RSA NETWITNESS® PLATFORM

Guide d'utilisation de NetWitness Investigate

pour la version 11.2

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

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

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

mai 2019

Sommaire

Fonctionnement de NetWitness Investigate

NetWitness Investigate offre aux analystes la possibilité d'analyser des données dans RSA NetWitness® Platform et d'analyser des données de paquet, de log et de point de terminaison, ainsi que d'identifier d'éventuelles menaces internes ou externes à la sécurité et à l'infrastructure IP.

Remarque : Dans la version 11.1 et versions ultérieures, les vues Hôtes et Fichiers fournissent une vue des données de point de terminaison. Les versions antérieures offrent un accès aux données de point de terminaison en utilisant un serveur NetWitness Endpoint autonome.

Métadonnées, clés méta, valeurs méta et entités méta

RSA NetWitness Platform audite et surveille l'ensemble du trafic sur un réseau. Un seul type de service, un Decoder, acquiert, analyse et stocke les données de paquets, logs et point de terminaison transitant sur le réseau.

Les analyseurs et feeds configurés sur le Decoder créent des *métadonnées* que les analystes peuvent utiliser pour enquêter sur les logs et paquets acquis. Un autre type de service, nommé Concentrator, indexe et stocke les métadonnées.

Les métadonnées se présentent sous la forme d'une *clé méta* et de *valeurs méta* pour la clé. Par exemple, `ip.src` est une clé méta et une adresse IP, source du trafic, est marquée en tant que `ip.src`. Lorsque vous affichez des données dans la vue Enquêter, vous voyez la méta clé `ip.src` et toutes les adresses IP (valeurs) qui sont marquées avec cette clé. Certaines clés méta sont intégrées et d'autres peuvent être des clés personnalisées définies par l'administrateur.

Les entités méta sont disponibles dans la version 11.1 ou supérieure. Une *entité méta* est un alias qui regroupe les résultats d'autres clés méta. Les entités méta organisent des clés méta similaires en un seul type de méta, plus facile à utiliser. Certaines entités méta sont déjà incluses par défaut et l'administrateur peut créer des entités méta personnalisées. Les analystes peuvent utiliser une entité méta dans une requête, un groupe méta, un groupe de colonnes et un profil. Les visualisations de coordonnées parallèles ne prennent pas en charge les entités méta. Les administrateurs peuvent utiliser des entités méta pour définir un préfixe de requête à appliquer à un rôle d'utilisateur et un utilisateur. Le *Guide de configuration de Decoder* fournit des informations supplémentaires sur la création d'entités méta et comment elles peuvent être utilisées dans les règles.

Par exemple, la langue de base de données de base par défaut comprend des clés méta distinctes pour l'IP source et l'IP de destination. L'une des entités méta intégrées nommées `ip.all` représente l'ensemble combiné de toutes les sources et destinations IP.

Généralement, les analystes interrogent le Concentrator pour détecter des menaces. Le Concentrator gère des requêtes et n'accède au Decoder que lorsqu'une reconstruction complète des sessions ou des logs bruts est nécessaire. ESA, Malware Analysis et Reporting Engine interrogent également le Concentrator, sur lequel ils peuvent obtenir rapidement toutes les métadonnées pertinentes associées à un événement et générer des informations à ce sujet sans avoir à accéder à chaque Decoder. Dans certains cas, les analystes peuvent interroger un Decoder.

Remarque : Bien qu'une appliance hybride peut effectuer la fonction de Concentrator, une appliance Concentrator distincte est nécessaire pour tous les environnements volumineux qui nécessitent davantage de bande passante ou d'événements par seconde (EPS). L'appliance Concentrator dispose d'une organisation de stockage qui utilise des disques SSD pour l'index, ce qui augmente les performances de lecture.

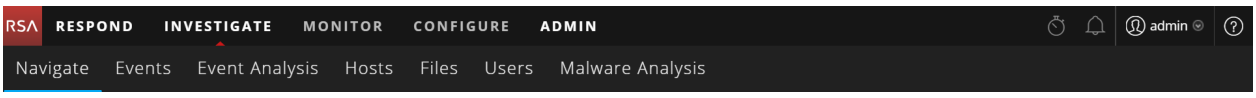
Déclencheurs pour une procédure d'enquête

Voici quelques exemples des déclencheurs pour une procédure d'enquête :

- Vous recevez des informations d'un tiers sur un nouveau hack de répertoire actif. À partir de la vue Événements, vous utilisez ces informations pour exécuter une recherche sur toutes vos données de fichiers log Active Directory brutes pour les dernières 24 heures.
- Le responsable du SOC vous demande de rechercher un programme malveillant Pokemon Go en raison de sa popularité actuelle. À partir de la vue Naviguer, créez une requête pour rechercher une session HTTP à l'aide d'un agent utilisateur spécifique lié au programme malveillant détecté dans un blog de sécurité.
- Un responsable de la réponse aux incidents fait remonter un ticket qui présente certains indicateurs impairs associés à un hôte. À partir de la vue Hôtes, examinez cet hôte pour connaître les détails spécifiques.
- Vous recherchez la prochaine attaque jour zéro et commencez à faire pivoter les métadonnées réseau dans la vue Naviguer pour rechercher les sessions automatisées anormales quittant l'entreprise.
- Vous êtes invité(e) par votre responsable du SOC à trouver les informations relatives à l'utilisateur `jarvis`, un employé qui vient d'être remercié. À partir de la vue Hôtes, vous effectuez une interrogation sur la semaine écoulée pour ce nom d'utilisateur.

Flux de travail d'une procédure d'enquête

Les analystes peuvent examiner les données capturées par NetWitness Platform et détailler les informations contenues dans un tableau de bord NetWitness Platform, un incident ou une alerte NetWitness Respond, un rapport créé par NetWitness Platform Reporting Engine ou une application tierce. Au cours d'une procédure d'enquête, les analystes peuvent se déplacer de manière transparente entre les vues Enquêter : la vue Naviguer, la vue Événements, la vue Analyse d'événements, la vue Hôtes, la vue Fichiers, et la vue Analyse de malware. Cette figure montre les sous-menus de NetWitness Investigate.



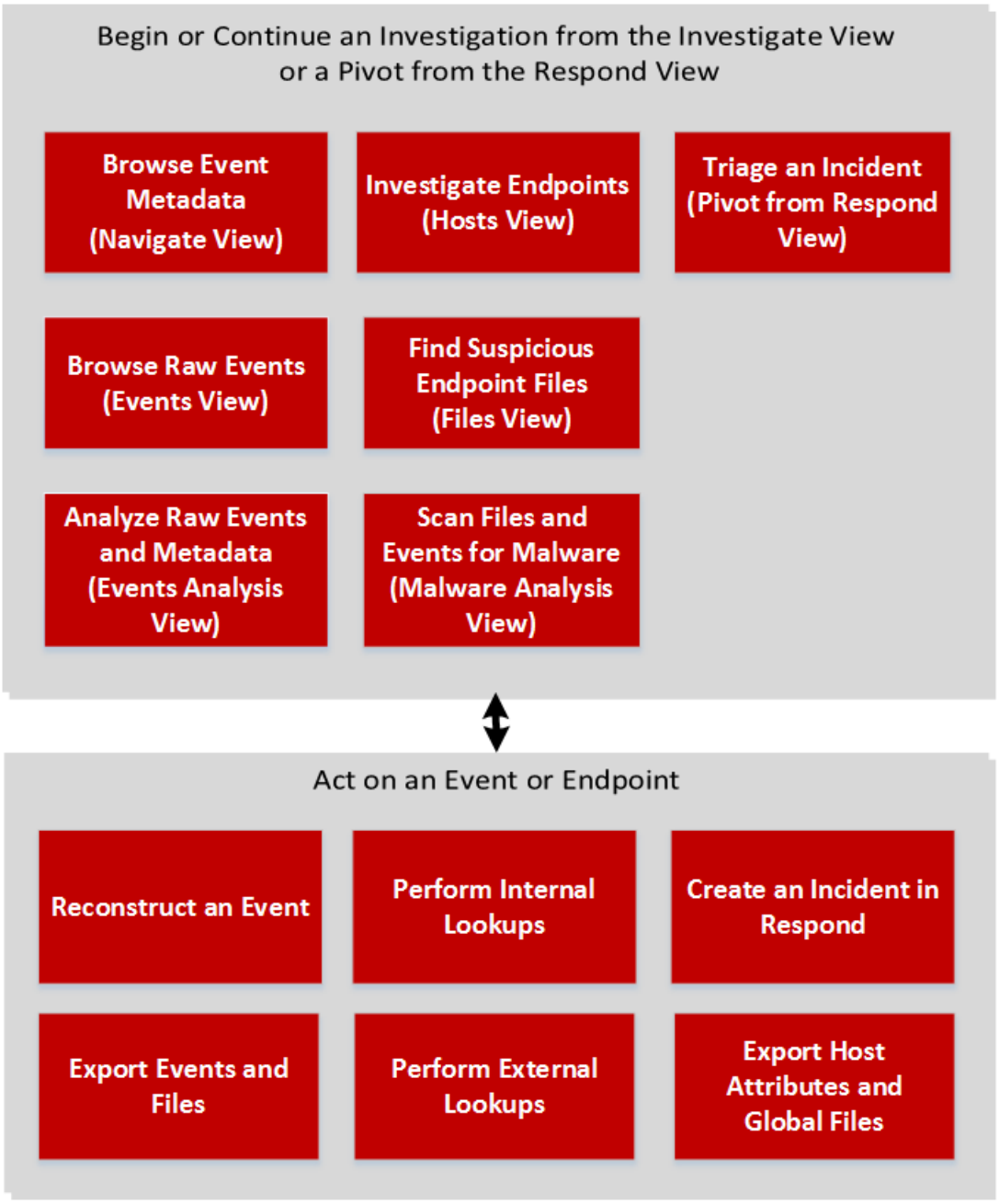
Remarque : Les vues Fichiers et Hôtes sont disponibles dans les versions 11.1 et supérieures. La vue Utilisateurs est disponible dans la version 11.2 et versions ultérieures. Des rôles d'utilisateurs et des autorisations spécifiques sont requis pour qu'un utilisateur puisse mener des procédures d'enquêtes et des analyses de programmes malveillants dans NetWitness Platform. Si vous ne pouvez pas réaliser de tâche d'analyse ou afficher une vue, il se peut que l'administrateur doive ajuster les rôles et autorisations configurés pour vous.

Vous pouvez accéder à chaque vue dans le sous-menu Enquêter et dans les vues Enquêter. Vous pouvez également accéder directement à une vue Enquêter à partir de NetWitness Respond et passer directement de NetWitness Investigate à NetWitness Respond et à NetWitness Endpoint autonome. Votre exemple d'utilisation détermine le point de départ de votre procédure d'enquête. Ce tableau fournit des conseils généraux sur la vue de départ pour différents exemples d'utilisation.

Accéder à...	Objectif
Vue Naviguer	Toutes les clés méta et les valeurs méta des logs, points de terminaison et paquets, regroupés par clé méta. Vous pouvez faire pivoter les données pour affiner les résultats, puis accéder à la vue Événements ou à la vue Analyse d'événements, ou encore effectuer une recherche dans Malware Analysis ou Live. Il s'agit de la vue NetWitness Investigate par défaut. (Voir Procédure d'enquête relative aux métadonnées dans la vue Naviguer.)
Vue Événements	Les événements sont répertoriés dans l'ordre chronologique. Vous pouvez afficher les événements bruts et les métadonnées associées, afficher une reconstruction et télécharger des fichiers et des événements. Vous pouvez accéder à la vue Analyse d'événements. (Consultez Examiner les événements bruts dans la vue Événements.)
Vue Analyse d'événements	Les événements sont répertoriés dans l'ordre chronologique. Vous pouvez afficher toutes les clés méta et les valeurs de métadonnées pour les logs, les paquets et les points de terminaison. Vous pouvez afficher l'événement brut et les métadonnées associées, afficher une reconstruction qui offre des files d'attente utiles pour identifier les points d'intérêt dans une reconstruction. Vous pouvez accéder à la vue Hôtes, pivoter vers un point de terminaison autonome, effectuer une recherche dans Live et effectuer des recherches externes. Les recherches externes vous permettent de rechercher sur Internet les valeurs de métadonnées avec lesquelles vous avez interagi, de déterminer les informations DNS passives associées à une adresse IP, de vérifier si une URL est mise en liste noire et d'autres intégrations de contexte tierces. (Consultez la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements)Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements
(Version 11.1 ou supérieure) Vue hôtes	Les hôtes sur lesquels s'exécutent les agents NetWitness Endpoint Insights sont répertoriés. Pour chaque hôte, vous pouvez voir les processus, les pilotes, les DLL, les fichiers (exécutables), les services et les exécutions automatiques en cours d'exécution, ainsi que les informations relatives aux utilisateurs connectés. Dans la vue Hôtes, vous pouvez accéder aux vues Naviguer et Analyse d'événements. (Voir Examiner les hôtes)
(Version 11.1 ou supérieure) Vue Fichiers	Les fichiers uniques tels que PE, Macho et ELF dans votre déploiement sont répertoriés. Pour chaque fichier, vous pouvez afficher des détails tels que la taille du fichier, l'entropie, le format, le nom de l'entreprise, la signature et la somme de contrôle. Dans la vue **Fichiers**, vous pouvez accéder aux vues Naviguer et Analyse d'événements. (Voir Examiner les fichiers)

Accéder à...	Objectif
Vue Analyse de malware	Si vous exécutez une appliance d'analyse de malware, vous pouvez analyser automatiquement ou manuellement les fichiers et voir les résultats de quatre types d'analyse : réseau, statique, communauté et sandbox. Si un fichier s'avère être un programme malveillant, vous pouvez accéder à la vue Hôtes pour voir quels hôtes ont téléchargé le fichier. (Voir Mener une analyse de malware).
(Version 11.2 ou supérieure) Vue Utilisateurs	La visibilité des comportements d'utilisateurs à risque dans votre entreprise est assurée à l'aide de NetWitness UEBA. Vous pouvez afficher une liste d'utilisateurs à haut risque et un résumé des alertes principales relatives aux comportements risqués dans votre environnement, puis sélectionner un utilisateur ou une alerte et afficher des détails sur le comportement risqué et une chronologie pendant laquelle les comportements se sont produits. Les utilisateurs de la plate-forme NetWitness ayant un rôle d'administrateur ou d'analystes UEBA ont accès à cette vue. Pour plus d'informations sur cette fonctionnalité, consultez *Guide d'utilisateur NetWitness UEBA*.Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Chaque situation est unique en termes de types d'informations que l'analyste tente de rechercher. De nombreuses procédures d'enquête commencent à un point de vue et se terminent à un autre point de vue lorsque l'analyste obtient une information et doit ensuite suivre ce résultat dans une autre ligne de questions. La figure suivante présente le workflow général d'une procédure d'enquête.



Se concentrer sur les métadonnées, la requête et l'heure

Les analystes utilisent NetWitness Investigate pour rechercher des événements qui dirigent le workflow de réponse aux incidents et pour réaliser une analyse stratégique après la génération d'un événement par un autre outil. À partir de la vue Naviguer, la vue Événements ou la vue Analyse d'événements :

- Commencez par exécuter une requête sur un service pour une période donnée, puis appliquez un filtre en utilisant des métadonnées dans un sous-ensemble d'événements, reconstruisez ou analysez un événement et répétez le processus pour reconstruire ou analyser un autre événement.
- Lorsque vous trouvez un événement qui doit être étudié de plus près, vous affichez le contexte de l'événement et déterminez si vous devez créer un incident ou ajouter l'événement à un incident. Si vous décidez de ne pas ajouter l'événement à un incident, vous exécutez une autre requête pour en savoir plus, qui commence à nouveau au début du workflow.
- Si vous remarquez une activité ou des fichiers suspects sur un hôte spécifique du réseau, vous pouvez recueillir des informations supplémentaires sur l'hôte et les fichiers trouvés sur l'hôte dans la vue Hôtes et Fichiers ou sur un serveur NetWitness Endpoint autonome.
- Si vous trouvez un fichier ou un événement qui contient potentiellement des programmes malveillants, vous pouvez effectuer une analyse Malware Analysis du fichier ou vous pouvez ouvrir Malware Analysis et démarrer une analyse du service sur lequel l'événement a été constaté.

Par exemple, en cas de souci concernant un trafic suspect avec des pays étrangers, la clé méta du pays de destination révèle toutes les destinations et la fréquence du contact. Naviguer dans ces valeurs permet d'obtenir les détails du trafic, tels que l'adresse IP de l'expéditeur et le destinataire. La vérification d'autres métadonnées peut exposer la nature des pièces jointes échangées entre les deux adresses IP.

Se concentrer sur l'analyse des points de terminaison

Les analystes utilisent la vue Hôtes et Fichiers pour rechercher ou analyser les hôtes ou les fichiers à l'aide de d'attributs, tels que l'adresse IP, le nom d'hôte, l'adresse Mac, etc.

- Lors d'un triage d'incidents dans la vue Répondre, passez en revue les informations importantes (nom d'hôte, nom de fichier) et affichez les points forts du contexte.
- Pivotez vers la vue Enquêter pour ouvrir la vue Naviguer. Sélectionnez le groupe méta de l'analyse des points de terminaison et passez en revue les métadonnées créées.
- Affichez les métadonnées dans la vue Analyse d'événements pour analyser les événements. Sélectionnez la recherche d'hôte à l'aide du panneau Méta de l'événement.
- Dans la vue Hôtes, cliquez sur le nom d'hôte pour afficher le récapitulatif des points de terminaison, snapshots, configurations de la sécurité, etc.
- Effectuez une analyse à la demande pour obtenir les informations les plus récentes (le cas échéant).
- Recherchez un nom de fichier, un chemin ou un hachage spécifique sur tous les snapshots pour affiner la recherche.
- Passez en revue les processus, les exécutions automatiques, les fichiers, les bibliothèques, les pilotes et les informations du système à examiner plus en détail.

- Dans la vue Fichiers, filtrez les fichiers en utilisant quelques indicateurs (tels que le nom de fichier, la taille du fichier, l'entropie, le format, le nom de société, la signature, la somme de contrôle) et faites pivoter la vue Naviguer pour voir si elle existe sur d'autres hôtes du réseau.

Se concentrer sur les incidents et les alertes de NetWitness Respond

Un analyste qui travaille sur un incident ou une alerte dans NetWitness Respond peut l'ouvrir dans l'incident NetWitness Investigate (vue Naviguer) pour effectuer une analyse plus approfondie de l'événement ou de l'alerte.

- Le worfklow pour répondre à un incident commence généralement dans la vue Répondre, où l'analyste qui enquête sur un incident doit recueillir des informations sur l'incident dans NetWitness Investigate. Vous pouvez survoler une entité soulignée dans un incident ou une alerte, par exemple une adresse IP, puis sélectionner l'action Pivoter vers Investigate > Naviguer. La vue Naviguer s'ouvre et est filtrée pour l'entité sélectionnée. Une fois que ou lancez une procédure d'enquête à partir de NetWitness Respond, les clés méta définies sont interrogées et le contenu des paquets, logs et événements de point de terminaison capturés s'affiche dans la vue Naviguer.
- Si vous trouvez des événements qui sont pertinents pour l'incident, vous pouvez ajouter les événements à l'incident dans la vue Répondre. Vous pouvez également créer un nouvel incident dans la vue Répondre en fonction d'un ou de plusieurs événements trouvés dans la vue Enquêter.
- (Version 11.2 et ultérieures) À partir du panneau Indicateurs de la vue Détails de l'incident dans Répondre, vous pouvez ouvrir la vue Analyse d'événements pour mieux comprendre un événement d'indicateur.

