Autorisation de lecture seule appliquée aux règles du graphique.

	Rôle (Analyste)	Autorisations appliquées aux groupes de graphiques, aux sous-groupes et aux graphiques en fonction des rôles d'utilisateur	Autorisations appliquées aux sous-groupe et aux graphiques dans le groupe	Autorisations (lecture seule) appliquées aux règles du graphique.
Graphique	Lecture et écriture	Lecture et écriture	Lecture et écriture	Lecture et écriture
Sous-groupes	Lecture	Lecture	Lecture et écriture - Héritée	Lecture et écriture
Graphique	Lecture	Lecture	Lecture et écriture - Héritée	Lecture et écriture
Règles	Lecture	Lecture	Lecture	**Lecture**

Il sera attribué au groupe de graphiques le rôle d'**Analyste de sécurité** et les autorisations sont définies en « Lecture et écriture ».

Pour le scénario 1, chacun des niveaux aura un ensemble d'autorisations en fonction du rôle d'utilisateur.

Pour le scénario 2, l'autorisation au niveau du groupe de graphiques est héritée par le sous-groupe et les graphiques dans le groupe.

Pour le scénario 3, l'autorisation de lecture est définie pour les règles. Toutefois, l'autorisation définie pour les règles ne peut pas être supérieure aux autorisations définies pour le groupe de graphiques.

Le tableau suivant répertorie les colonnes du panneau Autorisations des graphiques :

Colonne	Description
Rôles	Le rôle de l'utilisateur connecté dans l'interface utilisateur de NetWitness.
Lecture et écriture	L'utilisateur peut accéder, afficher, modifier, importer, exporter et supprimer le graphique dans la vue Graphiques. L'utilisateur peut également modifier l'autorisation d'accès au graphique.
Lecture seule	L'utilisateur peut uniquement accéder au graphique et l'afficher dans la vue Graphiques.
Aucun accès	L'utilisateur ne peut pas accéder au graphique pour lequel cette autorisation est définie, ou l'afficher.
☐Appliquer ces autorisations aux sous-groupes et aux graphiques dans ce groupe	Cochez cette case pour appliquer les autorisations sélectionnées au groupe de graphiques, aux sous-groupes dans le groupe et aux graphiques dans le groupe. **Remarque :** Cette case à cocher n'apparaît que lorsque vous définissez les autorisations d'accès pour un groupe de graphiques.
☐Appliquer une autorisation de lecture seule aux règles des graphiques	Cochez la case pour appliquer automatiquement les autorisations aux règles des graphiques.

Configurer un graphique

Après avoir défini un graphique avec les règles NetWitness ayant NWDB comme source de données, vous pouvez configurer ses propriétés d'exécution.

Créer un groupe de graphiques

Pour ajouter des groupes au dossier par défaut ou des sous-groupes sous un groupe de graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, cliquez sur +.
   Un groupe par défaut est ajouté dans le panneau Groupes de graphiques.
4. Saisissez le nom du nouveau groupe.
5. Appuyez sur **Entrée**.
   Le groupe est ajouté au panneau Groupes de graphiques.

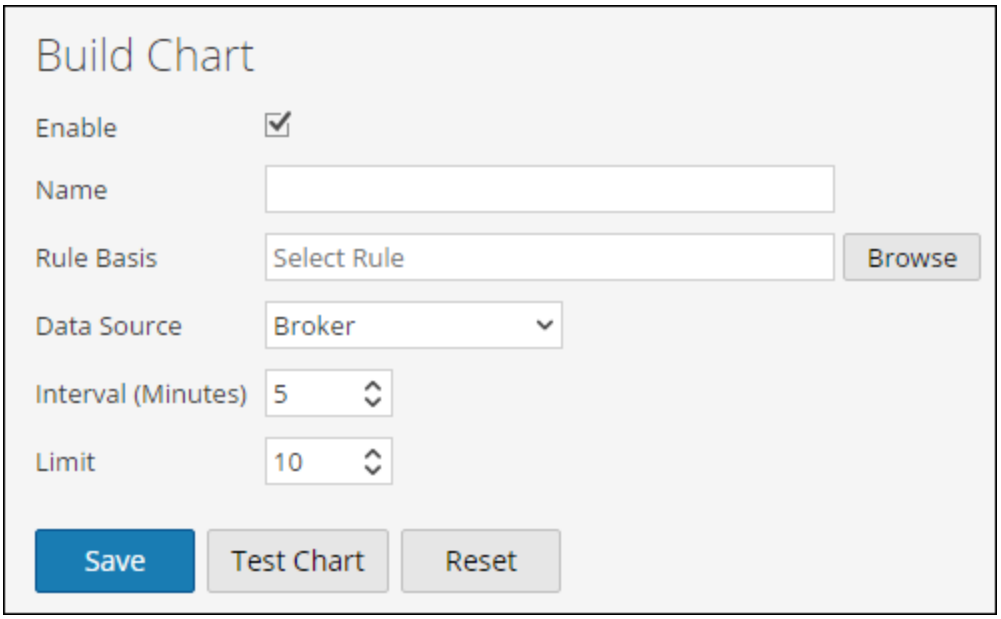
Créer un graphique

Pour ajouter des graphiques à un groupe ou un sous-groupe :

1. Accédez à **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques** pour afficher la vue Graphique.

3. Dans la barre d'outils **Graphique**, cliquez sur +.

   L'onglet Élaborer le graphique s'affiche.



4. Saisissez le nom du graphique.
5. Pour que le Reporting Engine puisse collecter les données et générer des résultats sous la forme d'un graphique, cochez la case **Activer**.
6. Dans le champ Base de règle, procédez comme suit :
   a. Cliquez sur **Parcourir**. La boîte de dialogue Ajouter une règle s'affiche.
   b. Accédez à l'arborescence Règle et sélectionnez une règle.
   c. Cliquez sur **Sélectionner**.
7. La règle s'affiche dans le champ Base de règle.
8. Sélectionnez la source de données dans la liste déroulante **Source de données**.

   Remarque : Si la source de données par défaut est configurée dans le Reporting Engine, la source de données s'affiche par défaut sur la page Élaborer le graphique. Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations Lecture définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubrique **Configurer les autorisations d'accès aux sources de données** dans le *Guide de configuration de l'hôte et des services*.

9. (Facultatif) Pour modifier la valeur Intervalle, cliquez sur la flèche vers le haut ou vers le bas.

   La valeur Intervalle correspond à l'intervalle d'exécution (en minutes) de la règle formant la

base du graphique en vue de collecter des données.

10. Sélectionnez la valeur **Limiter** pour limiter le nombre d'enregistrements à afficher.
11. **Axe X** et **Axe Y** permettent de spécifier les métas à tracer dans les tableaux.
    Dans **Axe X**, le méta de la règle « Regrouper par » s'affiche. Dans **Axe Y**, les fonctions agrégées utilisées dans la règle s'affichent.

    Remarque : Sommes, Nombre, Countdistinct et Moyenne sont les fonctions agrégées prises en charge pour le graphique. Par défaut, pour les règles personnalisées avec plusieurs « Regrouper par », vous pouvez sélectionner uniquement les premiers métas dans **Axe X**.

12. Cliquez sur **Enregistrer**.
    Un message de confirmation de l'enregistrement du graphique s'affiche.

Planifier un graphique

Vous devez planifier un graphique pour effectuer une enquête plus approfondie sur les détails du graphique.

En activant un graphique, ce dernier s'exécute conformément à la planification et fournit les informations configurées avec l'état du graphique changé en Planifié.

Pour planifier un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un ou plusieurs graphiques affichant dans la colonne **Activé**.
4. Cliquez sur .
   Un message de confirmation indique que l'état des graphiques a changé.

Afficher un graphique

Après avoir affiché un graphique, vous pouvez effectuer les opérations suivantes :

1. Vous pouvez imprimer, enregistrer, envoyer par e-mail et afficher des graphiques en mode plein écran.
2. Vous pouvez aussi sélectionner une date du calendrier pour afficher la liste des rapports correctement exécutés à la date choisie.

Pour afficher un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, exécutez l'une des opérations suivantes :
   - Sélectionnez un graphique, puis cliquez sur  > **Afficher**.
   - Sélectionnez un graphique et cliquez sur **Afficher**dans la colonne Afficher le graphique.
     L'onglet de la vue Afficher le graphique s'affiche.
4. Dans le champ **Options du graphique**, procédez comme suit :
   a. Sélectionnez la **période**.

   > **Remarque :** Lorsque vous sélectionnez l'option Période, vous pouvez choisir une période prédéfinie, par exemple la dernière heure, les 3 dernières heures, et ainsi de suite, ou vous pouvez personnaliser la sélection en choisissant N derniers jours ou Personnalisé. Si vous sélectionnez l'option N derniers jours, vous pouvez visualiser les données historiques sur un maximum de 15 jours. En revanche, si vous sélectionnez l'option Personnalisé, vous pouvez choisir une date de début et une date de fin afin de visualiser les données pour la période sélectionnée.

   b. Sélectionnez la **Série**, soit **Valeurs du graphique au fil du temps**, soit **Graphique avec totaux**.
   Lorsque vous sélectionnez **Valeurs du graphique au fil du temps**, le graphique affiche le changement de valeurs pour la période sélectionnée. Lorsque vous sélectionnez **Graphique avec totaux**, le graphique affiche le total de chaque valeur agrégée pour la période sélectionnée.

c. Sélectionnez **Éléments à tracer** pour définir le nombre d'événements à afficher sur le graphique.

d. Dans la liste déroulante **Type du graphique**, sélectionnez le type de graphique.

e. Cliquez sur **Recharger** pour recharger le graphique sélectionné.
En cas de retard lors de la récupération des données historiques pour la période sélectionnée, un message s'affiche.

Une fois le graphique généré, une notification s'affiche dans la barre de notifications disponible au sein de la barre d'outils NetWitness. Pour plus d'informations sur la barre d'outils NetWitness, reportez-vous à la rubrique **Fenêtre du navigateur** dans le *Guide de mise en route de NetWitness*.

Liste Afficher tous les graphiques

Pour afficher une liste de tous les graphiques :

1. Sélectionner **SURVEILLER** > **Rapports**.
L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
La vue Graphique s'affiche.
3. Dans la barre d'outils **Graphique**, cliquez sur **Affiche tous les graphiques**.
Tous les graphiques exécutés pour la date sélectionnée s'affichent dans un nouvel onglet.

> **Remarque :**
> * Si aucune liste ne s'affiche, vous pouvez sélectionner une date dans le calendrier pour afficher une liste des graphiques.
> * Si vous souhaitez afficher un graphique spécifique, saisissez son nom dans les critères de recherche.

4. Cliquez sur le nom du graphique pour afficher ses détails pour cette date.

Tester un graphique

Vous pouvez tester un graphique à partir de la vue **Tester un graphique**.

Pour tester un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Exécutez l'une des opérations suivantes :
   - Dans la barre d'outils **Graphique**, cliquez sur  .
   - Dans le panneau **Graphique**, double-cliquez sur un graphique ou sélectionnez un graphique et cliquez sur  .
   - Dans le panneau **Liste des graphiques**, cliquez sur  > **Modifier**.
     L'onglet de la vue Élaborer le graphique s'affiche.
4. Cliquez sur **Tester un graphique** pour afficher le graphique.
   L'onglet de la vue Afficher le graphique s'affiche.
5. Sélectionnez les plages de dates **Du** et **Au**.
6. Sélectionnez la **Série**, soit **Série chronologique** ou **Récapitulatif**.
7. Dans la liste déroulante **Type du graphique**, sélectionnez le type de graphique.
8. Cliquez sur **Exécuter le test** pour exécuter le test.
   Les données de graphique (éventuelles) correspondant à la période sélectionnée s'affichent.

Analyser un graphique

Vous pouvez analyser le graphique en accédant directement au module Investigation du graphique.

Pour analyser un graphique :

1. Sélectionner **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans la barre d'outils **Graphique**, cliquez sur **Afficher tous les graphiques**.
   Tous les graphiques exécutés à la date sélectionnée dans le panneau **Options du graphique** s'affichent dans un nouvel onglet.
4. Cliquez sur le nom du graphique pour en afficher les détails tels que l'heure à laquelle le graphique est exécuté et la source de données par défaut utilisée pour l'exécution du graphique.
5. Exécutez l'une des opérations suivantes :
   - Cliquez sur un point de données du graphique pour l'analyser.
   - Dans la barre d'outils, cliquez sur **Examiner** pour analyser la période entière.

Gérer un groupe de graphiques et un graphique

Vous pouvez gérer des groupes de graphiques et des graphiques à l'aide des procédures suivantes.

Gérer un groupe de graphiques

Selon les autorisations d'accès définies pour le rôle d'utilisateur, vous pouvez modifier ou supprimer, importer ou exporter, faire glisser et déposer un graphique, ou actualiser un groupe de graphiques.

Modifier un groupe de graphiques

Pour modifier un groupe de graphiques dans le dossier par défaut ou les sous-groupes sous un groupe de graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, sélectionnez le groupe de graphiques à modifier.
   Le groupe de graphiques sélectionné est modifié et peut être affiché dans le panneau Groupes de graphiques.

Supprimer un groupe de graphiques

Pour supprimer un groupe de graphiques du dossier par défaut ou des sous-groupes sous un groupe de graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, sélectionnez le groupe et cliquez sur .
   Une boîte de dialogue de confirmation vous demande de confirmer que vous souhaitez supprimer le groupe sélectionné.
4. Cliquez sur **Oui** pour supprimer le groupe.
   Le groupe sélectionné est supprimé du panneau Groupes de graphiques.

Importer un groupe de graphiques

Pour importer des groupes de graphiques depuis d'autres instances de NetWitness Suite :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, sélectionnez un dossier pour importer le fichier.
4. Exécutez l'une des opérations suivantes :
   - Dans le panneau Groupes de graphiques, cliquez sur  > **Importer**.
     La boîte de dialogue **Importer le graphique** s'affiche. Vous pouvez importer plusieurs groupes de graphiques en même temps. Pour sélectionner plusieurs groupes de graphiques, maintenez la touche CTRL enfoncée et sélectionnez les groupes de graphiques à importer.
5. Cliquez sur **Parcourir** pour sélectionner le fichier binaire.
   NetWitness fournit une vue système des fichiers.
6. Recherchez le fichier binaire, puis cliquez sur **Ouvrir**.
   Le fichier est alors ajouté dans la liste Importer le graphique.
7. (Facultatif) Pour écraser toutes les règles existantes dans la bibliothèque par une règle possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case **Règle**. Si vous ne sélectionnez pas l'option Remplacer et qu'une règle identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
8. (Facultatif) Pour écraser toutes les listes existantes dans la bibliothèque par une liste possédant un nom identique dans le fichier binaire, cochez la case **Liste**. Si vous ne sélectionnez pas l'option Remplacer et qu'une liste identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
9. (Facultatif) Pour écraser tous les graphiques existants dans la bibliothèque par un graphique possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case **Graphique**. Si vous ne sélectionnez pas l'option Remplacer et qu'un graphique identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
10. Cliquez sur **Importer** pour importer le fichier binaire.

Exporter un groupe de graphiques

Pour exporter des groupes de graphiques sélectionnés :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, sélectionnez un groupe de graphiques, cliquez sur  et exécutez l'une des options suivantes :
   - **Exporter** - Cette sélection exporte un graphique dans un fichier .zip.
   - **Exporter en tant que texte** - Cette sélection exporte tout le contenu du Reporting Engine dans un fichier .zip qui contient les données au format texte.

   Vous pouvez exporter plusieurs groupes de graphiques en même temps. Pour sélectionner plusieurs groupes de graphiques, maintenez la touche CTRL enfoncée et sélectionnez les groupes de graphiques à exporter. Le fichier exporté est enregistré sur le disque local.

Glisser-déplacer un graphique vers un groupe

Pour glisser-déplacer un graphique du panneau Liste des graphiques vers un groupe du panneau Groupes de graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Sélectionnez un graphique dans le panneau **Liste des graphiques** et glissez-déplacez le graphique vers un groupe du panneau **Groupes de graphiques**.
   Le graphique est copié dans le groupe du panneau Groupes de graphiques.

Actualiser un groupe de graphiques

Pour actualiser des groupes de graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, glissez-déplacez le groupe.
   Le groupe de graphiques est déplacé vers le nouvel emplacement.
4. Dans le panneau **Groupe de graphiques**, cliquez sur .
   Le groupe de graphiques est actualisé.

Gérer un graphique

Selon les autorisations d'accès définies pour le rôle d'utilisateur, vous pouvez modifier ou supprimer, dupliquer, importer et exporter, activer ou désactiver des graphiques, analyser des graphiques existants et actualiser une liste de graphiques.ledes

Contrôle d'accès pour un graphique

Pour définir les autorisations d'accès pour un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un graphique.
4. Cliquez sur  >**Autorisations**.
   La boîte de dialogue Autorisations des graphiques s'affiche.
5. En fonction du rôle d'utilisateur, sélectionnez les boutons appropriés.
6. (Facultatif) Pour accorder l'autorisation d'accès en lecture aux règles dépendantes, activez la case à cocher.

   Remarque : En activant la case à cocher, toutes les règles dépendantes avec une autorisation Aucun accès reçoivent une autorisation d'accès en LECTURE.
7. Cliquez sur **Enregistrer**.
   Un message de confirmation s'affiche indiquant que l'autorisation a été définie pour le rapport sélectionné.

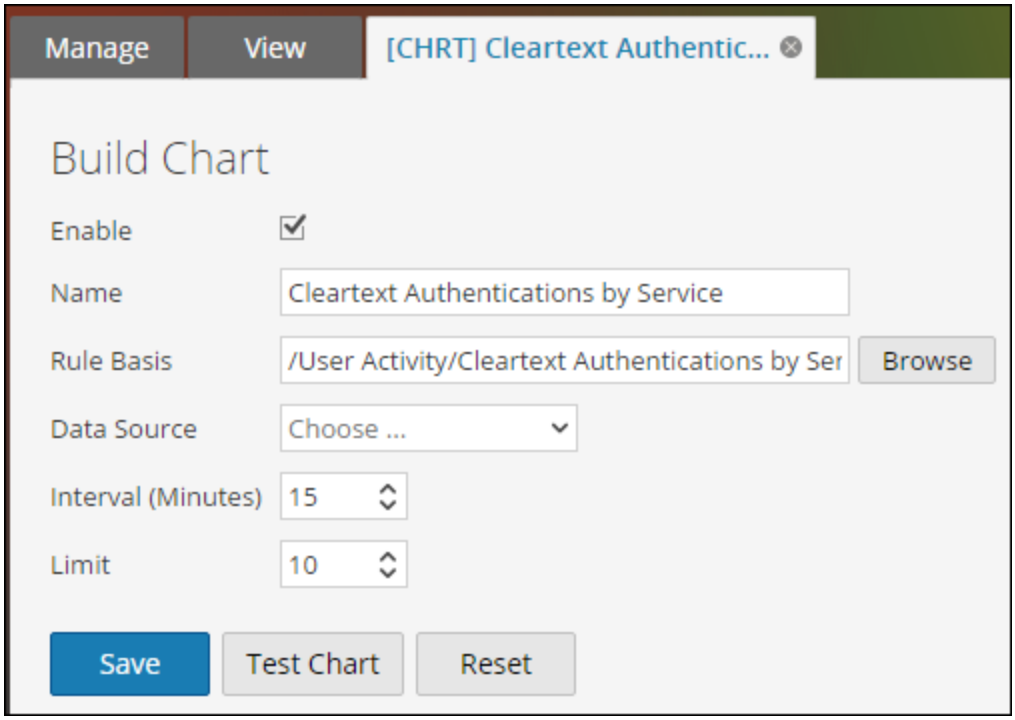
Modifier un graphique

Pour modifier un graphique dans un groupe ou un sous-groupe :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, exécutez l'une des opérations suivantes :
   - Double-cliquez sur un graphique ou sélectionnez un graphique et cliquez sur .

- Sélectionnez un graphique, puis cliquez sur  > **Modifier**.

  L'onglet de la vue Élaborer le graphique s'affiche.



4. Modifiez le nom du graphique.
5. Pour que le Reporting Engine puisse collecter les données et générer des résultats sous la forme d'un graphique, cochez la case **Activer**.
6. (Facultatif) Dans le champ **Base de règle**, procédez comme suit :
   a. Cliquez sur **Parcourir**.
      La boîte de dialogue Ajouter une règle s'affiche.
   b. Accédez à l'arborescence Règle et sélectionnez une règle.
   c. Cliquez sur **Sélectionner**.
      La règle s'affiche dans le champ Base de règle.
7. Sélectionnez la source de données dans la liste déroulante **Sources de données**.

   Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubrique **Configurer les autorisations d'accès aux sources de données** dans le *Guide de configuration de l'hôte et des services*.

8. (Facultatif) Pour modifier la valeur de l'intervalle, cliquez sur les flèches vers le haut ou vers le bas.
9. Sélectionnez la valeur limite pour limiter le nombre d'enregistrements à afficher.
10. Cliquez sur **Enregistrer**.
    Un message de confirmation de la modification du graphique s'affiche.

Supprimer un graphique

Pour supprimer un graphique dans un groupe ou un sous-groupe :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, exécutez l'une des opérations suivantes :
   - Sélectionnez les graphiques et cliquez sur .
   - Cliquez sur > **Supprimer**.
     Un message de confirmation vous demande si vous voulez supprimer le graphique sélectionné.
4. Cliquez sur **Oui** pour supprimer le graphique.
   Un message de confirmation de la suppression du graphique s'affiche et le graphique sélectionné est supprimé du panneau Liste des graphiques.

Dupliquer un graphique

Pour dupliquer un graphique existant :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un graphique à dupliquer.
4. Dans la barre d'outils **Graphique**, cliquez sur .
   Le graphique est dupliqué et ajouté au panneau Liste des graphiques.

Importer un graphique

Pour importer des graphiques depuis d'autres instances de NetWitness :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Groupes de graphiques**, sélectionnez un dossier depuis lequel importer le fichier.
4. Exécutez l'une des opérations suivantes :
   - Dans la barre d'outils Graphique, cliquez sur  > **Importer**.
     La boîte de dialogue **Importer le graphique** s'affiche. Vous avez également la possibilité d'importer plusieurs graphiques à la fois. Pour sélectionner plusieurs graphiques, maintenez la touche CTRL enfoncée et sélectionnez les graphiques à importer.
5. Cliquez sur **Parcourir** pour sélectionner le fichier binaire.
   NetWitness fournit une vue système des fichiers.
6. Recherchez le fichier binaire, puis cliquez sur **Ouvrir**.
   Le fichier est alors ajouté dans la liste Importer le graphique.
7. (Facultatif) Pour écraser toutes les règles existantes dans la bibliothèque par une règle possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case **Règle**. Si vous ne sélectionnez pas l'option Remplacer et qu'une règle identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
8. (Facultatif) Pour écraser toutes les listes existantes dans la bibliothèque par une liste possédant un nom identique dans le fichier binaire, cochez la case **Liste**. Si vous ne sélectionnez pas l'option Remplacer et qu'une liste identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
9. (Facultatif) Pour écraser tous les graphiques existants dans la bibliothèque par un graphique possédant un nom identique dans le fichier binaire lors de l'importation, cochez la case **Graphique**. Si vous ne sélectionnez pas l'option Remplacer et qu'un graphique identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
10. Cliquez sur **Importer** pour importer le fichier binaire.

Exporter un graphique

Pour exporter les graphiques sélectionnés vers un fichier externe :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un graphique, cliquez sur  et exécutez l'une des opérations suivantes :
   - **Exporter** - Cette sélection exporte un graphique dans un fichier .zip.
   - **Exporter en tant que texte** - Cette sélection exporte un graphique à partir de Reporting Engine dans un fichier .zip qui contient les données au format texte.

   Vous pouvez exporter plusieurs graphiques en même temps. Pour sélectionner plusieurs graphiques, cochez les cases des graphiques à exporter. Le fichier exporté est enregistré sur le disque local.

Activer un graphique

Pour activer un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un ou plusieurs graphiques affichant ○ dans la colonne **Activé**.
4. Cliquez sur ●.
   Un message de confirmation indique que l'état des graphiques a changé.

Désactiver un graphique

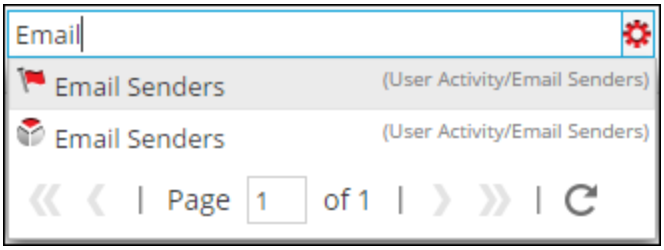
Pour désactiver un graphique :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, sélectionnez un ou plusieurs graphiques affichant ● dans la colonne **Activé**.
4. Cliquez sur ○.
   Un message de confirmation indique que l'état des graphiques a changé.

Analyser un graphique existant

Pour analyser un graphique existant :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans la barre d'outils **Graphique**, saisissez du texte dans la zone Rechercher.
4. Cliquez sur  > **Graphique**.
   Les graphiques présentant la sous-chaîne dans leur nom sont affichés dans la liste déroulante de recherche.



Actualiser un graphique

Pour actualiser des graphiques :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Graphiques**.
   La vue Graphique s'affiche.
3. Dans le panneau **Liste des graphiques**, faites glisser les graphiques dans le groupe voulu dans le panneau Groupes de graphiques.
   Les graphiques sont déplacés vers le nouvel emplacement.
4. Effectuez ce qui suit :
   - Dans le panneau **Liste des graphiques**, cliquez sur .
   - Dans le panneau **Barre d'outils Graphique**, sélectionnez **Actualisation automatique**.
     La liste des graphiques est actualisée.

Présentation des alertes

Des alertes peuvent être utilisées pour générer des informations en temps opportun à propos de problèmes de sécurité actuels, de vulnérabilités et d'attaques. Par exemple, lorsqu'un e-mail malveillant est envoyé à partir d'un compte compromis, il vous faut une alerte qui vous avertit automatiquement lorsqu'un tel événement se produit.

Les concepts suivants d'alerte vous permettront de mieux comprendre les règles d'alerte, les conditions, les notifications et les modèles.

Règles d'alerte

Les règles d'alerte spécifient la logique déterminant la génération d'alertes. Les règles d'alerte vous permettent de configurer les seuils et définissent le mode d'avertissement si ces limites sont dépassées. Par exemple, vous pouvez configurer une règle pour être alerté lorsque l'utilisation du CPU reste anormalement élevée pendant au moins 5 minutes.

Définitions des alertes

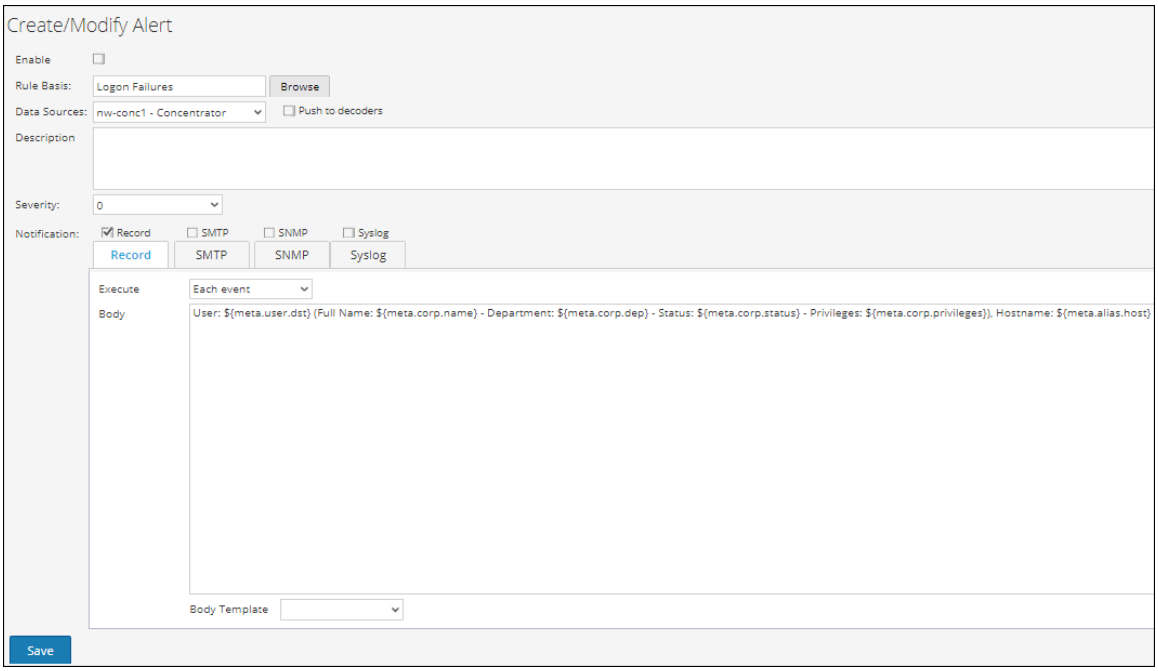
La définition d'alerte est similaire à la définition des règles pour des rapports. Ces règles doivent être définies en fonction de votre exemple d'utilisation. Pour définir une alerte, choisissez les règles d'alerte que vous définissez dans la vue Élaborer une règle. Vous sélectionnez cette règle lors de la définition d'une alerte.

Remarque : Vous pouvez uniquement créer une alerte à l'aide de règles définies pour la source de données NetWitness.

Une fois une alerte créée, ces données sont collectées par le Reporting Engine et affichées sur l'interface utilisateur.

Une fois une alerte définie, vous pouvez la planifier pour qu'elle s'exécute toutes les minutes (par défaut), maintenant ou très prochainement.

Remarque : Dans l'interface utilisateur NetWitness, quel que soit l'emplacement d'affichage de la date et de l'heure, le profil de fuseau horaire sélectionné par l'utilisateur est toujours respecté.



Notifications d'alertes

Les composants suivants sont requis pour configurer les notifications d'alerte :

- Serveur de notification – Le serveur de notification est utilisé pour envoyer des notifications d'alerte. Par exemple, le serveur de messagerie SMTP. Après avoir configuré un serveur de notification, vous pouvez l'ajouter à une règle. Lorsque la règle déclenche une alerte, la règle utilise ce serveur pour envoyer des notifications d'alerte.
- Notifications – Ce sont des résultats d'alerte, qui peuvent être de type e-mail, SMTP, SNMP et Syslog.
- Modèles – Le format prédéfini d'un message d'alerte.

À chaque fois que la condition de règle est rencontrée, des alertes sont générées en fonction du niveau de gravité et l'utilisateur est averti selon la méthode de notification définie pour cette alerte spécifique. Les différentes méthodes de notification sont les suivantes :

- E-mail/SMTP : Le protocole SMTP (Simple Mail Transport Protocol) envoie des e-mails d'alerte concernant l'activité du système. Les alertes par e-mail peuvent être envoyées à leurs destinataires en sélectionnant SMTP comme type de notification.
- SNMP : Le protocole SNMP (Simple Network Management Protocol) envoie des alertes à plusieurs ordinateurs concernant les traps SNMP. Des alertes SNMP peuvent être envoyées à d'autres ordinateurs en sélectionnant SNMP comme type de notification.

- Syslog : Les alertes Syslog génèrent des notifications à partir des messages Syslog. Des alertes Syslog peuvent être envoyées en sélectionnant Syslog comme type de notification.

Des alertes peuvent être configurées pour notifier des événements qui nécessitent une attention particulière, ou en tant que mécanismes pour effectuer des actions automatisées en fonction des conditions configurées dans une alerte. Une alerte est envoyée lorsque les conditions au sein de l'entité ont répondu aux critères sélectionnés pour l'alerte. Les critères de notification déterminent quand et à quelle fréquence l'alerte est générée.

Modèles d'alerte

Les modèles d'alerte sont un format prédéfini pour un message d'alerte. Vous pouvez utiliser ces modèles pour créer des alertes.

Contrôle d'accès pour l'Alerting

En fonction du rôle d'utilisateur, l'utilisateur reçoit un ensemble spécifique d'autorisations d'accès pour gérer une alerte. L'administrateur gère les droits d'accès fournis pour chaque rôle d'utilisateur depuis l'onglet **Administration > Sécurité > Rôles**. Vous pouvez définir des autorisations d'accès aux rôles d'utilisateur pour gérer une alerte. Le module Reporting fournit un contrôle d'accès au niveau de l'alerte.

Remarque : Les autorisations d'alerte de Reporting Engine sont précédées par « RE » pour les distinguer de l'Event Streaming Analysis (ESA).

Lorsque vous créez des utilisateurs et des rôles d'utilisateur, assurez-vous que les rôles que vous créez pour des tâches spécifiques ont accès à toutes les autorisations nécessaires. Cela peut nécessiter des autorisations à plusieurs niveaux de la hiérarchie des rôles.

Des alertes peuvent être combinées à un ensemble spécifique de rôles d'utilisateur de telle sorte que lorsqu'un utilisateur se connecte à NetWitness, les seules alertes auxquelles il peut accéder sont celles qui sont accessibles par le rôle auquel il appartient. Les utilisateurs appartenant à un rôle d'utilisateur avec l'accès en « **lecture écriture** » peuvent définir des alertes. L'accès peut être encore plus limité pour que les alertes ne soient accessibles que par ceux qui ont l'accès en « **lecture seule** ».

Au niveau de l'alerte, vous pouvez définir les autorisations d'accès suivantes pour les rôles d'utilisateur dans NetWitness :

- Lecture et écriture
- Lecture seule
- Aucun accès

Remarque : Avant d'appliquer les autorisations d'alertes, l'autorisation par défaut définie pour tous les rôles d'utilisateur est « **Aucun accès** » et la case est désactivée.

Si vous souhaitez modifier l'autorisation d'accès pour un rôle d'utilisateur spécifique, vous devez la définir au niveau de l'alerte. Excepté pour les administrateurs, l'autorisation par défaut définie pour tous les autres rôles d'utilisateur est « **Aucun accès** ».

Ces deux scénarios sont expliqués brièvement :

- Scénario 1 : Autorisations appliquées à l'alerte / aux règles basées sur le rôle d'utilisateur.
- Scénario 2 : Autorisation de lecture seule appliquée aux règles de l'alerte.

	Rôle (analystes)	**Autorisations appliquées à l'alerte / aux règles basées sur le rôle d'utilisateur**	**Autorisation (lecture seule) appliquée aux règles de l'alerte**
Alerte	**Lecture et écriture**	**Lecture et écriture**	**Lecture et écriture**
Règles	**Lecture**	**Lecture**	**Lecture**

Le rôle d'analyste de la sécurité est attribué à l'alerte et les autorisations sont définies pour les alertes de **lecture et écriture**.

Pour le scénario 1, chacun des niveaux a un ensemble d'autorisations en fonction du rôle d'utilisateur. Pour le scénario 2, l'autorisation de **lecture** est définie pour les règles, sauf que l'autorisation des règles ne doit pas être supérieure à l'autorisation des alertes.

Si l'autorisation des règles est supérieure à l'autorisation des alertes, l'autorisation n'est pas appliquée. Par exemple, si vous définissez les autorisations de l'alerte sur **Aucun accès** et si vous spécifiez l'option *Appliquer l'autorisation en lecture seule aux règles des alertes*, l'autorisation en lecture seule n'est pas définie pour les règles.

Contrôle d'accès pour une alerte lorsque plusieurs alertes sont sélectionnées

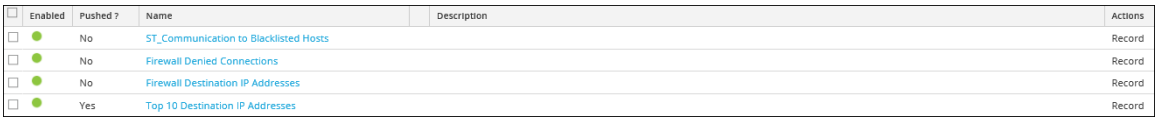
Lorsque vous souhaitez modifier les autorisations de plusieurs alertes, vous devez les sélectionner et définir leurs autorisations d'accès à l'aide du panneau Autorisations d'alerte. L'autorisation d'accès que vous choisissez est appliquée à toutes les alertes sélectionnées.

Se connecter en tant qu'utilisateur spécifique et afficher les détails d'accès

Lorsque vous vous connectez à l'interface utilisateur de NetWitness en tant qu'utilisateur ayant une autorisation d'accès en **lecture**, toutes les alertes sont annotées du symbole (📖). Lorsque vous cliquez sur ce symbole, la légende « Lecture seule » s'affiche dans le panneau Liste d'alertes.

Lorsque vous vous connectez à l'interface utilisateur de NetWitness en tant qu'utilisateur n'ayant pas d'autorisation d'accès en **lecture et écriture** sur une alerte, toutes les alertes sont annotées du symbole ( ) et apparaissent en grisé sur le panneau Liste des alertes.

La figure suivante montre le panneau Liste des alertes lorsque vous êtes connecté avec une autorisation d'accès en **lecture et écriture** minimale.

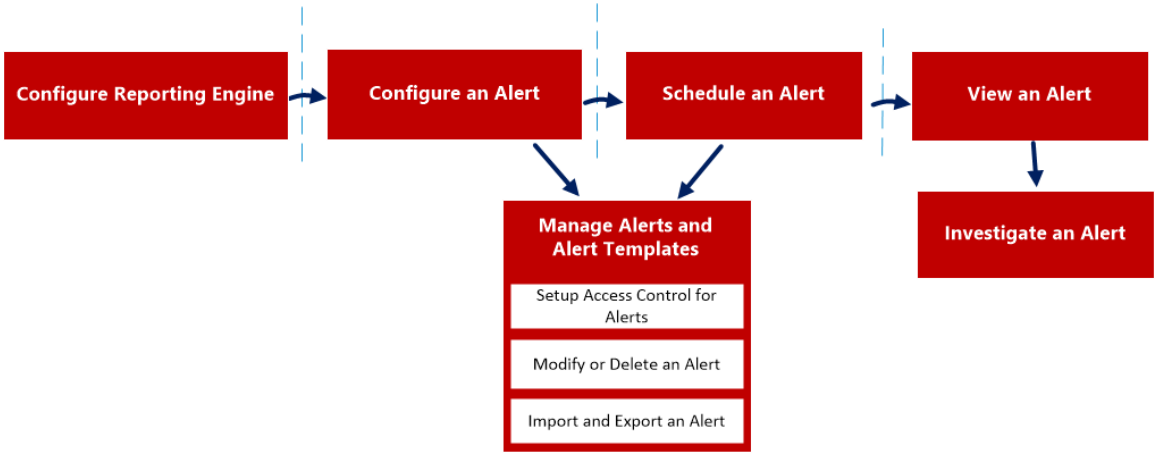


Remarque : Si un utilisateur (autre que ADMIN) crée une alerte, ADMIN ne pourra pas accéder à cette alerte.

Le tableau suivant répertorie les différentes colonnes du panneau Autorisations d'alerte.

Colonne	Description
Rôles	Le rôle de l'utilisateur connecté dans l'interface utilisateur de NetWitness.
Lecture et écriture	L'utilisateur peut accéder, visualiser, modifier, importer, exporter et supprimer l'alerte sur la page Alertes. L'utilisateur peut également modifier l'autorisation dans l'alerte.
accès en lecture seule	L'utilisateur peut uniquement accéder à l'alerte et la consulter sur la page Alertes.
Aucun accès	L'utilisateur ne peut pas accéder ou afficher l'alerte pour laquelle cette autorisation est définie.
Appliquer l'autorisation de lecture seule aux règles dans les alertes	L'utilisateur peut automatiquement appliquer les autorisations aux règles dans les alertes.