Vues NetWitness Investigate

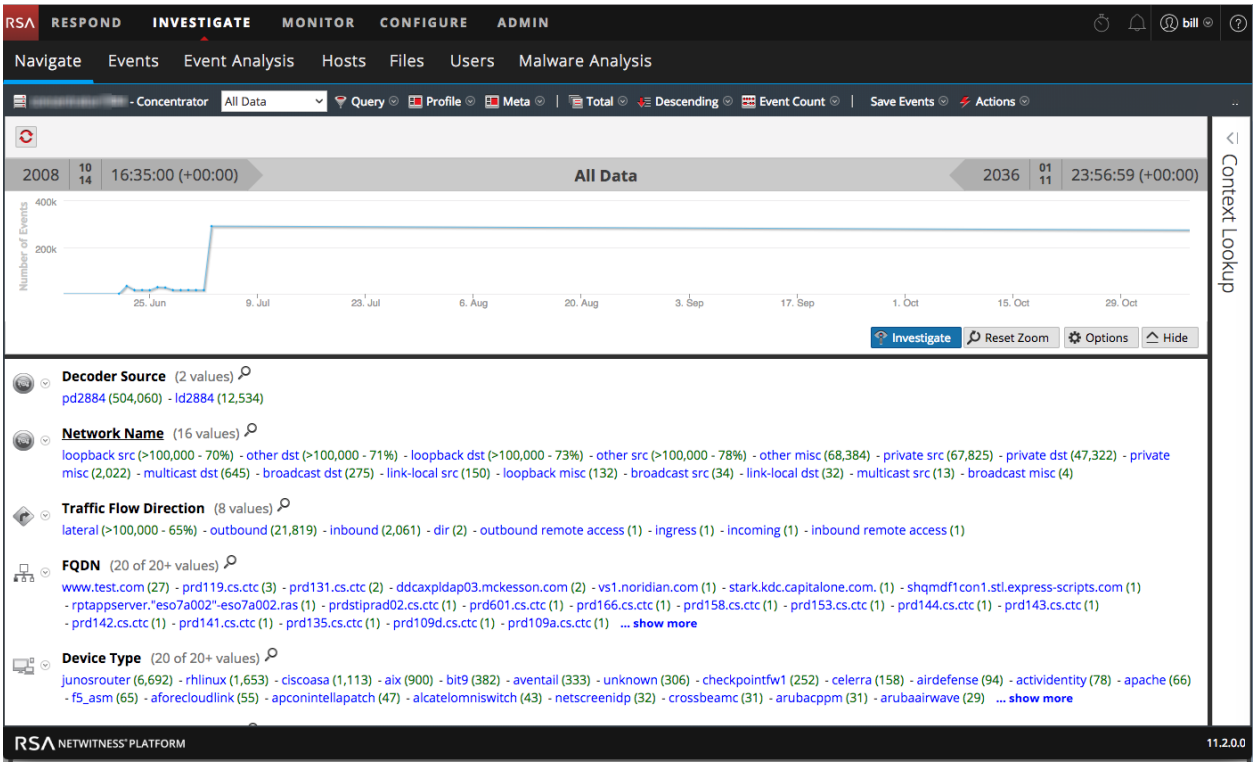
Cette section fournit une brève description et un exemple de chaque vue principale (Naviguer, Événements, Analyse d'événements, Hôtes, Fichiers et Analyse de malware) et présente des vues fournissant un contexte supplémentaire pour les données trouvées et reconstruction d'événement.

Vue Naviguer

La vue Naviguer permet d'explorer et d'interroger le contenu des paquets, des logs et des événements de point de terminaison capturés sur un service Broker, Concentrator ou Decoder (bien qu'une procédure d'enquête sur un service Decoder ne soit pas typique).

- Lorsque vous sélectionnez un service, les clés méta définies pour ce service sont interrogées, et les valeurs sont retournées avec le nombre d'événements. Cliquer sur une valeur à un niveau donné révèle les résultats en détail.
- Pour certaines clés méta configurées, telles que l'adresse IP ou le nom d'hôte, vous pouvez rechercher des informations contextuelles supplémentaires autour d'une valeur à l'aide de Context Hub. Le contexte supplémentaire peut inclure des incidents, des alertes et d'autres sources où la valeur a été abordée.
- La vue Naviguer fournit également une visualisation séquentielle des données dans un calendrier. Ici, vous pouvez zoomer sur une période sélectionnée.

La figure suivante illustre la vue Parcourir.

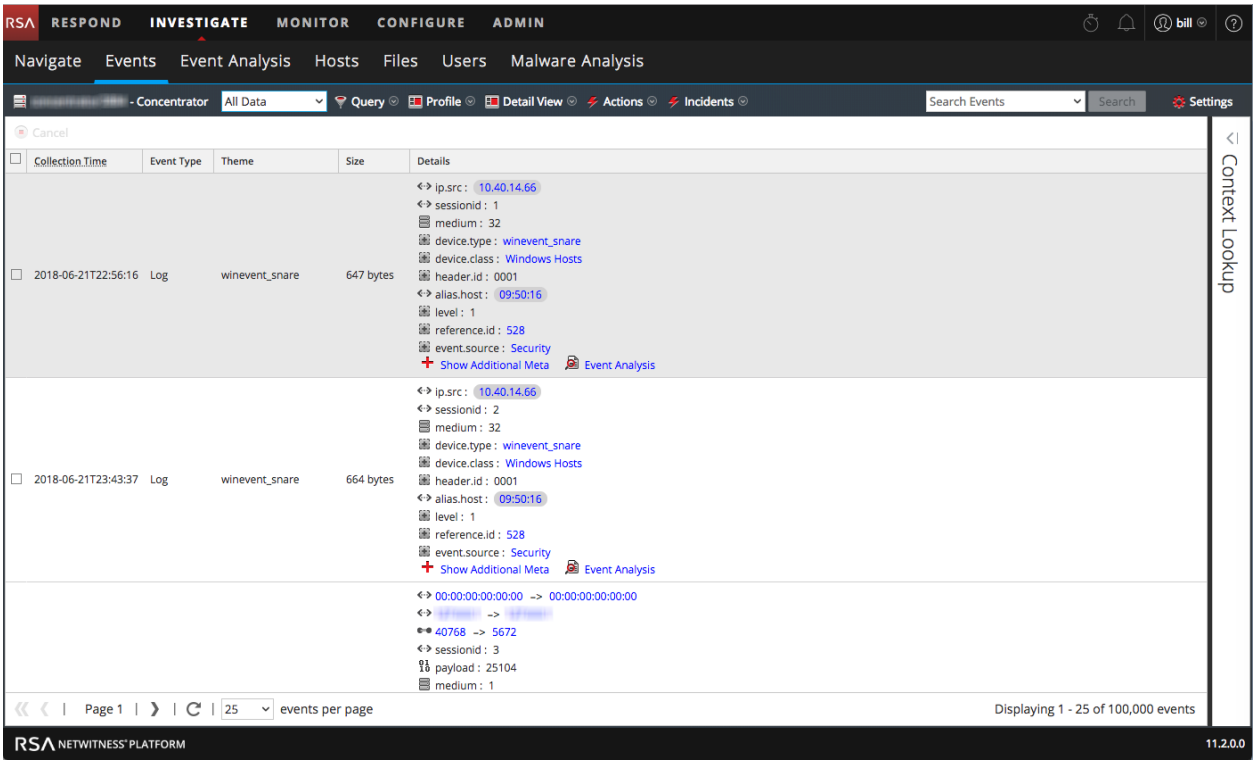


Vue Événements

La vue Événements fournit une vue des événements de paquet, log et point de terminaison sous forme de liste afin que vous puissiez les afficher dans l'ordre séquentiel et les reconstituer en toute sécurité.

- Vous pouvez ouvrir la vue Evénements pour une valeur méta que vous voyez dans la vue Naviguer.
- Pour les analystes sans privilèges suffisants pour naviguer dans un service, la vue Événements est une vue de procédure d'enquête autonome dans laquelle les analystes peuvent accéder à une liste de réseaux, logs et événements de point de terminaison à partir d'un service NetWitness Platform Core sans avoir à effectuer d'abord une recherche verticale à travers les métadonnées.
- La vue Événements présente des informations concernant l'événement sous trois formes standards : une simple liste restrictive d'événements, une liste détaillée des événements et une vue du log.
- Pour certaines clés méta configurées, telles que l'adresse IP ou le nom d'hôte, vous pouvez rechercher des informations contextuelles supplémentaires autour d'une valeur à l'aide de Context Hub. Le contexte supplémentaire peut inclure des incidents, des alertes et d'autres sources où la valeur a été abordée.
- Vous pouvez exporter les événements et les fichiers associés et créer un incident à partir d'un événement.

La figure suivante illustre la vue Événements.

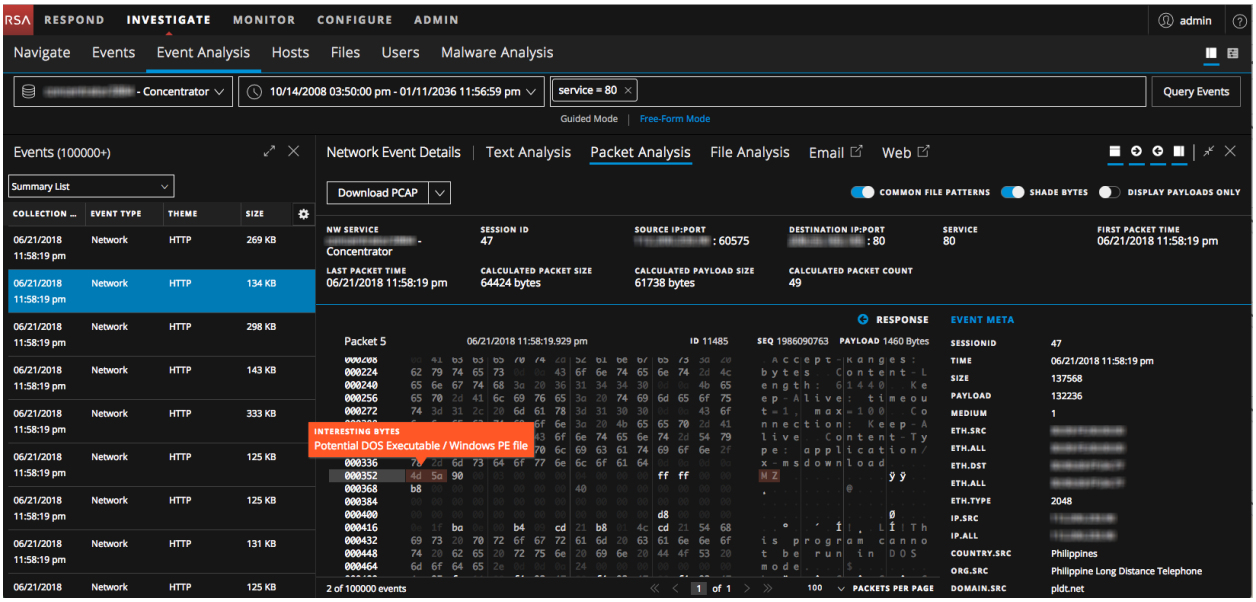


Vue Analyse d'événements

La vue Analyse d'événements est un outil interactif pour aider les analystes à voir les paquets, le texte ou les fichiers dans un événement présentant des indices visuels pour mettre en valeur certains types d'informations. Selon le type de reconstruction, les paquets, le texte ou les fichiers, des informations différentes sont appropriées.

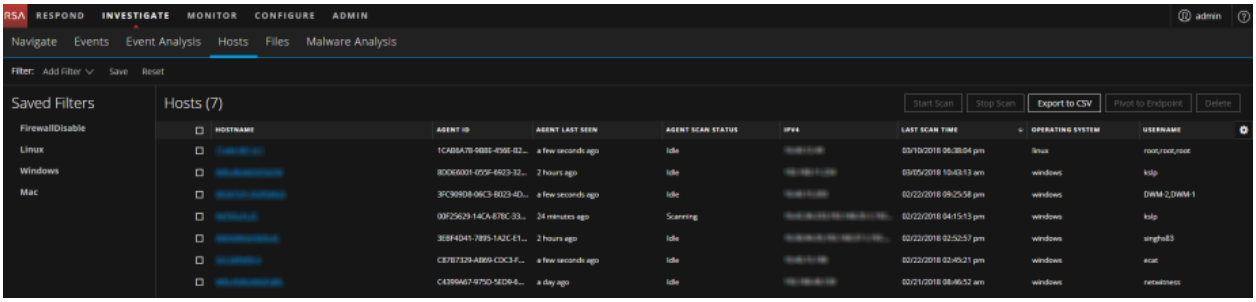
- Pour certaines clés méta configurées, telles que l'adresse IP ou le nom d'hôte, vous pouvez rechercher des informations contextuelles supplémentaires autour d'une valeur à l'aide de Context Hub. Le contexte supplémentaire peut inclure des incidents, des alertes et d'autres sources où la valeur a été abordée.
- Lors de l'affichage des fichiers, vous pouvez exporter des fichiers dans une archive zip sur votre système de fichiers local.
- Vous pouvez télécharger des logs à partir de la vue Texte, et exporter des paquets à partir de la vue Paquet.

Cette figure est un exemple de la vue Analyse d'événements.



Vue Hôtes

La vue Enquêter > Hôtes affiche tous les hôtes doté d'un agent. Par défaut, les hôtes sont répertoriés en fonction de la dernière heure d'analyse, avec les hôtes dernièrement analysés en tête de liste. Cela permet d'effectuer une recherche approfondie dans les détails de l'hôte. Voici un exemple de la vue Hôtes.

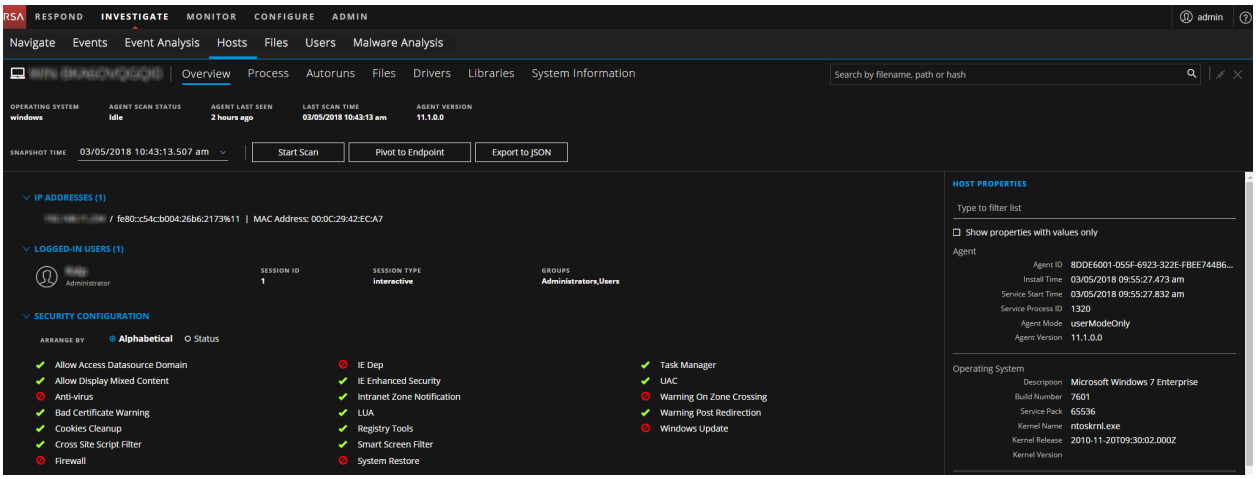


Cette vue vous permet d'effectuer les opérations suivantes :

- Filtrez et triez les hôtes pour affiner l'ienquête de l'hôte, afficher les détails de l'hôte et supprimer les hôtes.
- Exporter les attributs de l'hôte dans un fichier CSV.
- Démarrer ou arrêter une analyse pour les hôtes sélectionnés
- Pivoter vers la vue Naviguer ou Analyse d'événements pour enquêter sur l'hôte.

Remarque : Si vous disposez de NetWitness Endpoint 4.4.0.2 ou version ultérieure dans votre déploiement, les hôtes sur lesquels l'agent 4.4.0.2 est installé sont répertoriés et peuvent être identifiés à l'aide de la version de l'agent. Pour plus d'informations sur la façon dont vous pouvez étudier ces hôtes, voir Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure.

Vous pouvez afficher les résultats de l'analyse détaillée d'un hôte en cliquant sur son nom. Cette figure est un exemple des résultats d'analyse détaillés dans l'onglet Vue d'ensemble.



Vous pouvez :

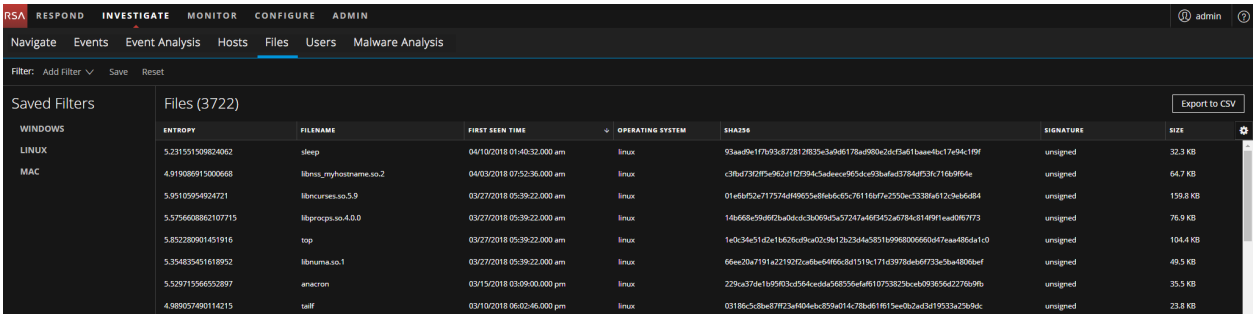
- Effectuer une recherche sur tous les snapshots (nom de fichier, chemin de fichier et fichier de contrôle SHA-256 sont les champs de recherche pris en charge.
- Afficher plusieurs snapshots. Par défaut, les données du dernier snapshot sont affichées.
- Afficher des informations sur les hôtes via les onglets suivants : Présentation, Processus, Exécutions automatiques, Fichiers, Pilotes, Bibliothèques et Informations du système.
- Exporter toutes les catégories de données de point de terminaison pour l'hôte sélectionné pour un snapshot spécifique au format JSON.

Vue Fichiers

La vue Fichiers fournit une liste de fichiers uniques trouvés dans votre déploiement et leurs propriétés associées. Par défaut, les fichiers sont répertoriés en fonction de la première heure d'affichage. Les types de fichiers suivants, chargés dans la mémoire, sont collectés pendant l'analyse.

- Portable Executable (PE) (Windows) - Il s'agit de fichiers `exe`, `dll` et `sys` Vous pouvez afficher les propriétés suivantes pour chaque fichier : somme de contrôle, détails de compilation, différentes sections présentes dans le fichier, bibliothèques importées et détails du certificat (signataire, empreinte, nom de l'entreprise).
- Macho (Mac) : Il s'agit d'ensembles d'applications, de dylibs et d'extensions de noyau. Vous pouvez afficher les propriétés suivantes pour chaque fichier : somme de contrôle, différentes sections présentes dans le fichier, bibliothèques importées et détails du certificat (signataire, empreinte, nom de l'entreprise).
- Format ELF (Executable and Linkable Format) (Linux) - Chaque fichier contient des informations sur la somme de contrôle, les différentes sections présentes dans le fichier et les bibliothèques importées.

Voici un exemple de la vue Fichiers.