Voici une vue d'ensemble du processus d'alerte complet :



Pour configurer et générer une alerte dans Reporting Engine, procédez comme suit :

1. Configurer le Reporting Engine
2. Configurer une alerte
3. Planifier une alerte
4. Afficher une alerte
5. Analyser une alerte
6. Gérer une alerte et un modèle d’alerte

Configurer le Reporting Engine

Assurez-vous que :

- Vos Decoders sont connectés au Concentrator ajouté à Reporting Engine pour la source de données sélectionnée, avant de créer une règle d'alerte.
- Vous avez installé et configuré un serveur Syslog qui prend en charge TCP/TLS dans votre environnement. Par exemple, WinSyslog. Vous pouvez configurer le Reporting Engine pour envoyer des messages Syslog via TCP avec Transport Layer Security (TLS) lorsqu'une alerte est déclenchée.

Pour configurer le Reporting Engine pour envoyer des alertes Syslog via TCP avec Transport Layer Security (TLS) :

1. Obtenez les certificats requis.
2. Ajoutez le certificat d'autorité de certification au fichier ca.pem sur le serveur NetWitness.
3. Configurez le serveur Syslog pour accepter des messages des machines client.
4. Configurez la remise des messages d'alerte dans l'interface utilisateur NetWitness.

Tâche 1 : Obtenir les certificats requis

Pour générer des certificats permettant de configurer le Reporting Engine pour l'envoi de messages Syslog via TCP avec TLS :

1. Générez un certificat de l'Autorité de certification (AC). Pour plus d'informations, reportez-vous à la rubrique http://www.rsyslog.com/doc/tls_cert_ca.html.

Remarque : Vous pouvez ignorer cette étape si vous avez déjà un certificat AC en cours d'exécution dans votre environnement.

2. Générez une paire de clés pour le serveur Syslog. Pour plus d'informations, reportez-vous à la rubrique http://www.rsyslog.com/doc/tls_cert_machine.html.

Remarque : Vous pouvez ignorer cette étape si vous avez déjà configuré la sécurité pour le serveur Syslog à l'aide de la clé et des certificats générés par la même autorité de certification.

Tâche 2 : Ajouter le certificat d'autorité de certification au fichier ca.pem sur le serveur NetWitness

Pour ajouter un certificat d'autorité de certification existant au fichier ca.pem :

1. Ajoutez manuellement le contenu du certificat d'autorité de certification que vous avez généré au fichier **/etc/pki/CA/certs/ca.pem**.
2. Exécutez la commande suivante sur le serveur NetWitness pour que le certificat alimente pour le magasin d'approbations :
   `keytool -import -file /etc/pki/CA/certs/ca.pem -keystore cacerts`

Tâche 3 : Configurer le serveur Syslog pour accepter des messages des machines client

Pour configurer le serveur Syslog afin qu'il accepte des messages des machines client ayant les mêmes certificats d'autorités de certification :

1. Copiez les fichiers suivants sur votre site de destination du serveur TCP sécurisé :
   - ca_cert.pem
   - server_cert.pem
   - server_key.pem

   Where:

   ca_cert.pem - est le certificat d'autorité de certification

   server_cert.pem - est le certificat du serveur

   server_key.pem - est la clé de serveur

   Pour plus d'informations, consultez la documentation spécifique à votre serveur Syslog. Si vous utilisez rsyslog, reportez-vous à la page http://www.rsyslog.com/doc/tls_cert_server.html.

Tâche 4 : Configurer la remise des messages d'alerte dans NetWitness

Configurez le Reporting Engine pour envoyer des messages Syslog sur TCP avec Transport Layer Security (TLS) lorsqu'une alerte est déclenchée par l'activation de **SECURE_TCP** sous l'onglet **Actions de résultat** pour le service Reporting Engine au sein de la vue Configuration des services du Reporting Engine. Pour plus d'informations, consultez la rubrique **Actions de résultat du Reporting Engine** dans le *Guide de configuration de l'hôte et des services*.

Configuration d’une alerte

Vous pouvez configurer une alerte en définissant des notifications d’alerte et en ajoutant une méthode de notification à une règle.

Remarque : Seuls les administrateurs peuvent configurer ces notifications.

Pour configurer une alerte :

1. Sélectionnez **Surveiller** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans la barre d’outils **Alerte**, cliquez sur  .
   Le panneau Créer/modifier une alerte s’affiche.
4. Cliquez sur **Activer** pour activer l'alerte.
5. Dans le champ **Base de règle** :
   a. Cliquez sur **Parcourir**.
      La boîte de dialogue Base de la règle de recherche s'affiche.
   b. Accédez à l'arborescence Règle et sélectionnez une règle.
   c. Cliquez sur **OK**.
      Le nom de la règle s'affiche dans le champ Base de règle.
6. Sélectionnez une source de données dans la liste déroulante **Source de données**.

   Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse Connector. Pour plus d'informations, reportez-vous à la rubrique**Configurer les autorisations d'accès aux sources de données** dans le *Guide de configuration de l'hôte et des services*.
7. Cochez la case **Transmettre aux décodeurs** pour Reporting Engine pour envoyer la règle à Decoder.
8. (Facultatif) Saisissez une description de l'alerte dans le champ **Description**.
9. Sélectionnez le niveau de gravité dans la liste déroulante **Gravité**.
10. Dans le champ **Notification** :
    a. Sélectionnez la notification appropriée.
       L'onglet de la notification sélectionnée s'affiche dans la boîte de dialogue Créer/modifier

une alerte.

b. (Facultatif) Annulez la sélection de la notification pour désactiver l'onglet de notification.

c. Définissez l'action dans l'un des onglets **Notification** :

   i. Dans le champ de l'onglet **Enregistrement** :

      a. Dans la liste déroulante **Exécuter**, sélectionnez la fréquence d'enregistrement d'une alerte.

      b. Saisissez le message ENREGISTRER. Vous pouvez créer un nouveau message ou sélectionner un modèle dans le champ **Modèle de corps**, puis modifier le modèle depuis cet emplacement.

      c. (Facultatif) Si des modèles ont été définis, sélectionnez un modèle pour le message ENREGISTRER que vous pouvez utiliser tel quel ou modifié.

   ii. Dans le champ de l'onglet **SMTP** :

      a. Dans la liste déroulante **Exécuter**, sélectionnez une valeur pour identifier le nombre de fois que vous souhaitez envoyer un message électronique pour l'alerte.

      b. Saisissez une adresse e-mail ou une liste d'adresses e-mail séparées par des virgules à laquelle vous souhaitez envoyer cette alerte.

      c. Saisissez l'objet du message électronique.

      d. Saisissez le corps du message. Vous pouvez créer un nouveau message ou sélectionner un modèle dans le champ **Modèle de corps**, puis modifier le modèle depuis cet emplacement.

   iii. Dans le champ de l'onglet **SNMP** :

      a. Dans la liste déroulante **Exécuter**, sélectionnez une valeur pour identifier le nombre de fois que vous souhaitez envoyer un message SNMP pour l'alerte.

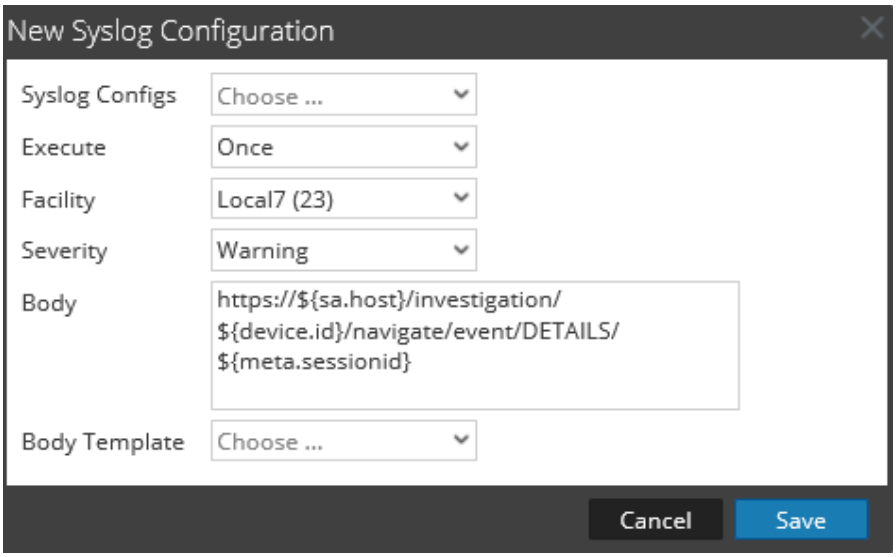
      b. Saisissez le message SNMP. Vous pouvez créer un nouveau message ou sélectionner un modèle dans le champ **Modèle de corps**, puis modifier le modèle depuis cet emplacement.

   iv. Dans le champ de l'onglet **Syslog** :

> **Remarque :** Vous pouvez configurer plusieurs serveurs Syslog sur le panneau de configuration Syslog. Pour plus d'informations, consultez la rubrique **Actions de résultat du Reporting Engine** dans le *Guide de configuration de l'hôte et des services*.

a. Cliquez sur +.

La boîte de dialogue Nouvelle configuration Syslog s'affiche :



b. Dans la liste déroulante **Configurations Syslog**, sélectionnez une valeur pour la configuration syslog.

c. Dans la liste déroulante **Exécuter**, sélectionnez une valeur pour identifier le nombre de fois que vous souhaitez envoyer un message Syslog pour l'alerte.

d. Sélectionnez la fonctionnalité dans la liste déroulante **Fonctionnalité**.

e. Sélectionnez le niveau de gravité dans la liste déroulante **Gravité**.

f. Saisissez le message Syslog. Vous pouvez créer un nouveau message ou sélectionner un modèle dans le champ **Modèle de corps**, puis modifier le modèle depuis cet emplacement.

Remarque : Si vous souhaitez ajouter une clé méta dans la règle, indiquez-le dans le format suivant : ${meta.metakey}. Par exemple, ${meta.ip.dst}.

g. Cliquez sur **Enregistrer**.

La configuration Syslog est ajoutée à l'alerte.

11. Cliquez sur **Créer**.

NetWitness crée l'alerte avec un message de confirmation indiquant que l'alerte est enregistrée. NetWitness génère une alerte et exécute les actions de résultat toutes les minutes.

Planifier une alerte

Vous devez planifier une alerte pour rechercher des événements à intervalles réguliers.

Pour planifier une alerte :

1. Sélectionnez **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Dans la barre d'outils **Alertes**, cliquez sur Afficher les alertes.
3. Sélectionnez une alerte à planifier.
4. Dans la barre d'outils **Alerte**, cliquez sur **Activer**.
   L'alerte sélectionnée est planifiée.

Afficher une alerte

Vous pouvez afficher une alerte ou une liste de toutes les alertes.

Vous pouvez afficher les alertes déclenchées et analyser toute alerte dans le module Investigation et personnaliser les vues pour afficher les alertes correspondant à une période spécifique. De plus, vous pouvez définir le nombre maximal d'alertes affichées dans une seule page.

Pour afficher une alerte :

1. Sélectionnez **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3. Dans la barre d'outils **Alerte**, cliquez sur **Afficher les alertes**.
   L'onglet de la vue Afficher les alertes s'affiche.

Analyser une alerte

Vous pouvez analyser chaque alerte déclenchée sur la vue Alerte. Pour une investigation plus détaillée sur une alerte spécifique, vous pouvez afficher l'alerte sur le module Investigation.

Pour analyser une alerte :

1. Dans la barre d'outils de la rubrique **Alerte**, cliquez sur **Afficher les alertes** pour accéder à la vue Afficher les alertes.
2. Exécutez l'une des opérations suivantes :
   - Cliquez sur le bouton  en regard de l'alerte à analyser.

     Le module Investigation affiche les détails de la première session qui a enregistré l'occurrence de l'alerte donnée en vue de son analyse immédiate.
   - Cliquez sur le nom de l'alerte à analyser.

     Le module Investigation affiche toutes les occurrences de cette alerte spécifique pour l'heure entourant l'alerte enregistrée.

Gérer une alerte et un modèle d’alerte

Vous pouvez gérer des alertes, des alertes planifiées et des modèles d’alerte à l’aide des procédures suivantes.

Gérer une alerte

Selon les autorisations d’accès définies pour le rôle d’utilisateur, vous pouvez modifier ou supprimer, importer et exporter, activer ou désactiver des alertes, afficher ou actualiser une liste d’alertes.

Contrôle d’accès pour une alerte lorsque une seule alerte est sélectionnée

Pour définir les autorisations d'accès pour une alerte :

1. Sélectionnez **Surveiller> Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau Liste des alertes, sélectionnez une alerte.
4. Cliquez sur > **Autorisations**.
   La boîte de dialogue Autorisations d'alerte s'affiche.
5. En fonction du rôle d'utilisateur, sélectionnez les options appropriées.
6. (Facultatif) Pour accorder automatiquement l'autorisation d'accès en lecture aux règles dépendantes, activez la case à cocher.

Remarque : En activant la case à cocher, toutes les règles dépendantes avec une autorisation Aucun accès auront une autorisation d'accès en LECTURE.

7. Cliquez sur **Enregistrer**.
   Un message de confirmation s'affiche indiquant que l'autorisation a été définie pour l'alerte sélectionnée.

Contrôle d'accès pour une alerte lorsque plusieurs alertes sont sélectionnées

Pour modifier les autorisations de plusieurs alertes :

1. Dans le panneau Liste des alertes, sélectionnez toutes les alertes dont les autorisations doivent être définies.
2. Cliquez sur > **Autorisations**.
   La boîte de dialogue Autorisations d'alerte s'affiche.

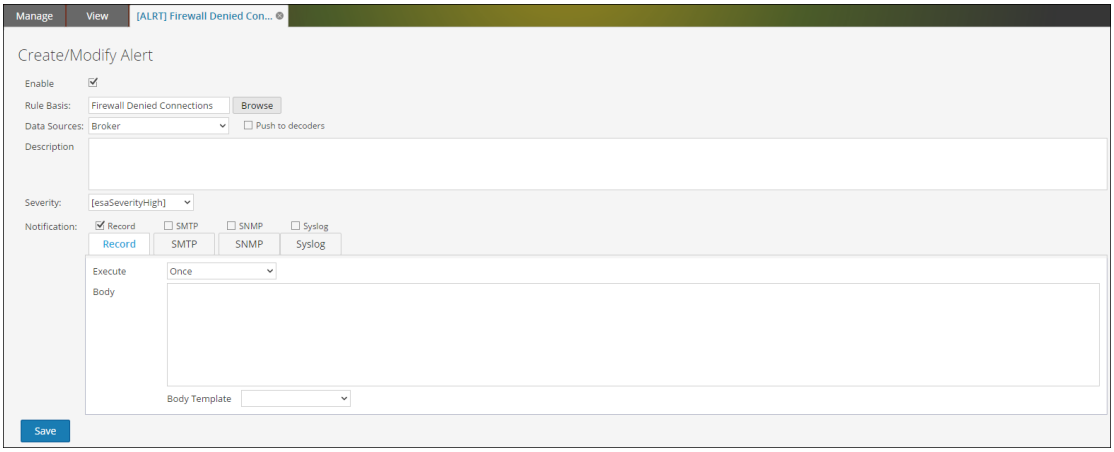
3. Sélectionnez l'autorisation à définir pour le rôle d'utilisateur respectif.
4. Cliquez sur **Enregistrer**.
   Un message de confirmation s'affiche indiquant que l'autorisation a été définie pour toutes les alertes sélectionnées.

Modifier une alerte

Par exemple, si vous souhaitez être averti à propos de l'alerte par e-mail via un identifiant d'e-mail différent, vous devrez modifier la rubrique de notification d'alerte pour que les nouvelles informations d'identifiants d'e-mail soient rétablies par e-mail lorsqu'une alerte est générée. En outre, vous pouvez également modifier la description de l'alerte et les notifications d'alerte dans le panneau Créer ou modifier une alerte.

Pour modifier une alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau **Liste des alertes**, sélectionnez une alerte et cliquez sur .
   L'onglet Créer ou modifier une alerte s'affiche.



4. Dans le champ **Base de règle**, accéder à l'arborescence des règles et sélectionnez une autre règle.
   Le nom de la règle s'affiche dans le champ Base de règle.
5. (Facultatif) Sélectionnez une source de données dans la liste déroulante **Sources de données**.

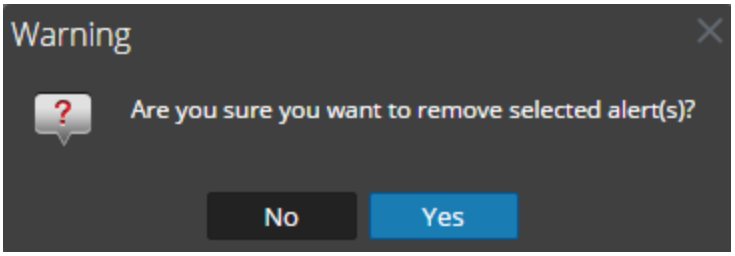
Remarque : Si la source de données n'est pas affichée, vérifiez que vous disposez des autorisations **Lecture** définies pour la source de données. Cela s'applique aux sources de données NWDB et Warehouse. Pour plus d'informations, reportez-vous à la rubrique **Configurer les autorisations d'accès aux sources de données** dans le *Guide de configuration de l'hôte et des services*.

6. (Facultatif) Modifiez la description de l'alerte dans le champ **Description**.
7. Modifiez les onglets **Notification** appropriés – **ENREGISTRER**, **SMTP**, **SNMP** et **Syslog**.
8. Cliquez sur **Enregistrer**.
   Un message de confirmation indiquant que l'alerte a été modifiée s'affiche.

Supprimer une alerte

Pour supprimer une alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau **Liste des alertes**, sélectionnez l'alerte et cliquez sur .
   Une boîte de dialogue d'avertissement vous invite à confirmer que vous souhaitez supprimer les alertes sélectionnées.



4. Cliquez sur **Oui** pour supprimer l'alerte.
   Un message de confirmation de la suppression de l'alerte s'affiche et l'alerte sélectionnée est supprimée du panneau Liste des alertes.

Importer l'alerte

Pour importer une alerte d'autres instances de NetWitness dans le panneau Liste des alertes :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.

3. Dans la barre d'outils **Alerte**, cliquez sur > Importer
   . La boîte de dialogue Importer l'alerte s'affiche.
4. Cliquez sur **Parcourir** pour sélectionner le fichier binaire.
   NetWitness fournit une vue système des fichiers. Vous pouvez importer plusieurs alertes à la fois. Pour sélectionner plusieurs alertes, sélectionnez la case à cocher de l'alerte à importer.
5. Recherchez le fichier binaire, puis cliquez sur **Ouvrir**.
   Le fichier est alors ajouté dans la liste Importer l'alerte.
6. (Facultatif) Pour écraser toutes les alertes de la bibliothèque possédant un nom d'alerte identique dans le fichier binaire lors de l'importation, cochez la case Alerte. Si vous ne sélectionnez pas l'option Remplacer et qu'une alerte identique est disponible dans le fichier binaire, ce dernier sera importé et aucun message d'erreur ne s'affichera.
7. Cliquez sur **Importer** pour importer le fichier binaire.

Exporter une alerte

Pour exporter une alerte vers un fichier externe qui peut être importé ultérieurement à NetWitness :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau **Liste des alertes**, sélectionnez une alerte, cliquez sur et exécutez l'une des options suivantes :
   - **Exporter** - Cette sélection exporte une alerte dans un fichier .zip.
   - **Exporter en tant que texte** - Cette sélection exporte tout le contenu du Reporting Engine dans un fichier .zip qui contient les données au format texte.
     Vous pouvez exporter plusieurs alertes à la fois. Pour sélectionner plusieurs alertes, activez la case à cocher de l'alerte à exporter.
4. Cliquez sur > **Exporter**.
   Le fichier binaire exporté est enregistré sur le disque local.

Activer une alerte

Pour activer une alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.

2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau **Liste des alertes**, sélectionnez l'alerte affichant ○ dans la colonne **Activé**.
4. Cliquez sur Enable.
   Un message indique que l'état des alertes a changé.

Désactiver une alerte

Pour désactiver une alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans le panneau **Liste des alertes**, sélectionnez l'alerte affichant ● dans la colonne **Activé**.
4. Cliquez sur ○ Disable.
   Un message de confirmation indique que l'état des alertes a changé.

Afficher une liste d'alertes

Pour afficher une liste d'alertes :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans la barre d'outils **Alerte**, cliquez sur **Afficher les alertes**.
   L'onglet de la vue Afficher les alertes s'affiche.
4. Dans la liste déroulante, sélectionnez le dernier nombre de jours.
5. Indiquez une valeur pour **Nb max. d'alertes**.
   La liste des alertes s'affiche en fonction de la valeur de filtre choisie.

Actualiser une liste d'alertes

Pour actualiser la liste des alertes :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.

3. Dans la barre d'outils Alerte, cliquez sur  pour actualiser la liste des alertes.
   Le panneau Liste des alertes est actualisé.

Gérer une alerte planifiée

Vous pouvez activer ou désactiver une alerte planifiée et afficher toutes les alertes planifiées.

Activer une alerte planifiée

Pour activer une alerte planifiée :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Cliquez sur View Schedule.
   L'onglet de la vue Afficher la planification des alertes s'affiche.
4. Dans le panneau **Liste des plannings des alertes**, sélectionnez la ou les alertes planifiées à activer.
5. Cliquez sur .
   Un message de confirmation s'affiche indiquant que l'état de l'alerte ou des alertes a été modifié et que l'alerte est maintenant disponible dans le panneau Liste des alertes.

Désactiver une alerte planifiée

Pour désactiver une alerte planifiée :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Cliquez sur View Schedule.
   L'onglet de la vue Afficher la planification des alertes s'affiche.
4. Dans le panneau **Liste des plannings des alertes**, sélectionnez la ou les alertes planifiées à désactiver.
5. Cliquez sur .
   Un message de confirmation s'affiche indiquant que l'état de l'alerte ou des alertes a été modifié et que l'alerte est maintenant disponible dans le panneau Liste des alertes.

Afficher toutes les alertes plannifiées

Pour afficher toutes les alertes planifiées :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.

2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans la barre d'outils **Alerte**, cliquez sur **Afficher le planning**.
   La vue Afficher la planification des alertes s'affiche et répertorie toutes les alertes planifiées.

Gérer un modèle d’alerte

Vous pouvez modifier ou supprimer un modèle d’alerte et afficher tous les modèles d’alerte.

Modifier un modèle d’alerte

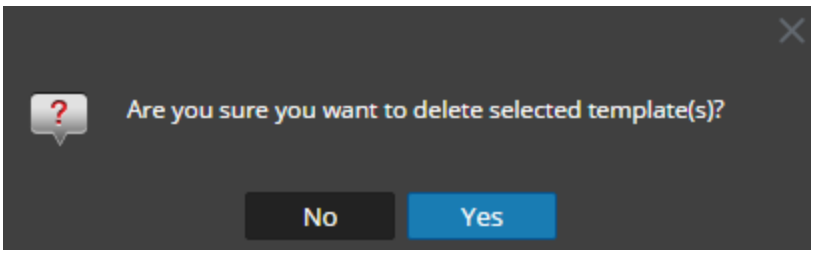
Pour modifier un modèle d’alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Cliquez sur Template.
   La vue Modèle s'affiche.
4. Dans le panneau **Liste des modèles**, sélectionnez un modèle et cliquez sur .
   La boîte de dialogue Créer/modifier un modèle s’affiche.
5. Cliquez sur **Enregistrer**.
   Un message de confirmation indiquant que le modèle a été modifié s'affiche.

Supprimer un modèle d'alerte

Pour supprimer un modèle d'alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Cliquez sur Template.
   L'onglet de la vue Modèle s'affiche.
4. Dans le panneau **Liste des modèles**, sélectionnez un modèle et cliquez sur .
   Une boîte de dialogue de confirmation s'affiche.



5. Cliquez sur **Oui** pour supprimer le modèle.
   Un message confirme la suppression du modèle.

Afficher tous les modèles d’alerte

Pour afficher tous les messages de modèle d’alerte :

1. Sélectionnez **Surveiller**> **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Alertes**.
   La vue Alerte s'affiche.
3. Dans la barre d'outils **Alerte**, cliquez sur **Modèle**.
   L'onglet de la vue Modèle s'affiche et répertorie tous les modèles.

Références de Reporting

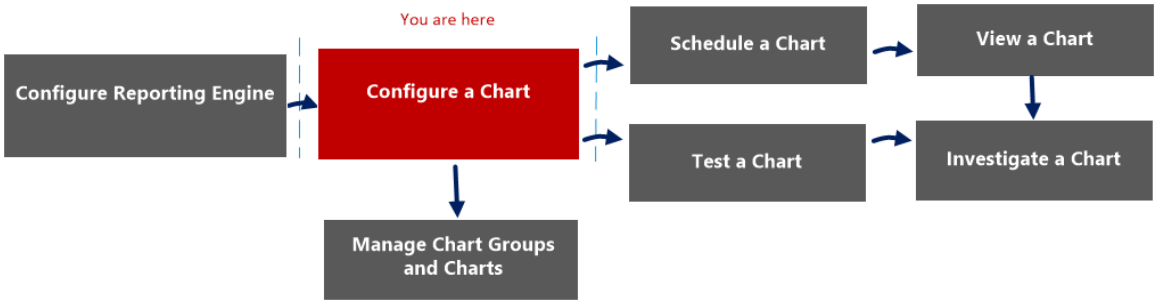
Cette rubrique fournit des informations sur l'interface utilisateur Reporting. Vous pouvez consulter votre place dans le workflow pour la création et la génération d'un rapport avec NetWitness Suite, obtenir un aperçu rapide des caractéristiques essentielles et suivre les liens vers les concepts détaillés et les procédures.

Vue Élaborer le graphique

Dans la vue Élaborer le graphique, vous pouvez définir et tester un graphique. Créez un graphique en lui attribuant un nom, puis en sélectionnant une règle à inclure.

Remarque : seules les règles de base de données NetWitness peuvent être utilisées dans les graphiques.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique*	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

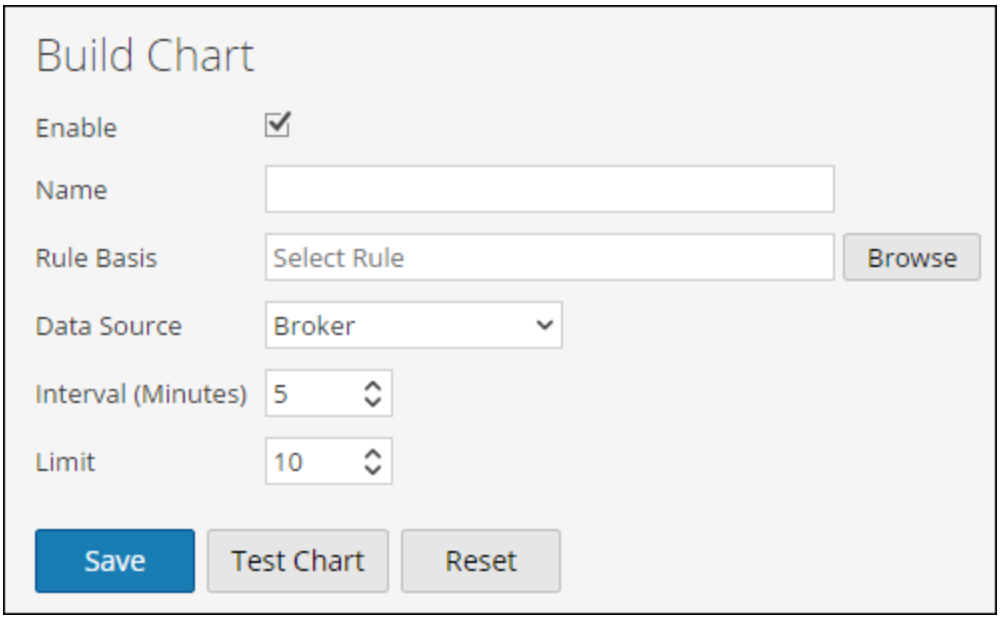
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique

Affichage rapide

La figure suivante donne un exemple de la vue Élaborer le graphique.



Le tableau suivant décrit les fonctions de la vue Élaborer le graphique.

Champ	Description
Activer	Spécifie si le Reporting Engine doit collecter les données et générer des résultats sous la forme d'un graphique. Si la case à cocher **Activer** n'est pas activée, les résultats ne s'affichent pas.
Nom du graphique	Identifie le nom du graphique.
Base de règle	Affiche la boîte de dialogue Ajouter des règles qui vous permet de sélectionner une règle servant de base à un graphique. La règle que vous sélectionnez ne doit pas être triée.

Champ	Description
Source de données	Si la source de données par défaut est configurée dans le Reporting Engine, la source de données s'affiche sur la page Élaborer le graphique. Si un graphique est configuré pour s'exécuter sur une autre source de données, celle-ci s'affiche dans la page Élaborer le graphique à la place de la source de données par défaut. Le module Reporting utilise les sources de données suivantes : • Broker • Concentrator • Decoder • Log Decoder • Log Collector
Intervalle (minutes)	Intervalle d'actualisation des données du graphique en minutes.
Limite	Nombre d'enregistrements pour lesquels un graphique est généré.
Enregistrer	Enregistre un graphique dans la base de données.
Tester le graphique	Trace un graphique de test sur la base de la définition du graphique.
Réinitialiser	Réinitialise les détails du graphique.

Vue Créer la liste

Dans la vue Créer la liste, vous pouvez saisir ou importer des valeurs pour créer une liste et enregistrer ou réinitialiser ces valeurs. Vous pouvez utiliser les listes lorsque vous écrivez les règles de reporting afin de simplifier le processus de spécification des valeurs dans la règle.

Workflow

Ce workflow présente la procédure à suivre pour définir des listes ou des groupes de listes. Vous pouvez définir un contrôle d'accès au niveau de la liste ou du groupe de listes afin que seuls les utilisateurs dotés des rôles spécifiques puissent accéder aux listes.

Vous devez vous assurer que le Reporting Engine est configuré sur NetWitness Suite.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle*	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

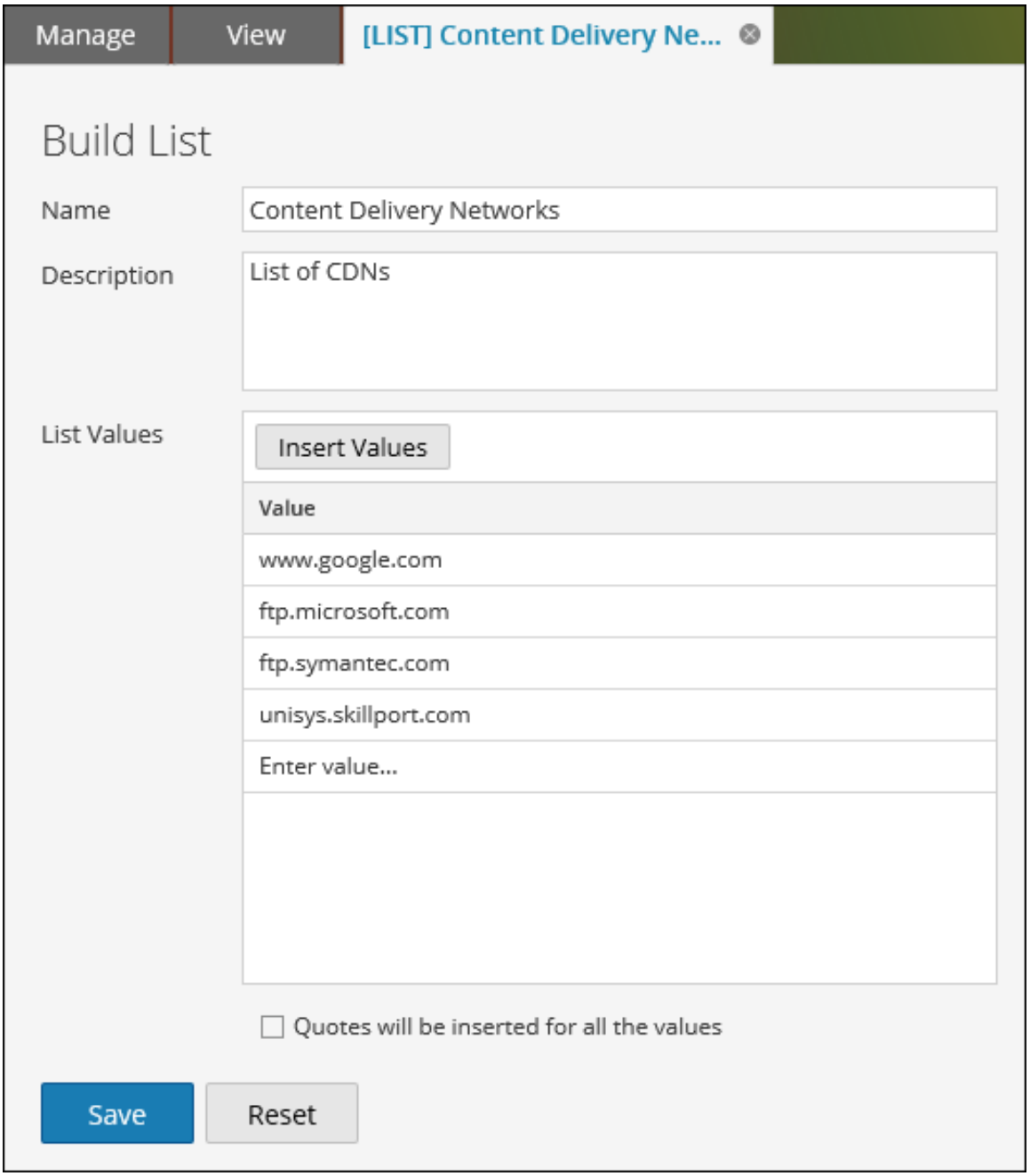
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Vue Liste
- Boîte de dialogue Autorisations des listes

Affichage rapide

La figure ci-dessous illustre la vue Créer la liste.



Pour accéder à cette vue

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Cliquez sur **Listes**.

   La vue Listes s'affiche.

3. Dans la barre d'outils **Listes**, cliquez sur + .

   L'onglet Créer la liste s'affiche.

Le tableau suivant décrit les fonctions de la vue Créer la liste.

Fonction	Description
Nom	Identifie la liste et lui attribue un libellé.
Description	Fournit une brève description de la liste.
Valeurs de la liste	Fournit la grille de valeurs associées à la liste sélectionnée issue du panneau Bibliothèque de liste. Vous pouvez importer ces valeurs à partir d'un fichier ou d'une liste. Vous pouvez également saisir les valeurs manuellement.
Des guillemets seront insérés pour toutes les valeurs	Inclut automatiquement des guillemets pour les valeurs au moment de l'exécution, si cette case est cochée. Si la case n'est pas cochée et que la liste contient une valeur qui comporte une virgule, cette valeur doit être placée entre apostrophes. Chaque valeur de liste d'une règle IPDB doit être placée entre apostrophes. Cette syntaxe ne s'applique pas aux valeurs de liste d'une règle NWDB.
Enregistrer	Enregistre la règle qui permet de créer un rapport, un graphique ou une alerte.
Réinitialiser	Cette option supprime toutes les informations contenues dans les champs.

Vue Élaborer le rapport

Dans la vue Élaborer le rapport, vous pouvez créer un rapport, ajouter du texte et des règles et planifier un rapport.

Workflow

Ce workflow présente la procédure à suivre pour créer et planifier un rapport.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport*	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

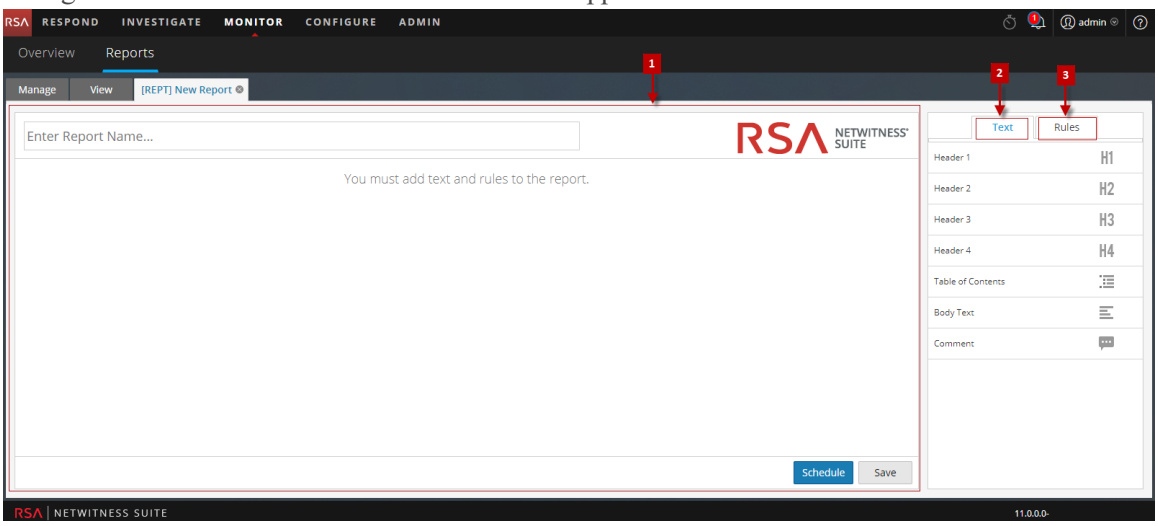
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Rapport
- Vue Rapports planifiés
- Boîte de dialogue Autorisations des rapports

Affichage rapide

La figure ci-dessous illustre la vue Élaborer le rapport.



Pour accéder à cette vue

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Cliquez sur **Rapports**.

   La vue Rapports s'affiche.

3. Dans la barre d'outils **Rapports**, cliquez sur + .

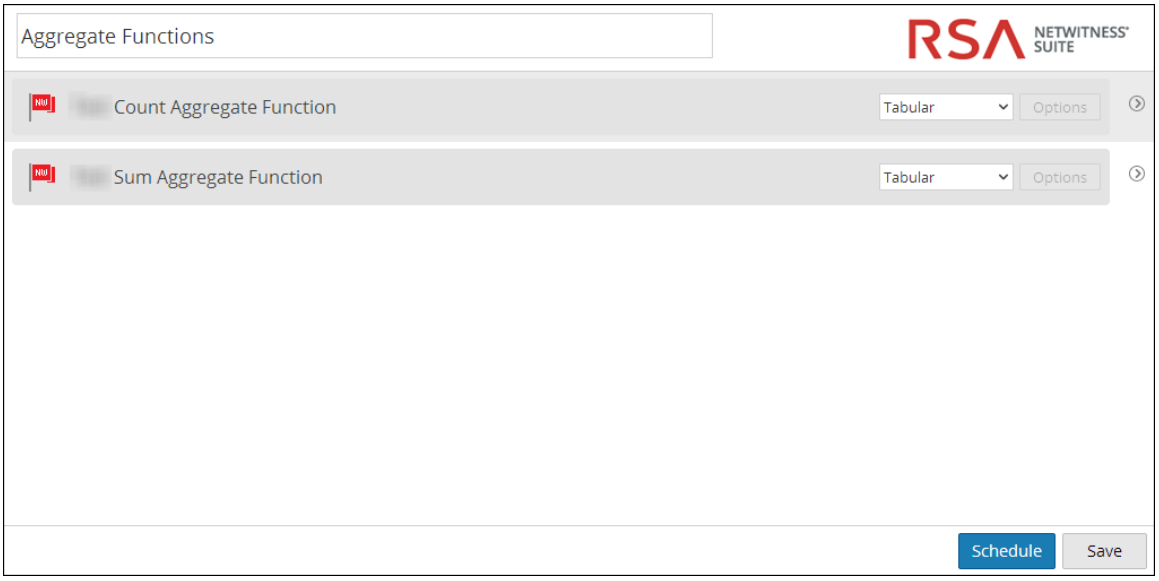
   L'onglet de la vue Élaborer le rapport s'affiche.