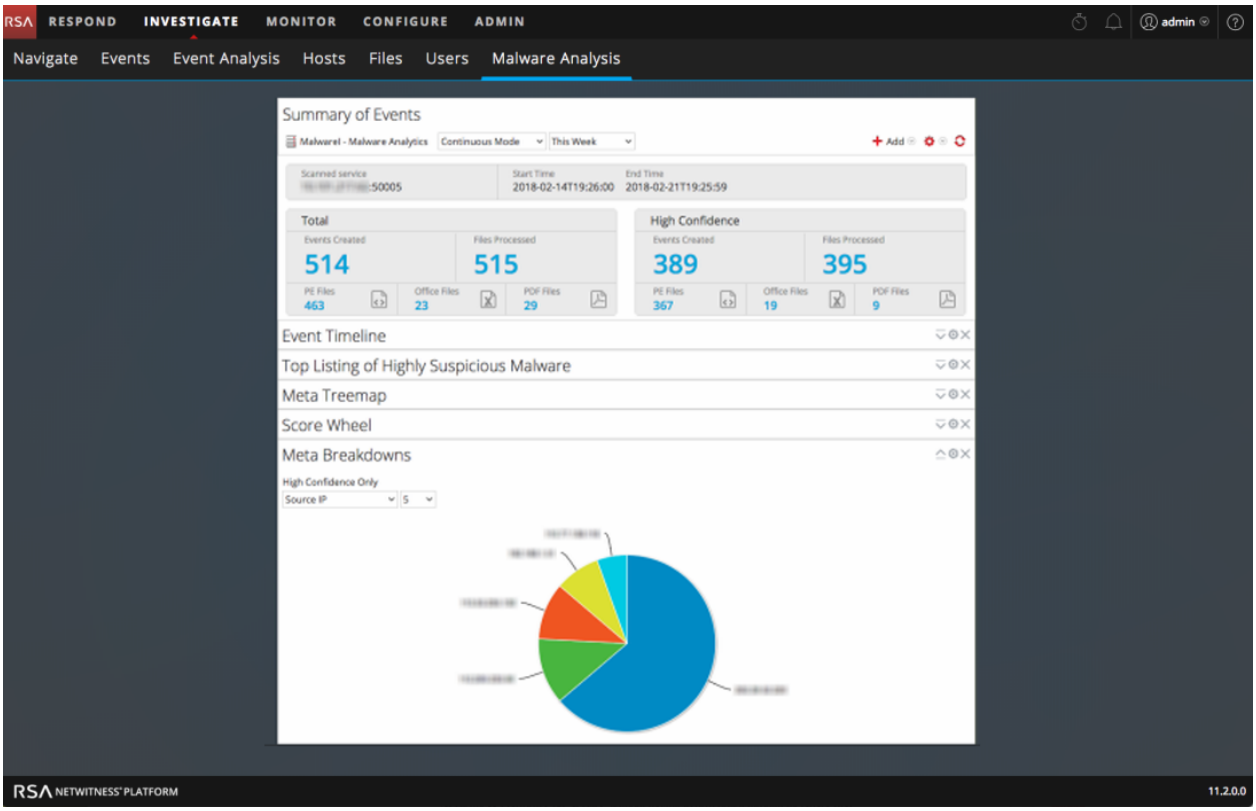


Dans la vue Fichiers, vous pouvez :

- Filtrer et trier les fichiers pour affiner les critères de l'enquête.
- Pivoter vers la vue Naviguer ou Analyse d'événements pour enquêter sur le fichier
- Exporter les fichiers dans un fichier CSV

Vue Analyse de malware

La vue Malware Analysis fournit un moyen d'analyser certains types d'objets de fichiers (par exemple, Windows Portable Executable [PE], PDF et Microsoft Office) pour évaluer la probabilité qu'un fichier est malveillant. La figure suivante illustre la vue Malware Analysis.



Vous pouvez ouvrir la vue Malware Analysis directement, ou vous pouvez utiliser faire un clic droit sur une action de menu contextuel pour analyser les malwares à partir d'une métavaleur dans un point d'extraction actuel dans la vue Naviguer. Vous pouvez valoriser les modules d'évaluation à plusieurs niveaux pour hiérarchiser le nombre massif de fichiers capturés afin de concentrer les efforts d'analyse sur les fichiers qui sont plus susceptibles d'être malveillants.

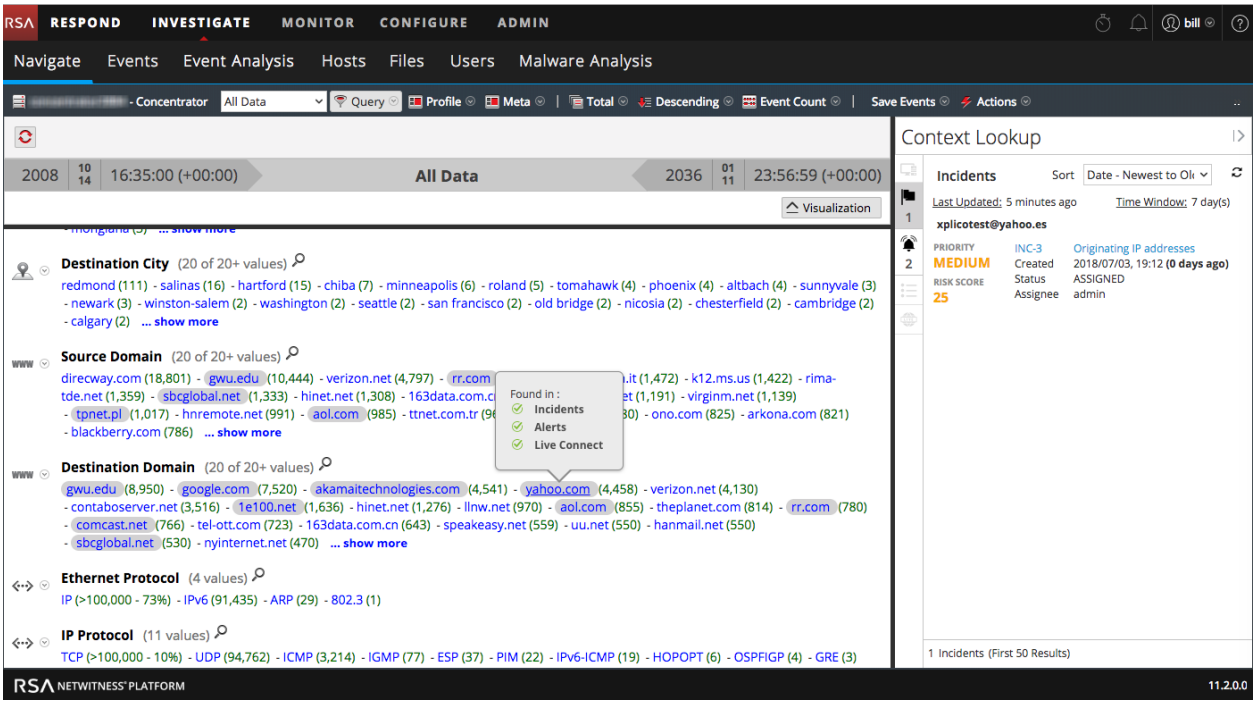
Informations contextuelles pour un événement

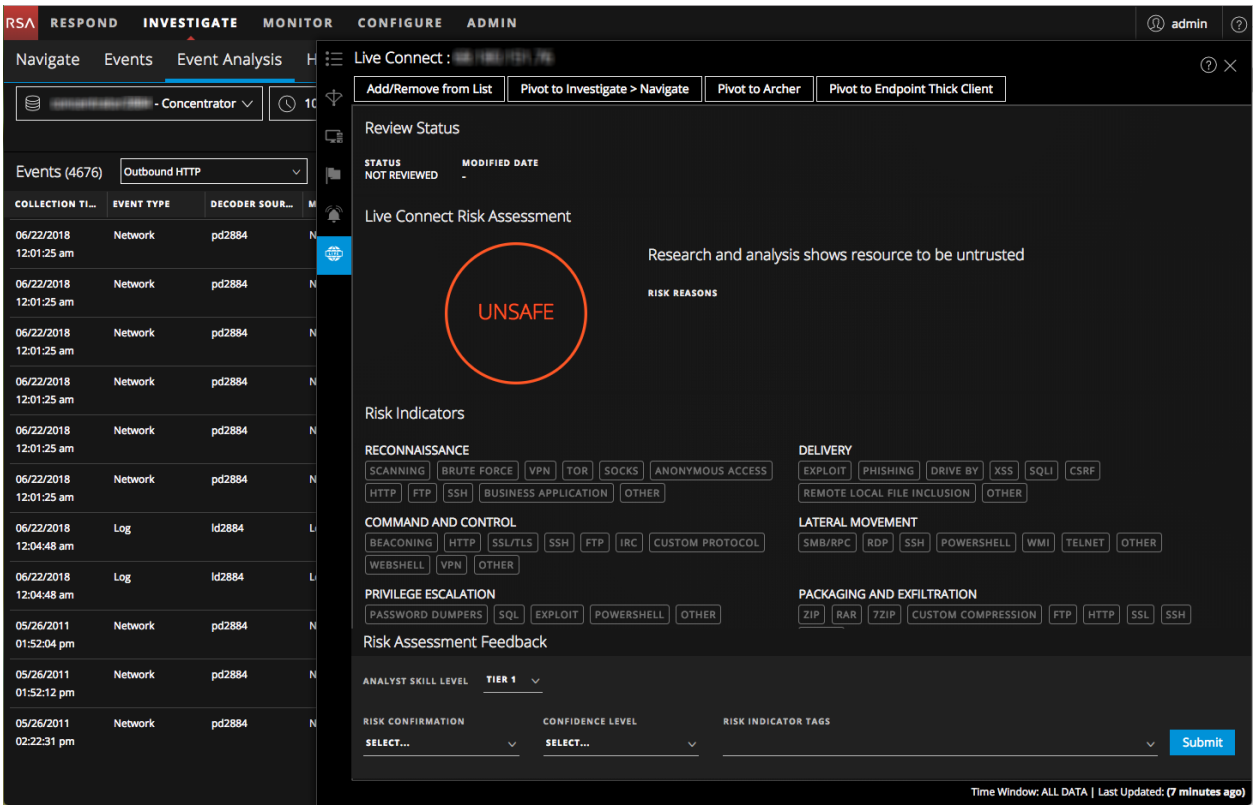
À partir de la vue Naviguer, de la vue Événements et de la vue Analyse d'événements (version 11.2 et versions ultérieures), le panneau Recherche contextuelle vous permet de consulter les détails à propos des éléments associés à un événement (adresse IP, utilisateur, hôte, domaine, adresse MAC, nom de fichier et hachage de fichier) dans Context Hub.

- Vous pouvez interagir avec les éléments d'un événement pour obtenir davantage d'informations, y compris les incidents associés, alertes, listes personnalisées, ressources Archer, informations Active Directory, et NetWitness Endpoint IIOC.
- Vous pouvez cliquer sur un point de données pour accéder à la vue Naviguer.

Remarque : Les ressources Archer et les détails Active Directory sont disponibles dans la recherche contextuelle de la vue Analyse d'événement. La recherche contextuelle Endpoint est uniquement disponible pour les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure, mais pas pour les hôtes NetWitness Endpoint 11.1.

Les figures suivantes montrent le panneau Recherche contextuelle dans Vue Naviguer et dans la vue Analyse d'événement.

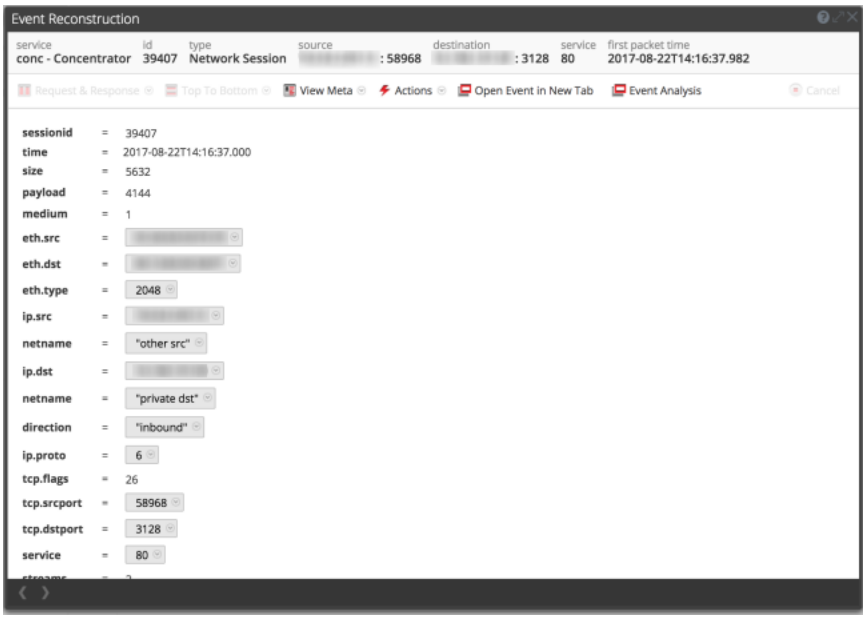




Reconstruction d'événement

Trois vues NetWitness Investigate offrent la possibilité de reconstruire un événement : Les vues Naviguer, Événements et Analyse d'événements. Lorsque vous découvrez un événement qui mérite une procédure d'enquête supplémentaire, vous pouvez reconstruire un événement en toute sécurité dans un format similaire à sa forme native. Le rendu des événements limite l'utilisation du code dynamique ou actif qui peut faire partie de l'événement pour limiter les effets négatifs sur votre système ou navigateur. Le cache est utilisé pour améliorer les performances lors de l'affichage d'événements précédemment affichés. Chaque analyste dispose d'un cache distinct de données de reconstruction, et vous ne pouvez accéder qu'à des événements reconstitués dans votre propre cache.

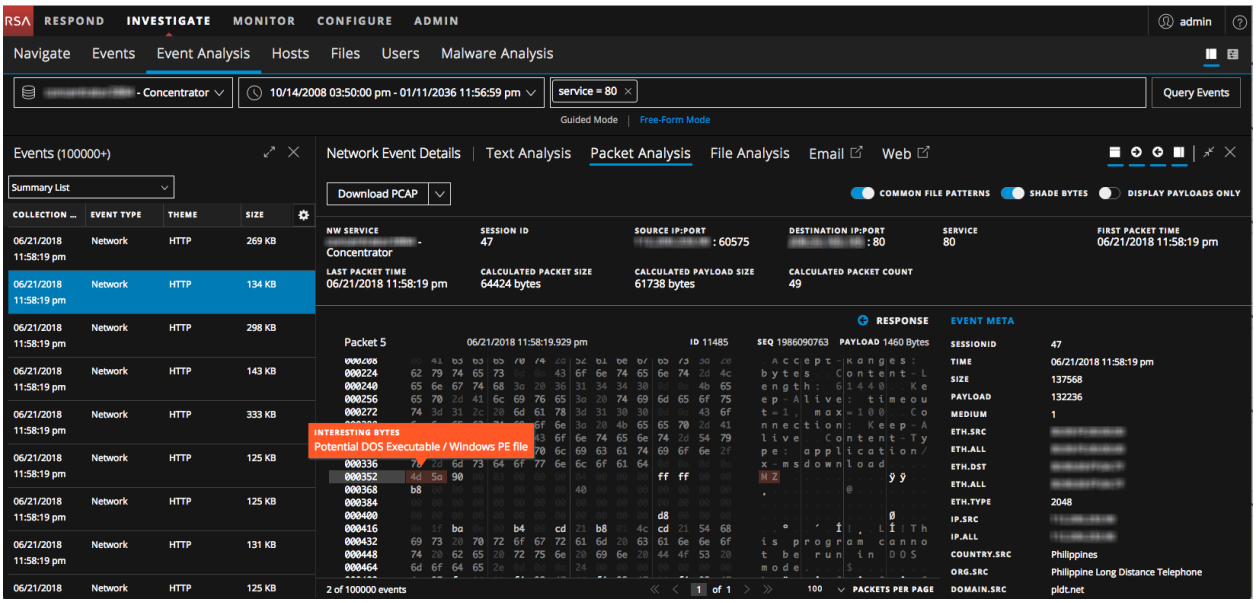
La Reconstruction d'événement dans la vue Événements ou la vue Naviguer présente les données brutes et les clés méta, ainsi que les valeurs de métadonnées pour un événement dans un formulaire de liste. Cette figure est un exemple de la Reconstruction d'événement.



Dans Reconstruction d'événement à partir de la vue Naviguer ou Événements :

- Vous pouvez faire défiler la reconstruction pour afficher l'événement suivant dans ce formulaire.
- Les événements peuvent être reconstruits à l'aide de différentes méthodes en fonction du type de données : données méta, texte, format hexadécimal, paquets, web, courrier, fichiers ou la meilleure reconstruction sélectionnée automatiquement.
- Vous pouvez exporter des fichiers de capture de paquets, extraire des fichiers et exporter les valeurs méta pour l'événement.

La vue Analyse d'événements présente une reconstruction d'événement interactive, ce qui inclut les données brutes, les clés et les valeurs méta. Cette figure est un exemple de reconstruction dans la vue Analyse d'événements.



Dans la reconstruction de la vue Analyse d'événements :

- Les événements peuvent être reconstruits à l'aide de différentes méthodes en fonction du type de données : données méta, texte, format hexadécimal, paquets, web, courrier et les fichiers.
- Les informations contenues dans les en-têtes et les charges utiles sont mises en surbrillance.
- Vous pouvez afficher les charges utiles décodées et codées et voir les signatures de fichiers courantes.
- Vous pouvez rechercher les emplacements de certaines clés ou valeurs méta dans la reconstruction.
- Permettent d'exporter les événements et les fichiers.

Configuration des vues et des préférences de NetWitness Investigate

Les analystes peuvent configurer certains aspects des vues et du comportement de NetWitness Investigate. Vous pouvez personnaliser la façon dont les vues Investigation s'affichent, les types d'information affichés et les facteurs agissant sur les performances lors du renvoi des résultats et des événements de reconstruction. Tous les paramètres configurables présentent des valeurs par défaut efficaces dans la plupart des déploiements ; cependant, les analystes ont la possibilité de les ajuster si nécessaire.

Les analystes qui mènent une analyse avec Investigation doivent disposer des rôles et autorisations du système appropriés pour leur compte utilisateur. Un administrateur doit configurer les rôles et les autorisations décrits dans le *Guide de la sécurité du système et de la gestion des utilisateurs*. (Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.)

Ces rubriques fournissent des détails :

- Configurer la vue Naviguer et la vue Événements
- Configurer la vue Analyse d'événements
- Configurer la vue Récapitulatif des événements de Malware Analysis

Configurer la vue Naviguer et la vue Événements

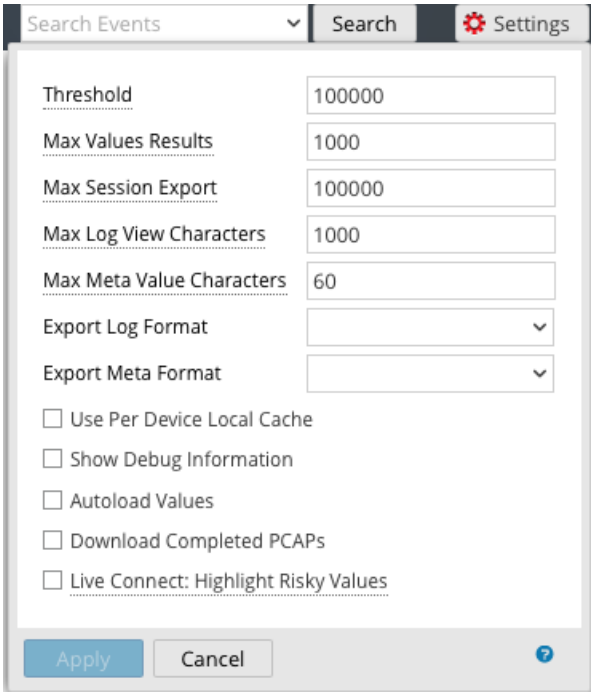
Les analystes peuvent configurer des préférences affectant les performances et le comportement de NetWitness Platform lors de l'analyse de données avec la vue Naviguer et la vue Événements. Ces paramètres sont disponibles à deux emplacements dans NetWitness Platform et les modifications effectuées dans l'un ou l'autre des emplacements sont répercutées dans l'autre vue :

- Vue Enquêter > boîte de dialogue Paramètres pour la vue Naviguer et la vue Événements.
- Profils > panneau Préférences > onglet Procédure d'enquête.
- Menu déroulant des options de recherche de la vue Navigation et de la vue Événements.

Accéder aux Paramètres des vues Naviguer et Événements

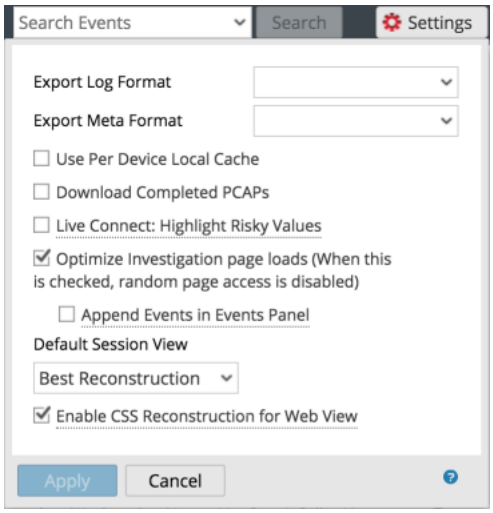
Pour accéder aux paramètres, procédez de l'une des façons suivantes :

- Dans la barre d'outils de la vue **Naviguer**, sélectionnez l'option **Paramètres**.
  La boîte de dialogue Paramètres de la vue Naviguer s'affiche.



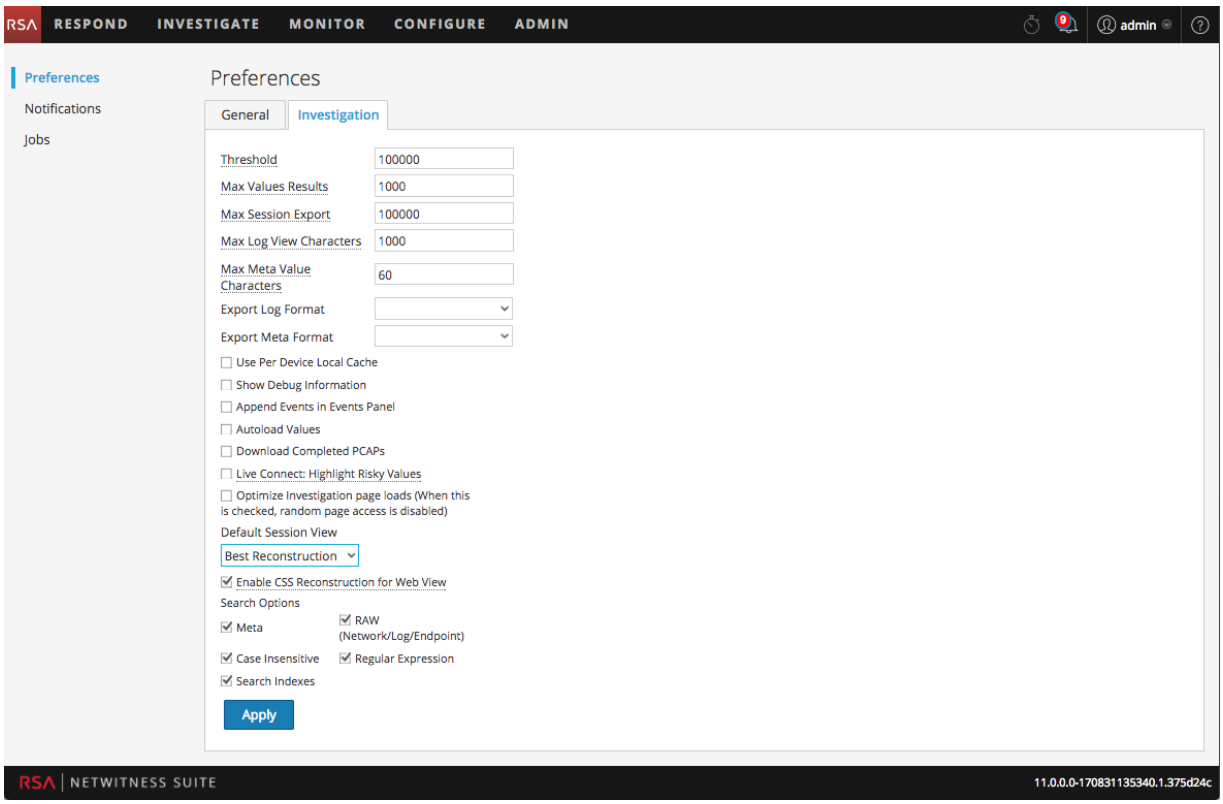
Remarque : La version 11.0 comprenait un paramètre permettant d'Ajouter des événements dans le panneau Événements, et il a été déplacé dans le panneau Paramètres de vue Événements dans la version 11.1.

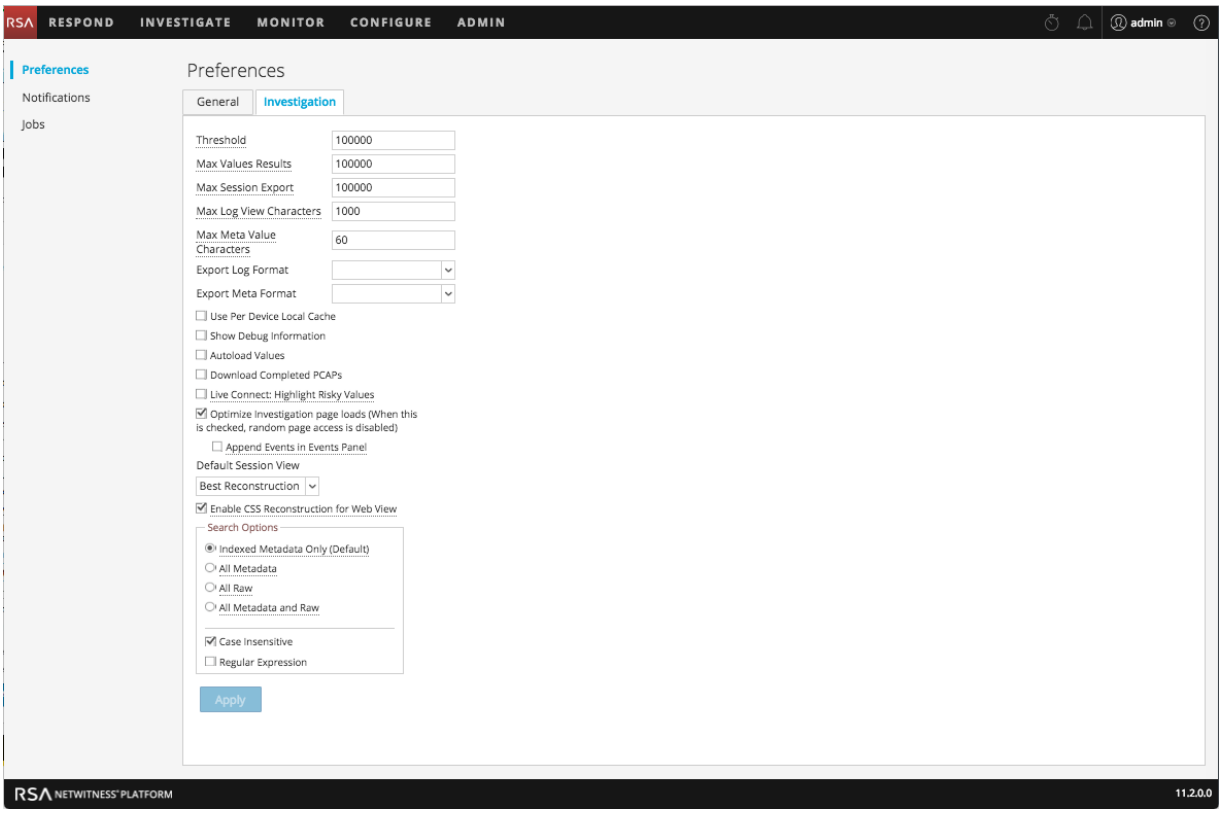
- Dans la barre d'outils de la vue **Événements**, sélectionnez l'option **Paramètres**.
  La boîte de dialogue Paramètres de la vue Événements s'affiche.



Remarque : La version 11.1 ou supérieure inclut le paramètre Ajouter des événements dans le panneau Événements.

- Dans le coin supérieur droit de NetWitness Platform, accédez à > , Profile et dans le panneau **Préférences**, cliquez sur l'onglet **Procédure d'enquête**.
  Le panneau Procédure d'enquête s'affiche. La première figure ci-dessous illustre le panneau Enquête version 11.1 et la deuxième figure illustre le panneau 11.2 avec une meilleure organisation des options de recherche.





Calibrer les paramètres de chargement des valeurs de la vue Naviguer

Plusieurs paramètres influencent les performances de NetWitness Platform lors du chargement de valeurs dans le panneau Valeurs. Les valeurs par défaut sont définies d'après l'usage commun. Les analystes individuels peuvent ajuster ces paramètres selon leurs propres procédures d'enquêtes. Pour ajuster ces paramètres :

1. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** dans la vue Événements.
2. Ajustez les paramètres suivants.
   - **Seuil :** Définissez le seuil du nombre maximum de sessions chargées pour une valeur de clé meta dans le panneau Valeurs. Un seuil supérieur offre des décomptes précis pour une valeur, et cause également des temps de charge plus longs. La valeur par défaut est **100000**.
   - **Nb max résultats de valeurs :** Définissez le nombre maximal de valeurs à charger dans la vue Naviguer lorsque l'option Résultats maximum est sélectionnée dans le menu Clé méta pour ouvrir une clé méta. La valeur par défaut est **1000**.
   - **Nb max exports de session :** Spécifiez le nombre d'événements pouvant être exportés dans un seul fichier PCAP ou Log.
   - **Caractères max affichage logs :** Définissez le nombre maximal de caractères à afficher sous **Enquêter > Événements > Texte du log**. La valeur par défaut est **1 000**.

- **Nombre maximal de caractères métavaleurs :** Définissez le nombre maximal de caractères autorisés dans un nom de métavaleur apparaissant dans la vue Naviguer, panneau Valeurs. La valeur par défaut est **60**.
- **Afficher les informations de débogage** Si vous souhaitez que NetWitness Platform affiche la clause `where` sous le fil d'Ariane dans la vue Naviguer, ainsi que le temps de charge écoulé pour chaque service agrégé sur un courtier, cochez cette option. La valeur par défaut est **Off**.
- **Ajouter des événements dans le panneau Événements :** Cette option a une incidence sur la pagination dans la vue Événements et est décrite ci-dessous, sous « Calibrer la récupération et la reconstruction par défaut de la vue Événements ».
- **Charger automatiquement les valeurs :** Si vous souhaitez que NetWitness Platform charge automatiquement les valeurs pour le service sélectionné dans la vue Naviguer, cochez cette option. Lorsqu'elle n'est pas sélectionnée, NetWitness Platform affiche un bouton **Charger les valeurs**, qui donne l'opportunité à l'utilisateur de modifier des options. La valeur par défaut est **Off**.

3. Cliquez sur **Appliquer**.

Les paramètres deviennent effectifs immédiatement mais seront visibles au prochain chargement des valeurs.

Configurer les paramètres de la vue Naviguer et la vue Événements

Plusieurs paramètres influencent les performances de NetWitness Platform lors du chargement de valeurs dans la vue Naviguer et la vue Événements. Les valeurs par défaut sont définies d'après l'usage commun. Les analystes individuels peuvent ajuster ces paramètres selon leurs propres procédures d'enquêtes. Vous pouvez définir ces paramètres séparément dans la vue Naviguer et la vue Événements. Lorsqu'il est configuré dans une vue unique, le paramètre ne s'applique pas automatiquement à une autre vue. Pour ajuster ces paramètres :

1. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour la vue Naviguer ou la vue Événements.
2. Ajustez les paramètres suivants.
   - **Live Connect : Mettre en évidence les valeurs risquées :** Si vous souhaitez que NetWitness Platform mette en surbrillance et affiche uniquement les adresses IP qui sont considérées comme risquées par la Communauté RSA, activez cette option. Lorsqu'elle n'est pas sélectionnée, NetWitness Platform affiche toutes les adresses IP. Par défaut, cette option n'est pas activée (**Désactivée**).
   - **Utiliser le cache local par appareil** Vous pouvez spécifier l'utilisation des données mises en cache localement à partir du service sélectionné. Par défaut, cette option n'est pas activée (**Désactivée**). Lorsque cette option est désactivée, Enquêter envoie une nouvelle requête à la base de données plutôt que d'afficher les données mises en cache dans les vues d'Enquêter après le chargement initial. Si elle est activée, Enquêter utilise les données provenant du cache local.
   - **Téléchargement des PCAP terminés** Vous pouvez automatiser le téléchargement des fichiers PCAP extraits de la vue Naviguer et de la vue Événements afin que le navigateur télécharge le fichier PCAP extrait et l'ouvre dans l'application par défaut pour ouvrir les fichiers PCAP tels que

Wireshark. Par défaut, cette option n'est pas activée (**Désactivée**). Si vous souhaitez activer cette option, vérifiez que l'application permettant d'ouvrir les fichiers PCAP est bien installée sur votre système de fichiers local et qu'elle est définie par défaut pour gérer les formats de fichier PCAP.

- **Live Connect : Mettre en évidence les valeurs risquées :** Si cette option est désactivée, toutes les métavaleurs qui disposent d'un contexte disponible dans Live Connect sont mises en surbrillance dans la vue Naviguer du panneau Valeurs. Si l'option est activée, parmi les valeurs qui disposent d'un contexte dans Live Connect, seules les valeurs jugées risquées/suspectes/dangereuses par la communauté sont mises en surbrillance. Par défaut, cette option est désactivée (**Off**).

3. Cliquez sur **Appliquer**.
   Les paramètres prennent effet immédiatement.

Configurer le format d'export de log par défaut

Vous pouvez exporter des logs à partir de la vue Naviguer et de la vue Événements dans différents formats. Les options disponibles sont Texte, XML, CSV et JSON. Il n'existe pas de valeur par défaut intégrée pour le format d'exportation de log. Si vous ne sélectionnez pas de format, NetWitness Platform affiche une boîte de dialogue de sélection lorsque vous invoquez l'exportation des logs. Pour sélectionner le format des logs exportés :

1. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour la vue Naviguer ou la vue Événements.
2. Sélectionnez l'une des options du menu déroulant **Format du log d'exportation**.
3. Cliquez sur **Appliquer**.
   Le paramètre prend effet immédiatement.

Configurer le format d'exportation des métadonnées par défaut

Vous pouvez exporter des métavaleurs à partir de la vue Naviguer et de la vue Événements dans différents formats. Les options disponibles sont Texte, CSV, TSV et JSON. Il n'existe pas de valeur par défaut intégrée pour le format d'exportation de métadonnées. Si vous ne sélectionnez pas de format ici, NetWitness Platform affiche une boîte de dialogue de sélection lorsque vous invoquez l'exportation des valeurs méta. Pour sélectionner le format des valeurs méta exportées :

1. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour la vue Naviguer ou la vue Événements.
2. Sélectionnez l'une des options du menu déroulant **Exporter le format de métadonnées**.
3. Cliquez sur **Appliquer.**
   Le paramètre prend effet immédiatement.

Calibrer la récupération et la reconstruction par défaut de la vue Événements

Vous pouvez configurer plusieurs paramètres contrôlant la manière dont NetWitness Platform récupère les événements et les reconstruit dans la vue Événements. Pour cela :

1. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour afficher la vue Événements.
2. Configurez les paramètres suivants.
   - **Optimiser les charges de la page Procédure d'enquête** : Définissez une option de pagination. Lorsqu'ils sont optimisés, les résultats sont renvoyés aussi rapidement que possible, en sacrifiant la capacité originale à accéder à une page spécifique dans la liste des événements. Désactiver cette case modifie la pagination de la liste Événements pour vous permettre d'accéder à une page spécifique de la liste (ou à la dernière page). La valeur par défaut est **activée**.
   - **Visualisation des sessions par défaut :** Sélectionne le type de reconstruction par défaut pour la reconstruction initiale dans la vue Événements. La valeur par défaut est **Meilleure reconstruction**, dans laquelle les événements sont reconstruits à l'aide de la méthode de reconstruction la plus appropriée pour l'événement.
3. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour afficher la vue Naviguer (11.1) ou Événements (11.2) et définissez l'option **Ajouter des événements dans le panneau Événements**. Lorsque cette option est sélectionnée, les événements affichés dans le **panneau Événements** sont ajoutés progressivement. Par exemple, chaque fois que vous cliquez sur l'icône de la page suivante, la prochaine incrément d'événement est ajouté, au début vous voyez 1 à 25, puis 1 à 50, puis 1 à 75, et ainsi de suite. Cette option est uniquement disponible si l'option **Optimiser les charges de la page Procédure d'enquête** est activée.
4. Pour activer les modifications immédiatement, cliquez sur **Appliquer**.

Activer ou désactiver l'affichage des feuilles de style en cascade dans les reconstructions de contenu Web

Les analystes peuvent activer l'utilisation des feuilles de style en cascade (CSS) lors de la reconstruction du contenu Web. Si elle est activée, la reconstruction Web comprend des styles CSS et des images pour que son apparence soit identique à celle de la vue originale dans un navigateur Web. Elle inclut l'analyse et la reconstruction des événements connexes, et la recherche de feuilles de style et d'images utilisées dans l'événement cible. L'option est activée par défaut. Désactivez cette option en cas de problèmes avec l'affichage de sites Web spécifiques.

Remarque : L'apparition du contenu reconstitué peut ne pas correspondre parfaitement à la page Web d'origine si les images et les feuilles de style sont introuvables ou si elles ont été chargées à partir de la mémoire cache du navigateur Web. De plus, tout style ou mise en page effectué dynamiquement via le javascript côté client n'est pas rendu dans la reconstruction, car tout le javascript côté client est supprimé pour des raisons de sécurité.

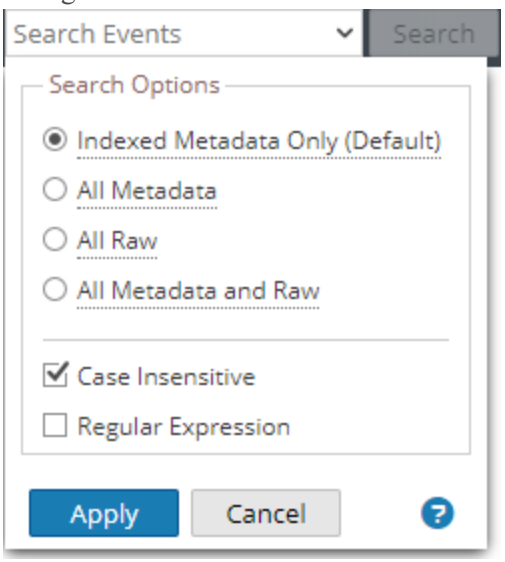
Pour activer ou désactiver cette option :

1. Cliquez sur l'onglet **Procédure d'enquête**.
2. Cochez la case **Activer la vue CSS Reconstruction pour le Web**.
3. Cliquez sur **Apply**.
   Le paramètre devient effectif immédiatement mais ne sera visible que dans la prochaine reconstruction de contenu Web.

Configurer les options de recherche

Vous pouvez configurer les options de recherche à appliquer lorsque vous saisissez une chaîne de recherche dans le champ de recherche. Modifiez les options de recherche dans l'onglet Profil > Panneau Préférences > Enquête ou dans le menu déroulant des options de recherche des vues Navigation et Événements. Configurer les options de recherche, en procédant comme suit :

1. Naviguez jusqu'aux options de recherche.
   La figure suivante illustre le menu déroulant des options de recherche pour la version 11.2.



2. Sélectionnez une ou plusieurs options de recherche à appliquer à la recherche. Rechercher des modèles de texte pour obtenir des informations détaillées sur chaque option.
3. Pour enregistrer les paramètres de recherche, cliquez sur **Appliquer**.
   Les préférences sont enregistrées et effectives immédiatement.