La vue Élaborer le rapport se compose des panneaux suivants :

1	Panneau Rapport
2	Panneau Texte
3	Panneau Règles

Panneau Rapport

Le panneau Rapport vous permet de créer un rapport en attribuant un nom au rapport. Le contenu d'un rapport dépend des éléments sélectionnés à partir des panneaux Texte et Règles.



Lorsque vous ajoutez des règles à un rapport, vous pouvez choisir différents formats de sortie pour ces règles : tabulaire, zone, ligne ou circulaire, en cliquant sur le bouton ⌄.

Le tableau suivant affiche les fonctions du panneau Rapport et leur description.

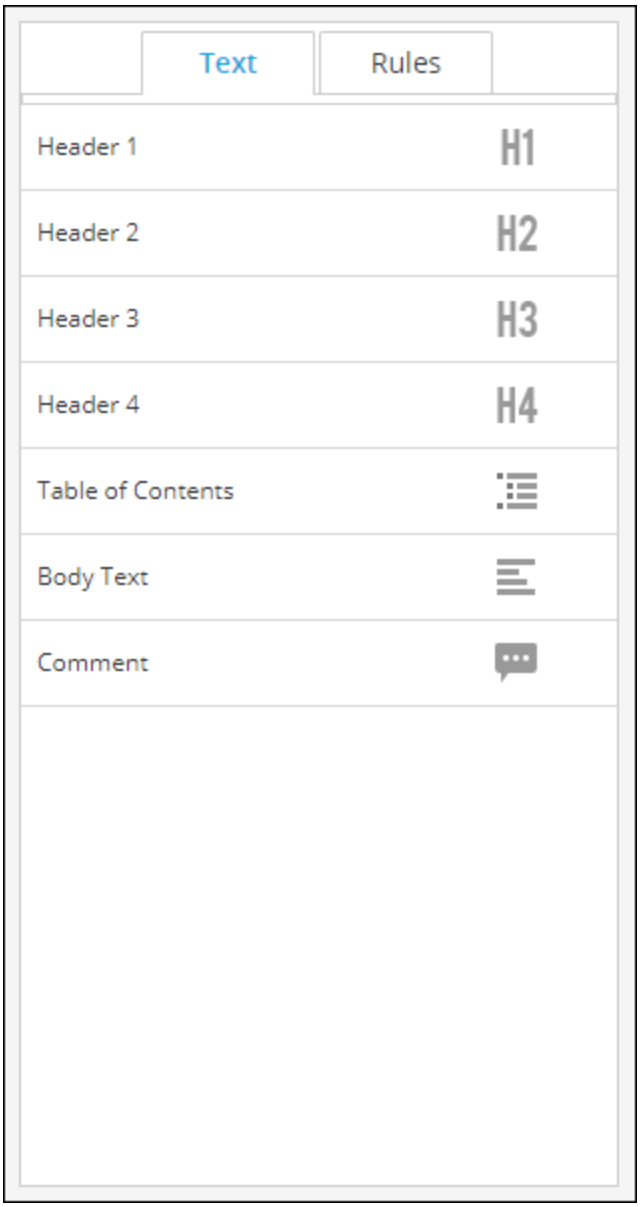
Fonction	Description
Nom	Ce champ vous permet de saisir le nom du rapport.

Fonction	Description
Options	Ce champ vous permet de sélectionner le format de sortie du rapport : Tabulaire, Zone, Barre, Bulle, Colonne, Linéaire, Sectoriel, Ligne d'escalier, Zone d'escalier, Zone de spline et Spline.
Planning	Cliquer sur cette option permet de générer le rapport.
Enregistrer	Cliquer sur cette option permet d'enregistrer le rapport.

Panneau Texte

Le panneau Texte se compose d'une liste d'éléments de texte qui améliorent l'aspect et les fonctionnalités du rapport. Vous pouvez utiliser ces éléments de texte pour mettre en forme le rapport.

- Pour ajouter plus de structure aux rapports, vous pouvez utiliser les en-têtes définis dans le panneau Texte pour appliquer un retrait jusqu'à quatre niveaux. Cela vous permet d'identifier des sections spécifiques dans un rapport, pouvant être incluses dans la Table des matières pour vous permettre de parcourir facilement aux résultats du rapport.
- Pour ajouter des en-têtes dans le panneau Rapport, faites glisser H1, H2, H3, ou H4 sur le volet Rapport, d'après le niveau de mise en retrait souhaité



Le tableau suivant répertorie les éléments de texte utilisés pour mettre en forme un rapport :

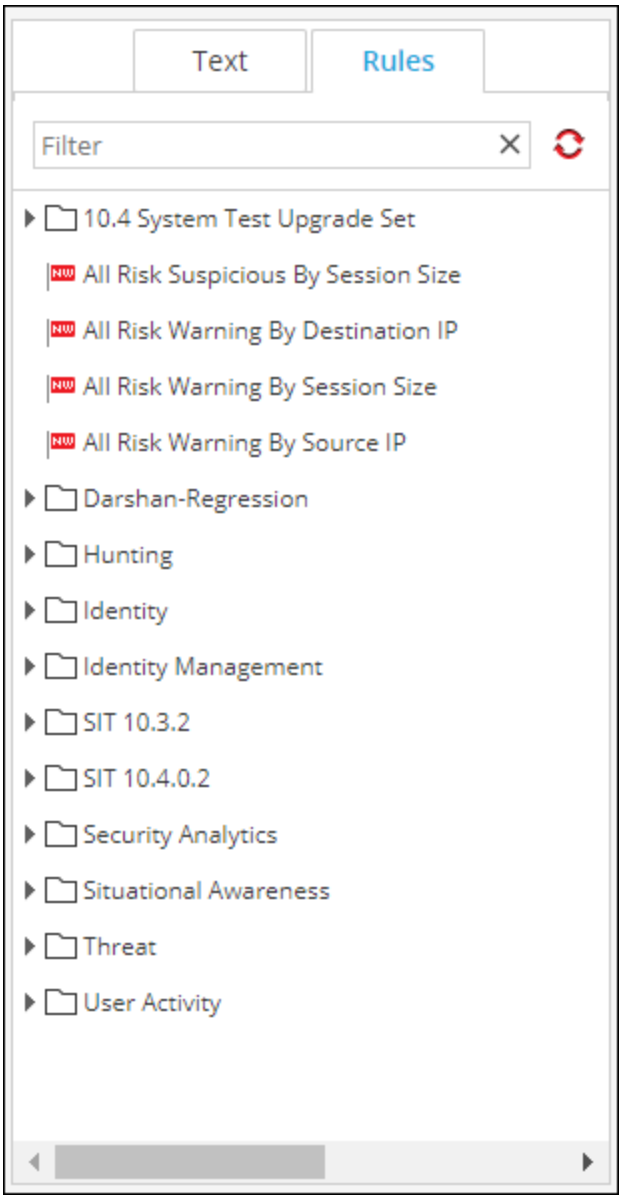
Éléments de texte	Description
Titre 1 H1	L'élément Titre 1 ajoute un en-tête de premier niveau à la définition du rapport.
Titre 2 H2	L'élément Titre 2 ajoute un en-tête de deuxième niveau à la définition du rapport.

Éléments de texte	Description
Titre 3 	L'élément Titre 3 ajoute un en-tête de troisième niveau à la définition du rapport.
Titre 4 	L'élément Titre 4 ajoute un en-tête de quatrième niveau à la définition du rapport.
Table des matières 	La Table des matières ajoute cet élément à la définition du rapport.
Corps du texte 	Le Corps du texte ajoute cet élément à la définition du rapport.
Commentaire 	L'élément Commentaire ajoute des commentaires dans la définition de rapport. **Remarque :** l'élément Commentaire n'est pas visible lorsque vous affichez tous les rapports.

Panneau Règles

Le panneau Règles se compose d'une liste de règles définies dans Règles. Dans la liste de règles, vous pouvez faire glisser des règles sur le panneau Rapport pour les associer au rapport.

Vous pouvez rechercher une règle spécifique à l'aide de la zone de texte de recherche fournie dans le panneau Règles.


Text
Rules
Filter
10.4 System Test Upgrade Set
All Risk Suspicious By Session Size
All Risk Warning By Destination IP
All Risk Warning By Session Size
All Risk Warning By Source IP
Darshan-Regression
Hunting
Identity
Identity Management
SIT 10.3.2
SIT 10.4.0.2
Security Analytics
Situational Awareness
Threat
User Activity

Vue Élaborer une règle

La vue Élaborer une règle explique les actions et les procédures associées que vous pouvez exécuter sous Règles.

Workflow

Ce workflow présente la procédure à suivre pour créer ou déployer une règle.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle*	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

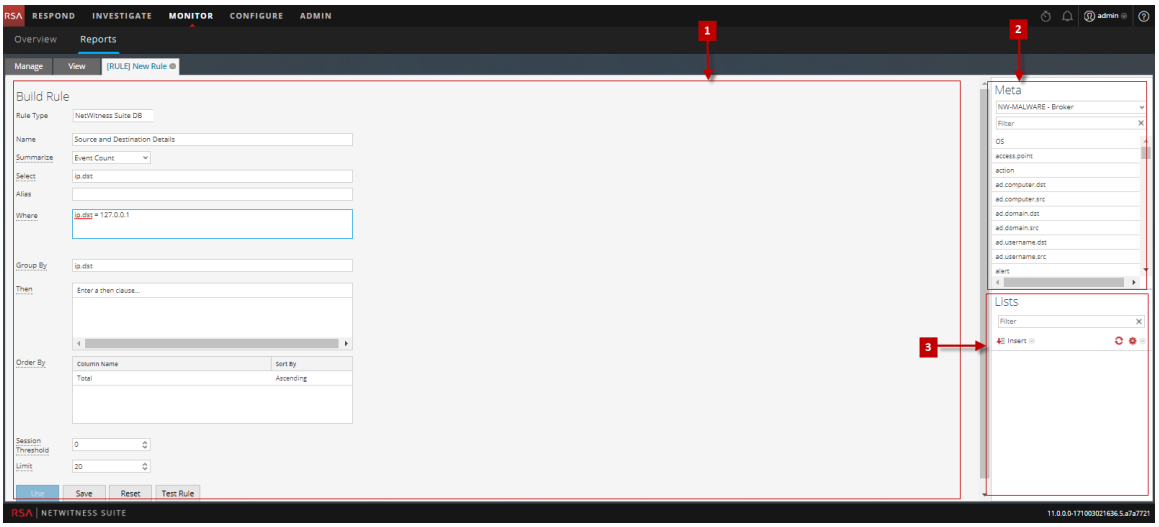
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Boîte de dialogue Autorisations des règles
- Vue Règle

Affichage rapide



Pour accéder à la vue Élaborer une règle :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans la barre d'outils Règle, cliquez sur + > **NetWitnessDB**.
   L'onglet de la vue Élaborer une règle s'affiche

Fonctions

La vue Élaborer une règle comprend les panneaux suivants :

1 Panneau Règle

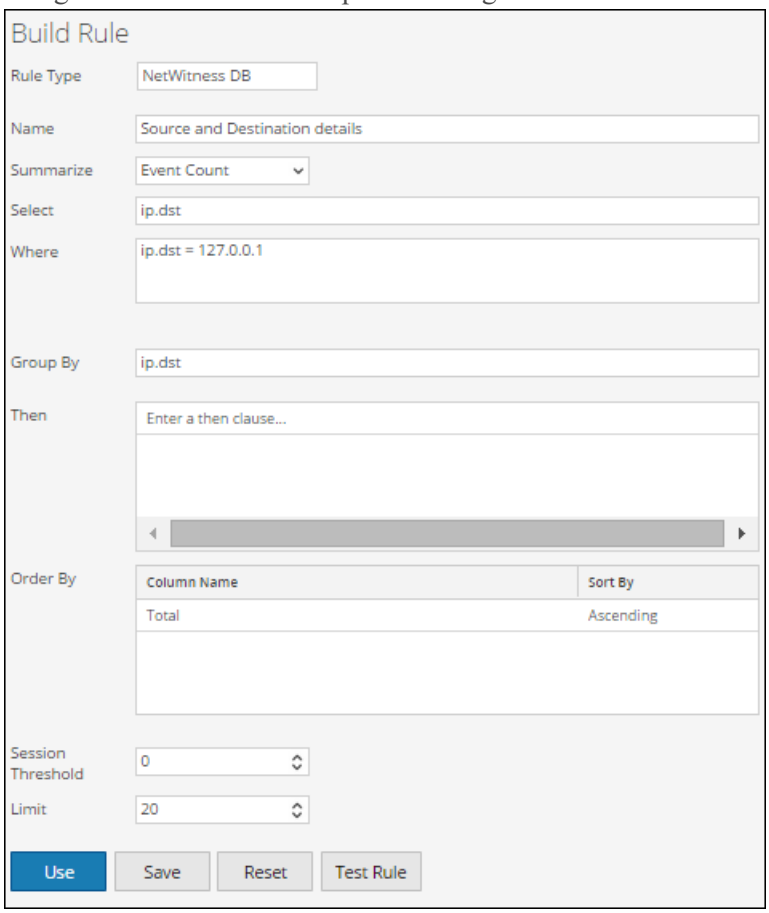
2 Panneau Métadonnées

3 Panneau Listes

Panneau Règle

Le panneau Règle vous permet de créer une règle pour le type de base de données sélectionné.

La figure suivante affiche le panneau Règle.



Le tableau suivant décrit les fonctions du panneau Règle.

Fonction	Description
Type de règle	Liste déroulante des types de bases de données pris en charge pour lesquels vous pouvez créer des règles. Les options sont les suivantes : Bases de données NetWitness, IPDB et Warehouse.
Nom	Nom de la règle que vous créez ou modifiez.

Fonction	Description
Résumé	Liste déroulante des options de résumé. Les options sont les suivantes : Aucun, Décompte d'événements, Nombre de paquets, Nombre de sessions et Personnalisé.
Sélectionner	Clé méta pour laquelle vous avez besoin des valeurs agrégées, par exemple, ip.dest.
Où	Clause Où qui définit les conditions qui déclenchent l'exécution de la règle, par exemple, ip.dest = 127.0.0.1.
Regrouper par	Méthode de regroupement des résultats. Par exemple, spécifier ip.dest permet de produire un rapport dans lequel les valeurs ip.dest sont regroupées.
Then	Clause Then qui définit les actions des règles pour un traitement supplémentaire sur la sortie.
Réorganiser par	Méthode de séquençage utilisée pour afficher les résultats. Par exemple, spécifier Regrouper par la valeur de la colonne Total, Croissant, produit un rapport dans lequel les résultats sont triés par ordre croissant en fonction de la valeur contenue dans la colonne Total.
Seuil de session	Liste de sélection du seuil de session, qui spécifie le nombre maximum de sessions devant être traitées pour les fonctions d'agrégation.
Limite	Liste de sélection du nombre maximum de lignes de résultats à extraire.
Utilisation	Cliquer sur Utiliser vous permet d'utiliser la règle pour générer un rapport, une alerte de graphique.
Enregistrer	Cliquer sur Enregistrer permet d'enregistrer la règle que vous modifiez ; le panneau Élaborer une règle reste ouvert. Avant de tester une règle, vous devez l'enregistrer si vous souhaitez conserver vos modifications.
Réinitialiser	Cliquer sur Réinitialiser permet d'effacer toutes les informations contenues dans un champ.

Fonction	Description
Tester la règle	Permet d'ouvrir la boîte de dialogue Tester la règle.

Boîte de dialogue Tester la règle

Pour accéder à la vue Tester la règle :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau Liste de règles, exécutez l'une des opérations suivantes :
   - Sélectionnez une règle, puis cliquez sur dans la barre d'outils Règles.
   - Cliquez sur > **Modifier**.
     L'onglet de la vue Élaborer une règle s'affiche.
3. Cliquez sur **Tester la règle**.
   La vue Tester la règle s'affiche.

Le tableau suivant décrit les fonctions de la boîte de dialogue Tester la règle.

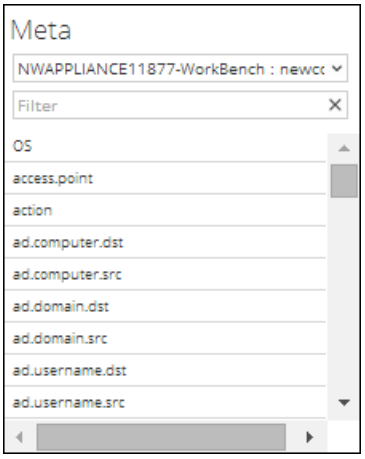
Fonction	Description
Source de données	Liste déroulante des sources de données pour le type de règle que vous testez. Les sources de données possibles sont les suivantes : Concentrator, Broker, Decoder ou Log Decoder.
Format	Liste déroulante des formats d'affichage des résultats d'une règle. Les formats possibles sont les suivants : Tabulaire, Zone, Barre, Bulle, Colonne, Linéaire, Sectoriel, Ligne d'escalier, Zone d'escalier, Zone de spline et Spline.
Période	Liste déroulante des méthodes de spécification d'une période. • Sélectionner Derniers/Dernières vous permet de spécifier un nombre d'années, de mois, de jours, de semaines ou d'heures. Par exemple, Heures, jours, semaines, mois ou années. • Sélectionner Plage vous permet de spécifier une plage de dates et uen période. Par exemple, une date de début et une date de fin. Dans l'interface utilisateur, la date ou l'heure qui s'affiche dépend du profil de fuseau horaire sélectionné par l'utilisateur.
Utiliser le calcul de temps relatif	La sélection de cette option permet de calculer la période relative à l'heure actuelle.
Axe X	L'axe X et l'axe Y permettent de spécifier les métadonnées à tracer dans les graphiques. Dans la liste déroulante de l'axe X, les types de méta du paramètre `Group by` de la règle s'affichent. Vous pouvez sélectionner plusieurs types de méta lorsque la règle n'a qu'un seul `Group by` paramètre. Pour les règles personnalisées avec plusieurs valeurs `Group by`, vous pouvez sélectionner uniquement le premier type de méta pour l'axe X.

Fonction	Description
Axe Y	Dans la liste déroulante de l'axe Y, les fonctions agrégées utilisées dans la règle s'affichent. Sommes, Nombre, Countdistinct et Moyenne sont les fonctions agrégées prises en charge pour la règle. Vous pouvez sélectionner une ou plusieurs fonctions agrégées.
Exécuter le test	Cliquer sur Exécuter le test permet d'exécuter un test de la dernière règle enregistrée dans la boîte de dialogue Générateur de règles. Une fois le test terminé, les données de la règle (cas échéant) de la période sélectionnée s'affichent.

Panneau Métadonnées

Le panneau Métadonnées fournit la liste des types de métadonnées disponibles que vous pouvez utiliser pour créer une règle. Vous pouvez utiliser les types de métadonnées dans les clauses Select, Where et Then. Le Reporting Engine conserve une liste active des noms de métadonnées disponibles en effectuant une synchronisation continue avec la source de données à laquelle il est connecté.

La figure suivante affiche le panneau Métadonnées.



Le tableau suivant décrit les fonctions du panneau Métadonnées.

Opération	Description
Sélectionner	D'après le type de règle que vous avez sélectionné, les sources de données disponibles s'affichent dans la liste déroulante du panneau Métadonnées. Sélectionnez la source de données requise. Les types de méta disponibles pour la source de données s'affichent. Sélectionnez une métadonnée.

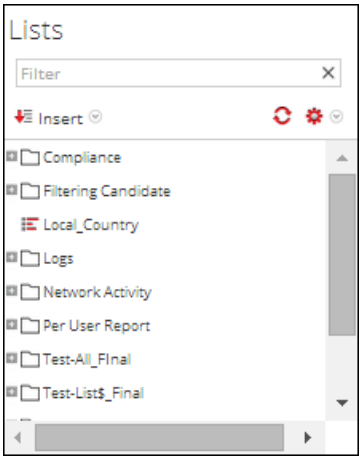
Opération	Description
Filtre	Filtrez la métadonnée selon une valeur spécifique.

Panneau Listes

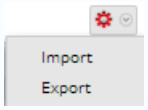
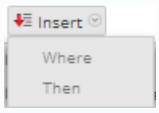
Une Liste est un espace réservé destiné à un ensemble de valeurs que vous pouvez utiliser dans une métadonnée ou une variable. Par exemple, vous pouvez définir une liste avec toutes les adresses IP de source d'événements sur liste blanche. Une fois la Liste définie, vous pouvez utiliser le Nom de la liste dans la règle. Ceci offre la flexibilité d'ajouter, de modifier et de supprimer les valeurs de liste.

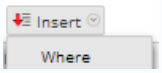
Le panneau Listes présente une collection de Listes. Le Reporting Engine conserve une liste active des noms de listes disponibles en effectuant une synchronisation continue avec la collection à laquelle il est connecté.

La figure suivante affiche le panneau Listes.



Le tableau suivant décrit les fonctions du panneau Listes.

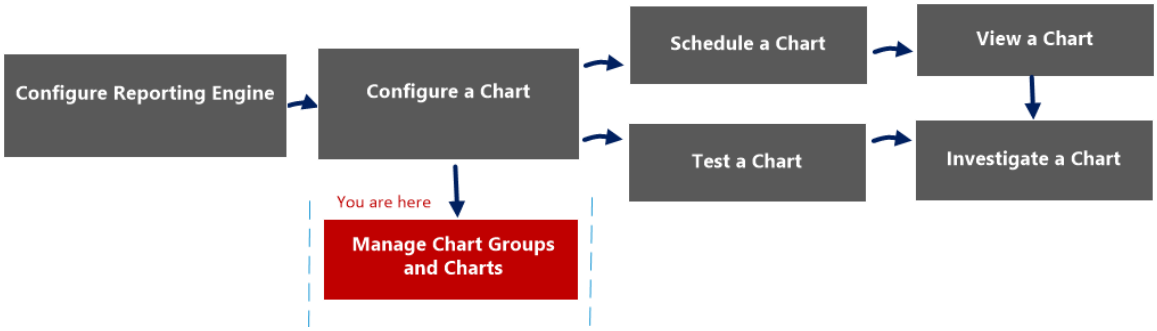
Opération	Description
	Importer ou exporter une liste.
	Actualiser des listes.
	Si vous sélectionnez le type de règle **Base de données NetWitness**, les options Where et Then s'affichent. Insérez la liste dans la clause Where ou Then dans la règle.

Opération	Description
	Si vous sélectionnez le type de règle **Base de données Warehouse**, l'option Where s'affiche. Insérez la liste dans la clause Where dans la règle.

Boîte de dialogue Autorisations des graphiques

Dans la boîte de dialogue Autorisations des graphiques, vous pouvez gérer les autorisations d'accès pour les rôles d'utilisateur au niveau du graphique et du groupe de graphiques. Seul un utilisateur détenant l'autorisation Lecture/écriture peut configurer le graphique dans le module Reporting.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique*	Gérer un groupe de graphiques et un graphique

*Vous pouvez effectuer ces tâches ici.

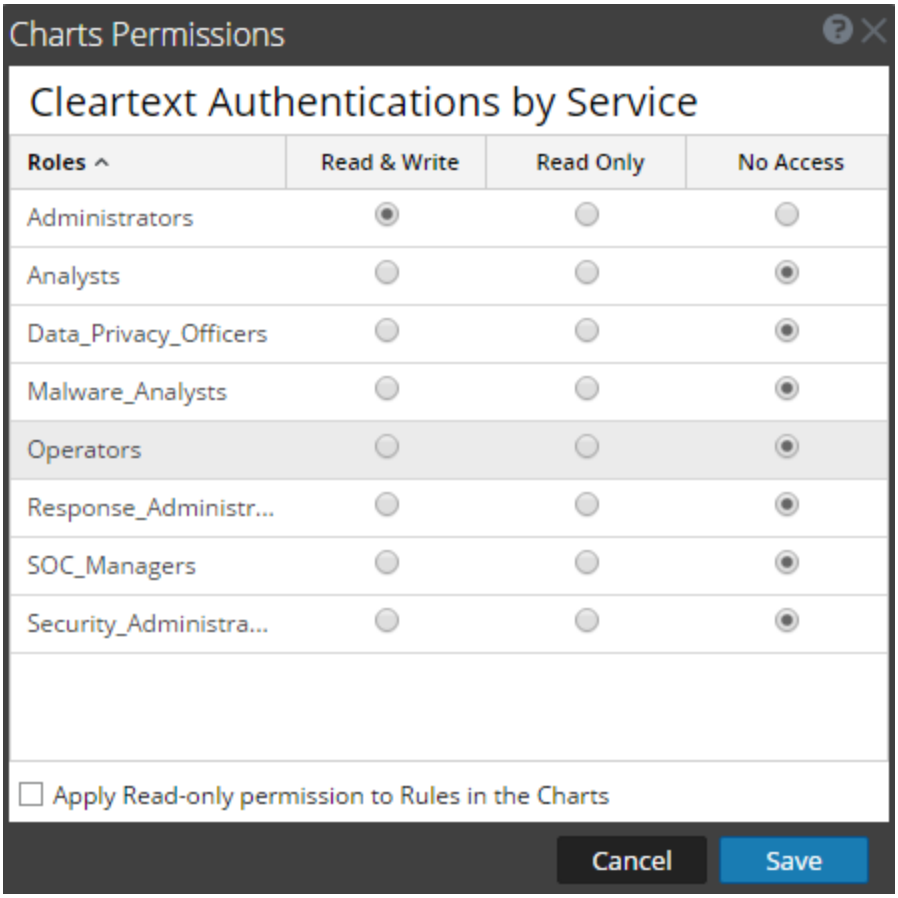
Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique
- Afficher un graphique
- Tester un graphique
- Analyser un graphique
- Gérer un groupe de graphiques et un graphique

Affichage rapide

La boîte de dialogue Autorisations des graphiques vous permet de définir des autorisations de graphique en fonction du rôle d'utilisateur.

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



1. Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Graphiques** pour afficher la vue Graphique.

3. Dans le panneau **Liste des graphiques**, sélectionnez un rapport et cliquez sur > **Autorisations**. La boîte de dialogue Autorisations des graphiques s'affiche.
4. En fonction du rôle d'utilisateur, sélectionnez les options appropriées.
5. (Facultatif) Pour accorder automatiquement l'autorisation d'accès en lecture aux règles dépendantes, activez la case à cocher.
6. Cliquez sur **Enregistrer**.

Le tableau suivant répertorie les colonnes de la boîte de dialogue Autorisations des graphiques.

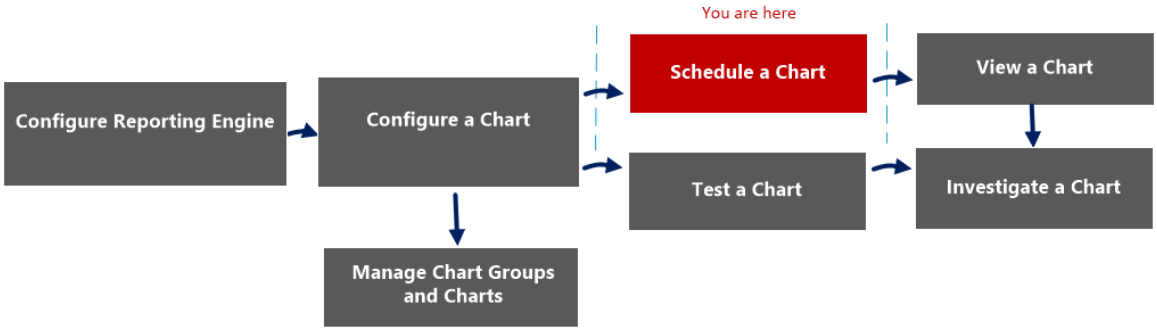
Colonne	Description
Rôles	Affiche tous les rôles d'utilisateur dans l'interface utilisateur de NetWitness.
Lecture et écriture	Vous permet d'appliquer l'accès en lecture/écriture au graphique.
Lecture seule	Vous permet d'appliquer uniquement l'accès en lecture au graphique.
Aucun accès	En sélectionnant cette autorisation, vous ne pouvez pas accéder au graphique ou l'afficher.
☐Appliquer ces autorisations aux sous-groupes et graphiques dans ce groupe	Vous permet d'appliquer les autorisations au groupe de graphiques, aux sous-groupes dans le groupe et aux graphiques dans le groupe. **Remarque :** cette case à cocher n'apparaît que lorsque vous définissez les autorisations d'accès pour un groupe de graphiques.
☐Appliquer l'autorisation de lecture seule aux règles des graphiques	Vous permet d'appliquer automatiquement des autorisations aux règles dans les graphiques.
Annuler	Annule toutes les modifications appliquées aux autorisations.

Colonne	Description
Enregistrer	Enregistre la sélection et fournit un accès aux rôles en fonction de la sélection.

Vue Graphique

Dans la vue Graphique, vous pouvez voir les graphiques et groupes disponibles dans une grille, et les planifier en activant les graphiques.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique*	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

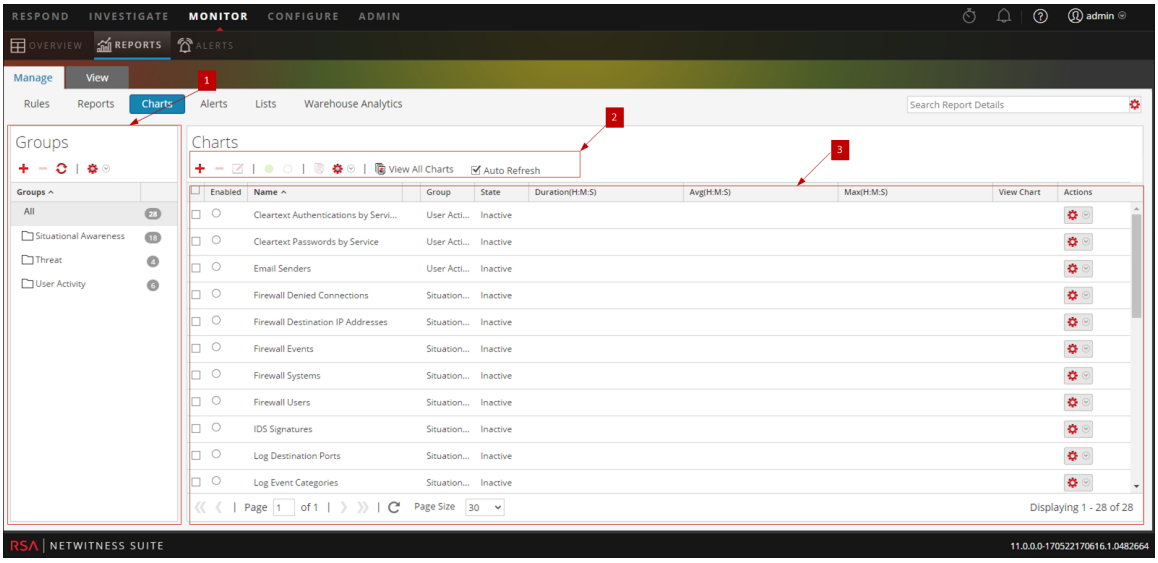
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.

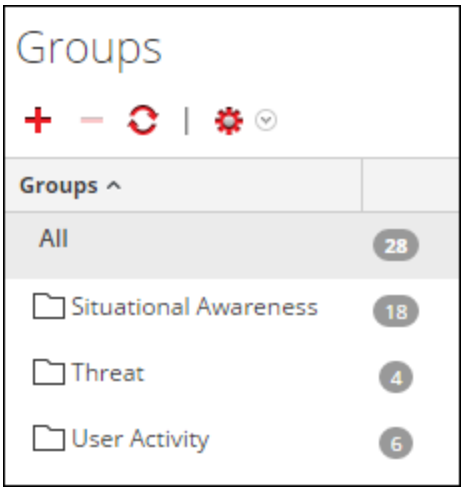


La vue Graphique inclut les panneaux suivants :

1	Panneau Groupes de graphiques
2	Barre d'outils Graphique
3	Panneau Vue Graphique

Panneau Groupes de graphiques

Ce panneau vous permet d'organiser les graphiques au sein d'un groupe. Vous pouvez créer un groupe, ajouter des graphiques au groupe et déplacer des graphiques entre groupes. La figure suivante illustre le panneau Groupe de graphiques.



Le panneau Groupes de graphiques comprend les options suivantes :

Fonction	Description
+	Ajoute un nouveau graphique au module Reporting.
−	Supprime un ou plusieurs graphiques sélectionnés.
	Modifie un graphique.
	Actualise la vue.
	Fournit les informations suivantes : Importer, Exporter et Autorisations.

Barre d'outils Graphique

La barre d'outils Graphiques vous permet d'ajouter, de modifier, de supprimer, de dupliquer, d'activer et de désactiver, d'importer et d'exporter un graphique. Vous pouvez également définir des autorisations d'accès aux graphiques inclus dans un groupe.

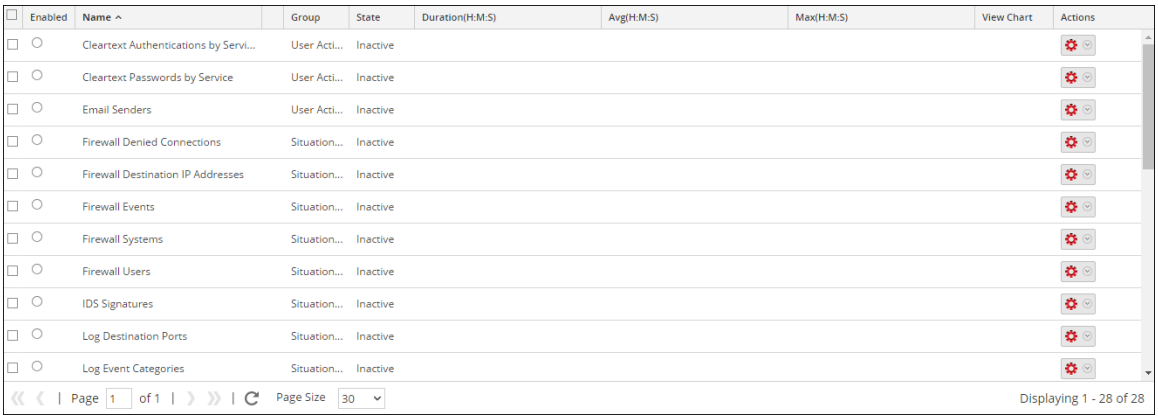
La barre d'outils Graphique comprend les options suivantes :

Fonction	Description
+	Ajoute un nouveau graphique au module Reporting.
−	Supprime un ou plusieurs graphiques sélectionnés.

Fonction	Description
	Modifie des graphiques.
	Active les graphiques sélectionnés.
	Désactive les graphiques sélectionnés.
	Crée une double instance du graphique sélectionné.
	Fournit les informations suivantes : Importer, Exporter, Exporter en tant que texte et Autorisations.
Afficher tous les graphiques	Affiche tous les graphiques exécutés.
Actualisation automatique	Actualise automatiquement la liste des graphiques.

Panneau Vue Graphique

Le panneau Vue Graphique présente tous les graphiques sous la forme d'un tableau ou d'une grille.



Le tableau suivant répertorie les colonnes du panneau Vue Graphique et leur description.

Fonction	Description
Activé	- Le graphique est activé. - Le graphique est désactivé.
Nom	Nom du graphique.

Fonction	Description
Groupe	Groupe auquel appartient le graphique.
État	État du graphique : • En attente • Terminé • Échec
Durée (H:M:S)	Durée d'exécution du dernier graphique.
Moy (H:M:S)	Durée moyenne nécessaire à l'exécution du graphique.
Max (H:M:S)	Durée maximale de l'exécution du graphique.
Afficher le graphique	Lien hypertexte qui renvoie au panneau Afficher un graphique.
	Le menu Actions comprend les options suivantes : Activer, Désactiver, Afficher, Supprimer, Modifier et Exporter.

Panneau Historique d'exécution

Le panneau Historique d'exécution vous permet de récupérer et d'afficher les détails de l'historique.

Workflow

Ce workflow présente la procédure à suivre pour afficher un rapport ou un groupe de rapports.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports*	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

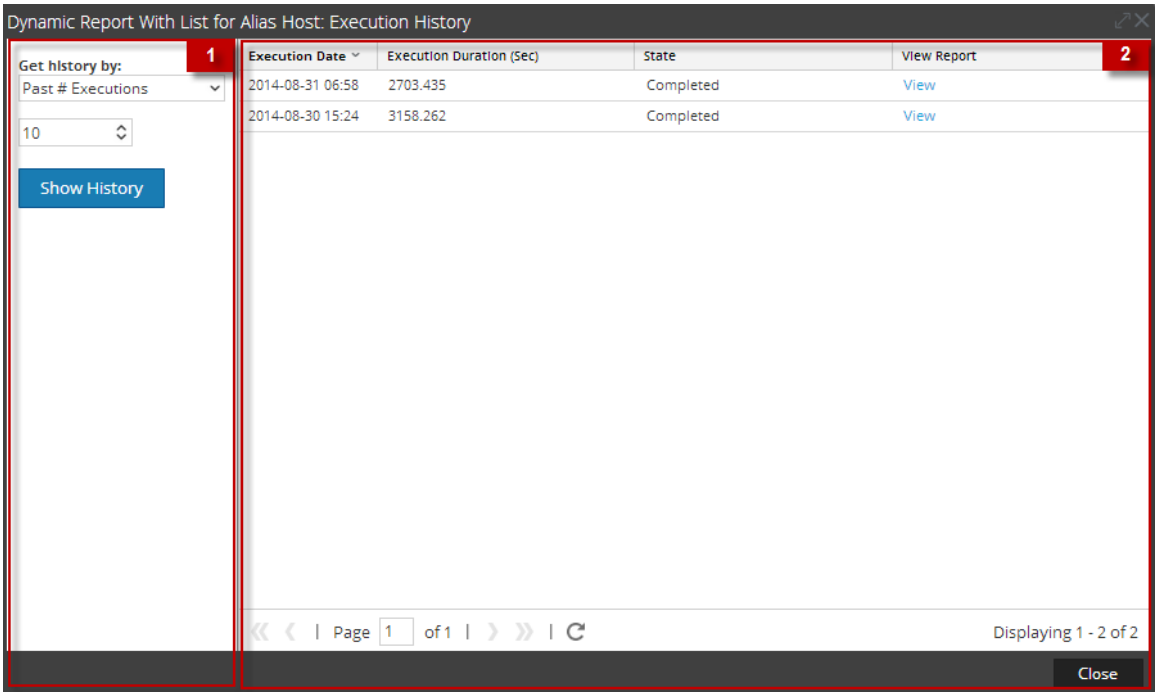
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Panneau Générer une liste
- Vue Rapports planifiés

Affichage rapide

La figure suivante donne un exemple de la vue Historique d'exécution.



Fonctions

La vue Afficher l'historique d'exécution contient les panneaux suivants :

1. Panneau Options de l'historique d'exécution
2. Panneau Sortie Historique d'exécution

Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau Liste de règles, exécutez l'une des opérations suivantes :
   - Placez le pointeur de la souris sur un rapport, puis cliquez sur  > **Afficher les rapports programmés**.
   - Cliquez sur la colonne **#Schedules**.
     La vue Planifier un rapports affiche l'état de chaque rapport planifié.
3. Sélectionnez un rapport planifié et procédez de l'une des manières suivantes :
   - Cliquez sur  > **Historique d'exécution**.
   - Cliquez sur  dans le panneau Barre d'outils Rapports planifiés.

Panneau Options de l'historique d'exécution

Le panneau Options de l'historique d'exécution vous permet d'extraire les détails de l'historique en fonction des n (nombre) derniers rapports planifiés ou d'une période spécifique.