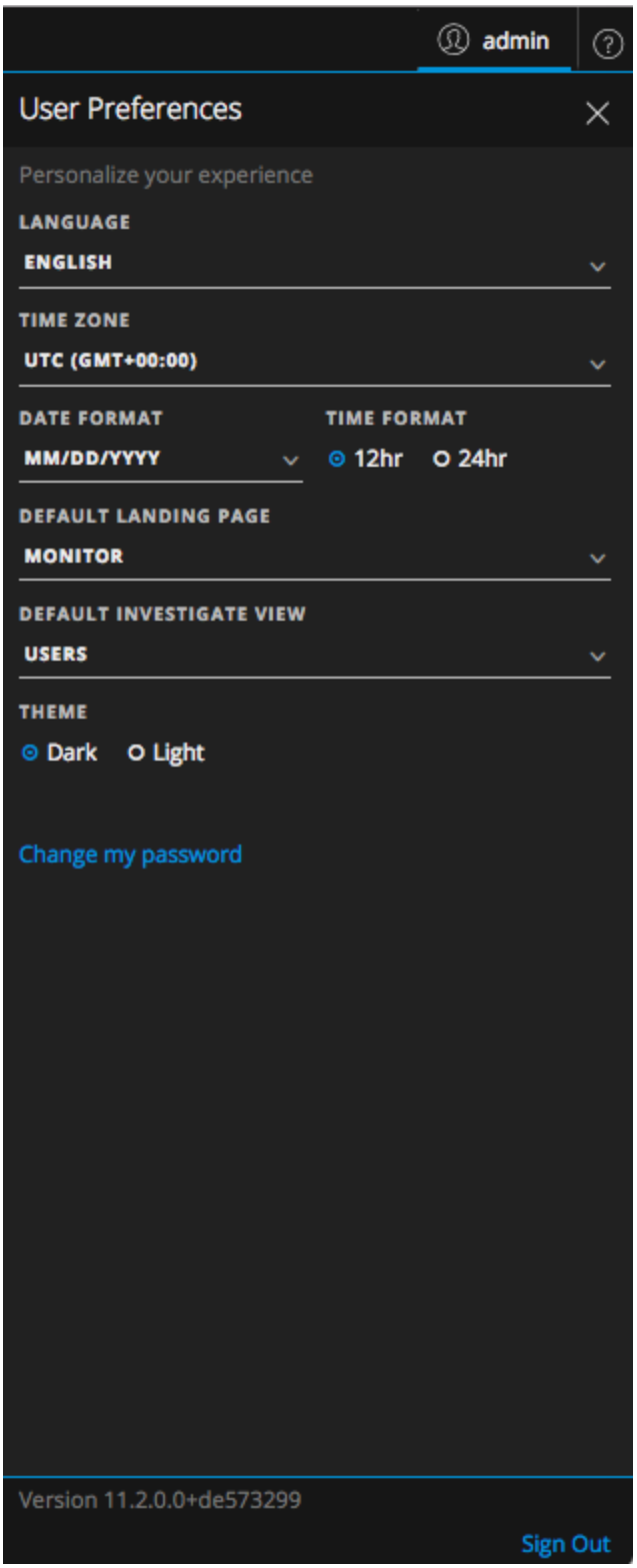
Configurer la vue Analyse d'événements

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

À partir de la Version 11.1, les analystes peuvent définir des préférences qui affectent le comportement de NetWitness Platform lors de l'analyse des données à l'aide de la vue Enquêter > Analyse d'événements. La barre d'outils principale de la vue Enquêter présente des apparences différentes lorsque la vue Analyse d'événements is ouverte. Ces deux boutons permettent d'accéder aux boîtes de dialogue Préférences :  et  . Le menu Utilisateur () concerne les préférences utilisateur globales telles que le fuseau horaire, alors que le menu Préférences de l'Analyse d'événements () concerne les préférences utilisateur pour le comportement de la vue Analyse d'événements. Le reste de cette section décrit les deux ensembles de préférences.

Définir la vue par défaut Enquêter

La vue Enquêter par défaut est définie dans la boîte de dialogue Préférences utilisateur globales (dans l'angle supérieur droit de la fenêtre NetWitness Platform du navigateur, sélectionnez ).
La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles pour la vue Investigate. Vous pouvez sélectionner la vue par défaut lorsque vous ouvrez Enquêter ici : Vue d'analyse des événements, vue Hôtes ou vue Fichiers.



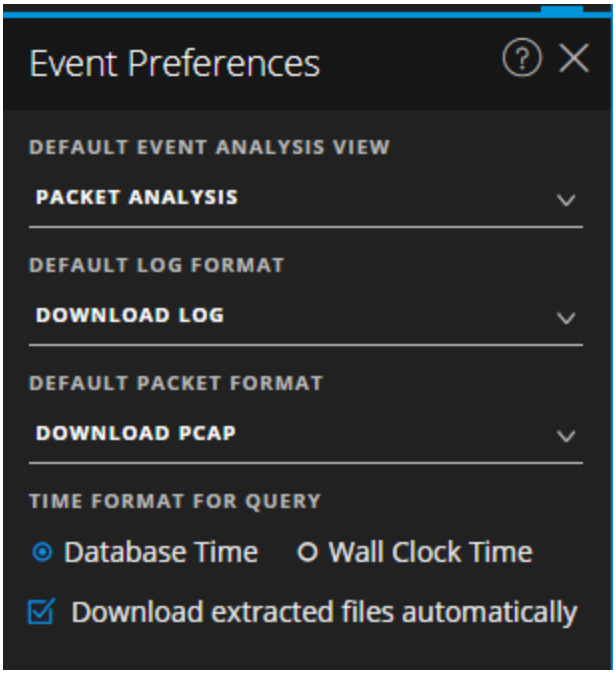
Les préférences utilisateur globales sont décrites en détail dans le *Guide de mise en route de la plate-forme NetWitness*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Définir les préférences utilisateur pour la vue Analyse des événements

Dans la version 11.1 et ultérieures, vous pouvez définir les préférences relatives à la vue Analyse d'événements. Les préférences sélectionnées ici persistent pour chaque utilisateur et sont disponibles à chaque fois que l'utilisateur se connecte à l'application.

Pour définir les valeurs par défaut pour l'utilisation de la vue Analyse d'événements :

1. Lorsque la vue Analyse d'événements est ouverte, cliquez sur .



2. Dans le menu déroulant **Vue Analyse d'événements par défaut**, sélectionnez le type de reconstruction par défaut lorsque vous ouvrez un événement dans le panneau Analyse d'événements : **Analyse de texte**, **Analyse de paquets** et **Analyse de fichiers**.
   Si vous n'avez pas sélectionné de type d'analyse par défaut, lorsque vous ouvrez un événement, le type de reconstruction par défaut est l'Analyse des paquets, sauf pour les événements de log et Endpoint qui ouvrent l'Analyse de texte. Si vous sélectionnez un type de reconstruction par défaut, le type de reconstruction est la reconstruction par défaut que vous avez spécifiée. Dans les deux cas, la valeur par défaut est le point de départ, et si vous modifiez le type en cours d'utilisation, le type que vous choisissez sera utilisé lors de la prochaine reconstruction.
3. Dans le menu déroulant **Format de log par défaut**, sélectionnez le format de téléchargement pour l'exportation des logs : **Télécharger le fichier log**, **Télécharger le fichier XML**, **Télécharger le fichier CSV** ou **Télécharger JSON**. Si vous ne sélectionnez pas de format, le format de téléchargement par défaut est **Télécharger le log**. Ces options sont également disponibles au moment du téléchargement, dans un menu déroulant.
4. Dans le menu déroulant **Télécharger le PCAP**, sélectionnez le format par défaut pour le téléchargement des paquets. Ces options sont également disponibles au moment du téléchargement, dans un menu déroulant.

- **Télécharger le fichier PCAP** pour télécharge l'intégralité de l'événement en tant que fichier de capture de paquets (*.pcap)
- **Télécharger toutes les charges utiles** pour télécharger la charge utile en tant que fichier *.payload
- **Télécharger la charge utile de demande** pour télécharger la charge utile de demande en tant que fichier *.payload1
- **Télécharger la charge utile de réponse** pour télécharger la charge utile de réponse en tant que fichier *.payload2

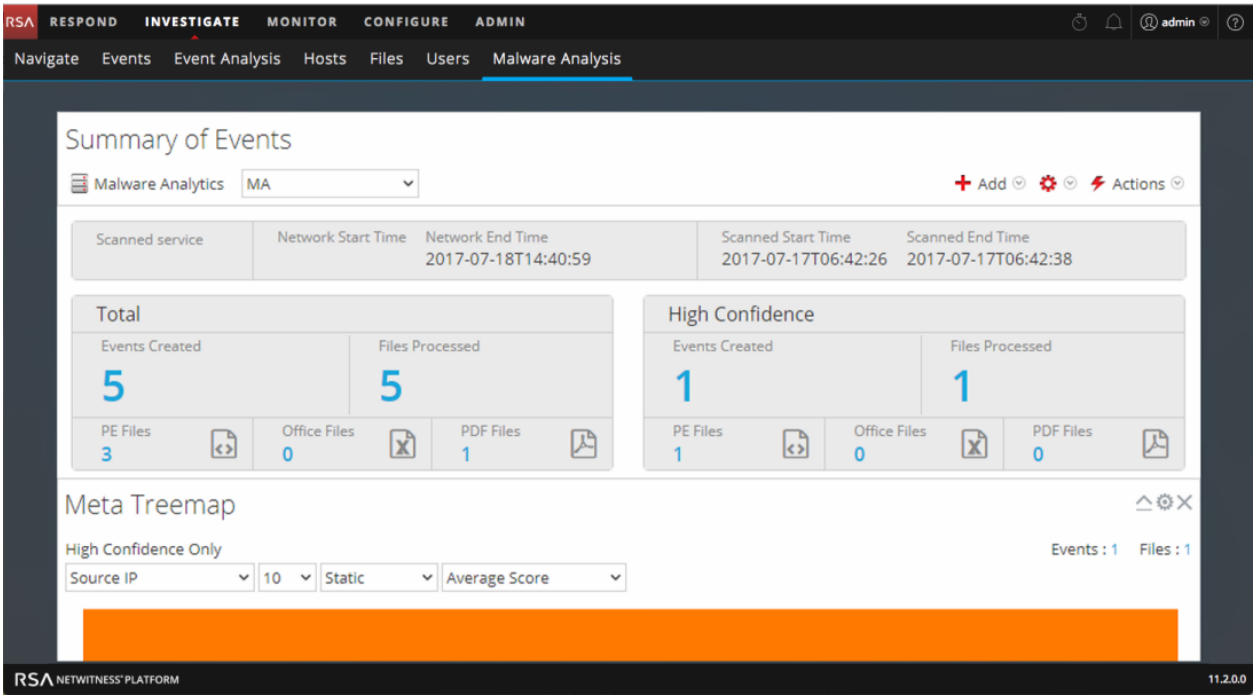
5. Sous **Format de l'heure pour les requêtes**, choisissez **Heure de la base de données** ou **Temps Horloge**. La vue Analyse d'événements peut afficher les résultats en fonction de l'heure de la base de données ou de l'heure actuelle de l'horloge. Lorsque vous définissez le format horaire ici, vos préférences utilisateur individuelles sont enregistrées jusqu'à ce leur nouvelle modification. Le paramètre par défaut pour cette préférence est **Heure de la base de données**, qui est le même format que celui utilisé pour afficher les résultats de la requête dans la vue Naviguer et dans la vue Événements.
   - Lorsque **l'Heure de la base de données** est sélectionnée, l'heure de début et l'heure de fin d'une requête se basent sur l'heure à laquelle l'événement a été stocké.
   - Lorsque **Temps Horloge** est sélectionné, la requête est exécutée avec l'heure actuelle, conformément au fuseau horaire défini dans les préférences utilisateur.

Configurer la vue Récapitulatif des événements de Malware Analysis

Le récapitulatif des événements fournit un résumé de l'analyse qui fait l'objet d'une enquête. Les dashlets configurables tels que les graphiques de visualisation et les listes se situent en dessous. Par défaut, le récapitulatif des événements d'une analyse s'ouvre avec les dashlets par défaut affichés. Vous pouvez personnaliser l'affichage en ajoutant, modifiant et en supprimant des dashlets par défaut. La personnalisation configurée des dashlets persiste à travers différentes procédures d'enquêtes. Vous pouvez restaurer les dashlets par défaut à tout moment. Les dashlets par défaut sont :

- Récapitulatif des événements (fixe)
- Chronologie d'événements
- Liste des principaux malwares fortement suspects
- Compartimentage des méta
- Roue des scores
- Répartition des méta

La figure suivante est un exemple de récapitulatif des événements par défaut.



Le reste de cette rubrique fournit des instructions sur la gestion et la configuration de dashlets.

Ajouter un dashlet

Vous pouvez ajouter plusieurs copies de dashlets dans le récapitulatif des événements d'analyse de Malware Analysis. Pour ajouter un dashlet :

1. Dans la barre d'outils, sélectionnez **Ajouter**.
   La liste déroulante des dashlets s'affiche. Vous disposez de quatre options de visualisation : Roue

des scores, Compartimentage des méta, Répartition des méta et Chronologie d'événements. Les trois autres dashlets sont les mêmes dashlets disponibles dans le tableau de bord NetWitness Platform : Malware à forte probabilité d'indicateur de compromission et scores élevés, Liste des principaux malwares fortement suspects, Liste des principaux malwares de type Zero Day. Les détails pour ces dashlets courants sont fournis dans « Dashlets » dans RSA Content for RSANetWitness Platform.

2. Sélectionnez un dashlet.
   Le nouveau dashlet est ajouté comme dernier dashlet sous les dashlets existants.
3. Si le dashlet est un réplica d'un dashlet existant, changez le nom du nouveau dashlet afin qu'il soit unique.

Modifier ou supprimer un dashlet à l'aide des options de la barre d'outils

Chaque dashlet dispose d'une barre d'outils qui offre des options pour modifier le dashlet. Les graphiques de visualisation ont les mêmes paramètres de configuration, tandis que certains des autres dashlets comportent d'autres paramètres supplémentaires.

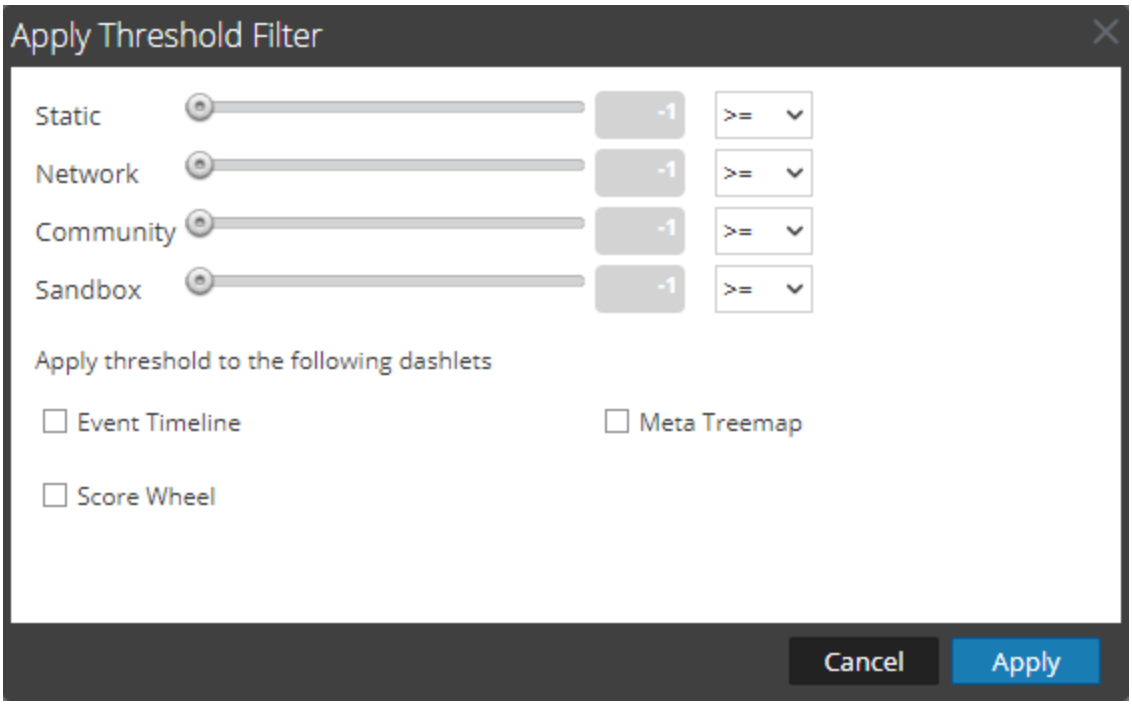
Pour utiliser les options de la barre d'outils :

- Pour fermer un dashlet pour afficher uniquement la barre de titre, cliquez sur .
- Pour ouvrir un dashlet qui est fermé, cliquez sur .
- Pour afficher les paramètres configurables pour un dashlet, cliquez sur .
  La boîte de dialogue Paramètres du dashlet s'affiche.
- Pour supprimer un dashlet, cliquez sur .

Appliquer un filtre de seuil à plusieurs dashlets

Dans les dashlets, vous pouvez définir un seuil pour afficher uniquement les événements égaux, supérieurs ou inférieurs à un certain score dans les quatre catégories (statique, réseau, communauté et Sandbox). Cette procédure définit les seuils par type de dashlet pour ces dashlets : Chronologie d'événements, Roue des scores et Compartimentage des méta. Vous pouvez également définir le seuil pour des dashlets individuels.

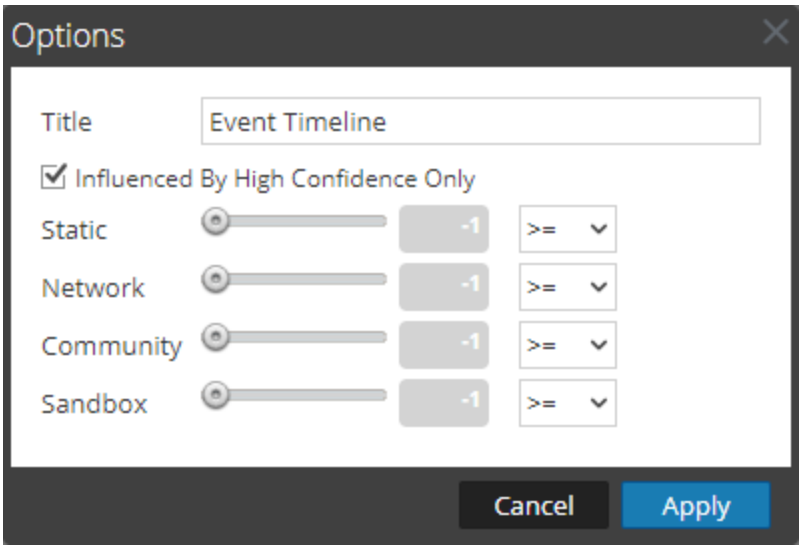
1. Dans la barre d'outils, sélectionnez > **Appliquer le filtre de seuil**.
   La boîte de dialogue Appliquer le filtre de seuil s'affiche.



2. Sélectionne un ou plusieurs types de dashlet : Chronologie d'événements, Roue des scores et Méta Treemap.
3. Faites glisser le curseur ou saisissez une valeur numérique, puis sélectionnez un opérateur dans la liste déroulante : =, >= ou <=.
4. Cliquez sur **Appliquer**.
   Les filtres de seuil sont appliqués aux types de dashlet sélectionnés dans le Récapitulatif des événements.

Définir les options de titre et catégorie pour un dashlet

1. Pour afficher les paramètres configurables pour un dashlet, cliquez sur ⚙.
   La boîte de dialogue Options du dashlet s'affiche.