Le tableau suivant affiche les opérations du panneau Options de l'historique d'exécution :

Opération	Description
Obtenir l'historique par :	Il s'agit des critères permettant d'afficher l'historique d'exécution : • **Nombre d'exécutions passées** : n derniers rapports planifiés Cette option est affichée par défaut. • **Plage (spécifique)** : Date de début et date de fin composant la période. **Remarque :** les champs **De** et **À** sont renseignés dans l'interface utilisateur de NetWitness Suite uniquement si vous sélectionnez « Plage (spécifique) » dans la liste **Obtenir l'historique par**.
De	Date de début de la période.
À	Date de fin de la période.
Nombre	Nombre d'historiques d'exécution dans le rapport planifié à afficher.
Show History	Affiche les détails de l'historique en fonction des critères sélectionnés.

Panneau Sortie Historique d'exécution

Le panneau Sortie Historique d'exécution affiche les détails de l'historique avec la date d'exécution, la durée d'exécution (secondes), l'état du rapport planifié et un lien permettant de visualiser le rapport.

Le tableau suivant répertorie les différentes colonnes du panneau Sortie Historique d'exécution :

Colonne	Description
Date d'exécution	Date à laquelle le rapport planifié a été exécuté. Par défaut, les dates d'exécution s'affichent dans l'ordre décroissant.
Durée d'exécution (sec)	Temps pris pour exécuter le rapport planifié.

Colonne	Description
État	État du rapport planifié : • Planifié : Si un rapport est planifié pour s'exécuter sur une base horaire, journalière, hebdomadaire, mensuelle ou ultérieurement, l'état du rapport est considéré comme étant planifié, pour la première exécution. • En attente : Si un rapport est toujours en attente d'exécution, l'état du rapport est considéré comme étant en file d'attente. • En cours d'exécution : si la planification du rapport est en cours de progression, l'état du rapport est considéré comme étant en cours d'exécution. • Partiel : Dans un rapport avec plusieurs règles, si l'exécution d'une seule règle échoue ou qu'une action de sortie échoue, ou encore que la création d'un fichier PDF/CSV échoue, l'état du rapport est considéré comme étant partiel. Par exemple, dans un rapport avec cinq règles dont quatre sont exécutées avec succès et une échoue, l'état du rapport est considéré comme étant partiel. • Échec : Dans un rapport avec plusieurs règles, si toutes les exécutions de la planification de règles échoue, l'état du rapport est considéré comme étant un échec. • Terminé : Si la planification du rapport est parfaitement exécutée, l'état du rapport est considéré comme étant terminé. • Annulé : Lorsque la demande d'annulation est prise en compte, l'état du rapport est considéré comme étant annulé. • Inactif : Si la planification du rapport est désactivée, l'état du rapport est considéré comme étant inactif. • Indisponible : si les informations d'exécution liées à la planification des rapports ne sont pas disponibles, l'état du rapport est considéré comme étant indisponible.
Afficher le rapport	Lien hypertexte correspondant à Afficher un rapport en mode plein écran.
Fermer	Ferme la vue de l'historique d'exécution.

Panneau Générer une liste

La boîte de dialogue Générer une liste permet de générer une liste et de la personnaliser.

Workflow

Ce workflow présente la procédure à suivre pour créer et planifier un rapport.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport*	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

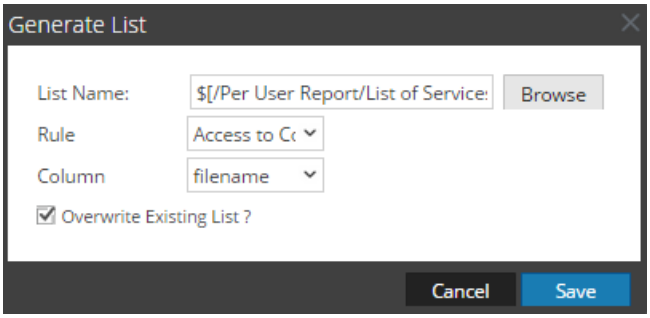
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Créer et planifier un rapport
- Gérer les listes, les règles ou les rapports
- Vue Liste
- Vue Créer la liste
- Boîte de dialogue Autorisations des listes

Affichage rapide

La figure suivante donne un exemple de la boîte de dialogue Générer une liste.



Pour accéder à cette vue :

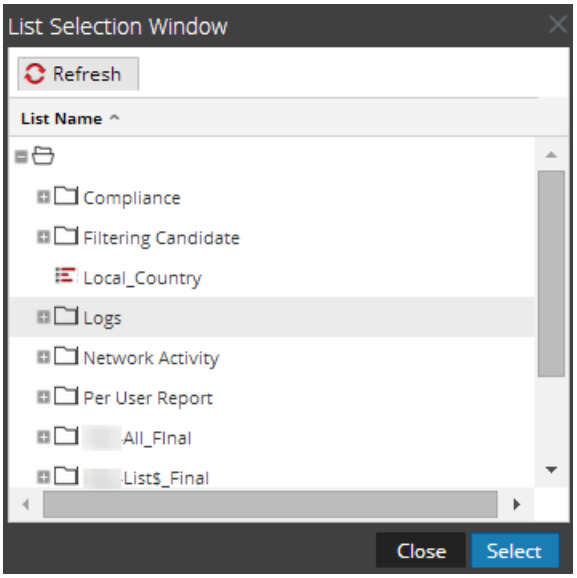
1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport et cliquez sur > **Planifier un rapport**.
   L'onglet de la vue Planifier un rapport s'affiche.
4. Dans le panneau **Liste dynamique**, cliquez sur .
   La boîte de dialogue Générer une liste s'affiche.

Fonctions

Le tableau suivant répertorie les fonctions de la boîte de dialogue Générer une liste.

Champ	Description
Nom de la liste	Nom de la liste choisie dans le panneau Sélection de listes
Parcourir	Cliquez sur ce bouton pour sélectionner une liste dans la boîte de dialogue Fenêtre de sélection de liste.
Règle	Sélectionnez une règle à utiliser pour créer la liste.
Colonne	Sélectionnez une valeur pour la colonne.
Remplacer la liste existante ?	Remplace la liste existante.
Enregistrer	Ajoute la liste voulue au panneau Générer une liste de la vue Planifier un rapport.

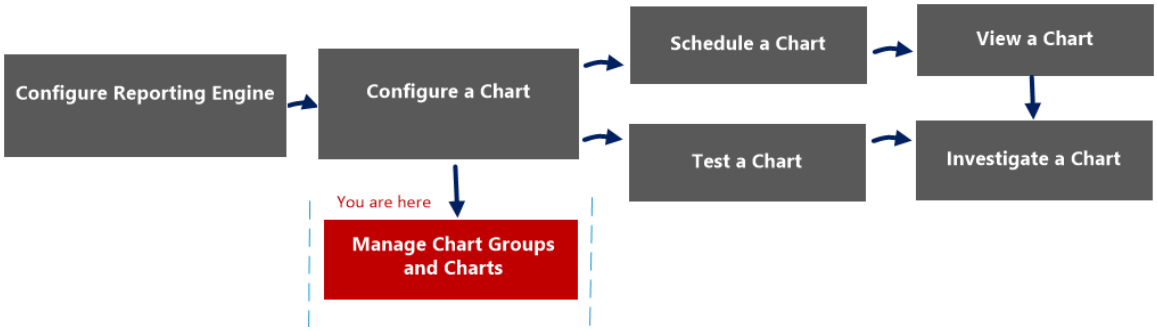
La boîte de dialogue Fenêtre de sélection de liste se compose de listes qui sont définies dans le panneau Listes. Vous pouvez y sélectionner une liste à associer au rapport. La figure suivante présente cette boîte de dialogue.



Boîte de dialogue Importer le graphique

Dans la boîte de dialogue Importer le graphique, vous pouvez importer des graphiques contenant des sous-groupes et graphiques issus d'autres instances de NetWitness dans le panneau Groupe de graphiques. Les graphiques doivent être dans un fichier binaire valide qui a été exporté à partir d'une autre instance de NetWitness.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique*	Gérer un groupe de graphiques et un graphique

*Vous pouvez effectuer ces tâches ici.

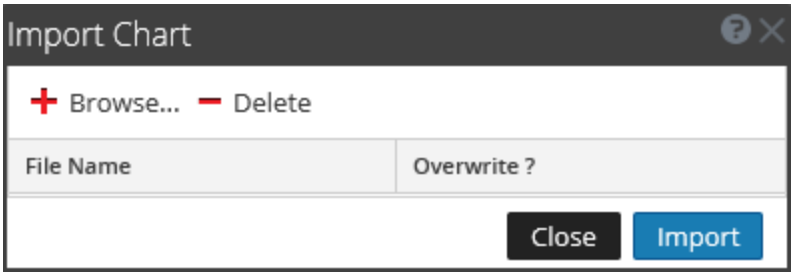
Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique
- Afficher un graphique
- Tester un graphique
- Analyser un graphique
- Gérer un groupe de graphiques et un graphique

Affichage rapide

Cette boîte de dialogue s'affiche différemment lorsque vous l'utilisez pour importer des groupes contenant des sous-groupes et des graphiques à partir d'autres instances de NetWitness dans le panneau Groupes de graphiques.

La figure suivante donne un exemple de la boîte de dialogue Importer le graphique.



1. Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Graphiques** pour afficher la vue Graphique.
3. Dans le panneau **Groupe de graphiques**, sélectionnez un dossier pour importer le fichier.
4. Dans le panneau Groupes de graphiques ou la barre d'outils Graphique, cliquez sur > **Importer** pour importer le fichier.

Le tableau suivant décrit les fonctionnalités de la boîte de dialogue Importer le graphique.

Fonction	Description
Parcourir	Affiche une vue du système de fichiers local pour que vous puissiez sélectionner le graphique à importer.
Supprimer	Supprime un rapport importé à partir de la liste des graphiques importés.

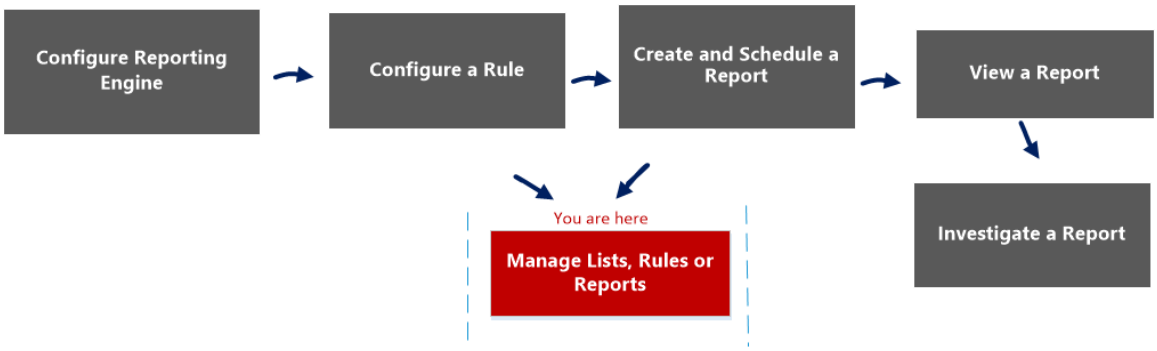
Fonction	Description
Nom de fichier	Affiche la liste des fichiers graphiques qui sont importés vers votre module Graphiques lorsque vous cliquez sur Importer.
Remplacer ?	Vous permet de sélectionner l'option pour remplacer une version existante du graphique que vous importez. Si vous ne sélectionnez pas l'option Remplacer, une copie du fichier est importée et aucun message d'erreur ne s'affiche.
Fermer	Ferme la boîte de dialogue. Si vous souhaitez sélectionner des graphiques à importer mais sans cliquer sur l'option Importer. Les graphiques ne sont pas importés et ne sont pas enregistrés dans cette boîte de dialogue.
Importer	Importe les graphiques sélectionnés vers le module Charts.

Boîte de dialogue Importer le rapport

Cette boîte de dialogue vous permet d'importer des groupes contenant des sous-groupes et des rapports d'autres instances de NetWitness Suite vers le panneau Groupes de rapports. Les rapports doivent figurer dans un fichier binaire valide qui a été exporté d'une autre instance de NetWitness Suite.

Workflow

Ce workflow présente la procédure à suivre pour gérer des rapports ou des groupes de rapports.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport

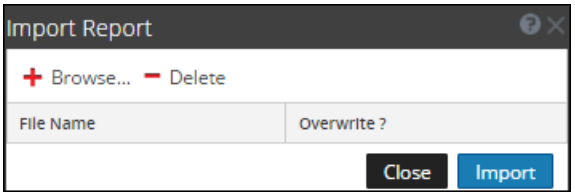
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Rapport
- Vue Élaborer le rapport
- Boîte de dialogue Autorisations des rapports

Affichage rapide



Pour accéder à la boîte de dialogue Importer le rapport :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Groupes de rapports**, sélectionnez un dossier pour importer le fichier.

4. Exécutez l'une des opérations suivantes :
   - Dans le panneau **Groupes de rapports**, cliquez sur  > **Importer** pour importer un groupe.
   - Dans la barre d'outils **Rapport**, cliquez sur  > **Importer** pour importer un rapport.

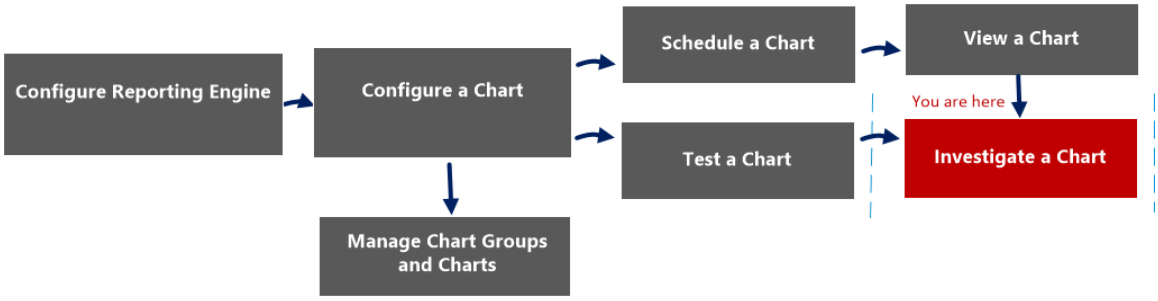
Le tableau suivant répertorie les fonctions de la boîte de dialogue Importer le rapport.

Fonction	Description
Parcourir	Cette option affiche une vue du système de fichiers local pour que vous puissiez sélectionner le rapport à importer.
Supprimer	Cette option supprime un rapport importé à partir de la liste des rapports importés.
Nom de fichier	Affiche la liste des fichiers de rapports qui sont importés vers votre module Rapports lorsque vous cliquez sur Importer.
Remplacer ?	Vous permet de sélectionner l'option pour remplacer une version existante du rapport que vous importez. Si vous ne sélectionnez pas l'option Remplacer, une copie du fichier est importé et aucun message d'erreur ne s'affiche.
Fermer	Cette option ferme la boîte de dialogue. Si vous sélectionnez un rapport et que vous ne cliquez pas sur Importer, les rapports ne sont pas importés et ne sont pas enregistrés dans cette boîte de dialogue.
Importer	Cette option importe les rapports sélectionnés vers le module Rapports.

Vue Analyser un graphique

Dans la vue Analyser un graphique, vous pouvez afficher et examiner les détails du graphique. Vous disposez de certaines options pour filtrer et trier les informations du graphique, ainsi que d'autres options pour définir le type du graphique, le nombre d'éléments à représenter, ainsi que les valeurs ou totaux du graphique. Lors de l'affichage d'un graphique, vous pouvez ouvrir les sessions de tracé de graphique dans le module Investigation, et enregistrer le graphique dans un fichier PDF.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique*	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

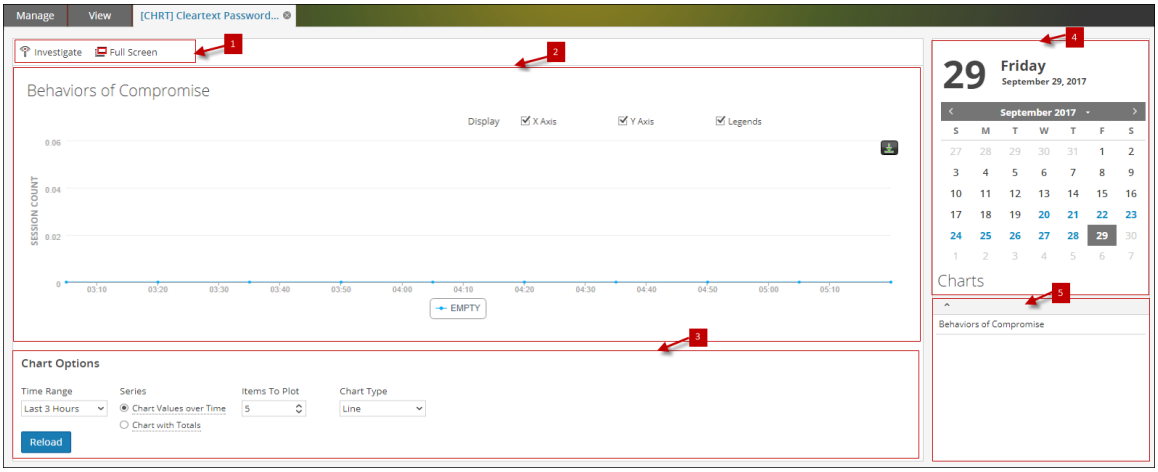
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique
- Afficher un graphique
- Tester un graphique
- Analyser un graphique

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



Le panneau Afficher un graphique inclut les panneaux suivants :

1	Barre d'outils Graphique
2	Panneau Sortie graphique
3	Panneau Calendrier des graphiques
4	Panneau Options du graphique
5	Liste des graphiques exécutés

Barre d'outils Graphique

La barre d'outils Graphique comporte des options qui vous permettent d'examiner le graphique, et de l'afficher sur un autre écran.

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

Opération	Description
Rechercher	Permet d'examiner les détails du graphique.
Plein écran	Affiche le graphique en mode plein écran.

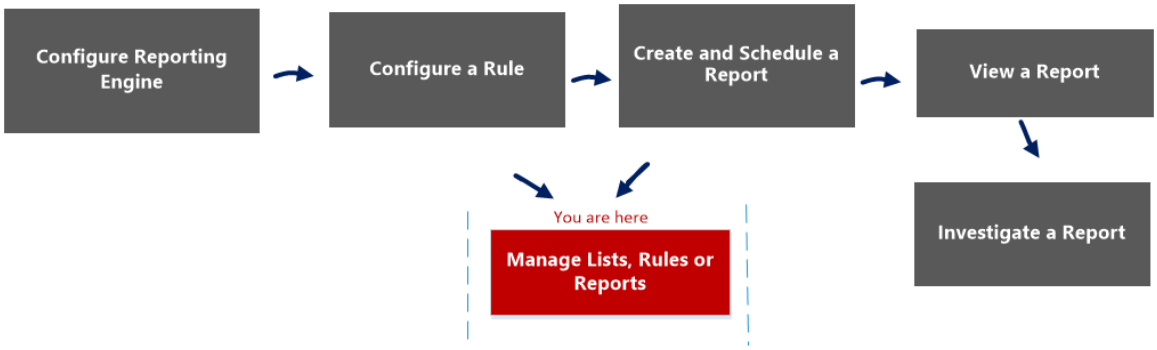
Boîte de dialogue Autorisations des listes

Dans la boîte de dialogue Autorisations des listes, vous pouvez gérer les autorisations d'accès applicables à un rôle d'utilisateur au niveau de la liste ou du groupe de listes. Seul un utilisateur détenant l'autorisation **Lecture/écriture** peut configurer la liste dans le module Reporting.

Workflow

Ce workflow présente la procédure à suivre pour gérer des listes ou des groupes de listes. Vous pouvez définir un contrôle d'accès au niveau de la liste ou du groupe de listes afin que seuls les utilisateurs dotés des rôles spécifiques puissent accéder aux listes. Vous pouvez utiliser des listes pour définir des règles de génération de rapports, graphiques et alertes.

Vous devez vous assurer que le Reporting Engine est configuré sur NetWitness Suite.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

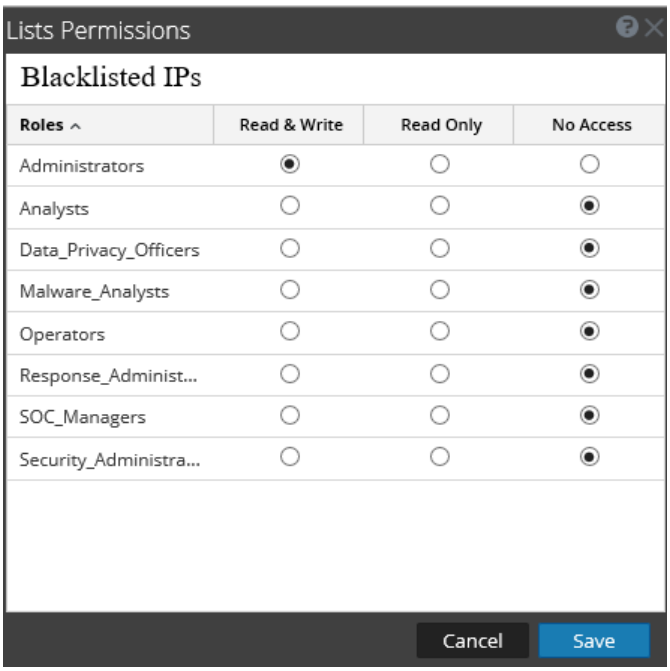
*Vous pouvez effectuer ces tâches ici.

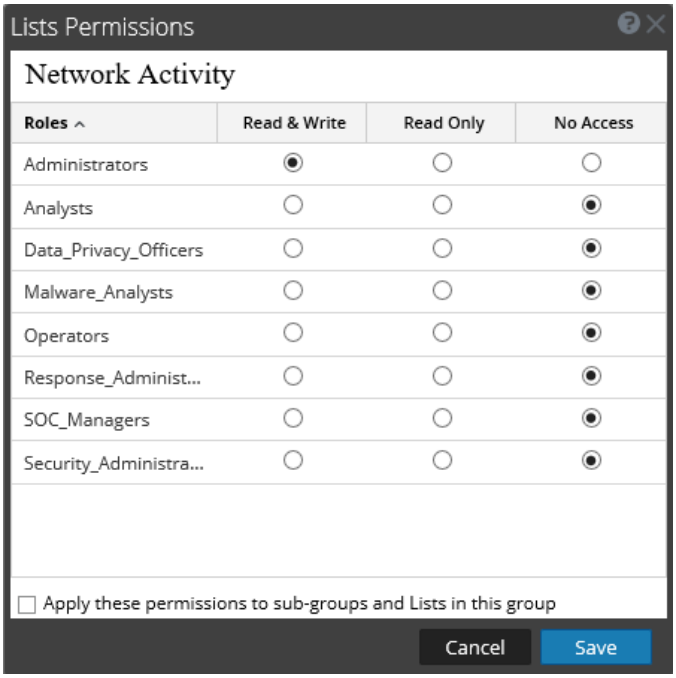
Rubriques connexes

- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Vue Liste
- Section Liste de la rubrique « Autorisations du rôle » du *Guide de la sécurité du système et de la gestion des utilisateurs*.

Affichage rapide

Les figures suivantes sont des exemples de la boîte de dialogue Autorisations des listes et de la boîte de dialogue des autorisations des groupes de listes :





Pour accéder à cette vue

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Listes**.
   La vue Listes s'affiche.
3. Dans la vue **Listes**, sélectionnez un rapport.

4. Dans la barre d'outils **Listes**, cliquez sur  > **Autorisations**.

   La boîte de dialogue Autorisations des rapports s'affiche.

Le tableau suivant décrit les fonctions de la boîte de dialogue Autorisations des listes.

Fonction	Description
Rôles	Décrit les rôles des utilisateurs connectés à l'interface utilisateur NetWitness Suite.
Lecture et écriture	Permet aux utilisateurs d'accéder, afficher, modifier, supprimer, importer et exporter les listes de la vue Listes. Les utilisateurs ne peuvent pas modifier l'autorisation dans la règle.
Lecture seule	Permet uniquement aux utilisateurs d'accéder à la liste et de l'afficher dans la vue Listes.
Aucun accès	Ne permet pas aux utilisateurs d'accéder aux listes ni de les afficher.
Appliquer ces autorisations aux sous-groupes et listes dans ces groupes	Applique automatiquement les autorisations aux sous-groupes et listes dans les groupes, si la case à cocher est sélectionnée.
Annuler	Annule toutes les modifications appliquées aux autorisations.
Enregistrer	Enregistre les sélections et fournit un accès aux rôles en fonction des sélections.

Vue Liste

Dans la vue Liste, vous voyez les listes et groupes disponibles dans une grille.

Workflow

Ce workflow présente la procédure à suivre pour définir des listes ou des groupes de listes. Vous pouvez définir un contrôle d'accès au niveau de la liste ou du groupe de listes afin que seuls les utilisateurs dotés des rôles spécifiques puissent accéder aux listes. Vous pouvez utiliser des listes pour définir des règles de génération de rapports, graphiques et alertes.

Vous devez vous assurer que le Reporting Engine est configuré sur NetWitness Suite.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle*	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

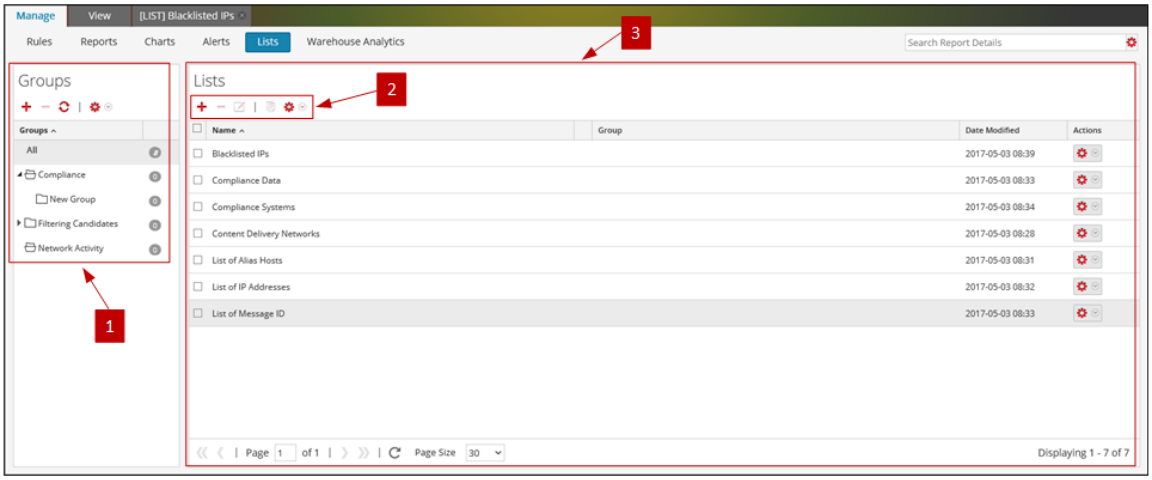
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Boîte de dialogue Autorisations des listes
- Vue Créer la liste

Affichage rapide

La figure ci-dessous montre la vue Liste.



Pour accéder à cette vue

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Cliquez sur **Listes**.

   La vue Listes s'affiche.

La vue Liste comprend les panneaux suivants :

1. Panneau Groupes de listes
2. Barre d'outils Liste
3. Panneau d'affichage des listes

Panneau Groupes de listes

Le panneau Groupes de listes fournit une liste des groupes utilisés pour l'organisation des listes. Il possède une barre d'outils qui vous permet de créer et de gérer des groupes.

Fonction	Description
	Permet aux utilisateurs d'ajouter un nouveau groupe au module Reporting.
	Permet aux utilisateurs de supprimer des groupes.
	Actualise la vue.
	Permet aux utilisateurs d'accéder aux options suivantes : Importer, Exporter et Autorisations.

Vous pouvez effectuer les actions suivantes dans le panneau Groupes de listes :

- Actualiser des listes dans un groupe.
- Déplacer les listes entre groupes. Vous pouvez déplacer une liste d'un groupe à un autre en la faisant glisser dans le groupe voulu.
- Créer des groupes de listes.
- Supprimer des groupes de listes.
- Importer des groupes de listes.
- Exporter des groupes de listes.
- Définir un contrôle d'accès pour des groupes de listes.

Barre d'outils Liste

Fonction	Description
	Permet aux utilisateurs d'ajouter une nouvelle liste au module Reporting.

Fonction	Description
	Permet à l'utilisateur de supprimer une ou plusieurs des listes sélectionnées.
	Permet à l'utilisateur de modifier les listes.
	Crée une double instance de la liste sélectionnée.
	Permet à l'utilisateur d'accéder aux options suivantes : Importer, Exporter et Autorisations.

Panneau d'affichage des listes

Ce panneau affiche toutes les listes définies sous la forme d'un tableau.

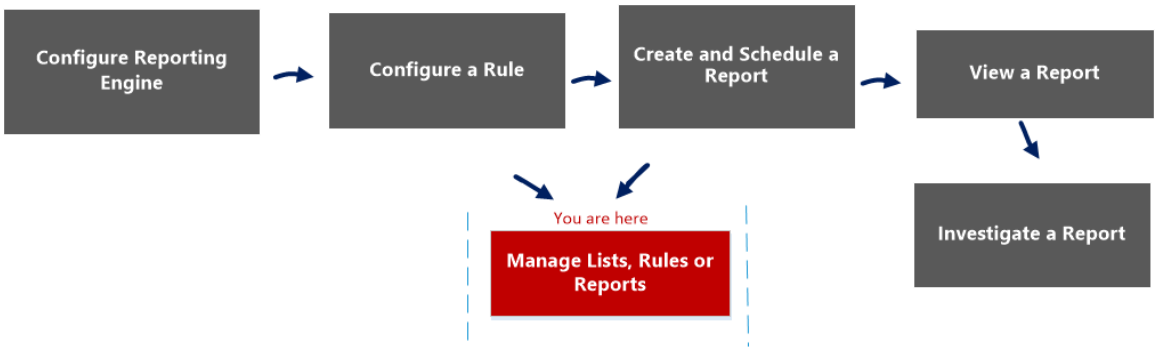
Colonne	Description
Nom	Affiche le nom de la liste. **Remarque :** pour le champ **Nom**, l'icône permettant d'étendre la taille de la colonne ne s'affiche pas à la fin du champ de colonne. Vous devez placer le pointeur de la souris un peu à gauche pour voir apparaître l'icône qui permet d'étendre la colonne.
Groupe	Affiche le groupe de listes auquel appartient la liste.
Date de modification	Affiche la date et l'heure de modification de la liste.

Boîte de dialogue Autorisations des rapports

Dans cette boîte de dialogue, les utilisateurs disposant de l'autorisation d'accès en lecture et écriture peuvent configurer les autorisations.

Workflow

Ce workflow présente la procédure à suivre pour gérer des rapports ou des groupes de rapports.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

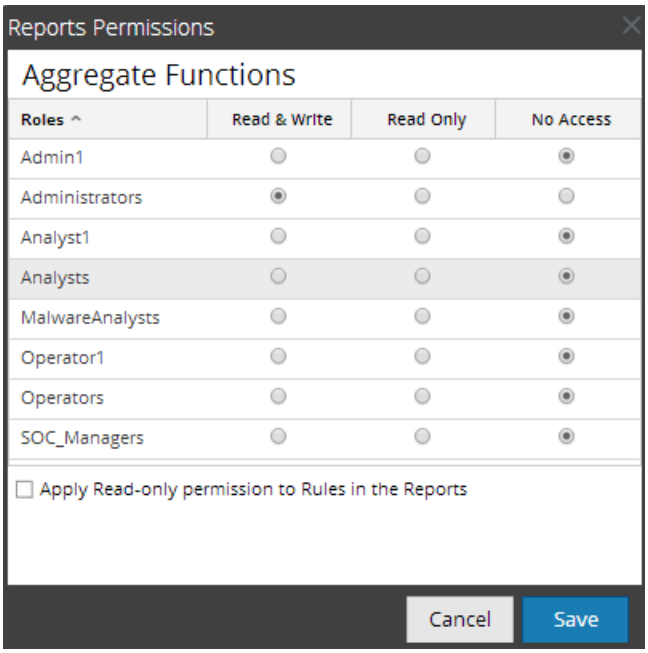
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Rapport
- Vue Élaborer le rapport
- Boîte de dialogue Importer le rapport

Affichage rapide



Pour afficher la boîte de dialogue Autorisations des rapports :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport.
4. Cliquez sur  > **Autorisations**.
   La boîte de dialogue Autorisations des rapports s'affiche.

Remarque : lorsque vous activez la case à cocher, toutes les règles dépendantes ont une autorisation d'accès en LECTURE, à condition que les autorisations du rapport soient supérieures aux autorisations des règles.

Le tableau suivant décrit les fonctionnalités de la boîte de dialogue Autorisations des rapports.

Fonction	Description
Rôles	Affiche tous les rôles pouvant avoir accès aux autorisations.
Lecture et écriture	Vous permet d'obtenir un accès en lecture et écriture aux règles appliquées aux rapports.
Lecture seule	Vous permet d'obtenir un accès en lecture seule aux règles appliquées aux rapports.
Aucun accès	Si vous sélectionnez cette option, vous n'obtiendrez aucune autorisation d'accès aux règles appliquées aux rapports.
Appliquer l'autorisation de lecture seule aux règles des rapports	Permet de définir les autorisations d'accès en lecture seule aux règles des rapports pour tous les rôles.
Annuler	Cette option annule toutes les modifications appliquées aux autorisations.
Enregistrer	Cette option enregistre les sélections et fournit un accès aux rôles en fonction des sélections.

Vue Rapport

Dans la vue Rapport, vous pouvez créer et gérer un rapport ou des groupes de rapports.

Workflow

Ce workflow présente la procédure à suivre pour créer et planifier un rapport.

Que voulez-vous faire ?

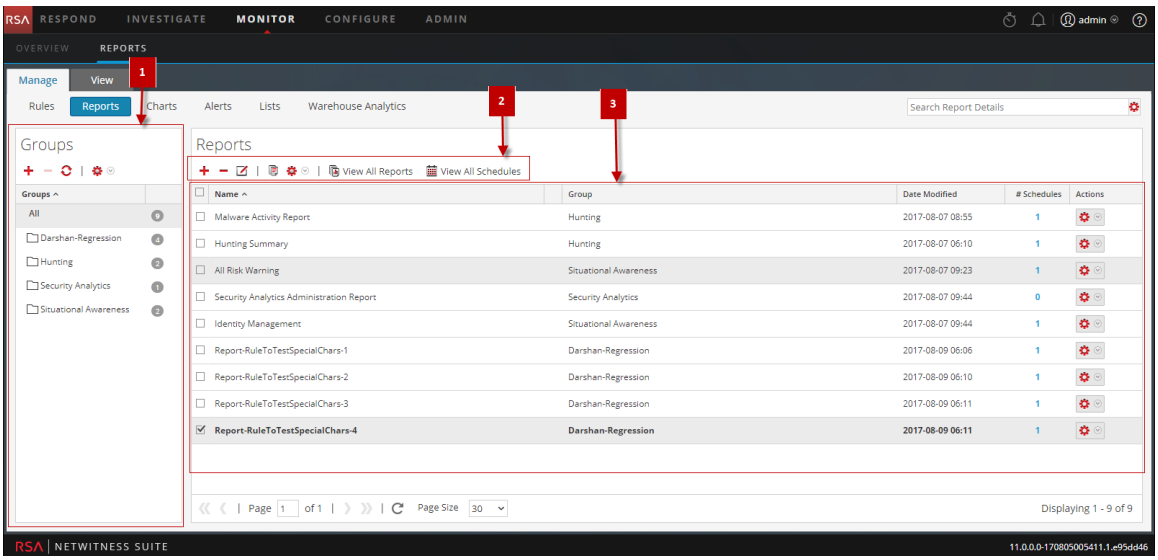
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport*	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Élaborer le rapport
- Boîte de dialogue Importer le rapport
- Vue Rapports planifiés
- Boîte de dialogue Autorisations des rapports

Affichage rapide



Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapports s'affiche.

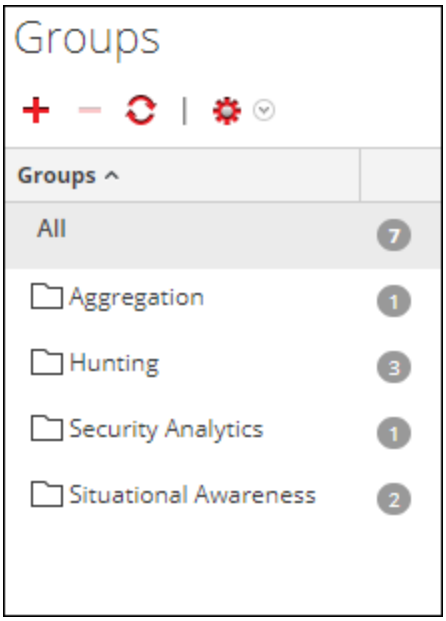
Fonctions

La vue Rapport comprend les sections suivantes :

1. Panneau Groupes de rapports
2. Barre d'outils Rapport
3. Panneau Liste des rapports

Panneau Groupes de rapports

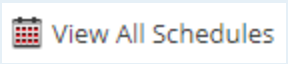
Ce panneau vous permet d'organiser les rapports au sein d'un groupe. Vous pouvez créer un groupe de rapports, ajouter des rapports au groupe et déplacer des rapports entre groupes. Vous pouvez afficher tous les rapports en sélectionnant l'option Tous située sous la colonne Groupe.



Fonction	Description
+	Cette option vous permet d'ajouter un nouveau rapport au module Reporting.
−	Cette option vous permet de supprimer un ou plusieurs des rapports sélectionnés.
↻	Cette option actualise la vue.
⚙	Le menu Actions comprend les options suivantes : Importer, Exporter et Autorisations.

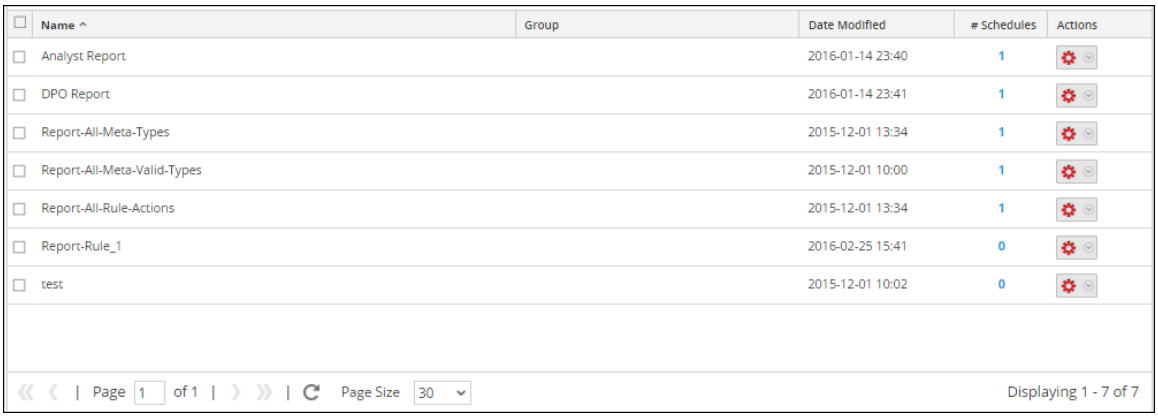
Barre d'outils Rapports

La barre d'outils Rapports vous permet d'ajouter, de modifier, de supprimer, de dupliquer, d'importer et d'exporter des rapports. Vous pouvez également définir des autorisations d'accès pour un rapport inclus dans un groupe.

Fonction	Description
	Cette option vous permet d'ajouter un nouveau rapport au module Reporting.
	Cette option vous permet de supprimer un ou plusieurs des rapports sélectionnés.
	Cette option vous permet de modifier un graphique.
	Cette option crée une double instance du rapport sélectionné.
	Le menu Actions comprend les options suivantes : Importer, Exporter, Exporter en tant que texte et Autorisations.
	Cette option vous permet d'afficher une liste de rapports, ainsi que le nom de leur planning et leur heure.
	Cette option vous permet d'afficher tous les rapports planifiés.

Panneau Liste des rapports

Ce panneau répertorie tous les rapports sous forme de tableau.



Le tableau suivant décrit les colonnes du panneau Liste des rapports.

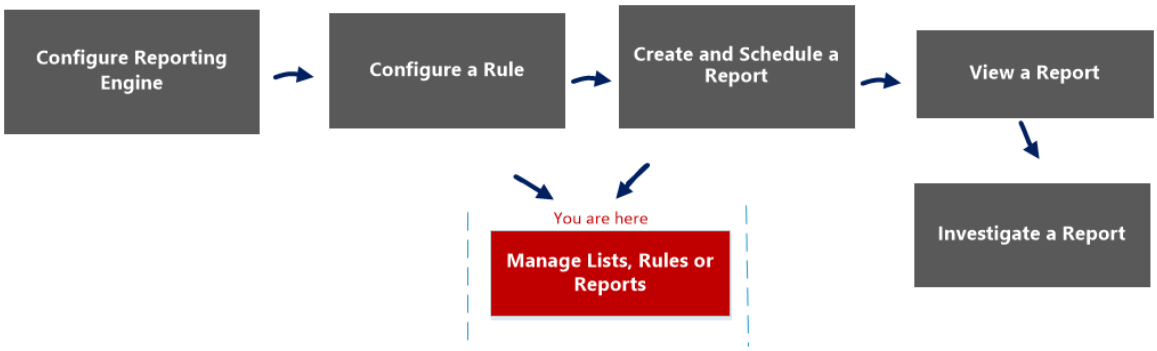
Colonne	Description
Nom	Nom du rapport.
Groupe	Groupe de rapports auquel appartient le rapport.
Date de modification	Date et heure de modification du rapport.
#Schedules	Nombre de plannings créés pour un rapport.
Actions	Le menu Actions comprend les options suivantes : Planifier un rapport, Afficher les rapports programmés, Supprimer, Modifier et Exporter.

Boîte de dialogue Autorisations des règles

Le module Reporting fournit un contrôle d'accès au niveau de la règle. Seul un utilisateur possédant le bon ensemble d'autorisations peut effectuer des tâches sur la règle. Lors de la création des rôles d'utilisateur, l'administrateur doit vérifier que les rôles créés pour des tâches spécifiques ont bien accès à toutes les autorisations supérieures dans la hiérarchie des rôles.

Workflow

Ce workflow présente la procédure à suivre pour gérer des règles ou des groupes de règles.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

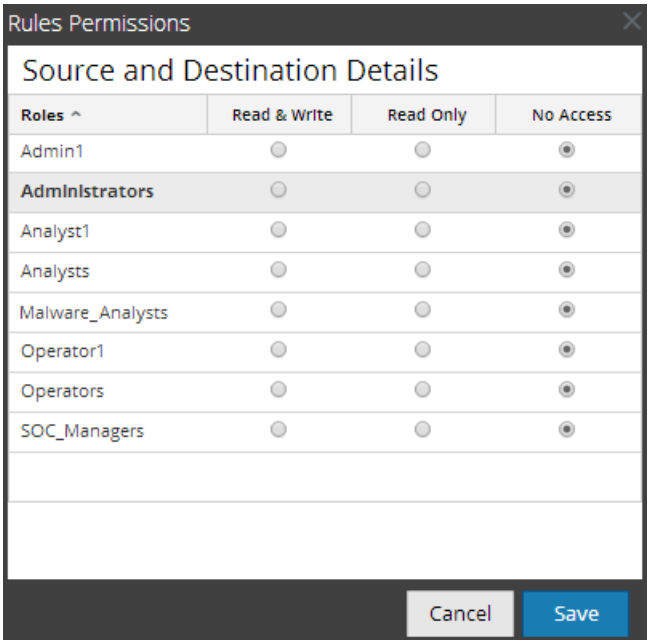
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

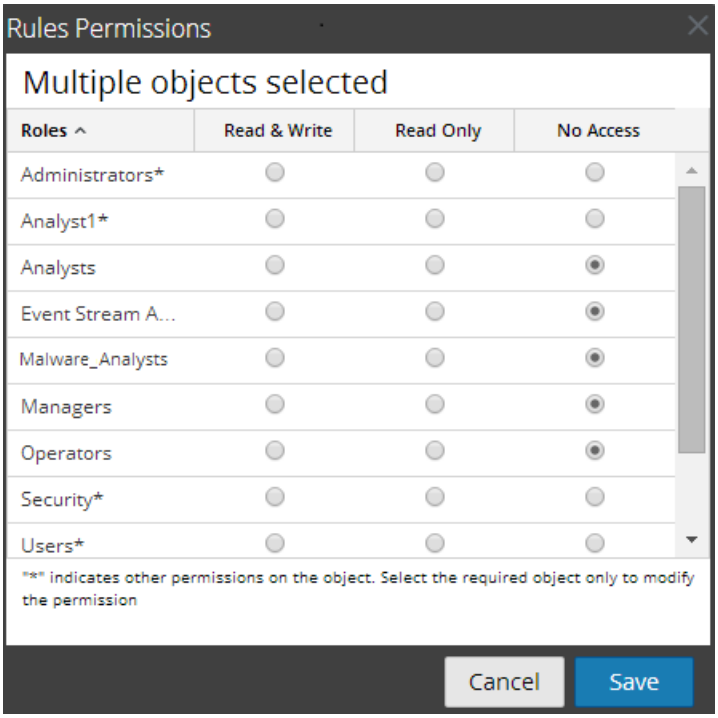
- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Vue Règle

Affichage rapide

Cette figure montre la boîte de dialogue Autorisations des règles pour une seule règle.



Cette figure montre la boîte de dialogue Autorisations des règles lorsque plusieurs règles sont sélectionnées.



La boîte de dialogue a une apparence différente pour les groupes de règles et les règles. Pour accéder à la boîte de dialogue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Dans le panneau **Liste de règles**, sélectionnez une ou plusieurs règles, ou un groupe de règles.
3. Cliquez sur  > **Autorisations** dans la barre d'outils.
   La boîte de dialogue Autorisations des règles s'affiche.

Fonction	Description
Colonne Rôles	Répertorie les rôles d'utilisateur NetWitness Suite intégrés et personnalisés. Chaque utilisateur connecté à NetWitness Suite se voit attribuer des rôles d'utilisateur. Lorsque plusieurs règles sont sélectionnées, l'astérisque situé à côté du nom de rôle, par exemple `Security*`, indique qu'il existe d'autres autorisations disponibles pour ce rôle d'utilisateur. Pour modifier les autres autorisations, sélectionnez le rôle d'utilisateur et changez l'autorisation d'accès.
Colonne Lecture et écriture	Lorsque la case à cocher de cette colonne est activée, le rôle d'utilisateur correspondant est autorisé à afficher, modifier, supprimer, importer et exporter des règles dans la vue Règles. L'utilisateur ne peut pas modifier l'autorisation dans la règle.
Colonne Lecture seule	Lorsque la case à cocher de cette colonne est activée, le rôle d'utilisateur correspondant est autorisé à afficher les règles du groupe de règles.
Colonne Aucun accès	Lorsque la case à cocher de cette colonne est activée, le rôle d'utilisateur correspondant ne peut pas afficher ou modifier les règles du groupe de règles. Avant l'application des autorisations des règles, ceci est l'ensemble d'autorisations par défaut défini pour tous les rôles d'utilisateur, bien que la case à cocher soit désactivée.
Case à cocher Appliquer ces autorisations aux sousgroupes et règles dans ce groupe	Lorsque cette case à cocher est activée, NetWitness Suite applique des autorisations aux sous-groupes et règles du groupe.
Option Annuler	Si vous cliquez sur Annuler, cela entraîne la fermeture de la boîte de dialogue sans enregistrement des modifications apportées.

Fonction	Description
Option Enregistrer	Si vous cliquez sur Enregistrer, cela entraîne la fermeture de la boîte de dialogue et la mise à jour des autorisations du groupe de règles pour les rôles d'utilisateur. Si cela est spécifié, les autorisations d'accès sont appliquées aux sous-groupes et aux objets enfants de ce groupe. Lorsque plusieurs règles sont sélectionnées, l'autorisation d'accès est appliquée à l'ensemble des règles sélectionnées.

Vue Règle

La vue Règle est l'interface utilisateur permettant de gérer les règles.

Workflow

Ce workflow présente la procédure à suivre pour définir des règles ou des groupes de règles.

Que voulez-vous faire ?

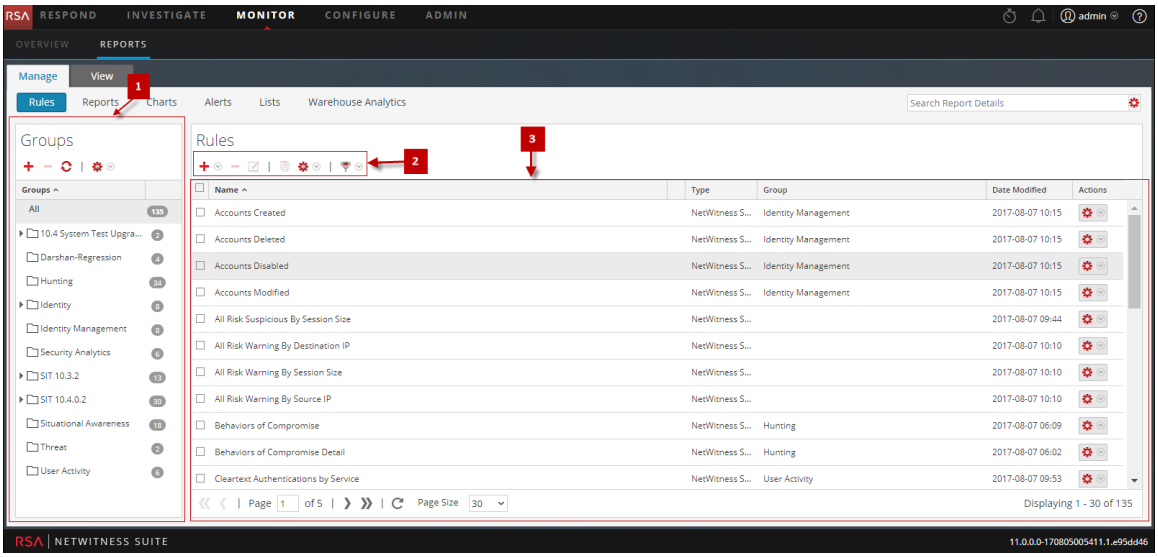
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle*	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer une règle
- Gérer les listes, les règles ou les rapports
- Boîte de dialogue Autorisations des règles
- Vue Élaborer une règle

Affichage rapide



Pour accéder à la vue Règles :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Règles**.

   La vue Règles s'affiche.

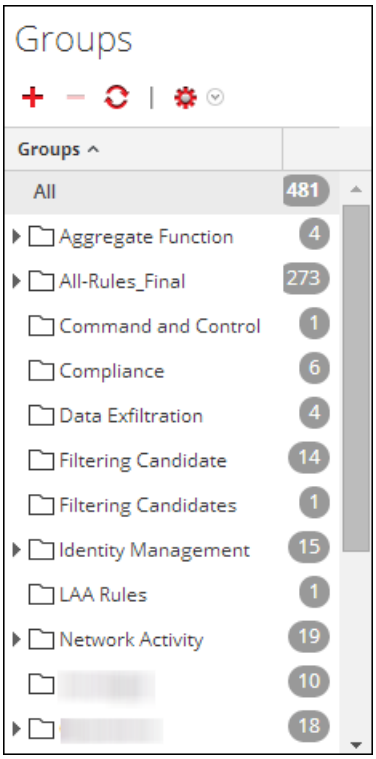
La vue Règles inclut les panneaux suivants :

1	Groupes de règles
2	Liste de règles
3	Barre d'outils Règle

Panneau Groupes de règles

Le panneau Groupes de règles vous permet d'organiser des règles en groupes à l'aide des options de la barre d'outils. Vous pouvez créer des groupes et des sous-groupes, et y ajouter des règles. Vous pouvez également regrouper et déplacer les règles entre les différents groupes.

La figure ci-dessous montre les groupes dans le panneau Groupes de règles :



Le tableau suivant décrit les fonctionnalités du panneau Groupes de règles.

Fonction	Description
+	Cette option vous permet d'ajouter un nouveau groupe de règles au module Reporting.
−	Cette option vous permet de supprimer un ou plusieurs groupes de règles.
↻	Cette option actualise la liste des groupes de règles.
⚙	Le menu Actions comprend les options suivantes : Importer, Exporter et Autorisations.
Tout	Affiche la liste de tous les groupes de règles.

Barre d'outils Règle

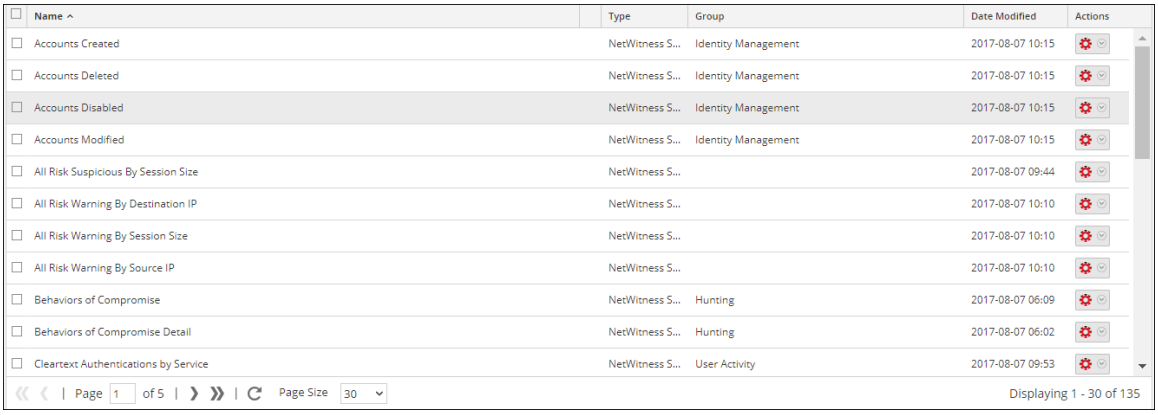
La barre d'outils Règle vous permet d'ajouter, de supprimer, de modifier et de répliquer une règle. La figure ci-dessous montre la barre d'outils.

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

Fonction	Description
	Cette option vous permet d'ajouter une nouvelle règle au module Reporting.
	Cette option vous permet de supprimer une ou plusieurs règles sélectionnées.
	Cette option vous permet de modifier une règle.
	Cette option vous permet de dupliquer une règle.
	Le menu Actions comprend les options suivantes : Utiliser, Importer, Exporter et Autorisations.
	Cette option vous permet de sélectionner le type de règle.

Panneau Liste de règles

La figure ci-dessous montre la liste de règles dans le panneau Liste de règles.



Le tableau suivant décrit les fonctionnalités du panneau Listes de règles.

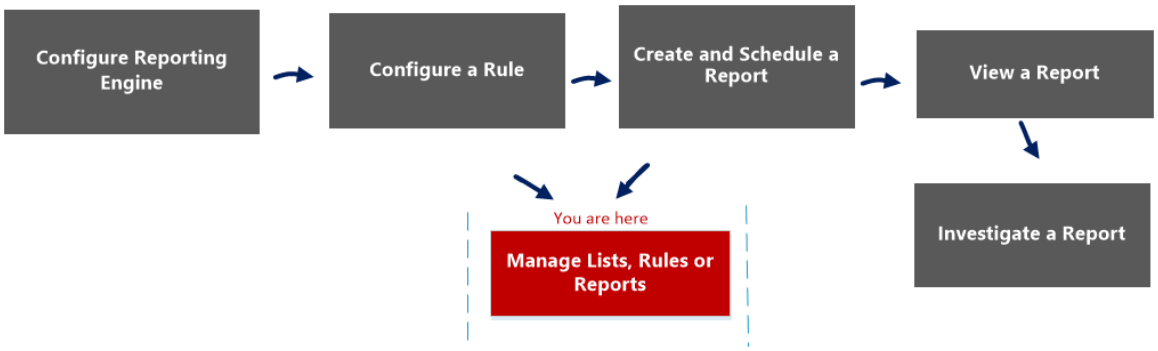
Fonction	Description
Nom	Affiche le nom de la règle que vous avez créée ou modifiée. **Remarque :** pour le champ **Nom**, l'icône permettant d'étendre la taille de la colonne ne s'affiche pas à la fin du champ de colonne. Vous devez placer le pointeur de la souris un peu à gauche pour voir apparaître l'icône qui permet d'étendre la colonne.
Type	Affiche le type de base de données pris en charge pour la règle que vous avez créée.
Groupe	Affiche les valeurs qui sont regroupées.
Date de modification	Affiche la date de dernière modification de la règle.
Actions	Affiche le menu Actions présentant les options suivantes : Créer une alerte, Créer un graphique, Créer un rapport, Supprimer, Modifier, Exporter et Dépendances.

Boîte de dialogue Sélectionner un logo

Dans la boîte de dialogue Sélectionner un logo, vous pouvez télécharger un nouveau logo non disponible dans la vue Configuration des services Reporting Engine ou choisir un logo existant dans la vue Configuration des services Reporting Engine.

Workflow

Ce workflow présente la procédure à suivre pour gérer des rapports ou des groupes de rapports.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport

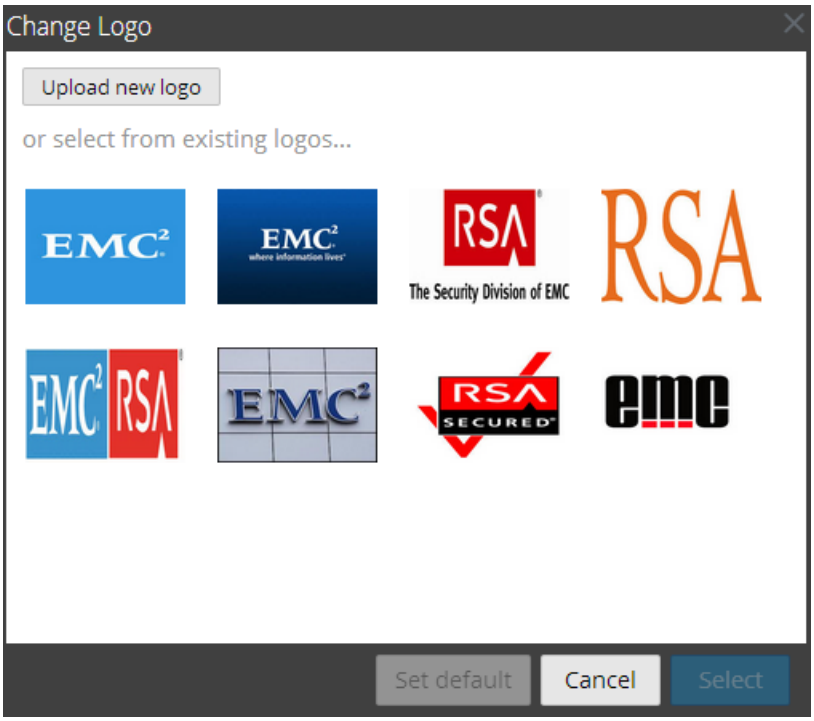
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Rapports planifiés
- Vue Rapport

Affichage rapide



Pour accéder à cette boîte de dialogue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapports s'affiche.
3. Dans le panneau **Liste des rapports**, sélectionnez un rapport.
4. Cliquez sur > **Afficher les rapports programmés**.
   L'onglet de la vue Afficher les rapports programmés s'affiche.
5. Sélectionnez un rapport planifié et cliquez sur > **Modifier le planning**.
   L'onglet de la vue Planifier un rapport s'affiche.
6. Cliquez sur le panneau **Logo** .
   La boîte de dialogue Modifier un logo s'affiche.

Le tableau suivant répertorie les champs de la boîte de dialogue Sélectionner un logo.

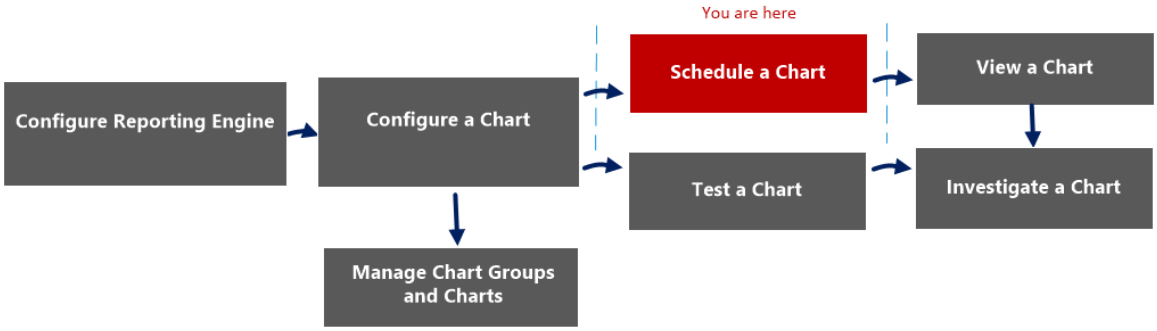
Champ	Description
Télécharger le nouveau logo	Cliquez sur l'icône pour télécharger un nouveau logo depuis le répertoire local.

Champ	Description
Sélectionner	Sélectionnez dans la liste existante un logo à utiliser dans le rapport planifié.
Annuler	Annule la sélection du logo et revient dans le panneau Planifier un rapport.
Définir la valeur par défaut	Sélectionnez un logo pour le définir comme le logo par défaut.

Vue Planifier un graphique

Dans la vue Planifier un graphique, vous pouvez activer ou désactiver un graphique.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique*	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

*Vous pouvez effectuer ces tâches ici.

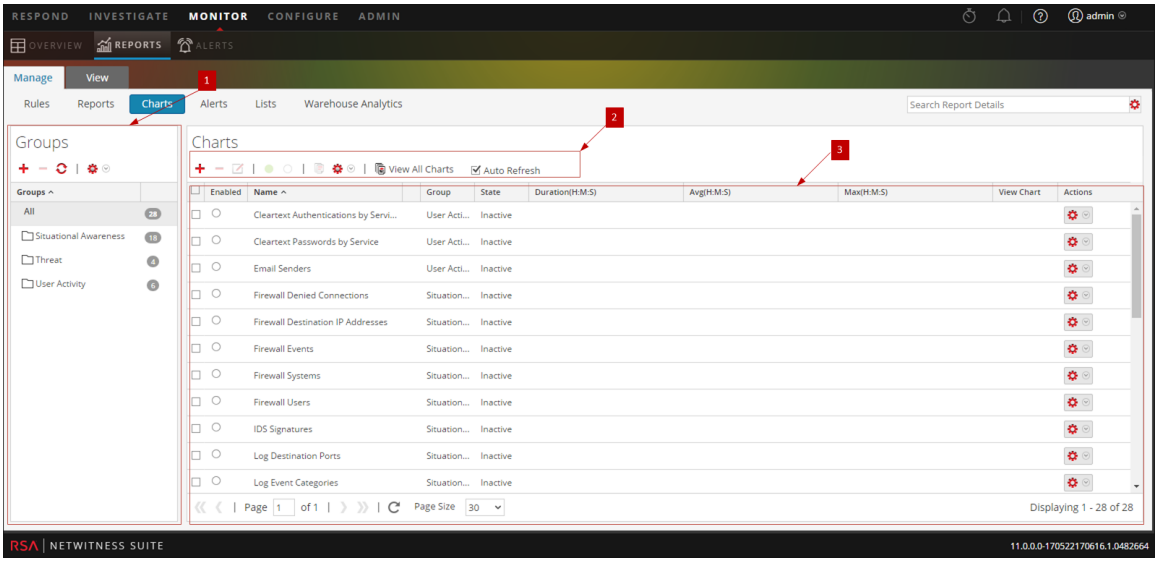
Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique

- Planifier un graphique

Affichage rapide

La figure ci-dessous montre la vue Planifier un graphique.



La vue Planifier un graphique inclut les panneaux suivants :

1	Panneau Groupes de graphiques
2	Barre d'outils Graphique
3	Panneau Vue Graphique

Barre d'outils Graphique

La barre d'outils Graphiques vous permet d'ajouter, de modifier, de supprimer, de dupliquer, d'activer, de désactiver, d'importer et d'exporter un graphique. Vous pouvez également définir des autorisations d'accès aux graphiques inclus dans un groupe.

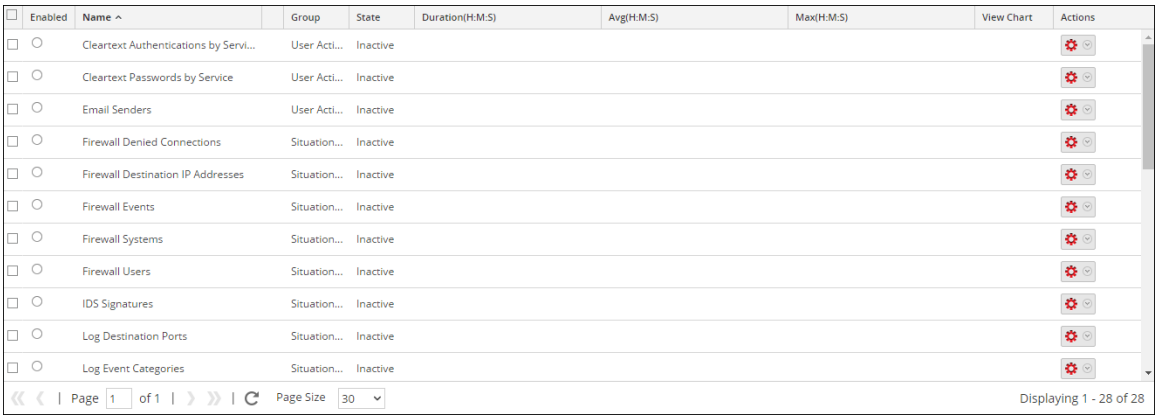
La barre d'outils Graphique comprend les options suivantes :

Fonction	Description
+	Ajoute un nouveau graphique au module Reporting.
−	Supprime un ou plusieurs graphiques sélectionnés.

Fonction	Description
	Modifie des graphiques.
	Active les graphiques sélectionnés.
	Désactive les graphiques sélectionnés.
	Crée une double instance du graphique sélectionné.
	Fournit les informations suivantes : Importer, Exporter, Exporter en tant que texte et Autorisations.
Afficher tous les graphiques	Affiche tous les graphiques exécutés.
Actualisation automatique	Actualise automatiquement la liste des graphiques.

Panneau Vue Graphique

Le panneau Vue Graphique présente tous les graphiques sous la forme d'un tableau ou d'une grille.



Le tableau suivant répertorie les colonnes du panneau Vue Graphique et leur description.

Fonction	Description
Activé	- Le graphique est activé. - Le graphique est désactivé.
Nom	Nom du graphique.

Fonction	Description
Groupe	Groupe auquel appartient le graphique.
État	État du graphique : • En attente • Terminé • Échec
Durée (H:M:S)	Durée d'exécution du dernier graphique.
Moy (H:M:S)	Durée moyenne nécessaire à l'exécution du graphique.
Max (H:M:S)	Durée maximale de l'exécution du graphique.
Afficher le graphique	Lien hypertexte qui renvoie au panneau Afficher un graphique.
	Le menu Actions comprend les options suivantes : Activer, Désactiver, Afficher, Supprimer, Modifier et Exporter.

Panneau Planifier un rapport

Le panneau Planifier un rapport vous permet de planifier un rapport personnalisé. Avant de planifier un rapport, vous pouvez créer une liste dynamique (avec l'option Remplacer sélectionnée) avec les services ajoutés. Pour plus d'informations, consultez la rubrique Générer une liste à partir du rapport planifié de Créer et planifier un rapport. Utilisez ensuite la liste pour générer un rapport avec des détails dans le rapport comme des services et noms d'hôtes.

Workflow

Ce workflow présente la procédure à suivre pour créer et planifier un rapport.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport*	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport

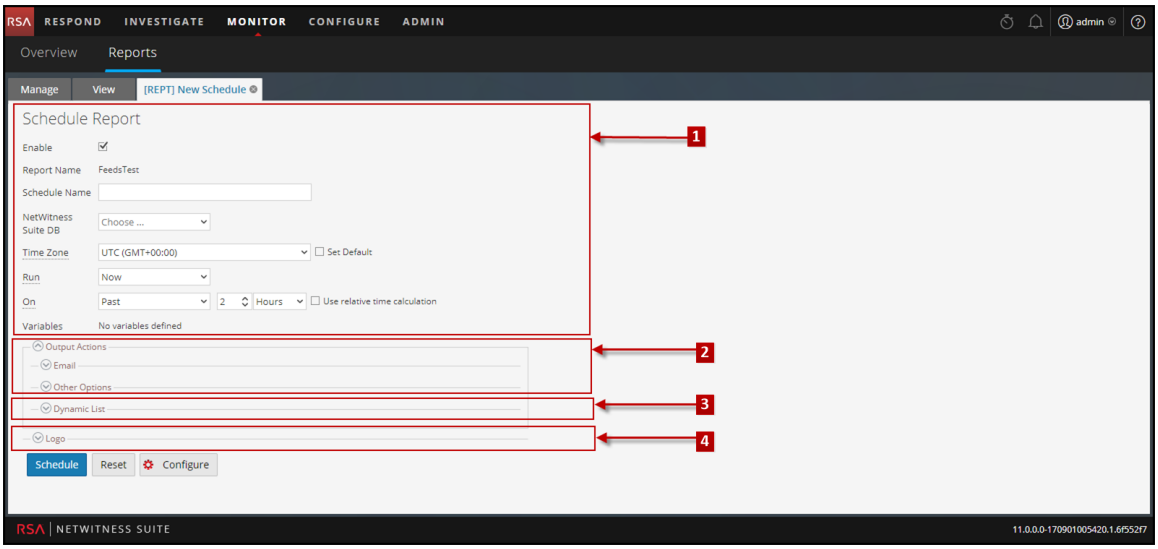
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Rapport
- Vue Élaborer le rapport
- Vue Rapports planifiés

Affichage rapide



Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapports s'affiche.
3. Dans le panneau **Liste des rapports**, cliquez sur  > **Planifier un rapport**.

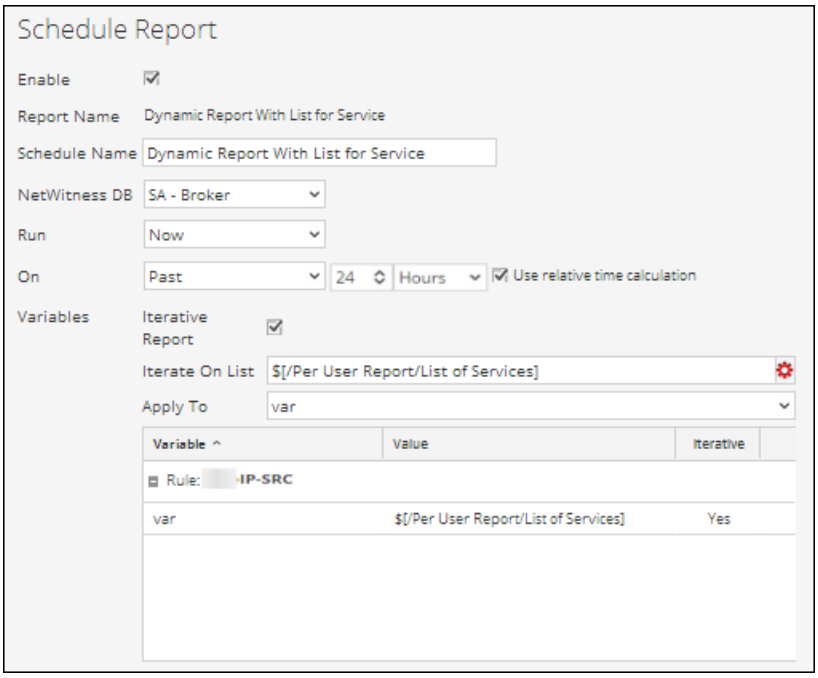
Fonctions

La vue Planifier un rapport se compose des panneaux suivants :

1	Vue Planifier un rapport
2	Panneau Actions de sortie
3	Panneau Liste dynamique
4	Panneau Logo

Vue Planifier un rapport

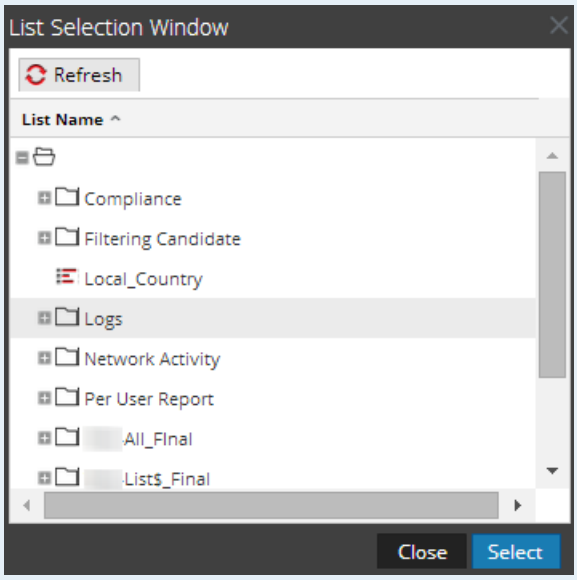
La vue Planifier un rapport vous permet de planifier des rapports.



Le tableau suivant répertorie les champs du panneau Planifier un rapport.

Champ	Description
Activer	Active les planifications de rapport et exécute le rapport.

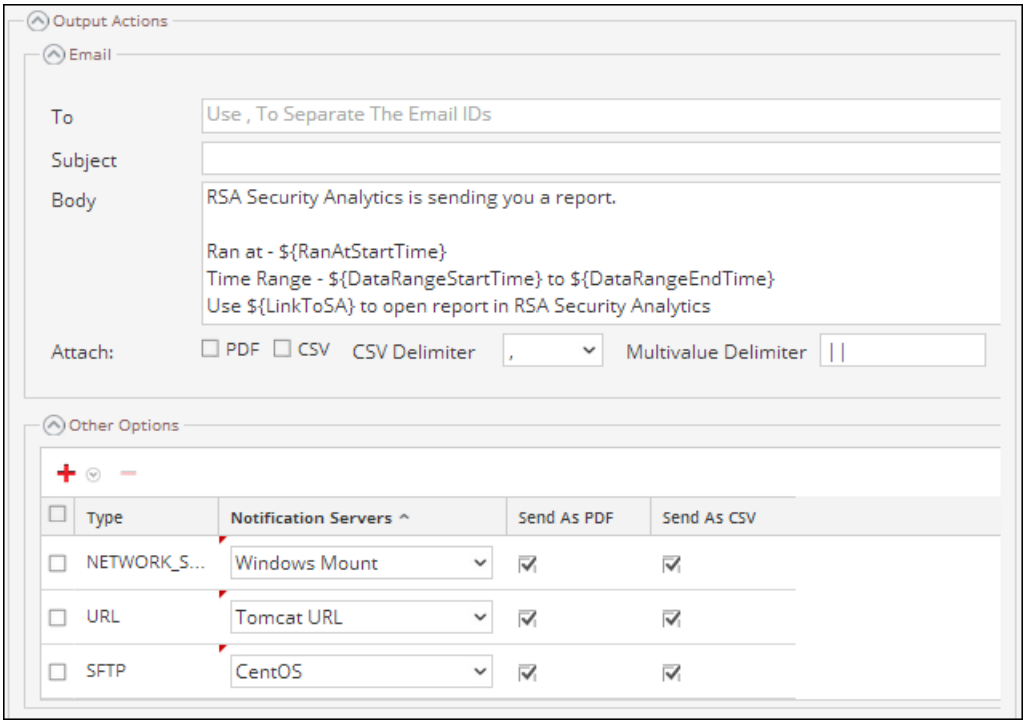
Champ	Description
Nom du rapport	Nom du rapport.
Nom de planning	Nom de la configuration du rapport planifié.
Base de données NetWitness	La base de données peut être une base de données NWDB, IPDB et Warehouse, selon le type de base de données sélectionné dans la définition de règle. Si le rapport dispose de règles de type NWDB, IPDB et Warehouse, tous les types de bases de données ou de règles s'affichent.
Pool de ressource Warehouse	Si le rapport dispose de règles de base de données Warehouse, le menu déroulant Pool de ressource Warehouse s'affiche afin de sélectionner les pools ou files d'attentes disponibles dans le cluster. Si aucun pool ou aucune file d'attente n'est indiqué pour le Reporting Engine, ce champ est désactivé. Pour plus d'informations, consultez la rubrique « Étape 5 : Configurer le Planificateur de tâches pour un Reporting Engine » dans le *Guide de configuration de l'hôte et des services*.
Exécuter	Indique le type de planning pour la configuration d'exécution : • Exécution ad-hoc • Exécution toutes les heures • Exécution quotidienne • Exécution hebdomadaire • Exécution mensuelle
Allumé	Plage de données sur laquelle la requête est exécutée.
Utiliser le calcul de temps relatif	Utilise la durée de temps relatif pour planifier un rapport.

Champ	Description
Rapport itératif	Cochez cette case afin de planifier un rapport pour la valeur de liste sélectionnée.
Itérer sur la liste 	Cliquez sur ce bouton pour accéder au panneau Sélection de liste et sélectionner une liste. La figure suivante affiche ce panneau :  Le panneau Sélection de liste est une collection de listes. Le Reporting Engine conserve une liste active des noms de listes disponibles en effectuant une synchronisation continue avec la collection à laquelle il est connecté.
S'applique à	Applique les valeurs de liste à la variable sélectionnée.
les variables.	Affiche les variables de règle avec leurs valeurs associées et les propriétés itératives incluses dans le rapport. **Remarque :** selon la règle choisie lors de la création d'un rapport, vous pouvez afficher les variables dynamiques définies pour la règle dans le champ **Variables** du panneau Planifier un rapport. Par exemple, Test-Country est la règle dont la variable dynamique est var.
Planning	Planifie le rapport.

Champ	Description
Réinitialiser	Réinitialise le rapport planifié.
Configurer	Vous permet de modifier les détails de configuration du Reporting Engine indiqués dans la rubrique « Onglet général du Reporting Engine » dans le *Guide de configuration de l'hôte et des services*. **Remarque :** ce bouton s'affiche dans le panneau Planifier un rapport, uniquement lorsque vous disposez de l'autorisation d'accès Gérer un périphérique dans le module Reporting.

Panneau Actions de sortie

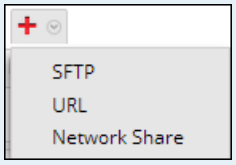
Le panneau Actions de sortie spécifie les actions de sortie permettant de notifier le destinataire de l'e-mail à la fin de l'exécution du rapport. Il permet également d'envoyer des rapports aux formats PDF et CSV sous forme de pièces jointes, en fonction de votre sélection.



Le tableau suivant répertorie les champs du panneau Actions de sortie.

Champ	Description
À	Liste des adresses e-mail, séparées par des virgules, qui reçoivent la sortie.