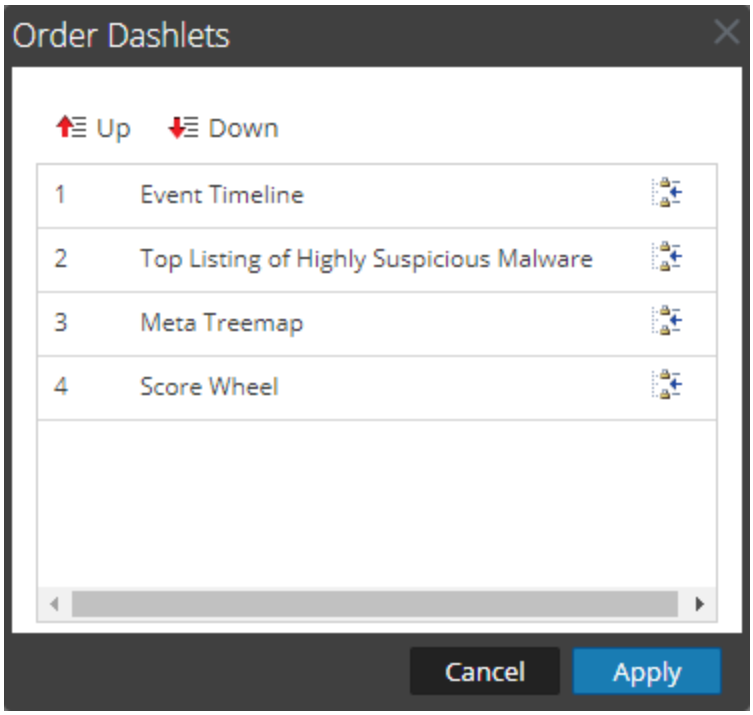


2. Saisissez un nouveau titre pour le dashlet dans le champ **Titre**.
3. Si vous voulez voir uniquement les événements qui sont influencés par une balise de forte probabilité, ce qui signifie qu'il y une grande probabilité que l'événement contienne un code malveillant, cochez l'option **Influencé par la forte probabilité uniquement**.
4. Si vous voulez afficher uniquement les événements avec un score supérieur à un certain score dans les quatre catégories (statique, réseau, communauté et Sandbox), faites glisser le curseur correspondant ou saisissez une valeur numérique, puis sélectionnez un opérateur dans la liste déroulante : =, = ou =.
5. Cliquez sur **Appliquer**.
   Le titre et les filtres sont appliqués au dashlet.

Organiser les dashlets

Pour changer l'ordre des dashlets tels qu'ils apparaissent sous le Récapitulatif des événements :

1. Dans la barre d'outils, sélectionnez > **Organiser les dashlets.**
   La boîte de dialogue Organiser les dashlets s'affiche.



2. Sélectionnez un dashlet que vous souhaitez déplacer vers le haut ou vers le bas, puis cliquez sur Up ou Down.
3. Une fois cette organisation terminée, cliquez sur **Appliquer**.
   La boîte de dialogue se ferme et l'ordre des dashlets sous le Récapitulatif des événements est modifié en fonction de vos choix.

Restaurer les dashlets par défaut

Une fois que vous avez ajouté, modifié et réorganisé les dashlets, vous pouvez revenir aux paramètres par défaut pour l'affichage des dashlets. Pour restaurer les dashlets par défaut :

1. Dans la barre d'outils, sélectionnez > **Restaurer la configuration par défaut.**
   Une boîte de dialogue vous demande de confirmer que vous souhaitez restaurer la configuration.
2. Exécutez l'une des opérations suivantes :
   a. Si vous décidez de conserver la réorganisation du dashlet que vous avez configuré, cliquez sur **Non**.
   b. Si vous êtes sûr de vouloir restaurer les valeurs par défaut, cliquez sur **Oui**, l'affichage du dashlet revient à l'affichage par défaut.

Commencer une procédure d'enquête

NetWitness Platform propose différents points de départ en fonction de la question à laquelle vous tentez de répondre : Vue Naviguer, vue Événements, vue Analyse d'événements, vue Hôtes, vue Fichiers et vue Malware Analysis.

Remarque : Des rôles d'utilisateurs et des autorisations spécifiques sont requis pour qu'un utilisateur puisse mener des procédures d'enquête et des analyses de programmes malveillants dans NetWitness Platform. Si vous ne pouvez pas réaliser de tâche d'analyse ou afficher une vue, il se peut que l'administrateur doive ajuster les rôles et autorisations configurés pour vous. Les vues Fichiers et Hôtes sont disponibles dans les versions 11.1 et supérieures. La vue Analyse d'événements est disponible dans la version 11.0, mais le mode d'accès s'effectue via la vue Événements. Accéder directement à la vue Analyse d'événements (version 11.1 et supérieure)

Se concentrer sur les vues Métadonnées, Événements bruts et Analyse d'événements

Pour rechercher les événements qui génèrent le flux de travail de réponse aux incidents et effectuer une analyse stratégique après qu'un autre outil ait généré un événement, vous devez commencer dans la vue Naviguer, la vue Evénements ou la vue Analyse d'événements. Analysez les métadonnées d'un seul service Broker ou Concentrator. Dans chacune de ces vues, démarrez la recherche en ouvrant la vue, où vous pouvez exécuter une requête et filtrer les résultats en réduisant la plage de temps et en interrogeant les métadonnées. Ces rubriques fournissent des détails sur l'ouverture d'une enquête dans chaque vue :

- Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
- Commencer une procédure d'enquête dans la vue Analyse d'événements

Se concentrer sur les vues Hôtes et Fichiers

Pour rechercher des informations sur les hôtes sur lesquels l'agent est en cours d'exécution, lancez l'analyse dans la vue Hôtes (**Procédure d'enquête > Hôtes**). Pour chaque hôte, vous pouvez voir les processus, les pilotes, les DLL, les fichiers (exécutables), les services et les exécutions automatiques en cours d'exécution, ainsi que les informations relatives aux utilisateurs connectés. (Reportez-vous à la section Examiner les hôtes)

Vous pouvez commencer la procédure d'enquête sur les fichiers de votre déploiement dans la vue Fichiers (**Enquête > Fichiers**). (Reportez-vous à la section Examiner les fichiers.)

Remarque : Pour charger la vue Hôtes et Fichiers, vous devez disposer de l'autorisation `endpoint-server.filter.manage`.

Se concentrer sur la recherche de programmes malveillants dans les fichiers

Pour analyser les fichiers à la recherche de programmes malveillants potentiels ou configurer une analyse continue d'un service, commencez dans la vue Malware Analysis. Les résultats sont exprimés en quatre types d'analyse : réseau, statique, communautaire et sandbox avec un indicateur de compromis (IOC). Il existe plusieurs façons de commencer à travailler dans Malware Analysis :

- Vous pouvez lancer Malware Analysis à partir des dashlets Malware Analysis dans la vue Moniteur pour afficher rapidement les menaces potentielles les plus dangereuses.
- Vous pouvez accéder à **Procédure d'enquête > Malware Analysis** pour ouvrir le récapitulatif des événements Malware Analysis.
- Vous pouvez cliquer avec le bouton droit sur une clé méta dans la vue Naviguer, puis sélectionnez **Analyser les malwares**.

Reportez-vous à la section Mener une analyse de malware pour plus d'informations sur l'utilisation de la vue Malware Analysis.

Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

La vue Parcourir est la vue par défaut pour la procédure d'enquête, sauf si vous avez sélectionné une vue différente comme vue d'ouverture. Cette préférence utilisateur est définie sur le niveau de l'application décrit dans Configuration des vues et des préférences de NetWitness Investigate. Dans les vues Naviguer et Événements, vous recherchez des événements d'intérêt basés sur une requête. Dans la vue Naviguer, vous pouvez également affiner les résultats en cliquant sur les clés méta et les valeurs méta. Lorsque vous trouvez des événements intéressants, vous pouvez analyser l'événement de plus près dans les autres vues Enquêter.

Pour commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements, un service doit être spécifié.

- NetWitness Platform ouvre la vue Naviguer ou la vue Événements avec le service par défaut spécifié par l'utilisateur sélectionné.
- Si aucun service par défaut n'est actuellement spécifié et que l'identifiant de service ne se trouve pas dans l'URL, NetWitness Platform présente une boîte de dialogue permettant de sélectionner le service ou la collection à examiner.
- Lorsqu'un service a été sélectionné manuellement ou par défaut dans la vue Naviguer ou la vue Événements, vous pouvez modifier le service ou la collection à examiner en sélectionnant le nom du service dans la barre d'outils. NetWitness Platform affiche la boîte de dialogue permettant de sélectionner le service à examiner.

Remarque : Le service Archiver ne figure pas dans la vue Naviguer pour réduire au minimum un ralentissement des performances lors de l'exécution des enquêtes au niveau de l'expérience utilisateur. Le service Archiver est disponible dans la vue Événements pour les exportations de logs et les fonctions de recherche améliorée.

Avec un service sélectionné ou une collection sélectionnée, NetWitness Platform est prêt à charger les données du service ou de la collection. Il est recommandé de sélectionner également une période afin que les résultats se chargent plus rapidement. Plusieurs paramètres de la vue Naviguer et de la boîte de dialogue Paramètres de la vue Événements ou Profils > panneau Préférences > onglet Procédures d'enquête affectent le processus de chargement : la page Seuil, Nb max résultats de valeurs, Afficher les informations de débogage, Charger automatiquement les valeurs et Optimiser l'investigation se charge (voir la rubrique Configuration des vues et des préférences de NetWitness Investigate).

Remarque : Dans la vue Événements, les données se chargent automatiquement. Si vous avez indiqué Charger automatiquement les valeurs dans les préférences de la vue Naviguer, NetWitness Platform renseigne automatiquement les données. Sinon, vous devez sélectionner le bouton Charger les valeurs. NetWitness Platform remplit les métadonnées dans le panneau Valeurs de la vue Naviguer et les résultats deviennent visibles presque immédiatement.

Le reste de cette rubrique fournit des instructions pour commencer la procédure d'enquête des données sur un service.

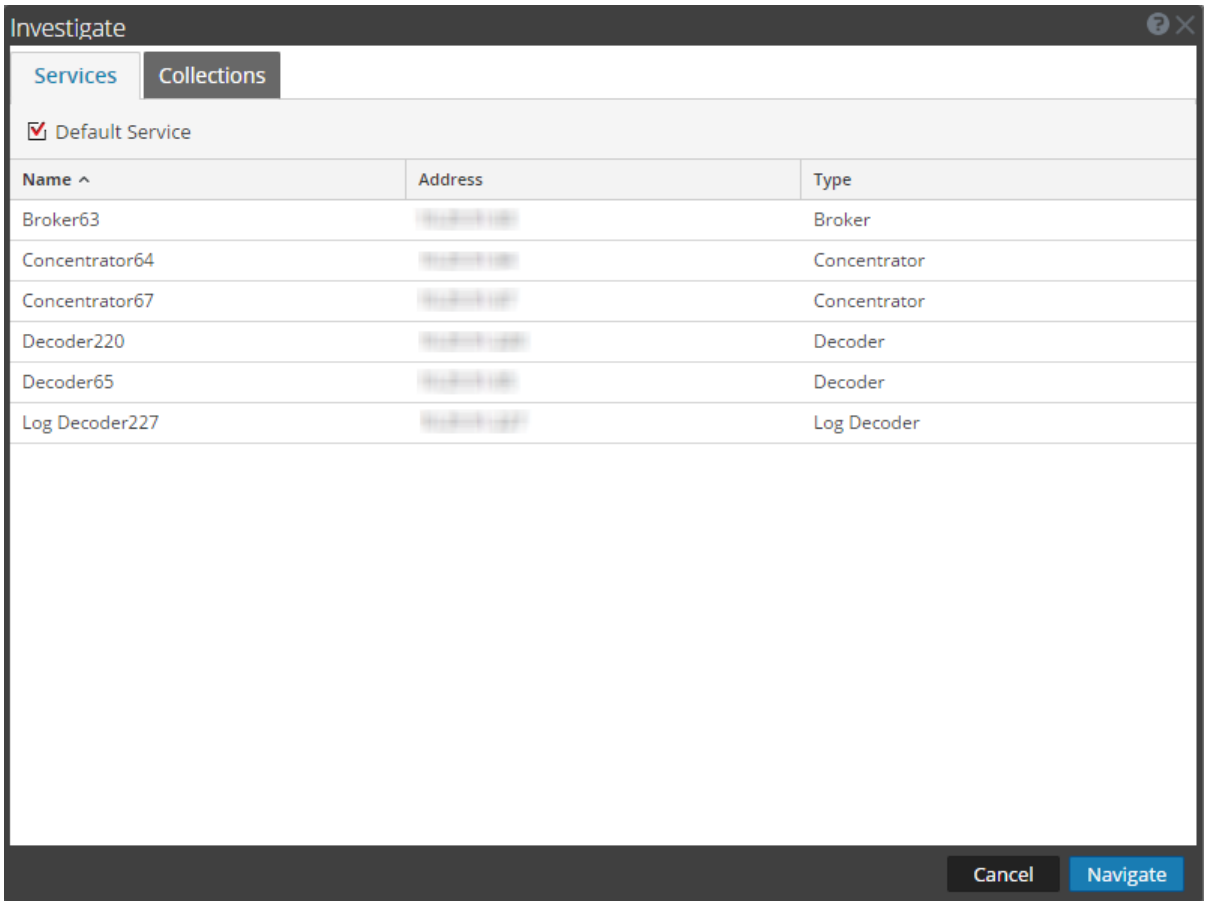
Remarque : Seuls les utilisateurs ayant le rôle d'administrateur peuvent créer une collection, et seul le créateur de la collection est en mesure d'enquêter sur elle.

Après le chargement des données dans la vue Naviguer ou Événements :

1. Affiner les résultats, visualiser les données et agir sur un point d'extraction (reportez-vous à la section Procédure d'enquête relative aux métadonnées dans la vue Naviguer et Examiner les événements bruts dans la vue Événements. Par exemple, vous pouvez Rechercher un contexte supplémentaire dans les vues Naviguer et Événements, Lancer une analyse Malware Analysis à partir de la vue Naviguer ou Ajouter des événements à un incident pour obtenir une réponse.
2. Reconstruisez un événement (reportez-vous à la section Reconstruire un événement) ou affichez l'analyse d'événement interactive d'un événement (reportez-vous à la section Commencer une procédure d'enquête dans la vue Analyse d'événements).

Commencer une procédure d'enquête (aucun service par défaut)

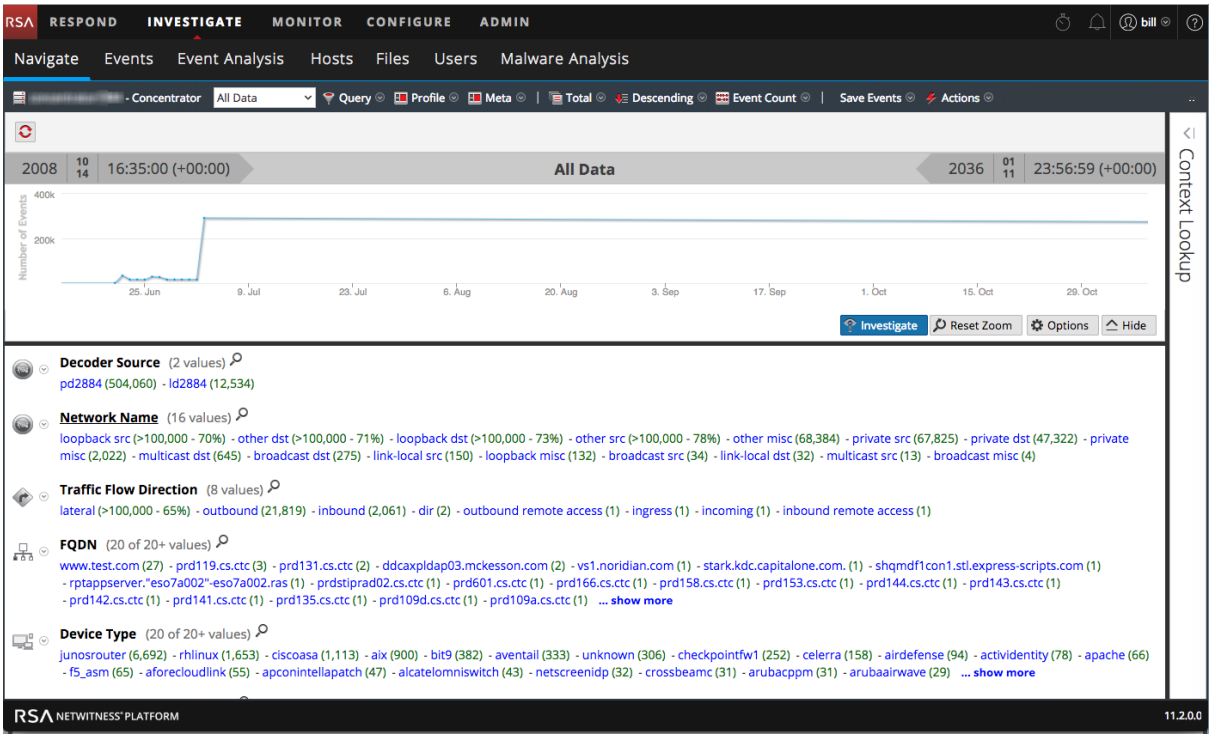
1. Accédez à **ENQUÊTER > Naviguer** ou **Événements**.
   La boîte de dialogue Enquêter s'affiche.



2. Double-cliquez sur un service ou sélectionnez un service, en général un Concentrator, puis cliquez sur **Naviguer**.
   Les données se chargent automatiquement dans la vue Événements. Si vous travaillez dans la vue

Naviguer, le panneau qui en résulte affiche l'activité pour le service sélectionné, mais les données ne sont pas chargées automatiquement.

3. (Recommandé) Sélectionnez une période spécifique afin que les résultats se chargent plus rapidement.
4. Si vous souhaitez modifier les options de procédure d'enquête avant le chargement, vous pouvez créer ou modifier un profil personnalisé, appliquer une période différente, créer ou appliquer un groupe méta, et effectuer une requête personnalisée, comme décrit dans la rubrique Interrogation et action sur les données dans les vues Naviguer et Événements. Vous pouvez également modifier les options à tout moment pendant la procédure d'enquête.
5. Pour charger les données dans la vue Naviguer, cliquez sur Load Values.
   Les données pour le service sélectionné commencent à se charger.

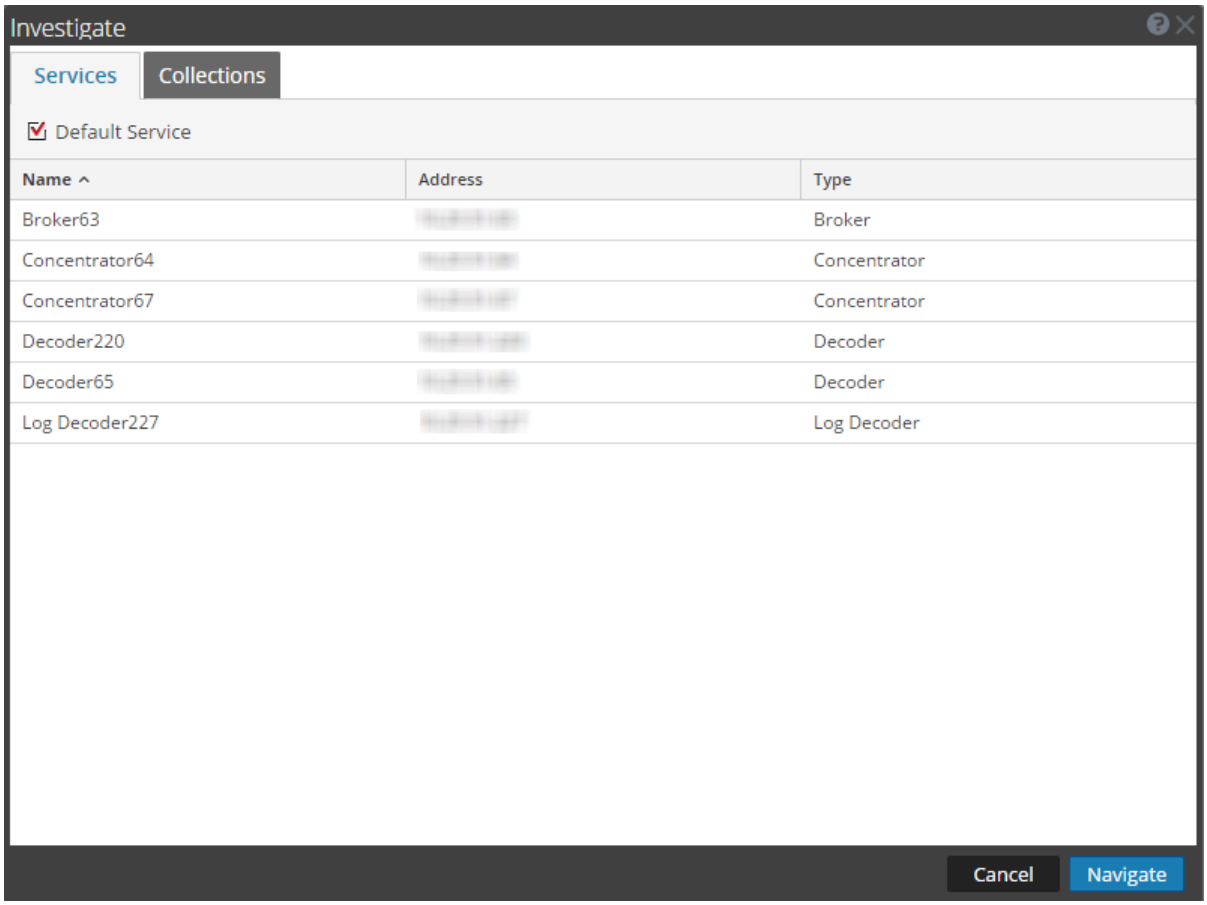


Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données.