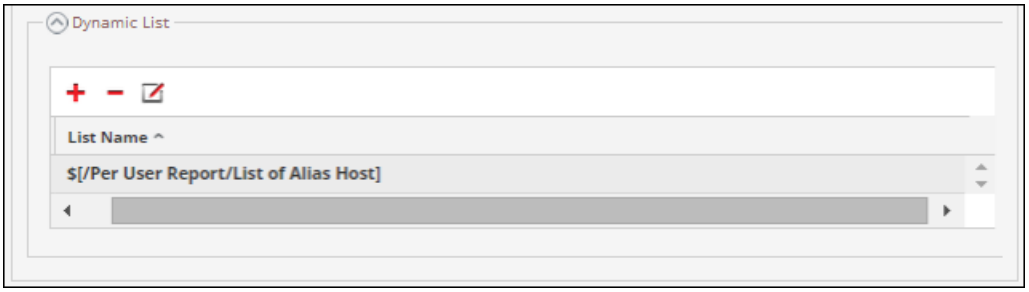
Champ	Description
Objet	Objet de l'e-mail.
Corps	Corps de l'e-mail. Par défaut, le champ du corps est renseigné par du texte prédéfini dont certaines variables ajouteront les méta appropriées au rapport généré. Dans le Reporting Engine, ces variables sont remplacées par des valeurs réelles. • `${RanAtStartTime}` : heure de début du rapport. • `${DataRangeStartTime}` : heure de début de la période des données. • `${DataRangeEndTime}` : heure de fin de la période des données. • `${LinkToSA}` : lien vers l'hôte NetWitness Suite dans l'e-mail qui, à son tour, ouvre le rapport dans l'interface NetWitness Suite. • `${ReportName}` : nom du rapport. • `${DataSource}` : nom de la source de données.
Joindre :	Format de sortie auquel le rapport est joint à l'e-mail, comme PDF ou CSV, tel qu'il a été configuré dans la boîte de dialogue Planifier un rapport.

Champ	Description
Séparateur CSV	Le séparateur CSV par défaut est la virgule (,). Si le contenu CSV contient une virgule, vous devez identifier un séparateur unique de façon à ce que le contenu soit stocké dans sa forme d'origine. Par exemple, si « msg » est une colonne du rapport à enregistrer au format CSV dont le contenu est le suivant : `ASA-SSM-CSC-20 Module in slot 1," application reloading ""CSC SSM""," version ""6.2.1599.0"" CSC SSM scan services are reloading because of a pattern file or configuration update` Le contenu ci-dessus sera inclus dans trois colonnes en raison des virgules (,). Pour éviter cela, vous devez spécifier un séparateur différent, comme le trait vertical « | ». **Remarque :** pour importer un fichier CSV dans Microsoft Excel, utilisez les données de l'option Données > À partir du texte, dans l'application Excel. Lorsque vous importez le fichier CSV, vous devez spécifier le type du fichier qui est importé en tant que séparateur, et utiliser le même séparateur pour générer le fichier CSV.
Séparateur de plusieurs valeurs	Les données des champs contenant plusieurs valeurs sont séparées par le séparateur de plusieurs valeurs. Le séparateur par défaut de plusieurs valeurs est le double trait vertical (||).
Autres options	Vous pouvez sélectionner l'emplacement SFTP, URL ou Partage réseau configuré dans {{RE}}, puis envoyer le rapport au format PDF ou CSV, en fonction de vos exigences.
	Sélectionnez cette option pour envoyer le rapport à l'emplacement SFTP, URL ou Partage réseau configuré dans la vue Configuration des services Reporting Engine.

Champ	Description
Type	Type d'action de sortie choisie. Par exemple, SFTP, URL ou Partage réseau.
Actions de sortie	Sélectionnez le nom SFTP, URL ou Partage réseau configuré dans la vue Configuration des services du Reporting Engine.
Envoyer sous PDF, Envoyer sous CSV	Sélectionnez ces options pour envoyer le rapport au format PDF ou CSV (ou les deux) au serveur de notification configuré (SFTP, URL ou Partage réseau).

Panneau Liste dynamique

Le panneau Liste dynamique génère les listes créées, que vous pouvez ensuite ajouter, modifier ou supprimer. La liste est générée en fonction du rapport planifié qui peut être affiché dans la vue Listes.



Le tableau suivant répertorie les opérations du panneau Générer la liste.

Opération	Description
+	Ajoute une nouvelle liste au rapport.
−	Supprime toutes les listes ajoutées au rapport.
	Affiche la boîte de dialogue Générer la liste.
Nom de la liste	Nom de la liste choisie dans le panneau Sélection de listes Pour plus d'informations sur le panneau Sélection de listes, consultez la rubrique Panneau Générer une liste.

Panneau Logo

Le panneau Logo génère le logo par défaut à partir du panneau Sélectionner un logo. Pour plus d'informations sur le choix d'un logo à partir de ce panneau, consultez la rubrique Gérer et sélectionner un logo de rapport dans Gérer les listes, les règles ou les rapports.

Vous pouvez définir le logo par défaut pour le Reporting Engine. Il s'agit du logo utilisé dans les rapports générés. Pour plus d'informations sur le choix d'un logo, consultez la rubrique Boîte de dialogue Sélectionner un logo.

Remarque : si vous n'avez sélectionné aucun logo, le logo RSA par défaut est utilisé dans le rapport. L'option **Enregistrer au format PDF** pour les rapports exécutés précédemment ne prend pas en charge un nouveau logo client. Elle affiche le logo RSA par défaut si le logo client doit être affiché dans la vue Planifier un rapport.

Vue Rapports planifiés

La vue Rapports planifiés permet de créer, d'afficher et de gérer les rapports planifiés.

Workflow

Ce workflow présente la procédure à suivre pour créer et planifier un rapport.

Que voulez-vous faire ?

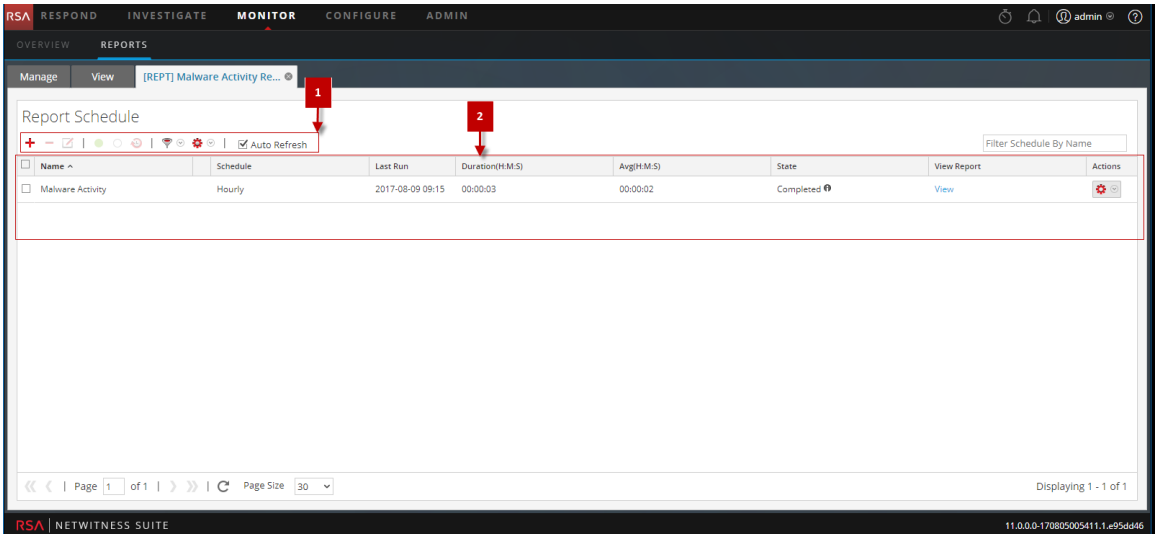
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport*	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports*	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Créer et planifier un rapport
- Gérer les listes, les règles ou les rapports
- Vue Élaborer le rapport
- Vue Rapport
- Panneau Planifier un rapport
- Boîte de dialogue Autorisations des rapports

Affichage rapide



Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.

   L'onglet Gérer s'affiche.

2. Cliquez sur **Rapports**.

   La vue Rapport s'affiche.

3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :

   - Cliquez sur  > **Afficher les rapports programmés**.
   - Cliquez sur la colonne **#Schedules**.

Fonctions

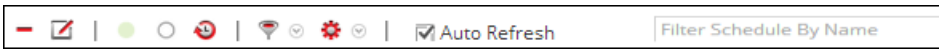
La vue Rapports planifiés est dotée des fonctionnalités suivantes :

1 Barre d'outils Planning de rapport

2 Panneau Liste des plannings de rapports

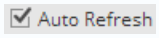
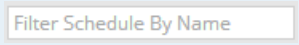
Barre d'outils Planning de rapport

Les Rapports planifiés permettent d'ajouter, de modifier et de supprimer le rapport planifié mais aussi d'activer ou de désactiver la configuration d'exécution sélectionnée.



Le tableau suivant présente les opérations de la barre d'outils Rapports planifiés.

Opération	Description
	Permet de créer un nouveau planning de rapport.
	Supprime le planning de rapport sélectionné.
	Modifie le planning de rapport sélectionné. **Remarque :** double-cliquez sur un planning de rapport souhaité pour le modifier.
	Active le planning du rapport sélectionné.
	Désactive le planning du rapport sélectionné.
	Permet d'afficher l'historique d'un rapport planifié.
	Permet de filtrer les plannings en fonction du type de planning. (Par exemple, AdHoc)

Opération	Description
	Permet de définir des autorisations pour le rapport planifié sélectionné.
	Actualise automatiquement la liste des rapports planifiés.
	Recherche des plannings sur la base du nom du planning.

Panneau Liste des plannings de rapports

Le panneau Liste des rapports planifiés répertorie les rapports planifiés sous forme de tableau.

Le tableau suivant répertorie les colonnes du panneau Liste des rapports planifiés.

Colonne	Description
Nom	Nom du rapport planifié.
Planning	Type de planning pour la configuration d'exécution : • Exécution ad-hoc • Exécution toutes les heures • Exécution quotidienne • Exécution hebdomadaire • Exécution mensuelle
Dernière exécution	Affiche la dernière date d'exécution du rapport.

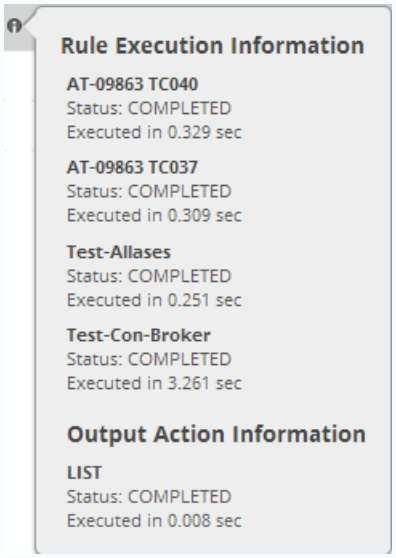
Colonne	Description
Durée (H:M:S)	Affiche le temps nécessaire pour la dernière exécution du rapport.
Moy (H:M:S)	Affiche le temps moyen nécessaire pour exécuter le rapport.

Colonne	Description
État	Indique l'état du rapport planifié. • Planifié : Si un rapport est planifié pour s'exécuter sur une base horaire, journalière, hebdomadaire, mensuelle ou ultérieurement, l'état du rapport est considéré comme étant planifié, pour la première exécution. • En attente : Si un rapport est toujours en attente d'exécution, l'état du rapport est considéré comme étant en file d'attente. • En cours d'exécution : si la planification du rapport est en cours de progression, l'état du rapport est considéré comme étant en cours d'exécution. • Partiel : Dans un rapport avec plusieurs règles, si l'exécution d'une seule règle échoue ou qu'une action de sortie échoue, ou encore que

Colonne	Description
	la création d'un fichier PDF/CSV échoue, l'état du rapport est considéré comme étant partiel. Par exemple, dans un rapport avec cinq règles dont quatre sont exécutées avec succès et une échoue, l'état du rapport est considéré comme étant partiel. • Échec : Dans un rapport avec plusieurs règles, si toutes les exécutions de la planification de règles échoue, l'état du rapport est considéré comme étant un échec. • Terminé : Si la planification du rapport est parfaitement exécutée, l'état du rapport est considéré comme étant terminé. • Annulé : Lorsqu'une demande d'annulation est terminée, l'état du rapport s'affiche comme Annulé.

Colonne	Description
	Remarque : l'option d'annulation peut ne pas fonctionner pour les tâches Warehouse Analytics. Vous devez supprimer la tâche manuellement. Voici les étapes pour supprimer la tâche : **Pour MapR** : 1. Obtenez l'identifiant de la tâche à partir des logs de la tâche. 2. Connectez-vous à l'interface utilisateur et recherchez l'identifiant de la tâche à supprimer sous « Tâches en cours ». Exemple d'URL : http://<job-tracker-host>:50030/jobtracker.jsp 3. Supprimez l'identifiant de la tâche : • Sélectionnez l'identifiant de la tâche sous « Tâches en cours », puis cliquez sur Supprimer les tâches sélectionnées. (ou) • cliquez sur le lien de l'identifiant de la tâche, faites défiler vers le bas et cliquez sur le lien Supprimer cette tâche. • Inactif : Si la planification du rapport

Colonne	Description
	est désactivée, l'état du rapport est considéré comme étant inactif. • Non disponible : Si les informations d'exécution liées à la planification des rapports ne sont pas disponibles, l'état du rapport est considéré comme étant indisponible.

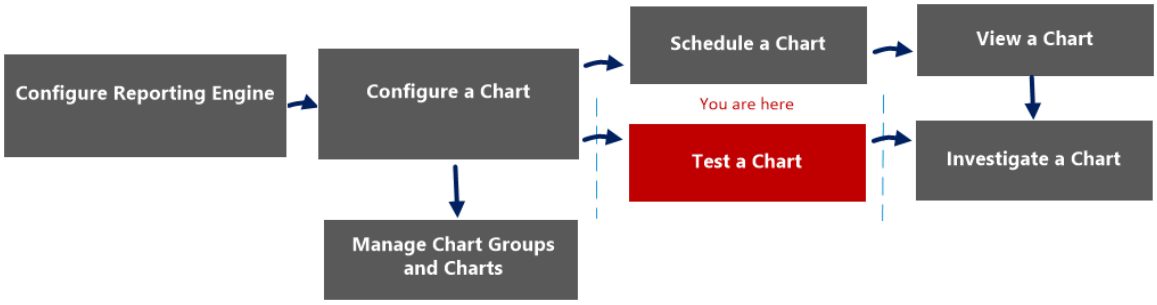
Colonne	Description
	Cliquez pour afficher les informations d'exécution de la règle et les informations de l'action de sortie. Cette fenêtre contextuelle indique l'état de plusieurs règles dans un rapport et le temps pris pour leur exécution. **Remarque :** vous pouvez afficher l'exécution de la règle et les informations d'action de sortie pour un rapport planifié ayant l'état **Terminé**, **En cours d'exécution**, **Partiel** ou **Échec**. Par défaut, les opérations de sortie pour les rapports exécutés à la page Configuration du Reporting Engine sont activées afin de recevoir un e-mail lorsque l'état du rapport est Terminé. Pour recevoir des e-mails pour les rapports dont l'état est **Échec** ou **Partiel**, vous devez désactiver cette option.

Colonne	Description
Afficher le rapport	Cliquez pour afficher les informations d'exécution de la règle sur le Panneau Afficher un rapport. Vous pouvez afficher les informations d'exécution de la règle pour un rapport planifié ayant l'état En cours d'exécution également.

Vue Tester un graphique

Dans la vue Tester un graphique, vous pouvez afficher et tester les graphiques.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique	Afficher un graphique
Administrateur/analyste	Tester un graphique*	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

*Vous pouvez effectuer ces tâches ici.

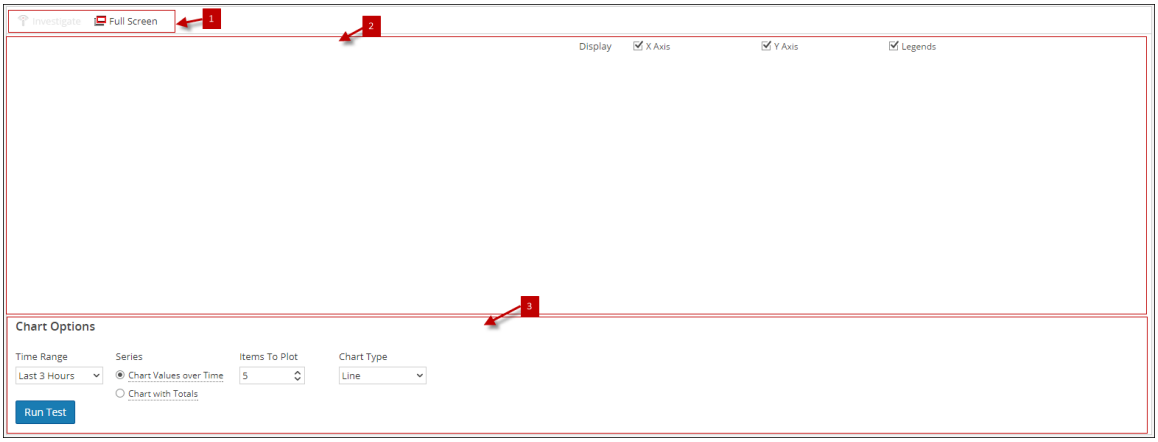
Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique

- Planifier un graphique
- Afficher un graphique
- Tester un graphique

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



La vue Tester un graphique se compose des panneaux suivants :

1	Barre d'outils Graphique
2	Panneau Sortie graphique
3	Panneau Options du graphique

Barre d'outils Graphique

La barre d'outils Graphiques vous permet d'enquêter sur un graphique particulier et de passer à un affichage plein écran.

Fonction	Description
Rechercher	Effectue une enquête supplémentaire sur le graphique sélectionné.
Plein écran	Affiche le graphique en mode plein écran.

Panneau Sortie graphique

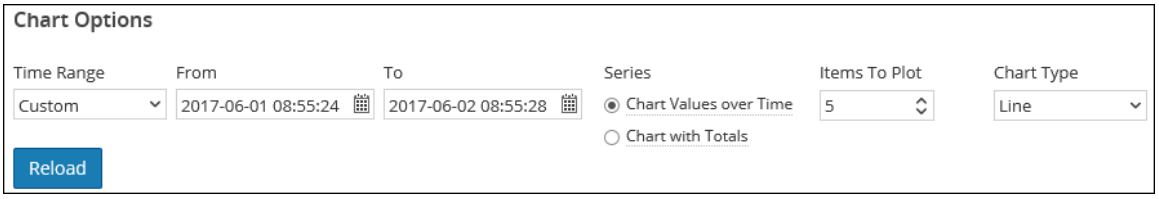
Le panneau Sortie graphique affiche les informations au format graphique en fonction des options de graphique chronologique sélectionnées.

Le tableau suivant répertorie les fonctions de la vue Tester un graphique et leurs descriptions.

Fonction	Description
Vidéo	Vous permet de sélectionner les valeurs à afficher, ainsi que les options suivantes : Axe X, Axe Y et légendes.
Axe X	Affiche le nombre de sessions.
Axe Y	Affiche la sortie réelle.
Légendes	Affiche la liste des variables apparaissant dans le graphique.

Panneau Options du graphique

La figure suivante présente le panneau Options du graphique qui contient les champs de période, de gamme et de type du graphique permettant de configurer l'affichage du graphique.



Le tableau suivant répertorie les champs du panneau Options du graphique et leurs descriptions.

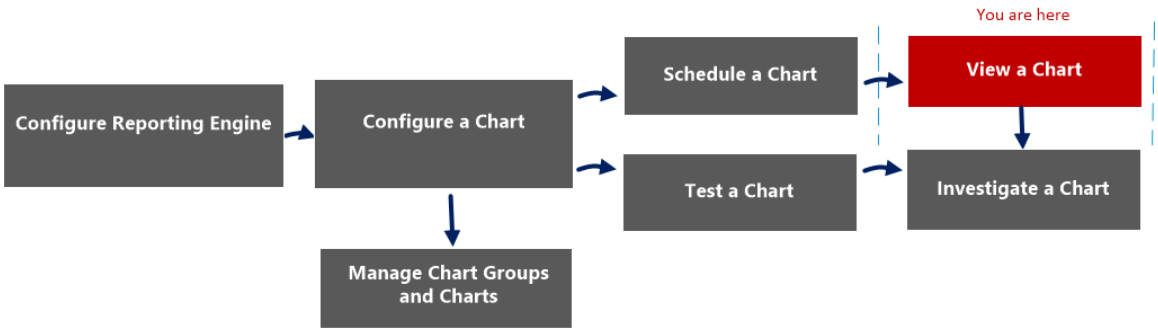
Fonction	Description
Période	La période par défaut est 3 dernières heures. Toutefois, vous pouvez sélectionner une autre valeur dans la liste déroulante, par exemple Dernière heure ou 6 dernières heures, qui sont les valeurs prédéfinies. Vous pouvez également personnaliser les valeurs en sélectionnant N derniers jours ou l'option Personnalisé.
De	La date et l'heure de début. (uniquement pour les options personnalisées).
À	La date et l'heure de fin. (uniquement pour les options personnalisées).
Gamme	Le champ Gamme vous fournit deux options : • Valeurs du graphique au fil du temps : Génère le graphique pour toute la période sélectionnée. • Graphique avec totaux : Fournit le résumé des données correspondant à la période sélectionnée.

Fonction	Description
Éléments à tracer	Nombre maximal d'événements que l'utilisateur souhaite visualiser sur le graphique.
Type de graphique	Type du graphique à afficher : graphique en escalier, graphique à barres, histogramme, graphique linéaire, graphique en escalier, graphique en escalier spline ou graphique spline.

Panneau Afficher un graphique

Dans le panneau Afficher un graphique, vous pouvez afficher et gérer les graphiques. Vous disposez de certaines options pour filtrer et trier les informations du graphique, ainsi que d'autres options pour définir le type du graphique, le nombre d'éléments à représenter, ainsi que les valeurs ou totaux du graphique. Lors de l'affichage d'un graphique, vous pouvez ouvrir les sessions de tracé de graphique dans le module Investigation, et enregistrer le graphique dans un fichier PDF.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique*	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

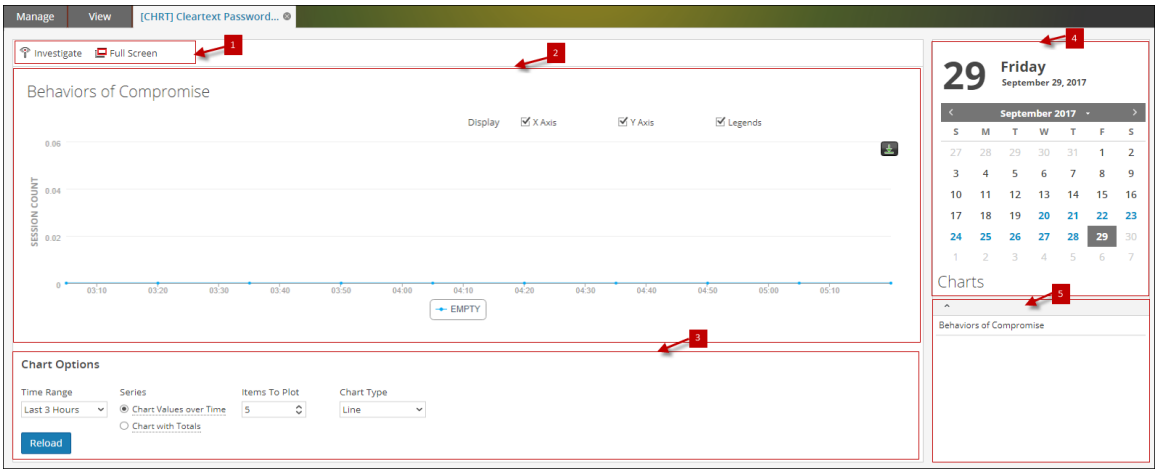
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique
- Afficher un graphique

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



Le panneau Afficher un graphique inclut les panneaux suivants :

1	Barre d'outils Graphique
2	Panneau Sortie graphique
3	Panneau Calendrier des graphiques
4	Panneau Options du graphique
5	Liste des graphiques exécutés

Barre d'outils Graphique

La barre d'outils Graphique comporte des options qui vous permettent d'examiner le graphique, et de l'afficher sur un autre écran.

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

Opération	Description
Rechercher	Permet d'examiner les détails du graphique.
Plein écran	Affiche le graphique en mode plein écran.

Panneau Sortie graphique

Ce panneau affiche le graphique en présentant le critère de tri sur l'axe des Y, la durée sur l'axe des X et les légendes.

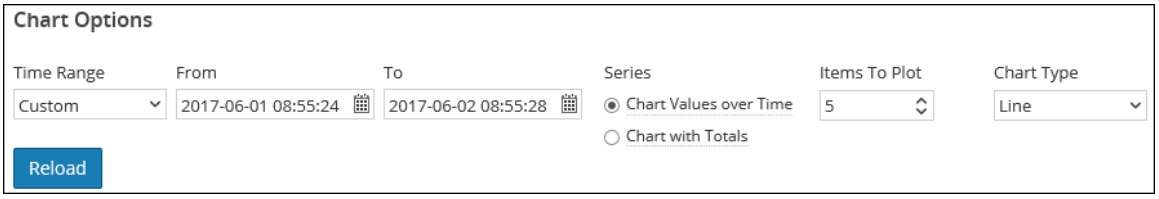
Remarque : vous pouvez enregistrer le graphique au format PDF en cliquant sur l'icône du panneau Sortie graphique.

Panneau Calendrier des graphiques

Ce panneau est le calendrier par défaut dans lequel vous pouvez filtrer la liste des graphiques en fonction de la date sélectionnée dans le calendrier, comme indiqué dans la figure suivante.

Panneau Options du graphique

Ce panneau affiche les champs de période, de gamme et de type du graphique permettant de configurer le graphique.



Le tableau suivant répertorie les champs du panneau Options du graphique.

Champ	Description
Période	La période par défaut est 3 dernières heures. Toutefois, vous pouvez sélectionner une autre valeur dans la liste déroulante, par exemple Dernière heure ou 6 dernières heures, qui sont les valeurs prédéfinies. Vous pouvez également personnaliser les valeurs en sélectionnant N derniers jours ou l'option Personnalisé. **Remarque :** la période choisie pour un graphique est enregistrée. La prochaine fois que vous ouvrez ce graphique, la période enregistrée est affichée. Ce comportement n'est pas applicable pour l'option Personnalisé.
De	La date et l'heure de début. (uniquement pour les options personnalisées).
À	La date et l'heure de fin. (uniquement pour les options personnalisées).
Gamme	Ce champ contient deux options : • Valeurs du graphique au fil du temps : Génère le graphique pour toute la période sélectionnée. • Graphique avec totaux. Fournit le résumé des données correspondant à la période sélectionnée.
Éléments à tracer	Nombre maximal d'événements que l'utilisateur souhaite visualiser sur le graphique.
Type de graphique	Type de graphique à afficher. Graphique en escalier, graphique à barres, histogramme, graphique linéaire, graphique en escalier, graphique en escalier spline ou graphique spline.

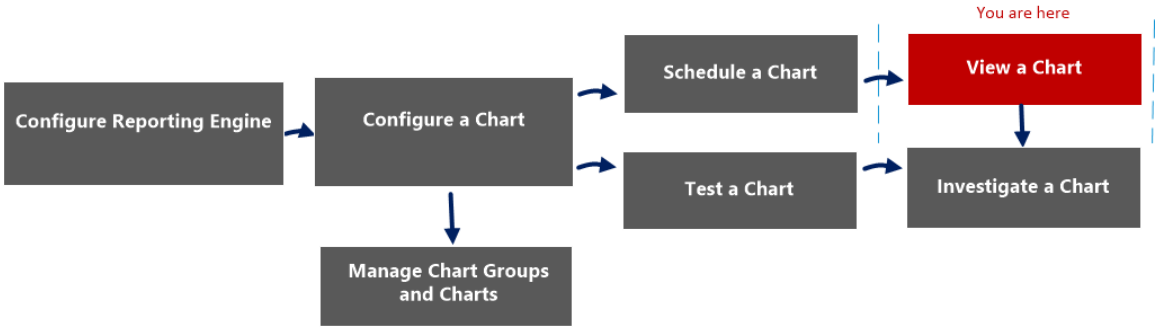
Panneau Liste des graphiques exécutés

Ce panneau affiche toutes les exécutions d'un graphique donné à la date sélectionnée. Double-cliquez sur l'une de ces exécutions pour charger le graphique dans le panneau Sortie graphique. Par défaut, le dernier graphique exécuté est affiché dans le panneau Sortie graphique.

Vue Afficher tous les graphiques

Dans la vue Afficher tous les graphiques, vous pouvez afficher, imprimer et enregistrer les graphiques, et les envoyer par e-mail.

Workflow



Que voulez-vous faire ?

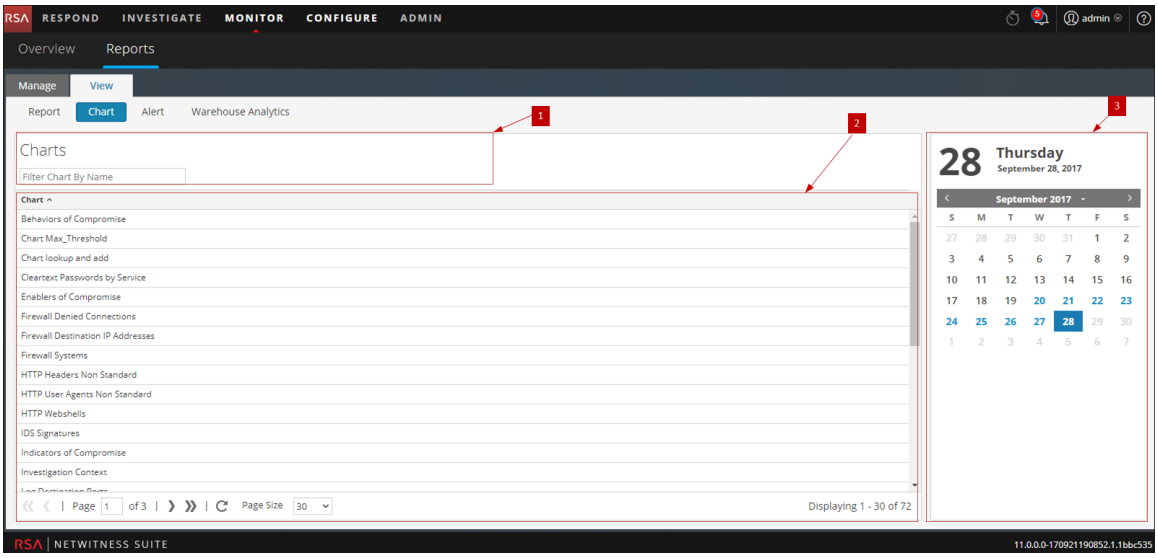
Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Configurer le Reporting Engine » dans le *Guide de configuration de Reporting Engine*.
Administrateur/analyste	Configurer un graphique	Configurer un graphique
Administrateur/analyste	Planifier un graphique	Planifier un graphique
Administrateur/analyste	Afficher un graphique*	Afficher un graphique
Administrateur/analyste	Tester un graphique	Tester un graphique
Administrateur/analyste	Analyser un graphique	Analyser un graphique
Administrateur/analyste	Gérer un groupe de graphiques et un graphique	Gérer un groupe de graphiques et un graphique

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un graphique
- Configurer un graphique
- Planifier un graphique
- Afficher un graphique

Affichage rapide



Le panneau Afficher tous les graphiques inclut les panneaux suivants :

1	Barre d'outils Graphiques
2	Panneau Sortie Graphiques
3	Panneau Calendrier des graphiques

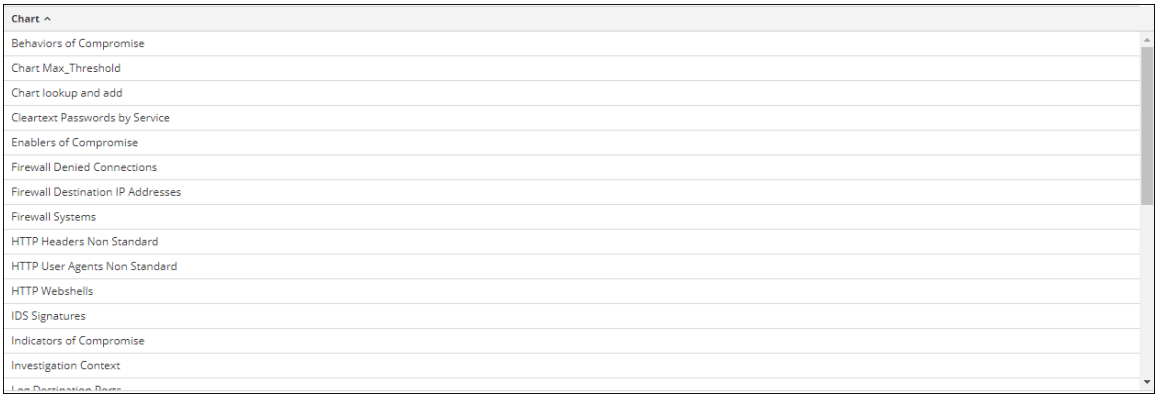
Barre d'outils Graphiques

Le tableau suivant répertorie les options de la barre d'outils Afficher tous les graphiques :

Opération	Description
Filter Chart By Name	Effectue une recherche dans les plannings sur la base du nom du graphique pour un jour calendaire sélectionné.

Panneau Sortie Graphiques

Le panneau Sortie Graphiques affiche le graphique avec le nom du planning du graphique.



Fonction	Description
Graphique	Ce champ affiche tous les graphiques exécutés avec succès.

Panneau Calendrier des graphiques

Le panneau Calendrier des graphiques permet de sélectionner une date dans le calendrier. En fonction de la date que vous sélectionnez dans la liste, la liste des graphiques qui ont été exécutés correctement pour cette date s'affiche.


28
Thursday
September 28, 2017
September 2017
S M T W T F S
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7

Panneau Afficher un rapport

Le panneau Afficher un rapport permet de consulter les rapports.

Workflow

Ce workflow présente la procédure à suivre pour afficher un rapport ou la liste de tous les rapports.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports*	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

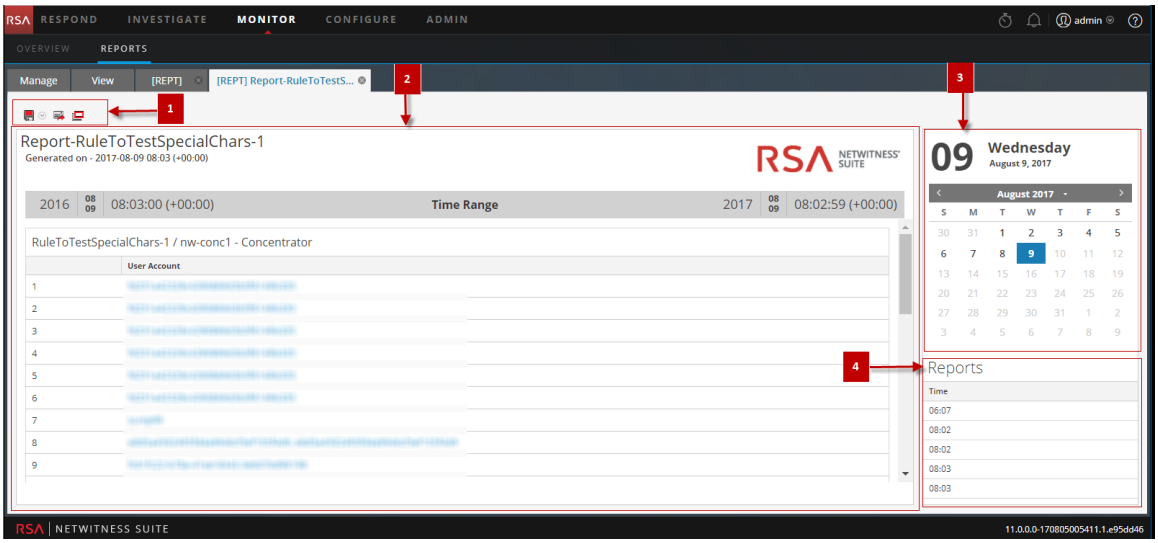
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Élaborer le rapport
- Boîte de dialogue Importer le rapport
- Vue Rapports planifiés
- Boîte de dialogue Autorisations des rapports
- Vue Afficher tous les rapports
- Vue Rapport

Affichage rapide



Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Liste des rapports**, exécutez l'une des opérations suivantes :
   - Cliquez sur  > **Afficher les rapports programmés**.
   - Cliquez sur la colonne **#Schedules**.
     La vue Planning de rapport s'affiche.
4. Cliquez sur **Afficher**.

Fonctions

Le panneau Afficher un rapport contient les sections suivantes :

1	Barre d'outils Rapports
2	Panneau Sortie Rapports
3	Panneau Calendrier des rapports
4	Panneau Heure des rapports

Barre d'outils Rapports

Cette barre d'outil vous permet d'imprimer, d'enregistrer et d'envoyer par e-mail des rapports, et de les consulter en mode plein écran.

Remarque : Reporting Engine est chargé de la génération des sorties des rapports au format PDF et CSV en fonction de leur définition. La taille des fichiers PDF d'un rapport ne doit pas excéder 50 000 cellules.

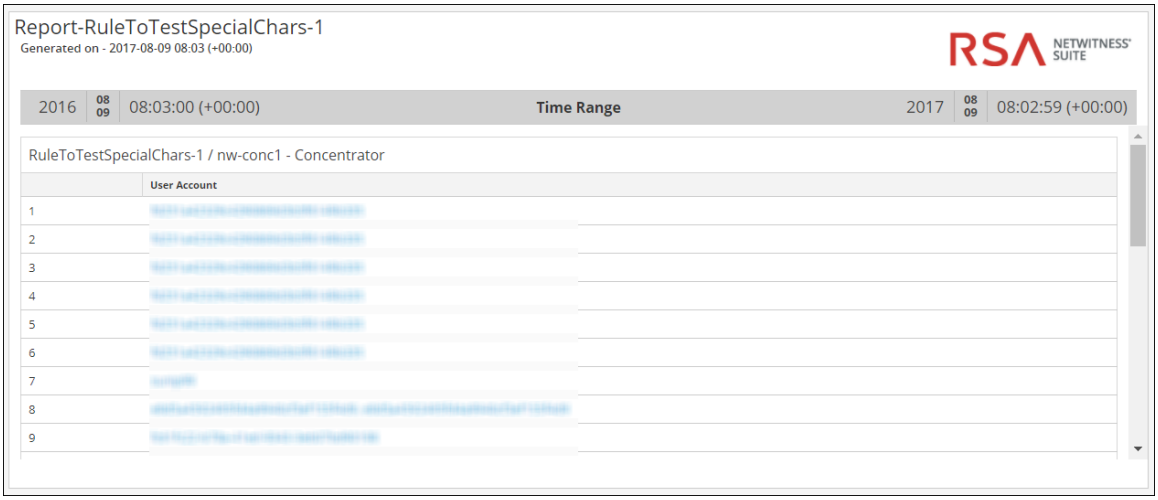
Le tableau suivant répertorie les options de la barre d'outils Rapports.

Opération	Description
	Imprime le rapport généré.

Opération	Description
	Enregistre le rapport au format PDF et CSV. **Remarque :** l'option **Enregistrer au format PDF** n'est pas disponible pour un rapport volumineux. Si vous générez un PDF pour un rapport mais que sa durée d'exécution est plus longue que prévu, le message d'avertissement suivant s'affiche :La génération du fichier PDF est en cours. Veuillez réessayer ultérieurement. **La génération du fichier PDF est en cours. Veuillez réessayer ultérieurement**. Lorsque vous cliquez sur Télécharger au format CSV, la boîte de dialogue Sélectionner la règle à télécharger s'affiche. Vous devez sélectionner une règle dans cette boîte de dialogue pour en télécharger le résultat dans un fichier CSV. Si la génération du fichier PDF ou CSV est longue, vous pouvez cliquer sur l'option **M'avertir** pour être informé dès qu'elle est terminée. Une fois le fichier PDF ou CSV généré, vous pouvez afficher les notifications d'état.
	Envoie le rapport par e-mail avec une pièce jointe au format PDF ou CSV.
	Ouvre le rapport généré dans une nouvelle fenêtre.

Vue Sortie Rapports

La vue Sortie Rapports affiche le rapport avec son nom de planning, l'heure de sa génération et le rapport réel avec les variables de règle sélectionnées.



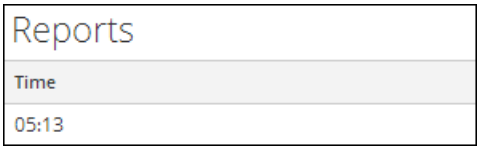
Fonction	Description
Nom	Ce champ affiche le nom du rapport programmé.
Heure	Ce champ affiche l'heure à laquelle le rapport est généré.
Rapport	Ce champ affiche le rapport détaillé avec les variables de règle sélectionnées.

Vue Calendrier des rapports

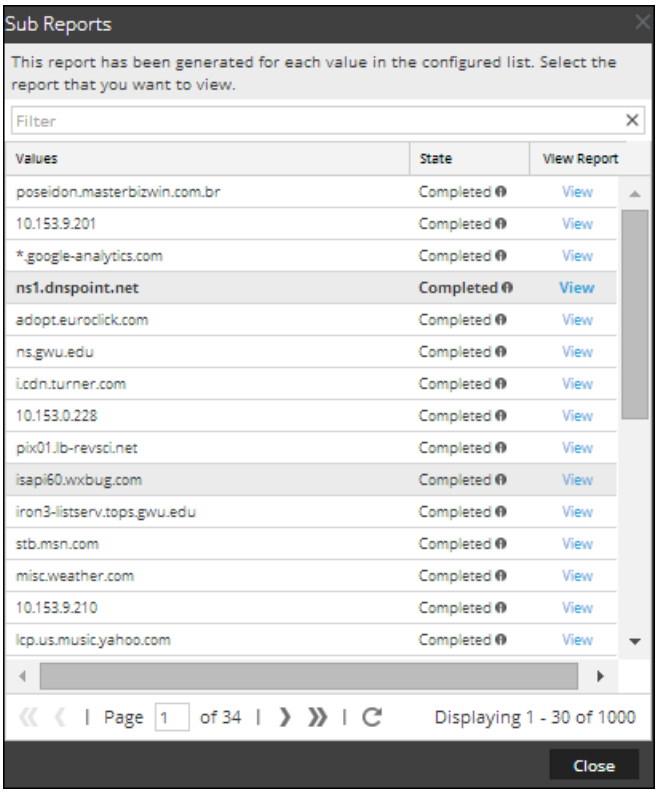
La vue Calendrier des rapports permet de sélectionner une date dans le calendrier. La liste des rapports correctement générés à la date choisie est affichée.

Vue Heure des rapports

La vue Heure des rapports indique l'heure d'exécution réelle du rapport.



Lorsque vous cliquez sur **Afficher** dans le rapport planifié dont l'option **Itératif** est sélectionnée, le panneau **Sous-rapports** s'affiche. Pour chaque valeur de la liste configurée, un rapport est généré.



Le tableau ci-dessous répertorie les colonnes du panneau Sous-rapports.

Colonne	Description
Valeurs	Valeurs de liste choisies pour une variable dynamique dans le panneau Sélection de listes.

Colonne	Description
État	Indique l'état du rapport planifié pour chacune des valeurs de liste. • Partiel : Si, dans un rapport avec plusieurs règles, l'exécution d'une seule règle, d'une action de sortie ou de la création d'un PDF/CSV a échoué, l'état Partiel du rapport s'affiche. Par exemple, si un rapport a cinq règles, que quatre règles sont exécutées avec succès et qu'une règle échoue, l'état Partiel s'affiche. • Échec : Dans un rapport avec plusieurs règles, si toutes les exécutions de règle échouent, l'état du rapport est considéré comme étant un échec. • Terminé : Si un rapport est exécuté avec succès, son état est considéré comme étant terminé.
Vue	Cliquez sur l'une des planifications de rapport ou l'un des sous‑rapports répertoriés, puis cliquez sur **Afficher** pour afficher le rapport souhaité. **Remarque :** vous pouvez afficher les règles terminées à la page **Afficher un rapport** même lorsque le rapport est en cours d'exécution.

Vue Afficher tous les rapports

Dans la vue Afficher tous les rapports, vous pouvez afficher, imprimer et enregistrer les rapports, et les envoyer par e-mail.

Workflow

Ce workflow présente la procédure à suivre pour afficher un rapport ou la liste de tous les rapports.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Configurer le Reporting Engine	Pour plus d'informations, consultez la rubrique « Étape 3 : Configurer les sources de données du Reporting Engine » dans le *Guide de configuration de Reporting Engine*
Administrateur/analyste	Créer une liste ou un groupe de listes/créer ou déployer une règle/tester une règle	Configurer une règle
Administrateur/analyste	Créer et planifier un rapport	Créer et planifier un rapport
Administrateur/analyste	Afficher un rapport ou la liste de tous les rapports*	Afficher un rapport
Administrateur/analyste	Analyser un rapport	Analyser un rapport

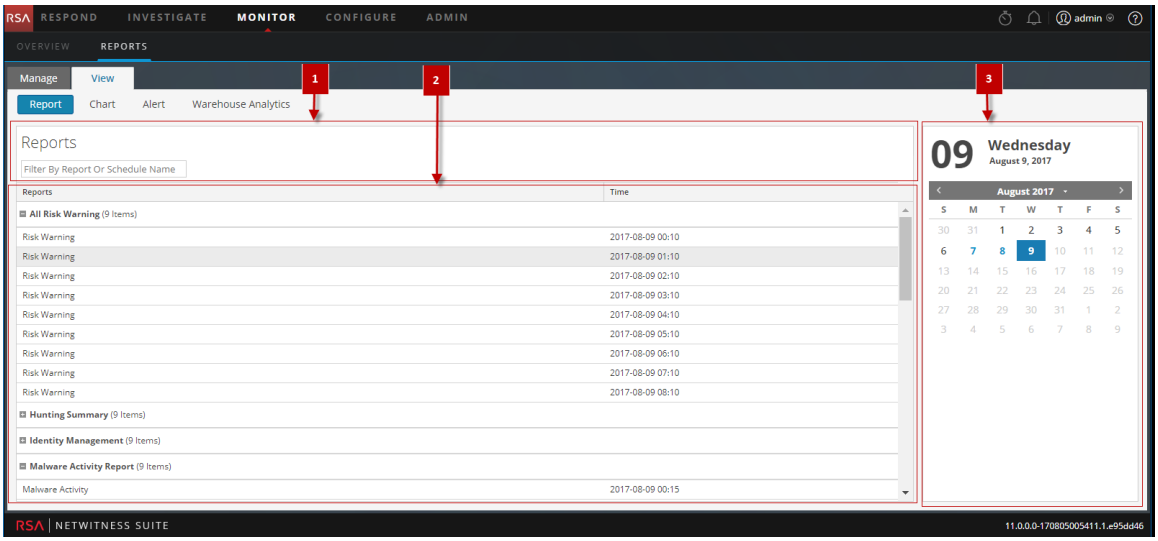
Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer/contrôler l'accès aux listes, règles ou rapports	Gérer les listes, les règles ou les rapports

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Configurer et générer un rapport
- Configurer une règle
- Créer et planifier un rapport
- Afficher un rapport
- Analyser un rapport
- Gérer les listes, les règles ou les rapports
- Vue Élaborer le rapport
- Boîte de dialogue Importer le rapport
- Vue Rapports planifiés
- Boîte de dialogue Autorisations des rapports
- Panneau Afficher un rapport
- Vue Rapport

Affichage rapide



Pour accéder à cette vue :

1. Sélectionnez **SURVEILLER** > **Rapports**.
   L'onglet Gérer s'affiche.
2. Cliquez sur **Rapports**.
   La vue Rapport s'affiche.
3. Dans le panneau **Rapport**, cliquez sur **Afficher tous les rapports**.
   Le panneau Rapports s'affiche. Il vous suffit de cliquer sur l'un des rapports répertoriés pour l'afficher.

Fonctions

Le panneau Afficher tous les rapports contient les fonctions suivantes.

1. Barre d'outils Rapports
2. Panneau Sortie Rapports
3. Panneau Calendrier des rapports

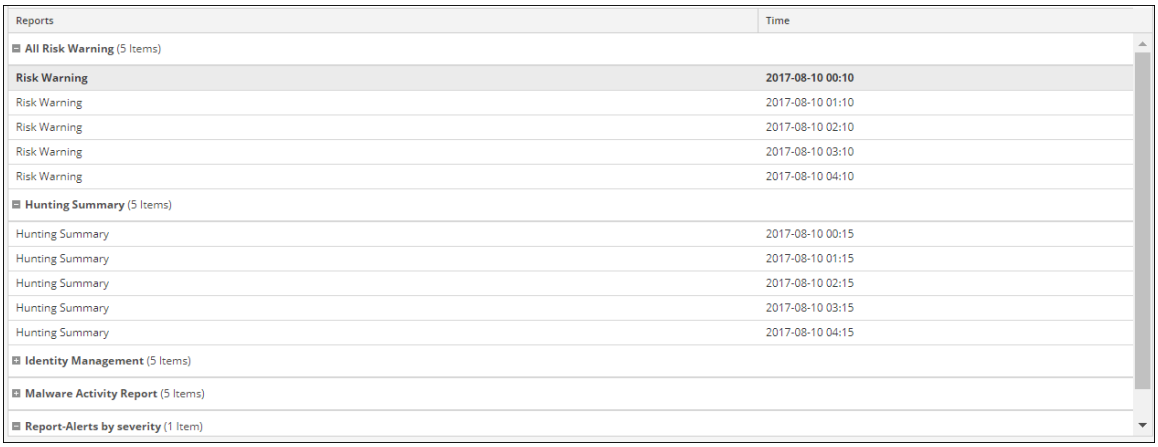
Barre d'outils Rapports

Le tableau suivant répertorie les options de la barre d'outils Afficher tous les rapports :

Opération	Description
Filter By Report Or Schedule Name	Recherche les plannings d'après le nom du rapport ou du planning pour la journée sélectionnée dans le calendrier.

Panneau Sortie Rapports

Le panneau Sortie Rapports affiche le rapport avec son nom de planning et l'heure de sa génération.



Fonction	Description
Rapports	Ce champ affiche le rapport détaillé avec les variables de règle sélectionnées.
Heure	Ce champ affiche l'heure à laquelle le rapport est généré.

Vue Calendrier des rapports

La vue Calendrier des rapports permet de sélectionner une date dans le calendrier. La liste des rapports correctement générés à la date choisie est affichée.

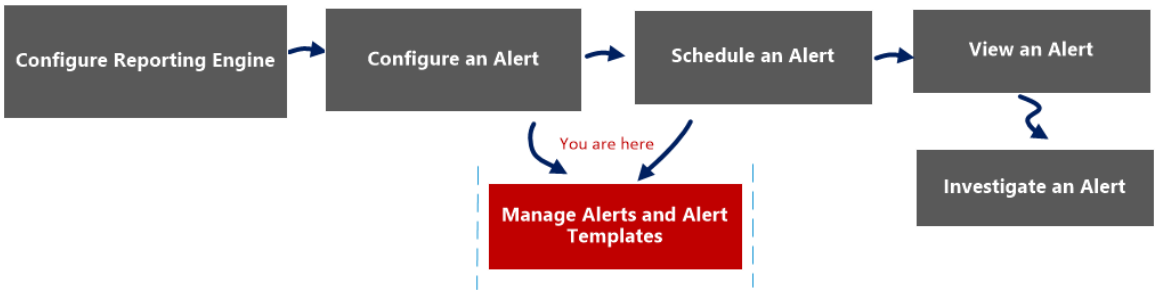
Références aux alertes

L'interface utilisateur du module Reporting fournit un accès aux alertes NetWitness. Cette rubrique contient des descriptions de l'interface utilisateur ainsi que d'autres informations de référence pour aider les utilisateurs à gérer les alertes.

Vue Liste des alertes

La vue Liste des alertes vous permet d'importer, d'exporter, de gérer et d'ajouter des alertes.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte*	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

Configuration d'une alerte

Planifier une alerte

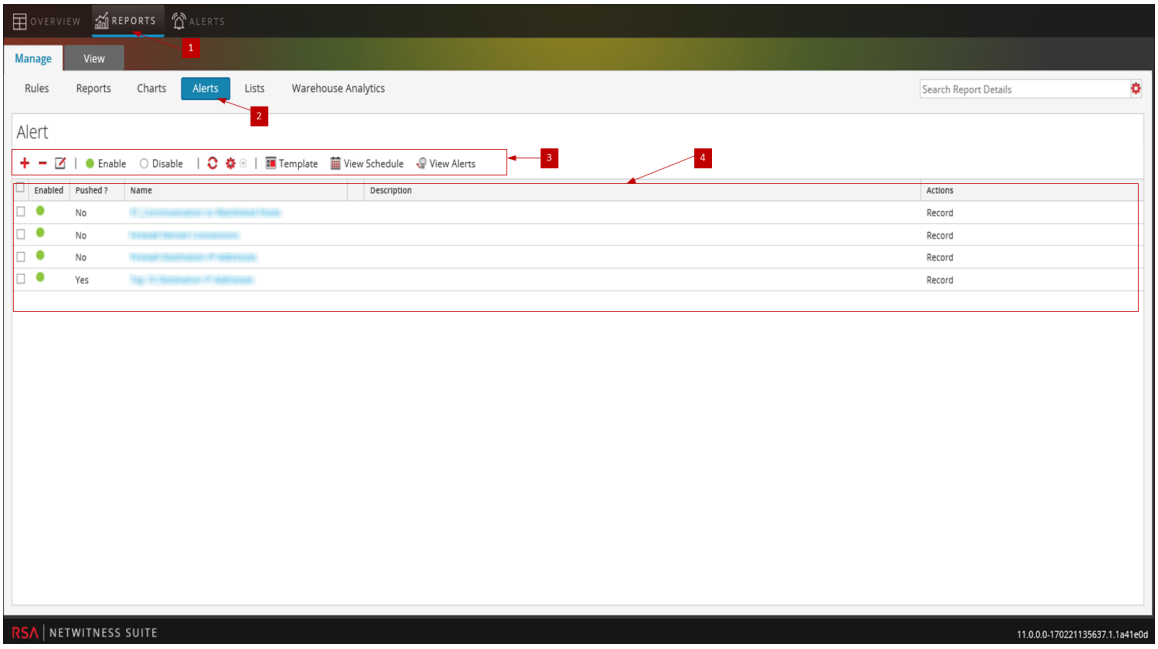
Afficher une alerte

Analyser une alerte

Gérer une alerte et un modèle d'alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



1	Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2	Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3	La barre d'outils Alerte vous permet d'ajouter, de modifier, de supprimer, d'activer, de désactiver, d'actualiser, d'importer et d'exporter une alerte. Elle vous permet également d'accéder aux autorisations d'accès pour l'alerte sélectionnée.
4	Le panneau Liste des alertes répertorie toutes les alertes au format tabulaire.

La vue Liste des alertes contient les panneaux suivante :

- Barre d'outils Alerte
- Liste des alertes

Barre d'outils Alerte

Le panneau Barre d'outils Alerte contient les fonctions suivantes :

Fonction	Description
+	Ajoute une nouvelle alerte au module Reporting.
−	Supprime une ou plusieurs alertes sélectionnées.
✎	Modifie une alerte.

Fonction	Description
Activer	Active les alertes sélectionnées.
Désactiver	Désactive les alertes sélectionnées.
	Actualise la vue.
	Active les options suivantes : Importer, Exporter et Autorisations.

Liste des alertes

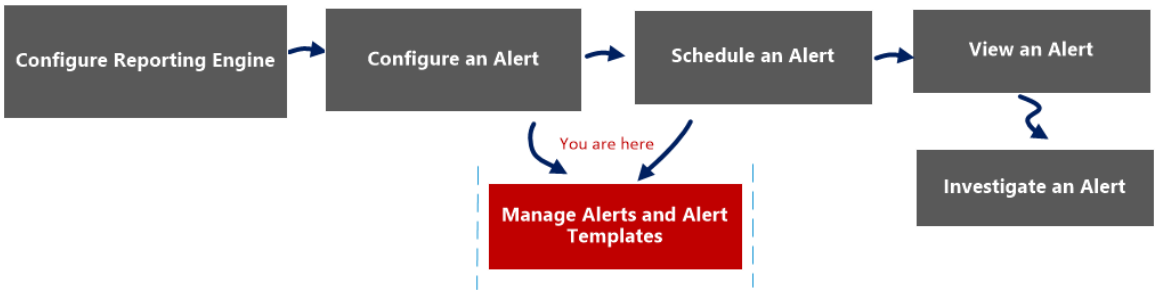
Le panneau Liste des alertes répertorie toutes les alertes au format tabulaire. Le tableau ci-dessous répertorie les colonnes du panneau Liste des alertes et leur description.

Fonction	Description
Activé	Affiche l'état de l'alerte : • Activé - L'alerte est active et se déclenche en fonction de la règle qui lui est attribuée. • Désactivé - L'alerte n'est pas active.
Transmis ?	Indique si l'alerte est envoyée aux Decoders ou Log Decoders : • Oui - L'alerte est envoyée aux Decoders ou Log Decoders. • Non - L'alerte n'est pas envoyée aux Decoders ou Log Decoders.
Nom	Identifie le nom de l'alerte. Cliquer sur le nom de l'alerte affiche la règle en fonction de laquelle cette alerte est basée dans le panneau Définir des règles.
Description	Indique la description de l'alerte.
Actions	Indique l'action exécutée par le système lors du déclenchement de l'alerte. Les différents types d'action disponibles sont : • Enregistrement • SMTP • SNMP • Syslog

Boîte de dialogue Autorisations d'alerte

Dans la boîte de dialogue Autorisations d'alerte, les utilisateurs avec l'autorisation d'accès en lecture et écriture, peuvent définir les autorisations d'accès à une alerte pour configurer les autorisations dans la boîte de dialogue Autorisations d'alerte.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte*	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

Configuration d'une alerte

Planifier une alerte

Afficher une alerte

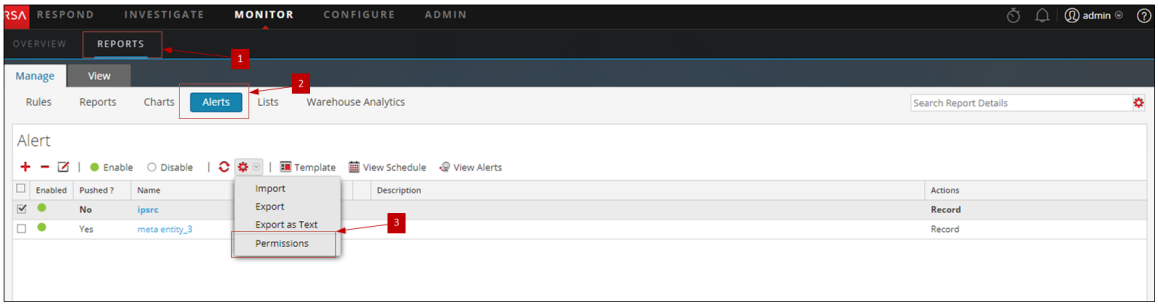
Analyser une alerte

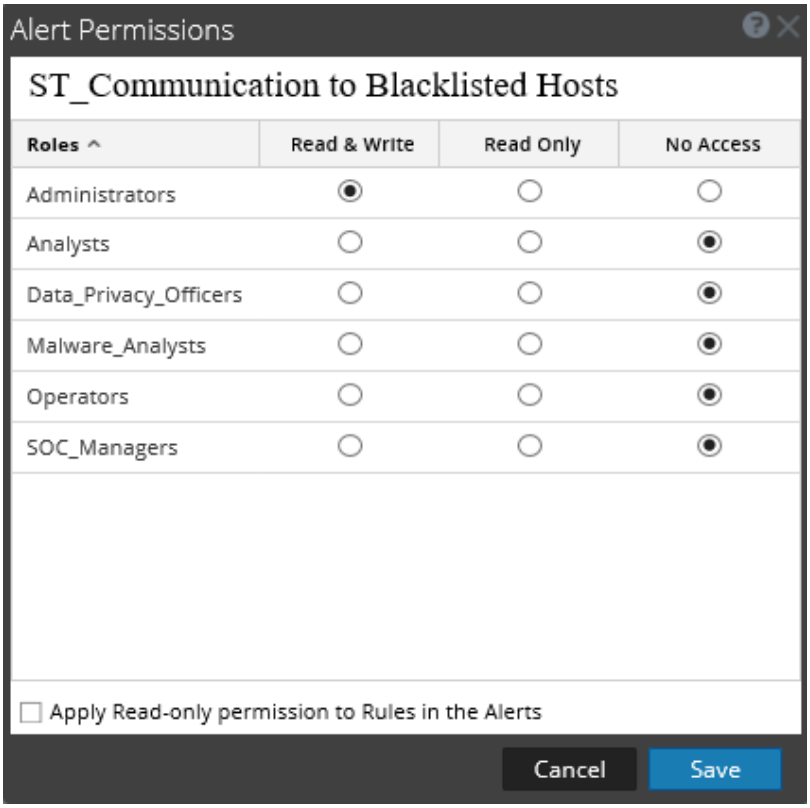
Gérer une alerte et un modèle d'alerte

Affichage rapide

La boîte de dialogue Autorisations d'alerte vous permet de définir des autorisations d'alerte en fonction du rôle d'utilisateur.

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.





1. Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3. Cliquez sur > **Autorisations**. La boîte de dialogue Autorisations d'alerte s'affiche.
4. En fonction du rôle d'utilisateur, sélectionnez les options appropriées.
5. (Facultatif) Pour accorder automatiquement l'autorisation d'accès en lecture aux règles

dépendantes, activez la case à cocher.

6 Cliquez sur **Enregistrer.**

Remarque : si un utilisateur (autre qu'un superutilisateur) crée une alerte, les superutilisateurs ne pourront pas accéder à l'alerte.

Le tableau suivant répertorie les colonnes de la boîte de dialogue Autorisations d'alerte.

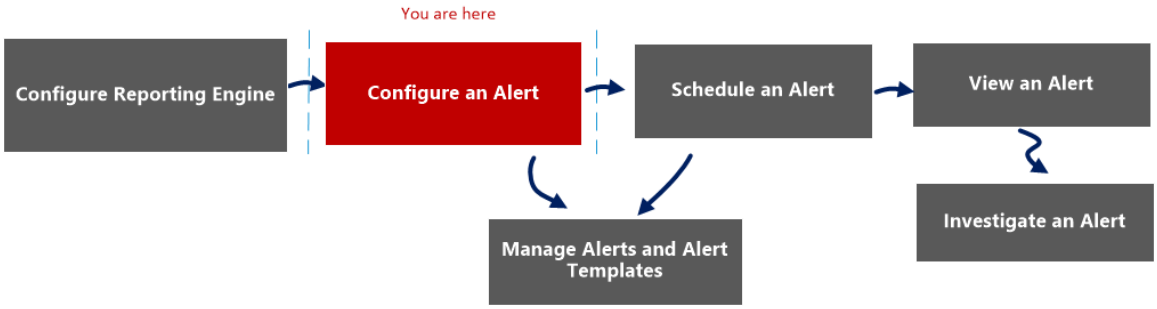
Colonne	Description
Rôles	Affiche tous les rôles d'utilisateur dans l'interface utilisateur de NetWitness.
Lecture et écriture	Vous permet d'appliquer l'accès en lecture/écriture à l'alerte.
Lecture seule	Vous permet d'appliquer uniquement l'accès en lecture à l'alerte.
Aucun accès	En sélectionnant cette autorisation, vous ne pouvez pas accéder à l'alerte ou l'afficher.
Appliquer l'autorisation de lecture seule aux règles dans les alertes	Vous permet d'appliquer automatiquement des autorisations aux règles dans les alertes.
Annuler	Annule toutes les modifications appliquées aux autorisations.
Enregistrer	Enregistre la sélection et fournit un accès aux rôles en fonction de la sélection.

Vue Planning des alertes

Dans la vue Planning des alertes, vous pouvez afficher toutes les alertes planifiées. Vous pouvez également désactiver les alertes planifiées.

Workflow

Le workflow suivant présente les tâches impliquées dans la création ou la modification d'une alerte.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte*	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

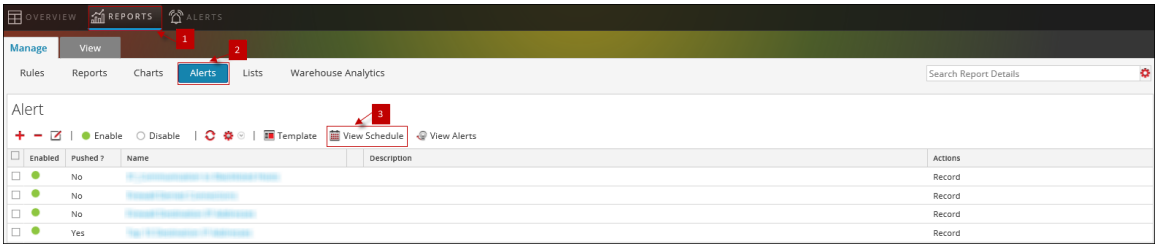
Rubriques connexes

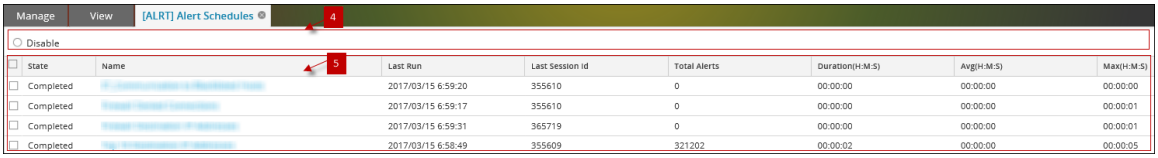
Présentation des alertes

Configuration d'une alerte

Affichage rapide

L’exemple suivant vous montre comment accéder à la boîte de dialogue Vue Planning des alertes.





1. Cliquez sur **Surveiller**> **Rapports** pour afficher l’onglet Gérer.
2. Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3. Cliquez sur **Afficher le planning** pour ouvrir la vue Afficher la planification des alertes.
4. La barre d'outils Planification des alertes vous permet de modifier l'état de l'alerte planifiée.
5. Le panneau Liste des plannings d'alertes répertorie uniquement les alertes activées, au format tabulaire.

Fonctions

Les différents panneaux contenus dans la boîte de dialogue Vue Planning des alertes sont les suivants :

- Panneau Barre d'outils de la planification des alertes
- Panneau Liste des plannings d'alertes

Panneau Barre d'outils de la planification des alertes

Dans le panneau Barre d'outils de la planification des alertes, l’icône Désactiver permet de désactiver l’alerte sélectionnée. Lorsque des alertes planifiées ne sont plus nécessaires ou qu'elles s'avèrent inefficaces, vous pouvez les désactiver afin qu'elles ne soient plus exécutées. Vous pouvez sélectionner une ou plusieurs alertes à désactiver. Lorsqu'une alerte est désactivée, elle est supprimée de la liste des alertes planifiées. En outre, elle n'est plus exécutée tant que vous ne l'exécutez pas manuellement ou que vous ne configurez pas un nouveau planning.

Panneau Liste des plannings d'alertes

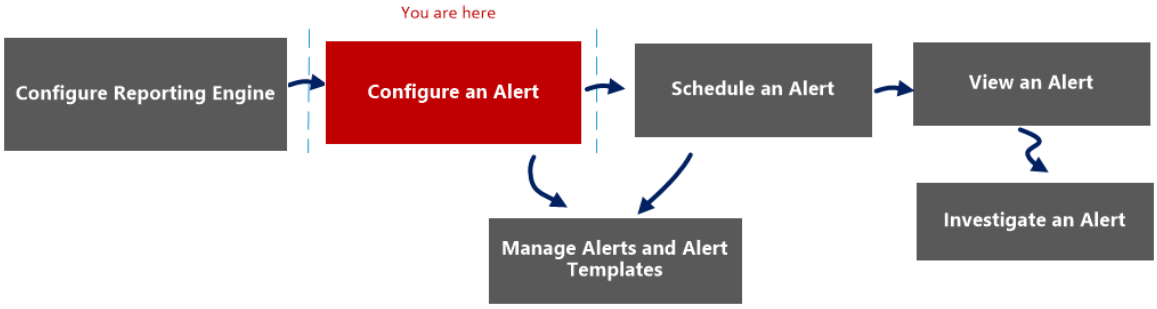
Le tableau suivant répertorie les colonnes du panneau Liste des plannings d'alertes et leur description.

Colonne	Description
État	État de l'alerte planifiée : • Terminé • Échec
Nom	Nom de l'alerte planifiée.
Dernière heure d'exécution	Heure de la dernière exécution de l'alerte.
ID de dernière session	ID de session de la dernière alerte planifiée.
Nombre total d'alertes	Nombre total des occurrences des événements.
Durée	Durée d'exécution de l'alerte planifiée.
Moy. (s)	Durée moyenne d'exécution de l'alerte planifiée.
Max. (s)	Durée maximale d'exécution de l'alerte planifiée.

Panneau Créer/Modifier une alerte

Le panneau Créer/Modifier une alerte est un panneau de la vue Liste des alertes. Ce panneau vous permet de créer ou modifier une alerte selon les besoins.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte*	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

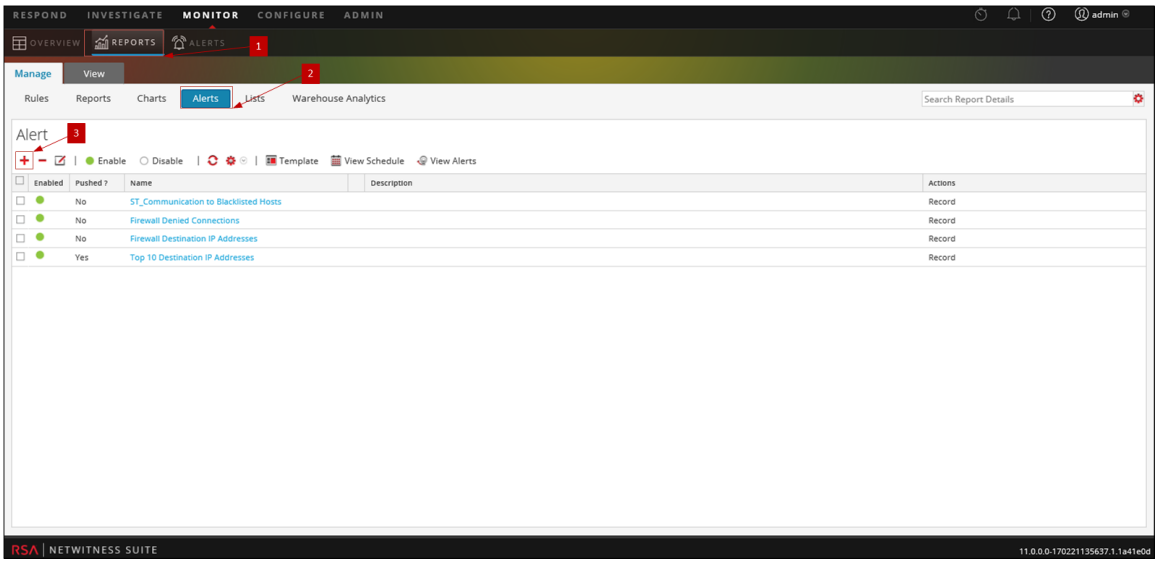
Rubriques connexes

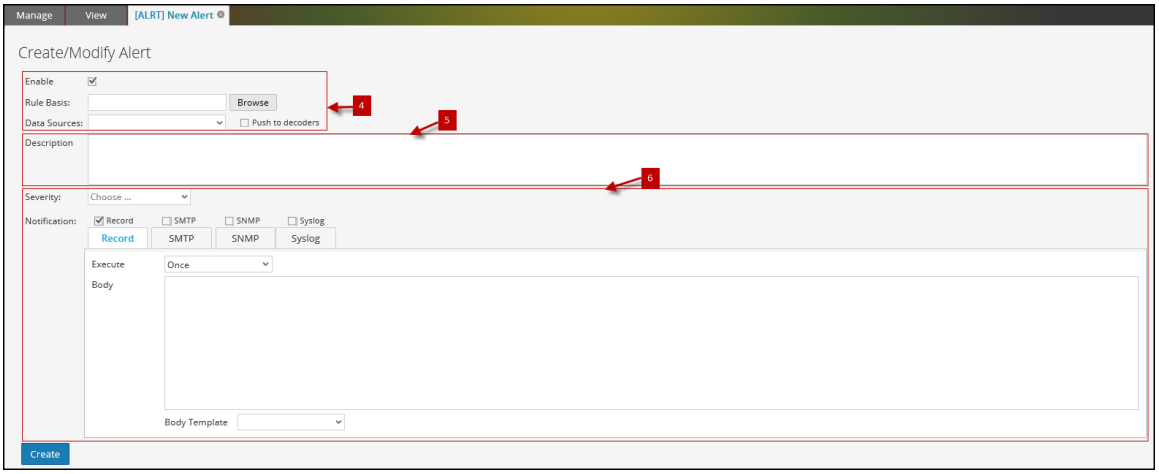
Présentation des alertes

Configuration d'une alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.





1	Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2	Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3	Cliquez sur + pour accéder au panneau Créer/Modifier une alerte.
4	Activez l'alerte, accédez la règle et sélectionnez une source de données pour l'alerte.
5	Saisissez une brève description de l'alerte.
6	Définir les méthodes de notification d'alerte (ENREGISTREMENT, SMTP, SNMP, Syslog) pour l'alerte, lorsqu'une condition d'alerte est remplie.

Le panneau Créer/modifier une alerte comprend les sections suivantes :

- Définition d'alerte
- Description de l'alerte

- Notification d'alerte

Définition d’alerte

Le tableau suivant décrit les champs de Définition d'alerte :

Champ	Description
Activer	• **Activer** - active l'alerte. L'alerte s'exécute et envoie des actions de sortie toutes les minutes (par défaut) lorsque les conditions d'alerte sont remplies. • **Désactiver** - désactive l'alerte. L'alerte ne s'exécute pas et n'envoie pas d'actions de sortie.
Base de règle	Cliquez sur **Parcourir** pour afficher le panneau Bibliothèque de règles dans lequel vous sélectionnez la règle qui constitue la base de cette alerte. Vous devez sélectionner une règle disposant d'une clause ‘where’ unique pour une alerte.
Sources de données	Spécifie la source de données pour l'alerte.
Transmettre aux décodeurs	Transmettez la clause ‘where’ de la règle d'alerte aux Decoders connectés à la source de données NWDB sélectionnée. Il s'agit de l'option utilisée pour créer des alertes RE, car les conditions d'alerte sont vérifiées au niveau du Decoder lui-même et les requêtes d'alerte seront plus rapides avec NWDB. Si vous désélectionnez cette option, une requête sera envoyée avec la clause ‘where’ de la règle d’alerte vers la source de données NWDB sélectionnée. En fonction de la complexité et des métas dans la clause ‘where’ de la règle, il se peut que le traitement des requêtes d'alertes soit plus long dans NWDB. **Remarque :** NetWitness n'envoie pas de règles au Decoder de manière automatique.

Description de l’alerte

Le tableau suivant décrit les champs de Description de l'alerte :

Champ	Description
Description	Décrit l'alerte.
Créer	Crée une alerte. (Cette option s'affiche lorsque vous créez une alerte.)
Enregistrer	Enregistrer les modifications apportées à l'alerte. (Cette option s'affiche lorsque vous modifiez une alerte.)

Notification d'alerte

Notification d'alerte vous permet de définir l'action de notification prise par NetWitness lorsqu'une alerte est générée, comme l'enregistrement ou l'envoi de l'alerte à l'aide de l'une des actions de sortie définies. Les actions de sortie sont un message Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) ou Syslog.

La section Notification présente l'onglet par défaut Enregistrement que vous utilisez pour créer une alerte. L'icône située à côté de l'onglet Enregistrement vous permet de sélectionner le type de notification à partir de la liste déroulante pour la sortie à spécifier pour cette alerte : SMTP, SNMP ou Syslog.

Selon le type de notification sélectionné, la section Notification est renseignée avec un texte prédéfini contenant certaines variables qui ajoutent des méta adaptés à l'alerte. Dans le Reporting Engine, ces variables sont remplacées par des valeurs réelles. Le tableau suivant répertorie les variables et leurs descriptions.

Variable	Description
`${meta.<metakey>}`	Valeur de la clé méta. **Remarque :** si <metakey> n'extrait aucune valeur, la chaîne vide ("") est imprimée. Par défaut, Reporting Engine affiche toutes les valeurs répétées pour une clé méta. Si vous ne souhaitez pas répéter les métavaleurs dans la sortie d'alerte, activez l'option « removeRepeatedMetaValue » en accédant à **Configuration > Configuration des alertes** disponible pour le Reporting Engine sous **Services - Configuration > vue Explorer**. Par exemple, dans une session HTTP, la valeur de l'action s'affiche sous la forme get, get, put, put, post, get. Lorsque cette option est activée, la valeur s'affiche en tant que get, put, post.

Variable	Description
`${meta.time}` / `${meta.time:<time_format>}`	`${meta.time}` - La durée de la session s'affiche au format « aaaa-MMM-jj HH:mm:ss ». `${meta.time:<time_format>}` - La durée de la session s'affiche au format horaire personnalisé défini par l'utilisateur. Par exemple, `${meta.time:dd-MM-yyyy HH:mm:ss}`. Pour plus d'informations sur les formats horaires pris en charge, consultez http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html **Remarque :** si le format horaire fourni par l'utilisateur n'est pas valide, le format horaire par défaut sera utilisé. Le format horaire par défaut est "aaaa-MMM-jj HH:mm:ss".
`${name}`	Nom de l'alerte défini dans Reporting Engine.
`${count}`	Nombre de fois qu'une alerte est détectée sur une période donnée. (Par défaut, il s'agit d'une minute)
`${nw.host}`	Nom d'hôte NetWitness tel qu'il est configuré dans Reporting Engine.
`${device.id}`	ID de périphérique NetWitness de la source de données.

Notification d'alerte comporte quatre onglets :

- **Onglet Enregistrement**
- **Onglet SMTP**
- **Onglet SNMP**
- **Onglet Syslog**

Onglet Enregistrement

Utilisez l'onglet Enregistrement pour définir la fréquence d'enregistrement d'une alerte et le message que vous souhaitez générer lorsqu'une alerte est générée.

Le tableau suivant répertorie les champs de l'onglet Enregistrement et leur description.

Champ	Description
Exécuter	Fréquence à laquelle enregistrer une alerte. • **Une fois** - N'enregistre l'alerte qu'une seule fois selon la fréquence de l'alerte, quel que soit le nombre de fois où l'alerte est générée. NetWitness enregistre le nombre de fois où l'alerte a été générée effectivement pendant cet intervalle dans le fichier log. Ainsi, les analystes peuvent savoir combien de fois l'alerte a enregistré une correspondance sur un jour spécifique. • **À chaque événement** - Enregistre l'alerte à chaque génération. Si une alerte est générée un nombre illimité de fois pendant une journée, cette alerte est considérée comme parasite et elle est ignorée, sauf dans le cas d'alertes qui requièrent une surveillance continue comme les modifications de configuration réseau et les attaques DDOS. **Remarque :** sélectionnez le paramètre **À chaque événement** à partir de la liste déroulante **Exécuter** pour les actions de sortie SNMP et Syslog.
Corps	Corps du message.
Modèle de corps	(Facultatif) Si les modèles ont été définis, sélectionnez un modèle pour le message d'alerte.