Définir ou effacer le service par défaut

Vous pouvez définir le service par défaut et désactiver le service par défaut dans la boîte de dialogue Rechercher un service.

1. Cliquez sur le nom du service dans la barre d'outils.
   La boîte de dialogue Enquêter s'affiche.



2. Sélectionnez un service dans la grille **Services** et cliquez sur Default Service.
   Le service devient la valeur par défaut (indiqué par **Par défaut** entre parenthèses après le nom du service).

3. Pour effacer le service par défaut, sélectionnez-le dans la grille, cliquez sur Default Service, puis sur **Annuler** pour fermer la boîte de dialogue.
   Aucun service par défaut n'est défini.

> **Remarque :** Le bouton Annuler n'annule pas votre sélection du service par défaut. Il ferme simplement la boîte de dialogue sans avoir à naviguer vers le service actuellement sélectionné dans la grille. La définition d'un service par défaut, différent du service actuellement à l'étude, n'actualise pas la vue Naviguer. Vous devez le sélectionner explicitement et naviguer vers un autre service.

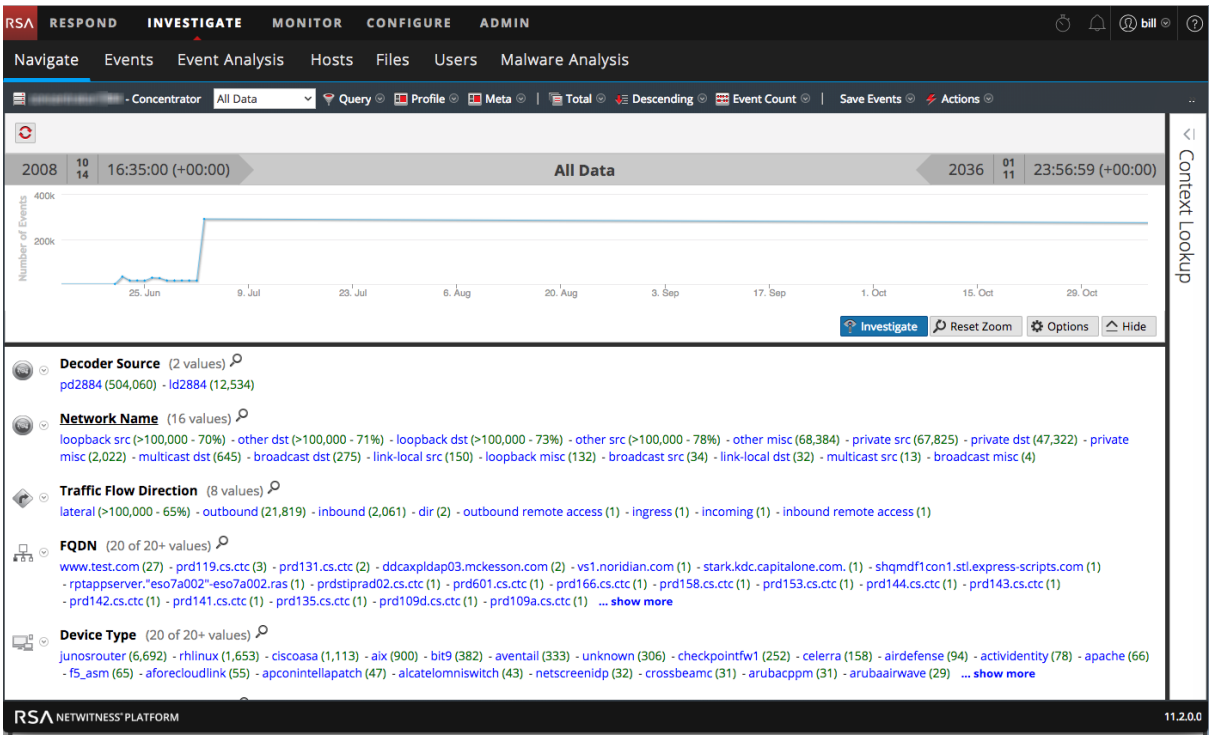
Commencer une procédure d'enquête (service par défaut spécifié)

1. Accédez à **ENQUÊTER > Naviguer** ou > **Événements**.
   Si le paramètre Charger automatiquement les valeurs est désactivé, la vue Naviguer s'affiche avec le service par défaut sélectionné et est prête à charger les données. Si le paramètre Charger automatiquement les valeurs est activé, les valeurs sont chargées comme indiqué à l'étape 3. Dans la

vue Événements, les données se chargent automatiquement.

2. Si vous souhaitez modifier les options de procédure d'enquête dans la vue Naviguer avant le chargement, vous pouvez créer ou modifier un profil personnalisé, appliquer une période différente, créer ou appliquer un groupe méta, et effectuer une requête personnalisée.

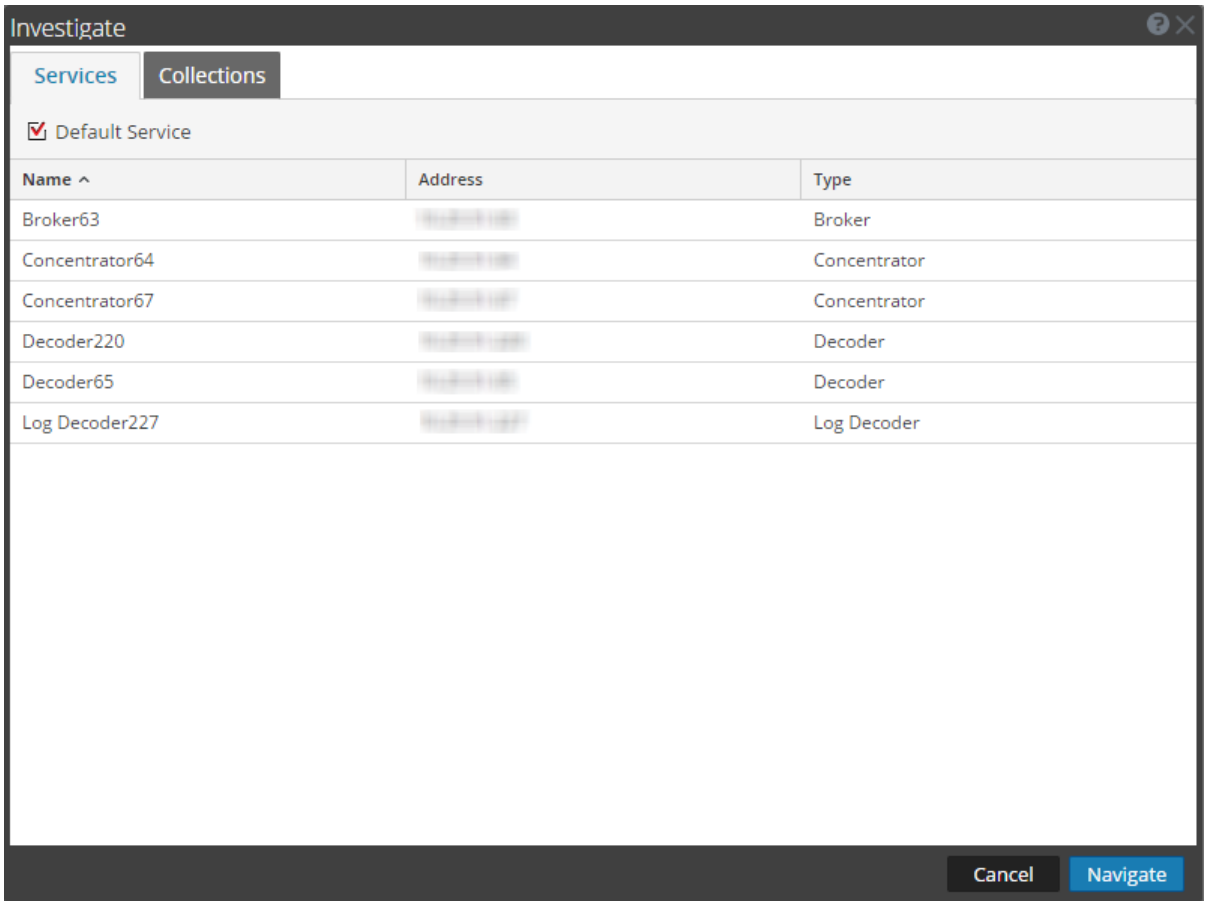
3. Lorsque vous êtes prêt, cliquez sur Load Values.
   Les valeurs du service sont chargées selon les options choisies.



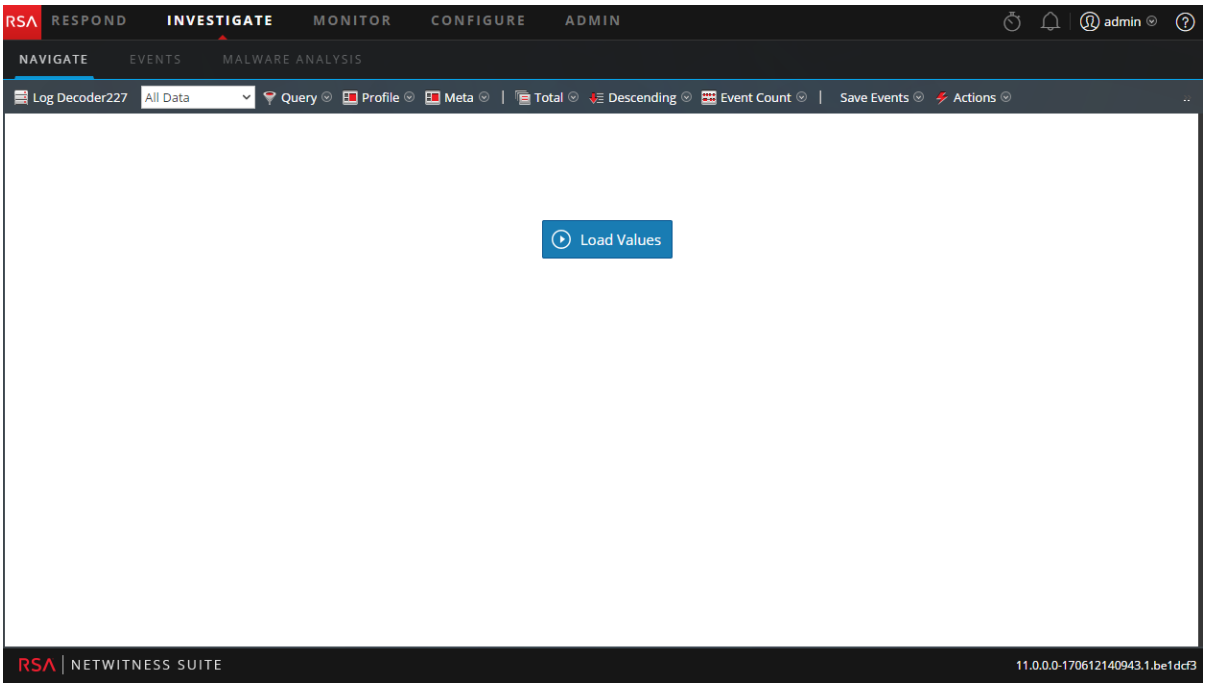
Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données.

Modifier le service ou la collecte à examiner

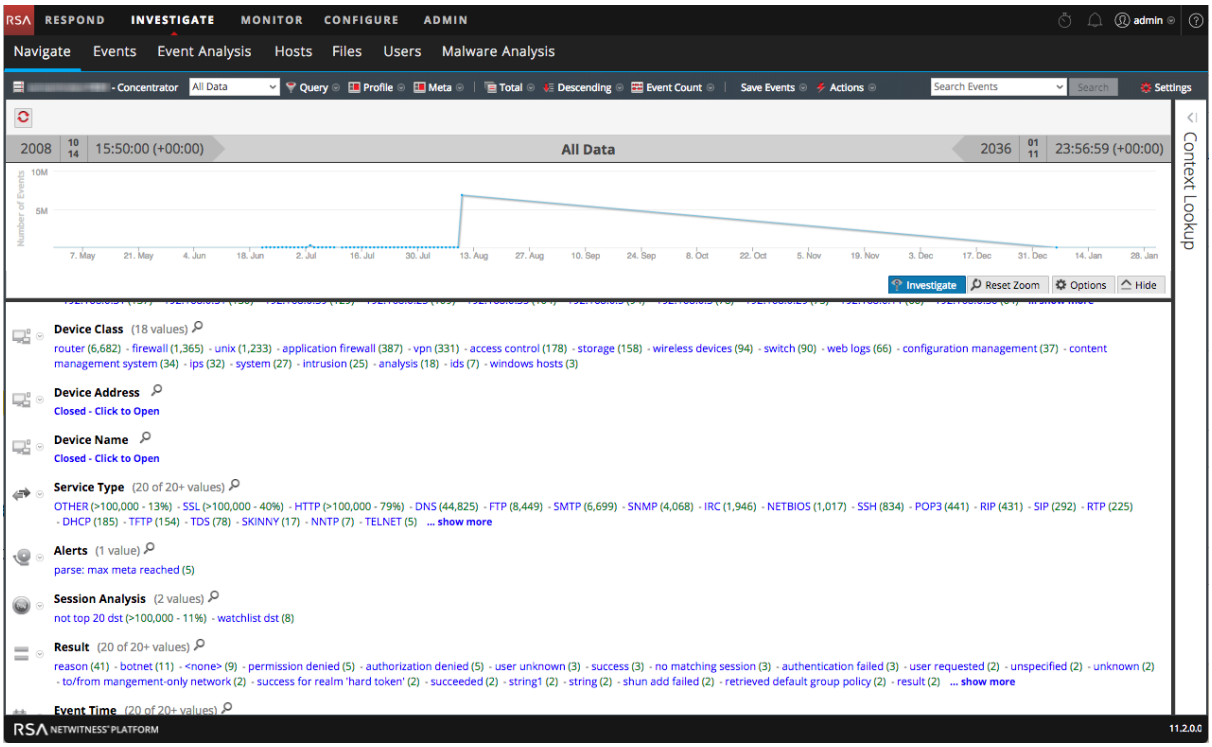
1. Dans la vue Naviguer ou la vue Événements, cliquez sur le nom du service en haut du panneau d'options.
   La boîte de dialogue Enquêter s'affiche.



2. Double-cliquez sur un service ou sélectionnez un service, puis cliquez sur **Naviguer**. Le panneau résultant affiche l'activité pour le service sélectionné.
   Si le paramètre Charger automatiquement les valeurs est activé, les valeurs sont chargées comme indiqué à l'étape 3. Dans le cas contraire, la vue Naviguer s'affiche avec le service sélectionné par défaut et les données sont prêtes à charger. Dans la vue Événements, les données sont chargées automatiquement.



3. Lorsque vous êtes prêt, cliquez sur Load Values.
   Les valeurs du service commencent à se charger selon les options choisies.



Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données.

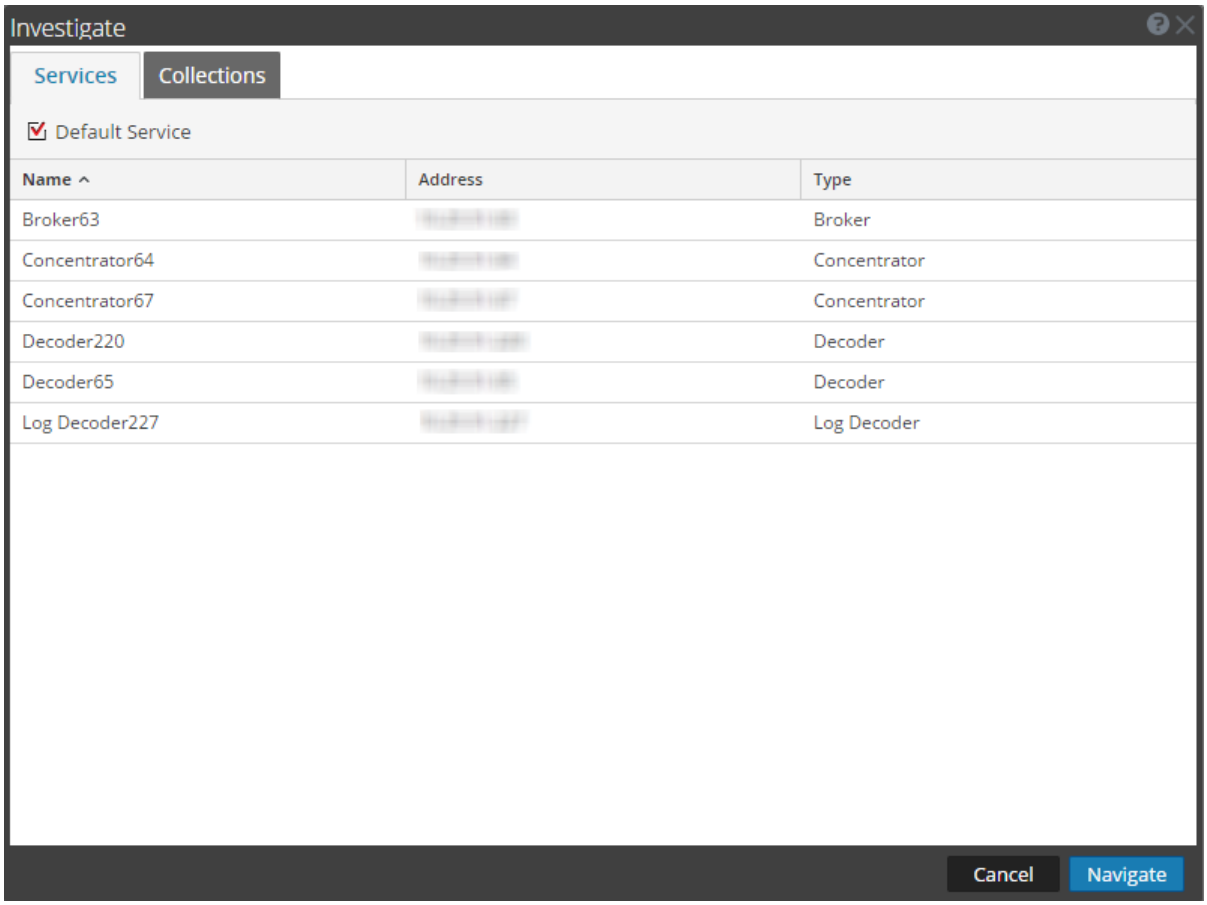
Examiner des collections de restauration Workbench

Cette procédure permet aux administrateurs de sélectionner le contenu à partir d'une collection existante pour le retraiter en vue d'une étude plus approfondie. Cela s'applique aux services Decoder qui utilisent des services Workbench.