Onglet SMTP

L'onglet SMTP vous permet de définir la sortie SMTP (e-mail) pour cette alerte.

Le tableau suivant répertorie les champs de l'onglet SMTP et leur description.

Champ	Description
Exécuter	Fréquence d'envoi un message électronique de l'alerte. • **Une fois** - Envoie uniquement un e-mail par intervalle si l'alerte se déclenche dans cet intervalle, peu importe le nombre de déclenchements d'alerte. • **À chaque événement** - Envoie un e-mail avec l'alerte pour chaque événement pour lequel les critères de règles sont réunis.
À	Adresses e-mail auxquelles envoyer cette alerte.
Objet	Objet du message électronique.
Corps	Corps du message.
Modèle de corps	(Facultatif) Si des modèles ont été définis, sélectionnez un modèle pour le message SMTP que vous pouvez utiliser tel quel ou modifié.

Onglet SNMP

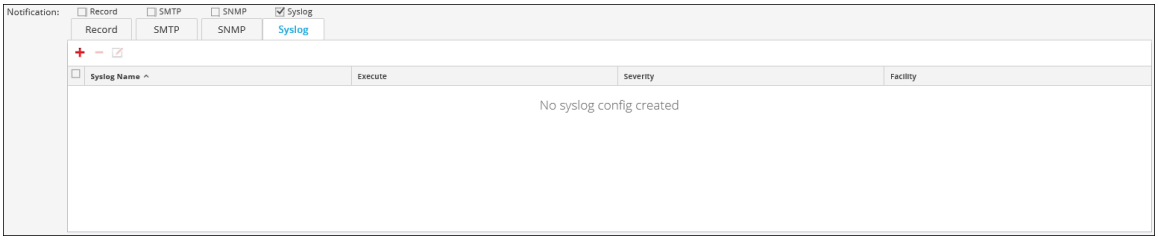
L'onglet SNMP vous permet de définir la sortie SNMP pour l'alerte.

Le tableau suivant répertorie les différents champs dans l'onglet SNMP et leur description.

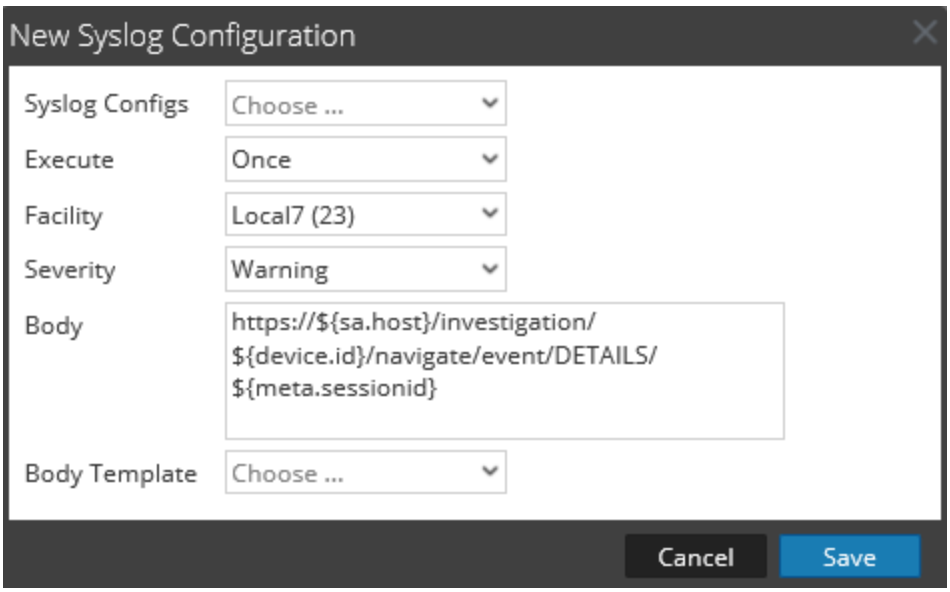
Champ	Description
Exécuter	Fréquence d'envoi d'une sortie SNMP pour une alerte. • **Une fois** - Envoie un message SNMP avec un e-mail par intervalle si l'alerte est générée dans cet intervalle, peu importe le nombre de générations d'alerte. • **À chaque événement** - Envoie un message SNMP avec l'alerte pour chaque événement pour lequel les critères de règles sont réunis.
Corps	Corps du message.
Modèle de corps	(Facultatif) Si des modèles ont été définis, sélectionnez un modèle pour le message SNMP à utiliser tel quel ou modifié.

Onglet Syslog

L'onglet Syslog vous permet de définir la sortie du message Syslog pour cette alerte.



Cliquez sur + pour ajouter une configuration Syslog à une alerte. La boîte de dialogue Nouvelle configuration Syslog s'affiche :



Le tableau ci-dessous décrit les champs de la boîte de dialogue Nouvelle configuration Syslog :

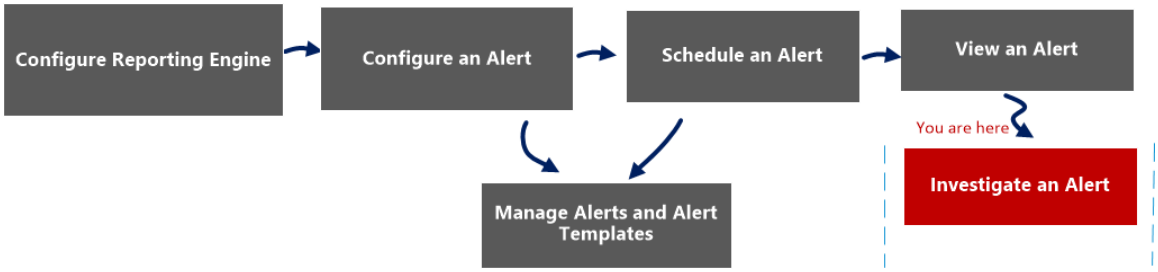
Champ	Description
Configurations Syslog	Indique la configuration Syslog de la vue Configuration de périphérique située dans le panneau Configuration Syslog.
Exécuter	Nombre de fois que vous souhaitez envoyer une sortie Syslog pour l'alerte. • **Une fois** - Envoie une sortie Syslog avec un e-mail par intervalle. Une l'alerte est générée dans cet intervalle quel que soit le nombre de générations d'alerte. • **À chaque événement** - Envoie une sortie Syslog avec l'alerte pour chaque événement pour lequel les critères de règles sont réunis.

Champ	Description
Site	Type de programme qui consigne le message. Syslog, processus, messagerie et noyau sont des exemples de types de programmes.
Gravité	Niveau de gravité des alertes générées. • Urgence • Alerte • Critique • Erreur • Avertissement • Avis • Information • Débogage
Corps	Corps du message.
Modèle de corps	(Facultatif) Si des modèles ont été définis, sélectionnez un modèle pour le message Syslog à utiliser tel quel ou modifié.

Vue Analyser une alerte

Dans la vue Analyser une alerte, vous pouvez afficher et examiner les détails de l'alerte. Au cours de l'enquête sur une alerte, vous pouvez ouvrir les sessions dans le module Investigation pour une procédure d'enquête plus approfondie.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte*	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

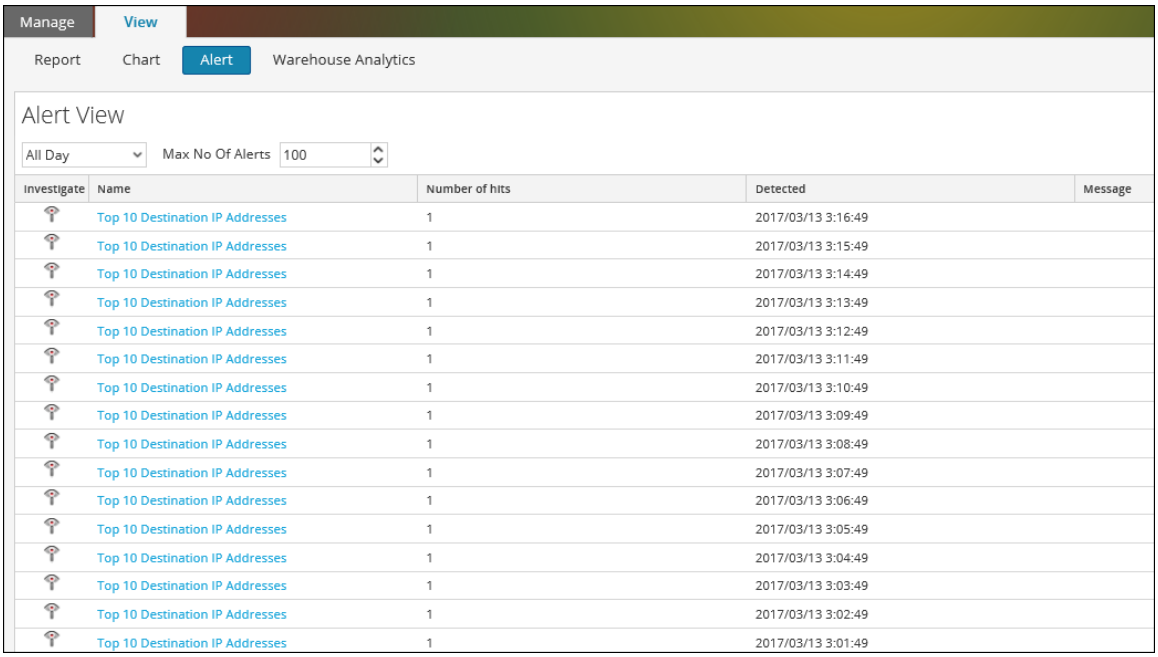
Configuration d'une alerte

Planifier une alerte

Afficher une alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



La vue Afficher une alerte comprend les panneaux suivants :

- Barre d'outils Afficher les alertes
- Afficher la liste des alertes

Afficher la liste des alertes

Le tableau ci-dessous répertorie les colonnes du panneau Afficher la liste des alertes.

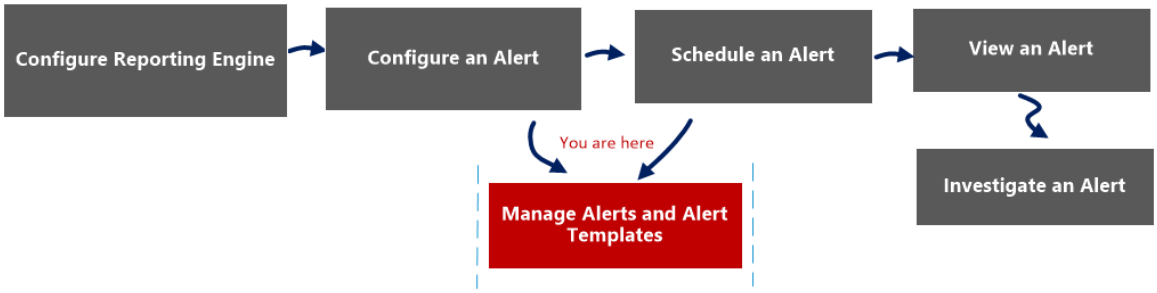
Colonne	Description
	Icône qui permet d'ouvrir le module Investigation dans lequel s'affichent les détails de la première session qui a enregistré la correspondance de l'alerte donnée pour une analyse immédiate. **Remarque :** vous n'êtes pas redirigé vers le module Investigation dans les cas suivants : -Vous reconfigurez une source de données pour une alerte existante et exécutez une alerte sur la nouvelle source de données. -Vous saisissez un nom d'hôte à la place d'une adresse IP dans le champ Source de données.
Nom	Nom de l'alerte qui a enregistré la correspondance. Le lien hypertexte du nom ouvre le module Investigation pour afficher toutes les correspondances de cette alerte spécifique pour l'heure entourant l'alerte enregistrée.

Colonne	Description
Nombre de correspondances	Nombre de fois où l’alerte est générée.
Détecté	Date et heure auxquelles l’alerte est génèrée.
Message	Messages d’alerte.

Boîte de dialogue Importer l'alerte

La boîte de dialogue Importer l'alerte, vous permet d'importer une archive d'alertes et spécifier si elle doit remplacer des règles, listes et alertes existantes.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte*	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

Configuration d'une alerte

Planifier une alerte

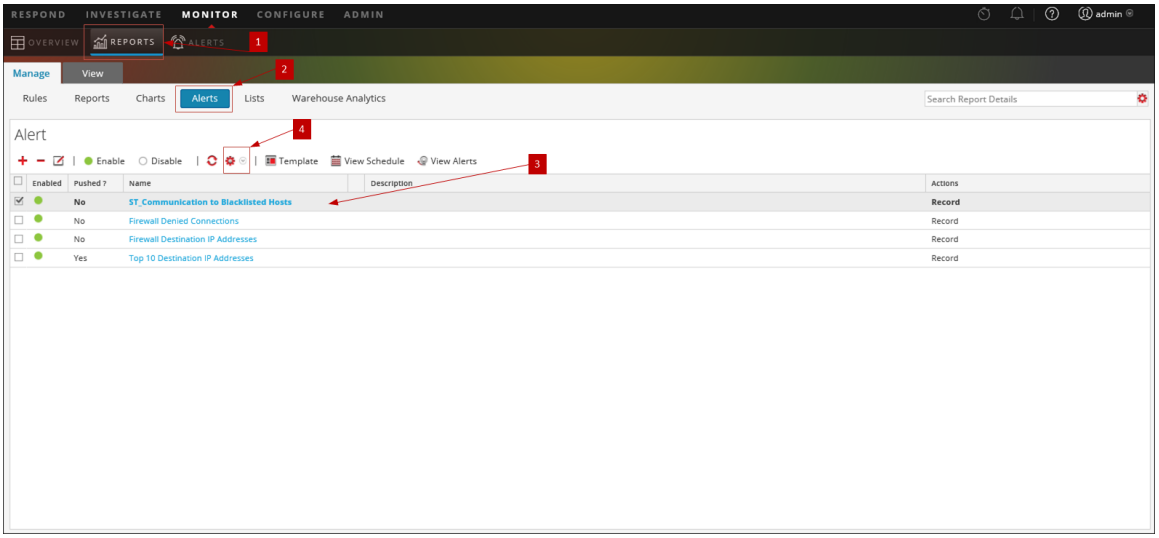
Afficher une alerte

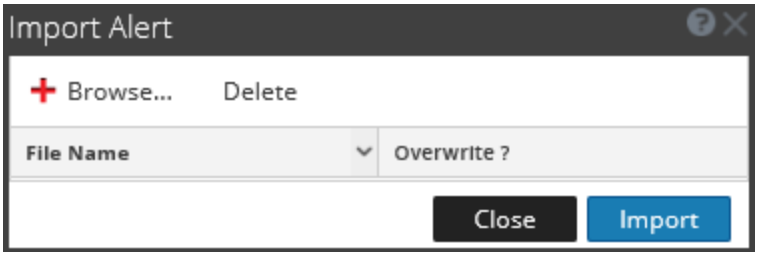
Analyser une alerte

Gérer une alerte et un modèle d'alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.





1. Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3. Dans le panneau **Alerte**, sélectionnez un dossier pour importer le fichier.
4. Dans la barre d'outils **Alerte**, cliquez sur > **Importer** pour importer une alerte.

Le tableau suivant répertorie les actions de la boîte de dialogue Importer l'alerte et leurs descriptions.

Actions	Description
Browse...	Affiche une vue du système local de fichiers zip pour sélectionner l'alerte à importer.
	Supprime l'alerte sélectionnée dans la boîte de dialogue Importer l'alerte.

Actions	Description
Nom de fichier	Nom du fichier binaire importé.
Remplacer ?	Permet de sélectionner l'option pour remplacer une version existante de l'alerte que vous importez. Si vous ne sélectionnez pas l'option Remplacer, une copie du fichier est importée et aucun message d'erreur ne s'affiche.
Fermer	Ferme la boîte de dialogue Importer l'alerte.
Importer	Importe l'alerte avec un message de confirmation.

Références aux modèles d’alerte

L'interface utilisateur du module Reporting fournit un accès aux alertes et modèles d'alerte NetWitness. Cette rubrique contient des descriptions de l'interface utilisateur ainsi que d'autres informations de référence pour aider les utilisateurs à gérer les modèles d'alerte.

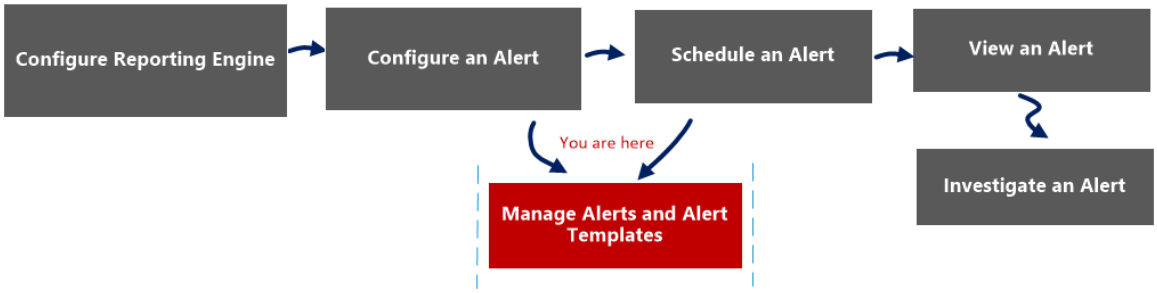
Rubriques :

- Vue Créer/Modifier un modèle
- Vue Modèle

Vue Modèle des alertes

La vue Modèle vous permet d'ajouter, d'afficher et de supprimer des modèles d'alerte.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte*	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

Configuration d'une alerte

Planifier une alerte

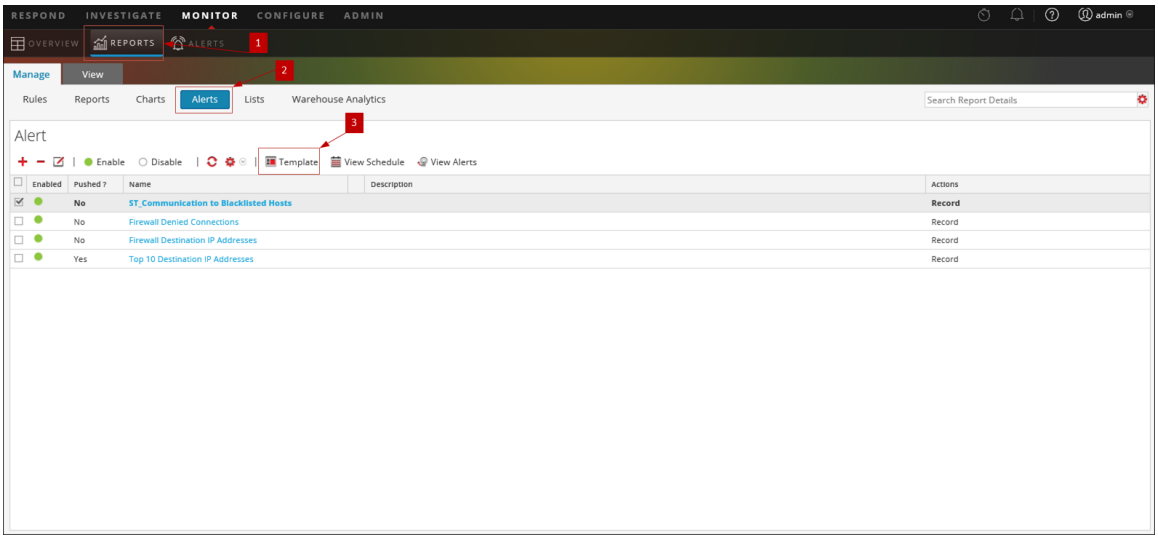
Afficher une alerte

Analyser une alerte

Gérer une alerte et un modèle d'alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.



1. Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2. Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3. Cliquez sur Template pour ouvrir la vue Modèle.
4. La barre d'outils Modèle permet d'ajouter, de modifier et de supprimer des modèles d'alerte.
5. Le panneau Liste des modèles vous permet d'afficher une liste de tous les modèles dans un format tabulaire.

La vue Modèle des alertes comprend les panneaux suivants :

- Barre d'outils Modèle
- Liste des modèles

Barre d'outils Modèle

Lorsque des modèles ont été définis, vous pouvez sélectionner un modèle pour simplifier la définition et la modification des messages d'alerte.

Le tableau suivant affiche les différentes actions dans la vue Modèle et leur description.

Actions	Description
	Crée un nouveau modèle d’alerte.
	Supprime le modèle d’alerte sélectionné.
	Modifie un modèle d’alerte existant.

Liste des modèles

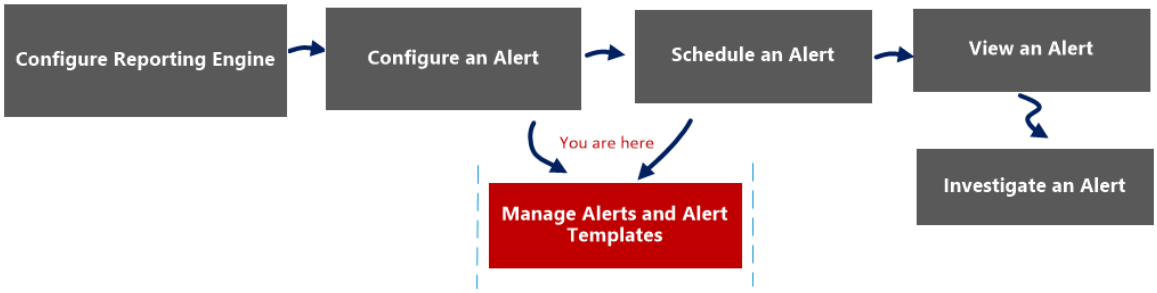
Le tableau suivant décrit les colonnes du panneau Liste des modèles.

Colonne	Description
Nom	Nom du modèle
Message	Message d'alerte défini pour le modèle.

Vue Créer/Modifier un modèle

Dans la vue Créer/Modifier un modèle, vous pouvez personnaliser des modèles d'alertes à utiliser lors de la création d'alertes.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte*	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

Configuration d'une alerte

Planifier une alerte

Afficher une alerte

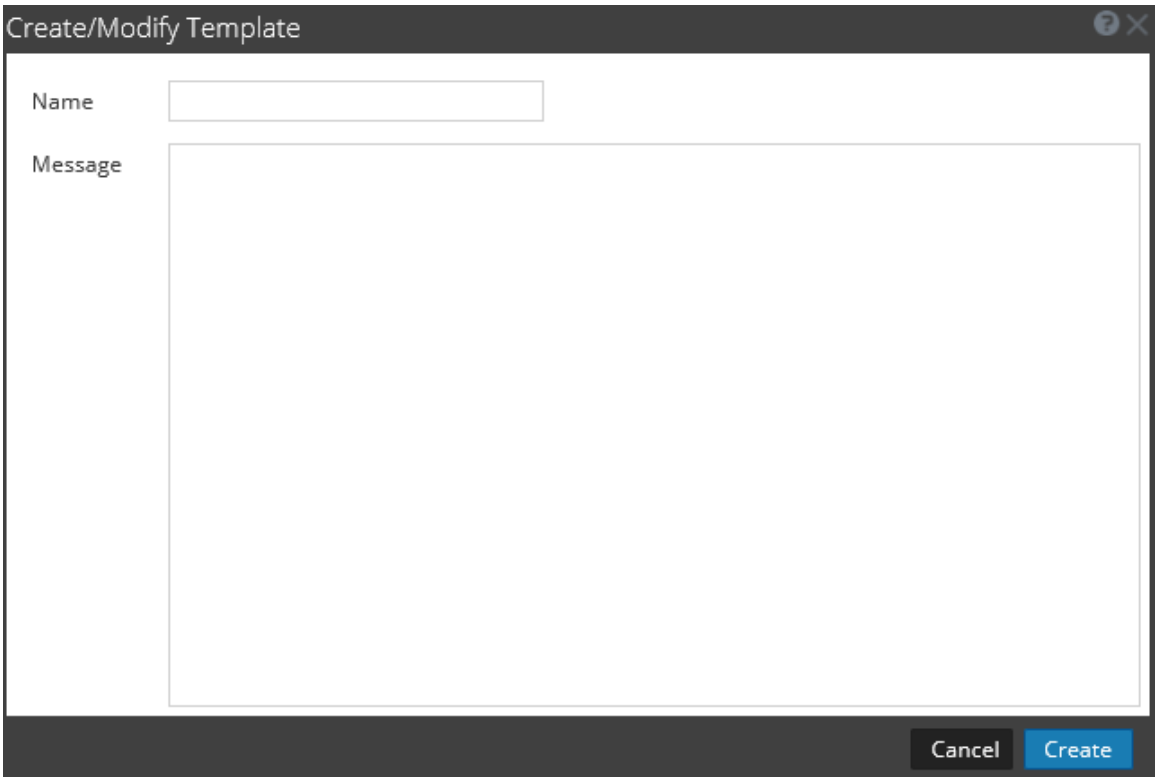
Analyser une alerte

Gérer une alerte et un modèle d'alerte

Affichage rapide

Vous pouvez créer ou modifier un nom de modèle d’alerte et le message sur cette vue.

La figure suivante est un exemple du modèle Créer ou modifier une alerte.



Le tableau ci-dessous décrit les champs de la boîte de dialogue Créer/Modifier un modèle.

Fonction	Description
Nom	Indique le nom du modèle pour les alertes de Reporting. Par exemple, l'adresse IP source.
Message	Spécifie le message à envoyer lorsqu'une alerte se déclenche.
Créer	Crée le modèle avec un message de confirmation dont la disponibilité est immédiate pour l’utilisation dans Reporting.
Enregistrer	Enregistre le modèle avec les détails modifiés ou lorsqu'un nouveau modèle est créé. Ce bouton est visible uniquement en mode modification.
Annuler	Ferme la boîte de dialogue sans enregistrer le modèle ou toute modification apportée au modèle.

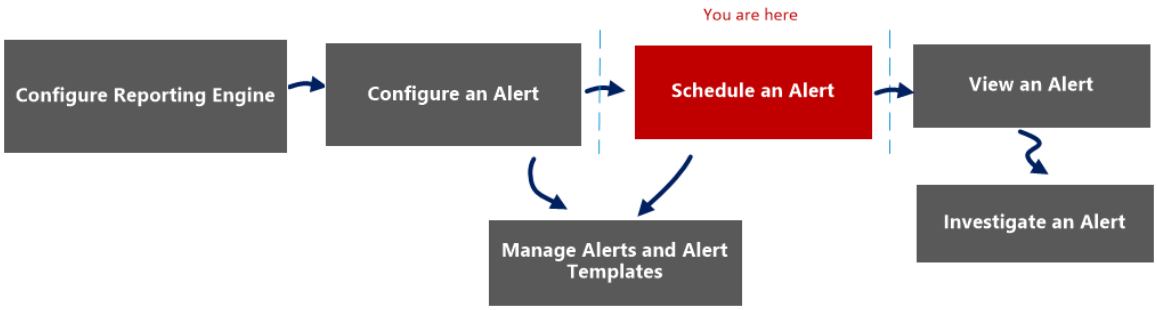
Vue Afficher la planification des alertes

Dans la vue Afficher la planification des alertes, vous pouvez afficher les informations suivantes pour chacune de vos alertes planifiées :

- état d'achèvement, nom, dernière exécution, dernier identifiant SID, nombre total d'alertes déclenchées ;
- statistiques relatives à la durée d'exécution de l'alerte planifiée : durée, durée moyenne, durée maximale.

Remarque : vous pouvez également désactiver les alertes planifiées.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte*	Planifier une alerte
Administrateur/analyste	Afficher une alerte	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

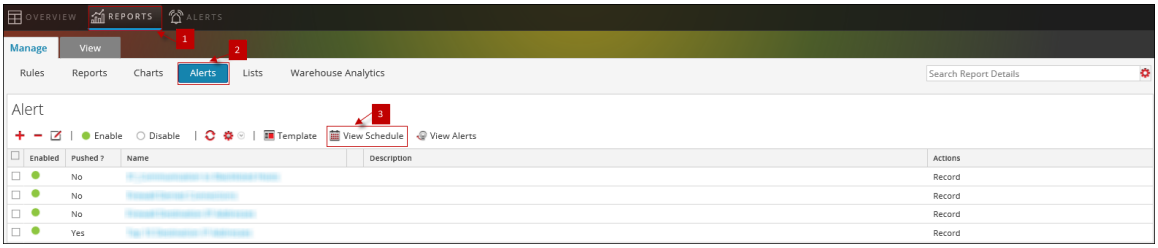
Présentation des alertes

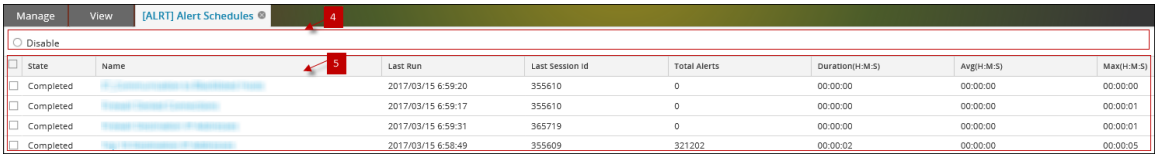
Configuration d'une alerte

Planifier une alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.





1	Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2	Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3	Cliquez sur **Afficher le planning** pour afficher toutes les alertes planifiées.
4	La barre d'outils Planification des alertes vous permet de désactiver l'alerte planifiée.
5	La liste des plannings d'alertes vous permet d'afficher les détails de l'alerte planifiée.

La vue Afficher la planification des alertes comprend les panneaux suivants :

1. Barre d'outils Planification des alertes
2. Liste des plannings d'alertes

Barre d'outils Planification des alertes

Le panneau Barre d'outils de la planification des alertes vous permet de modifier l'état de l'alerte planifiée.

Fonction	Description
Désactiver	Cliquez sur **Désactiver** pour désactiver l'alerte sélectionnée. Lorsque des alertes planifiées ne sont plus nécessaires ou qu'elles s'avèrent inefficaces, vous pouvez les désactiver afin qu'elles ne soient plus exécutées. Vous pouvez sélectionner une ou plusieurs alertes à désactiver. Lorsqu'une alerte est désactivée, elle est supprimée de la liste des alertes planifiées. En outre, elle n'est plus exécutée tant que vous ne l'exécutez pas manuellement ou que vous ne configurez pas un nouveau planning.

Panneau Liste des plannings d'alertes

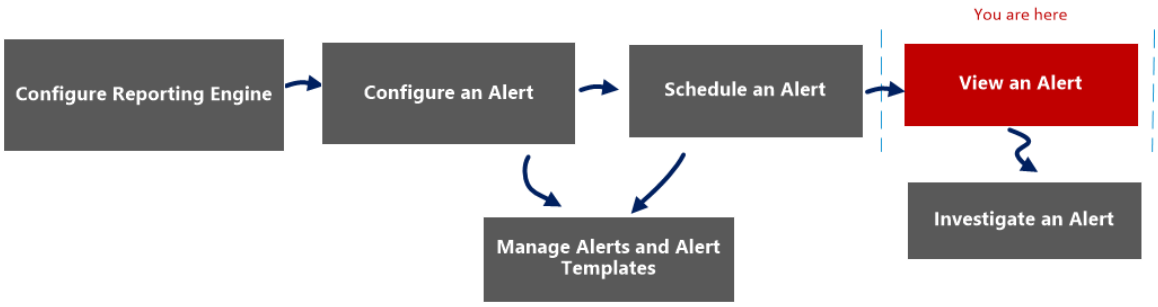
Le panneau Liste des plannings d'alertes répertorie uniquement les alertes activées, au format tabulaire. Le tableau suivant répertorie les colonnes du panneau Liste des plannings d'alertes et leur description.

Fonction	Description
État	État de l'alerte planifiée : • Terminé • Échec
Nom	Nom de l'alerte planifiée.
Dernière heure d'exécution	Heure de la dernière exécution de l'alerte.
ID de dernière session	ID de session de la dernière alerte planifiée.
Nombre total d'alertes	Nombre total des occurrences des événements.
Durée	Durée d'exécution de l'alerte planifiée.
Moy. (s)	Durée moyenne d'exécution de l'alerte planifiée.
Max. (s)	Durée maximale d'exécution de l'alerte planifiée.

Vue Afficher les alertes

Dans la vue Afficher les alertes, vous pouvez afficher toutes les alertes. Vous pouvez aussi personnaliser la vue pour afficher les alertes correspondant à une période spécifique. De plus, vous pouvez définir le nombre maximal d'alertes affichées dans une seule page.

Workflow



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur/analyste	Configurer le Reporting Engine	Configurer le Reporting Engine
Administrateur/analyste	Configurer une alerte	Configuration d'une alerte
Administrateur/analyste	Planifier une alerte	Planifier une alerte
Administrateur/analyste	Afficher une alerte*	Afficher une alerte
Administrateur/analyste	Analyser une alerte	Analyser une alerte
Administrateur/analyste	Gérer une alerte et un modèle d'alerte	Gérer une alerte et un modèle d'alerte

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

Présentation des alertes

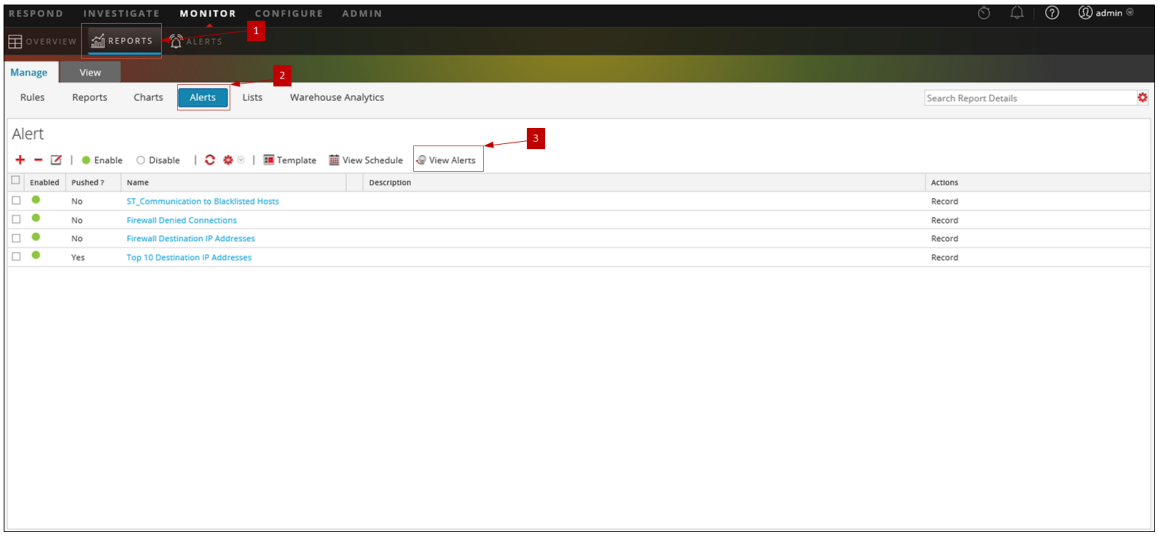
Configuration d'une alerte

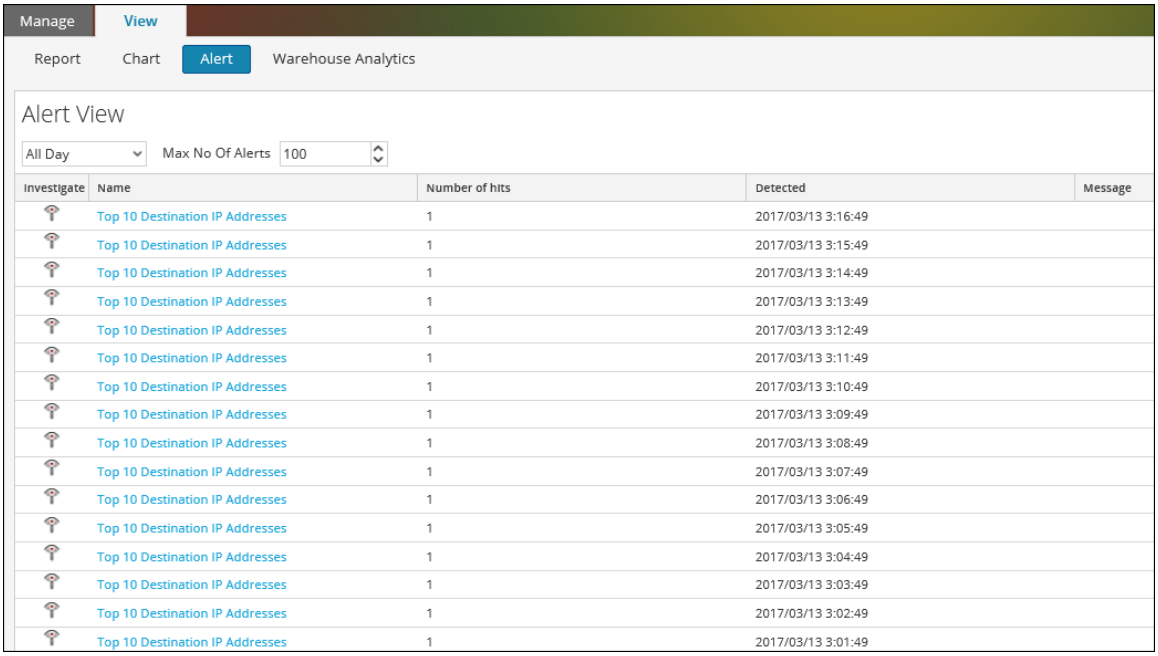
Planifier une alerte

Afficher une alerte

Affichage rapide

La figure suivante illustre un exemple avec les fonctions importantes portant un libellé.





1	Cliquez sur **Surveiller**> **Rapports** pour afficher l'onglet Gérer.
2	Cliquez sur **Alertes** pour ouvrir la vue Alerte.
3	Cliquez sur **Afficher les alertes** pour afficher les différents panneaux sur Afficher les alertes.
4	La barre d'outils Afficher les alertes vous permet de filtrer les alertes en fonction d'un nombre ou de la date de début ou de fin des alertes.
5	Le panneau Afficher la liste des alertes répertorie toutes les alertes filtrées au format tabulaire.

La vue Afficher les alertes comprend les panneaux suivants :

- Barre d'outils Afficher les alertes
- Afficher la liste des alertes

Barre d'outils Afficher les alertes

Le tableau ci-dessous répertorie les opérations disponibles dans le panneau Barre d'outils Afficher les alertes.

Option	Description
Données de la dernière heure	Données extraites de la précédente exécution.
Nb max. d'alertes	Le nombre maximal d'alertes que vous souhaitez extraire à partir du service Reporting Engine pour une période spécifique.

Afficher la liste des alertes

Le tableau ci-dessous répertorie les colonnes du panneau Afficher la liste des alertes.

Colonne	Description
	Icône qui permet d'ouvrir le module Investigation dans lequel s'affichent les détails de la première session qui a enregistré la correspondance de l'alerte donnée pour une analyse immédiate. **Remarque :** vous n'êtes pas redirigé vers le module Investigation dans les cas suivants : -Vous reconfigurez une source de données pour une alerte existante et exécutez une alerte sur la nouvelle source de données. -Vous saisissez un nom d'hôte à la place d'une adresse IP dans le champ Source de données.
Nom	Nom de l'alerte qui a enregistré la correspondance. Le lien hypertexte du nom ouvre le module Investigation pour afficher toutes les correspondances de cette alerte spécifique pour l'heure entourant l'alerte enregistrée.
Nombre de correspondances	Nombre de fois où l'alerte est générée.

Colonne	Description
Détecté	Date et heure auxquelles l’alerte est génèrée.
Message	Messages d’alerte.