Remarque : Seul un utilisateur avec des privilèges d'administration peut créer une collection. Vous pouvez afficher uniquement les collections que vous avez créées.

Pour retraiter des données en vue d'une étude plus approfondie :

1. Accédez à **ENQUÊTER > Naviguer** ou **Événements**.
   La boîte de dialogue Enquêter s'affiche.



2. Sélectionnez un service Workbench et le nom du Workbench que vous souhaitez étudier.
3. Cliquez sur **Naviguer** pour effectuer une procédure d'enquête sur votre service Workbench sélectionné.
   Cliquez sur **Annuler** pour sélectionner un service Workbench différent à examiner.
   La vue Procédure d'enquête s'affiche.

Avec la collection sélectionnée et les données chargées, vous êtes prêt à commencer à analyser les données.

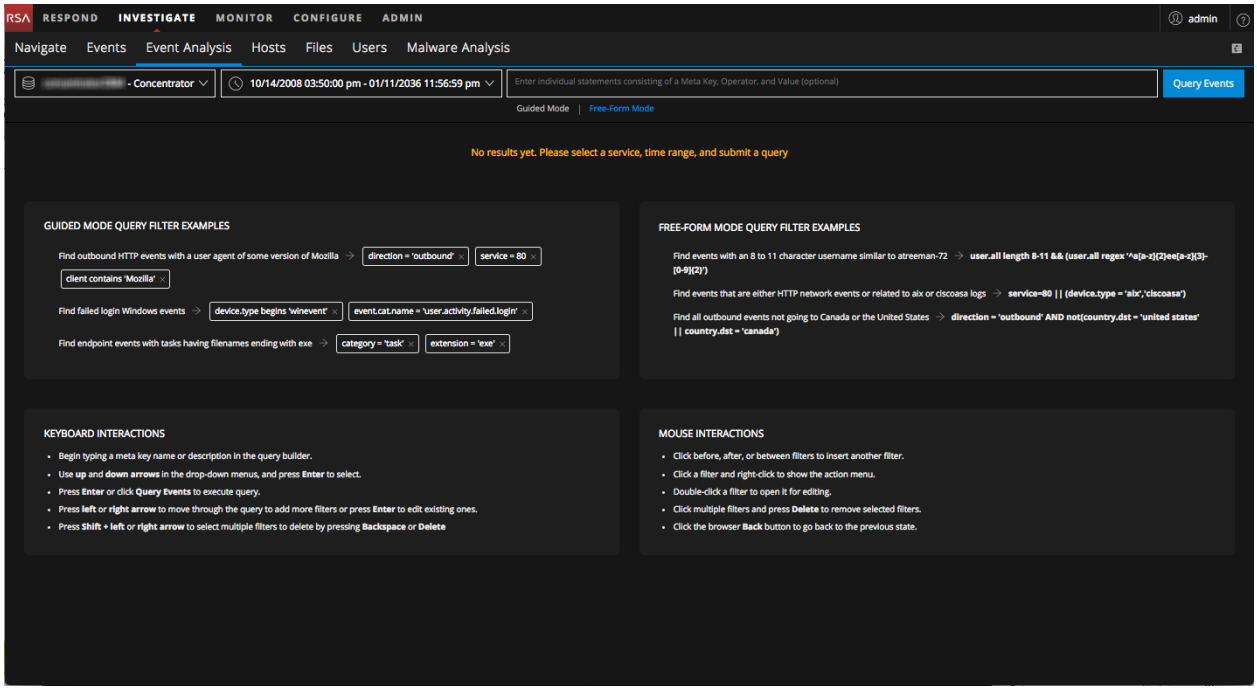
Commencer une procédure d'enquête dans la vue Analyse d'événements

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

La vue Analyse d'événements propose la plupart des fonctionnalités disponibles dans la vue Naviguer et la vue Événements. À l'instar de la vue Naviguer, il existe une vue pour les clés méta et les valeurs méta des logs, points de terminaison et paquets. Comme dans la vue Événements, une liste d'événements affiche des événements répertoriés dans l'ordre par heure, et vous pouvez afficher l'événement brut, les métadonnées associées, et la reconstruction d'un événement. La reconstruction de l'Analyse d'événements dispose d'aides visuelles permettant d'identifier les points d'intérêt dans une reconstruction. Consultez la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements

Remarque : Dans la version 11.0, vous ne pouvez pas commencer une procédure d'enquête dans la vue Analyse d'événements. Au lieu de cela, vous commencez la procédure d'enquête dans la vue Naviguer ou dans la vue Événements et ouvrez un événement dans la vue Analyse d'événements. Dans la version 11.1, le sous-menu PROCÉDURE D'ENQUÊTE vous offre un accès direct à la vue Analyse d'événements, avec la possibilité de sélectionner un service différent, une période et de créer une requête.

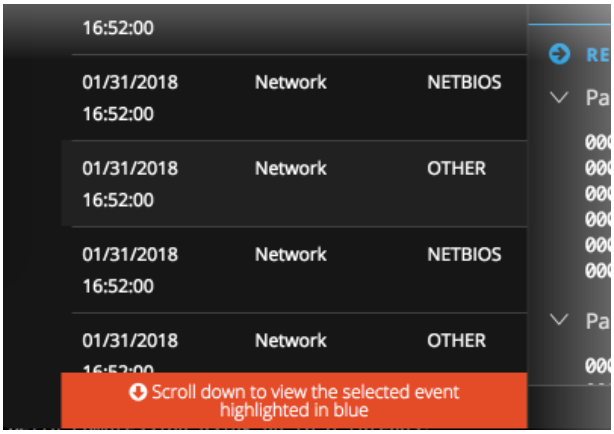
La figure suivante montre la vue Analyse d'événement initiale avec une info-bulle fournissant des exemples de requêtes.



Accéder à la vue Analyse d'événements (version 11.1 et supérieure)

Plusieurs méthodes permettent d'accéder à la vue Analyse d'événements dans la version 11.1.

- Lorsque vous utilisez **Actions > Accéder à un événement dans Analyse d'événements** dans la vue Naviguer et saisissez un ID d'événement, la vue Analyse d'événements ouvre l'événement unique en tant que reconstruction. Pour simplifier l'affichage, la barre d'outils n'inclut pas d'options superflues pour développer, réduire et fermer les fenêtres. Vous pouvez commencer à travailler comme le décrit la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements.
- Lorsque vous pointez le curseur de la souris sur un nombre (le nombre vert après une valeur méta) dans la vue Naviguer, puis cliquez sur **Ouvrir l'analyse d'événements dans un nouvel onglet**, la vue Analyse d'événements s'ouvre avec la liste d'événements pour le point de recherche verticale sélectionné et vous pouvez commencer à travailler comme le décrit la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements. La liste d'événements peut être très volumineuse, et il est possible que l'événement que vous avez sélectionné ne soit pas visible dans la page actuelle d'événements. Dans ce cas, un message vous conseille de faire défiler vers le bas pour afficher l'événement.



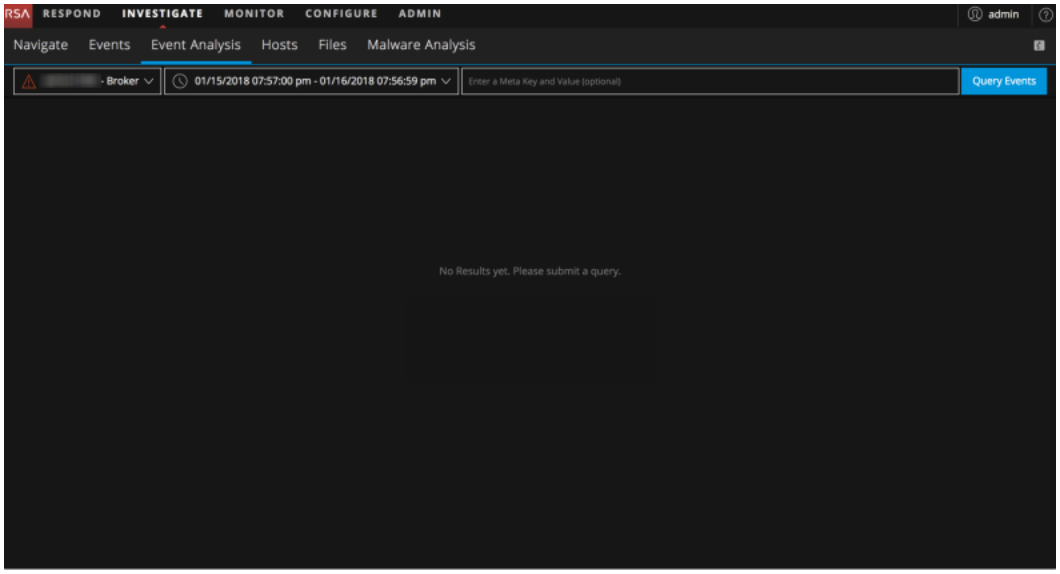
- Vous pouvez également accéder à la vue Analyse d'événements directement en accédant à **ENQUÊTER > Analyse d'événements** ou **ENQUÊTER** si vous avez fait de la vue Analyse d'événements celle qui s'ouvre lorsque vous cliquez sur Enquêter. Lorsque vous accédez à la vue Analyse d'événements pour la première fois, vous devez sélectionner un service pour commencer l'analyse. Si ce n'est pas la première fois que vous ouvrez Analyse d'événements, le dernier service utilisé est mémorisé jusqu'à ce que le cache du navigateur soit effacé.
  Lorsque vous ouvrez la vue Analyse d'événements à partir de l'une des autres vues Enquêter, le service et la requête de cette vue s'appliquent. Vous pouvez modifier le service, sélectionner une période et saisir une requête si vous souhaitez affiner les résultats avant d'ouvrir la vue Analyse d'événements, comme décrit dans Filtrer les résultats dans la vue Analyse d'événements.

Pour accéder directement à la vue Analyse d'événements,

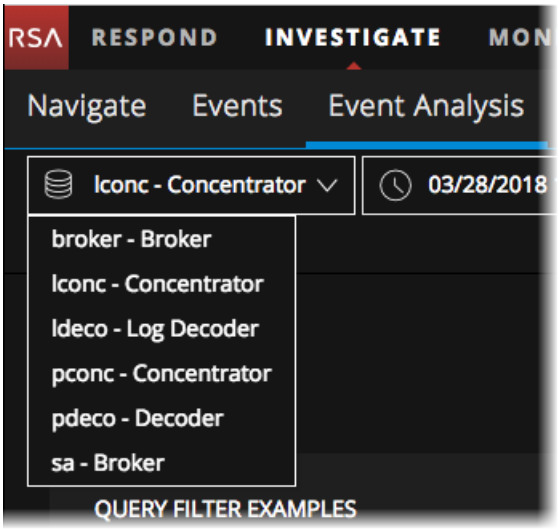
1. Accédez à **ENQUÊTER** > **Analyse d'événements**.
   La vue Analyse d'événements s'ouvre sur le premier service sélectionné de la liste de services et aucune donnée ne s'affiche. Le champ **Sélectionner un service** est d'abord renseigné avec le premier service de la liste ou le dernier service sélectionné. Un menu déroulant propose une liste de services disponibles par ordre alphabétique. Par défaut, la liste de services disponibles est extraite toutes les 12 heures et mise en cache dans le serveur NetWitness. Si un service est ajouté ou supprimé sur le serveur NetWitness, le cache est mis à jour avec la toute dernière liste de services.

Au début du champ, une icône indique l'état de la requête.

- et aucun nom de service = aucun service n'est sélectionné.
- et un nom de service sélectionné = le service est sélectionné.
- = Enquêter tente de se connecter au service sélectionné.
- = Enquêter ne peut pas se connecter au service sélectionné ou il n'y a pas de données. Dans cet état, la commande du sélecteur de services passe également au rouge, et une info-bulle explique pourquoi la tentative de connexion a échoué et vous conseille de choisir un autre service.

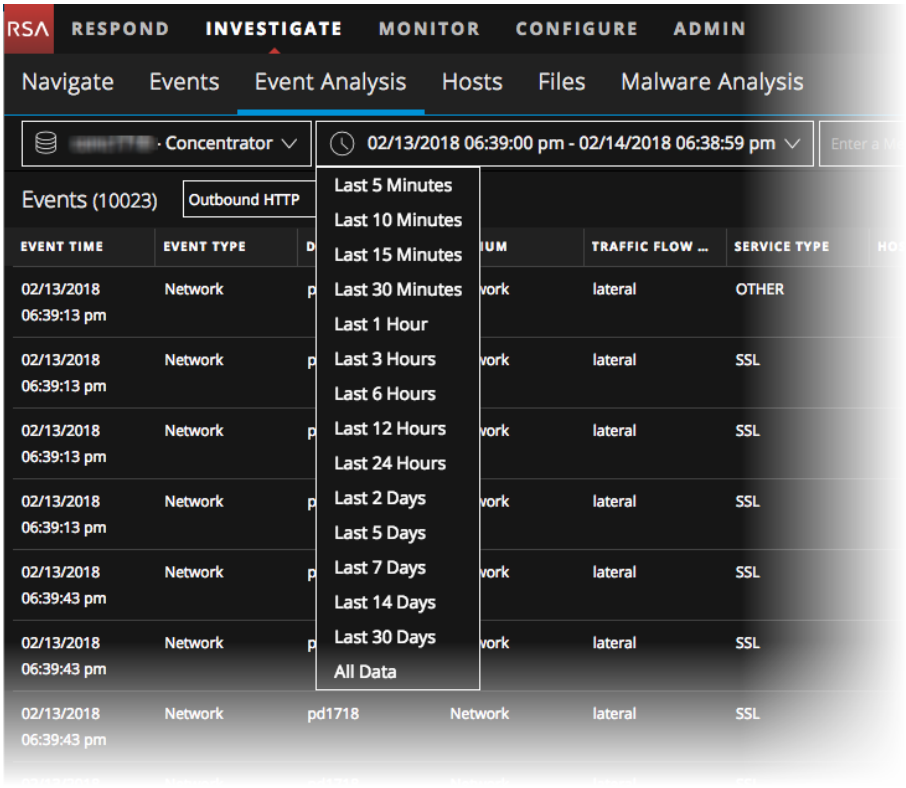


2. (Optionnel) Sélectionnez un service, en général un Concentrator, dans la liste déroulante.



Le sélecteur de période indique soit la période par défaut de 24 heures, soit la période que vous avez sélectionnée pour ce service. Le bouton Interroger des événements devient actif et vous pouvez saisir des filtres. Si vous lancez une requête maintenant, la période sélectionnée est utilisée.

3. (Facultatif) Pour sélectionner une période à partir du sélecteur de période, cliquez sur le sélecteur de **Période** et sélectionnez une période dans la liste déroulante. Les options sont les 5, 10, 15 ou 30 dernières minutes, l'heure dernière ou les 3, 6, 12 ou 24 heures dernières, les 2, 5, 7, 14 ou 30 jours derniers, ou Toutes les données. (La période se base sur le jeu de préférences de la vue Analyse d'événements. La base par défaut pour la période est l'heure de la base de données. Vous pouvez la modifier pour le Temps Horloge.)
   La période sélectionnée est stockée dans votre navigateur pour ce service. Vous pouvez définir différentes périodes pour différents services.

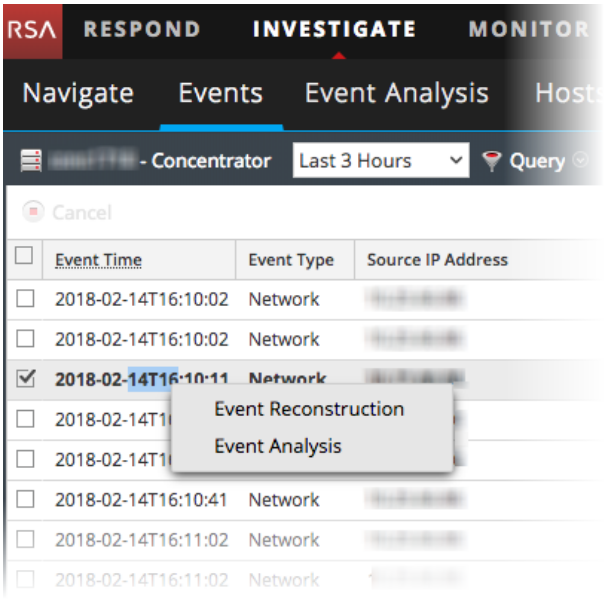


4. Saisissez une requête en créant un ou plusieurs filtres qui contiennent au moins une clé méta ou une entité méta, un opérateur et une valeur facultative. Reportez-vous à la section Filtrer les résultats dans la vue Analyse d'événements pour plus d'informations sur la saisie de requêtes.
5. Cliquez sur **Événements de requête**.
   La vue Analyse d'événements affiche l'activité pour le service sélectionné et la période, conformément aux autorisations attribuées à votre rôle par l'administrateur. Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données. Reportez-vous à la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements pour savoir comment utiliser la vue Analyse d'événements.

Accédez à la vue Analyse d'événements (version 11.0)

Pour ouvrir un événement dans la vue Analyse d'événements :

1. Accédez à **ENQUÊTER** > **Événements**.
2. Cliquez avec le bouton droit sur un événement parmi les événements répertoriés, puis sélectionnez **Analyse d'événements**.



Reportez-vous à la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements pour savoir comment utiliser la vue Analyse d'événements.

Procédure d'enquête relative aux métadonnées dans la vue Naviguer

Lors d'une procédure d'enquête dans la vue Naviguer, les analystes disposent de plusieurs méthodes, spécifiques à la vue Naviguer, pour affiner les résultats, visualiser les données et agir sur les données.

- Filtrer les résultats dans la vue Naviguer
- Gérer les groupes méta
- Visualiser des métadonnées en tant que coordonnées parallèles
- Ouvrir un événement de la liste Événements
- Exporter ou imprimer un point d'extraction
- Lancer la recherche externe d'une clé méta
- Lancer une analyse Malware Analysis à partir de la vue Naviguer
- Visualiser le point d'extraction verticale actuel dans Informer

En outre, vous pouvez utiliser ces méthodes pour interroger des données et agir sur les résultats communs à la vue Naviguer et à la vue Événements.

- Rechercher des modèles de texte
- Créer une requête personnalisée
- Afficher et modifier des requêtes avec l'intégration URL
- Utiliser des profils pour encapsuler les vues personnalisées
- Gérer Listes Context Hub et Valeurs de la liste dans les vues Naviguer et Événements
- Rechercher un contexte supplémentaire dans les vues Naviguer et Événements
- Reconstruire un événement

Filtrer les résultats dans la vue Naviguer

Lors d'une procédure d'enquête dans la vue Naviguer, il existe plusieurs méthodes disponibles pour affiner les résultats affichés lorsque des valeurs de clé méta sont chargées dans la vue Naviguer. Les méthodes basiques de filtrage dont disposent les analystes sont les suivantes :

- Définir la période
- Définir la méthode de quantification et trier la séquence des résultats de clé méta
- Gérer et appliquer des clés méta par défaut dans une procédure d'enquête
- Effectuer une recherche verticale dans les données au sein du graphique chronologique de la vue Naviguer
- Effectuer une recherche verticale dans les données dans le panneau Valeurs

Le reste de cette rubrique est axé sur les méthodes basiques de filtrage des données. En outre, des méthodes plus avancées permettent la configuration de groupes méta, profils et visualisations de coordonnées parallèles.

- Visualiser des métadonnées en tant que coordonnées parallèles
- Gérer les groupes méta
- Utiliser des profils pour encapsuler les vues personnalisées

Une rubrique distincte est fournie pour chacune des méthodes plus avancées.

Définir la période

Lorsque vous menez une procédure d'enquête dans la vue Naviguer, les options de période limitent les résultats renvoyés. Vous pouvez sélectionner :

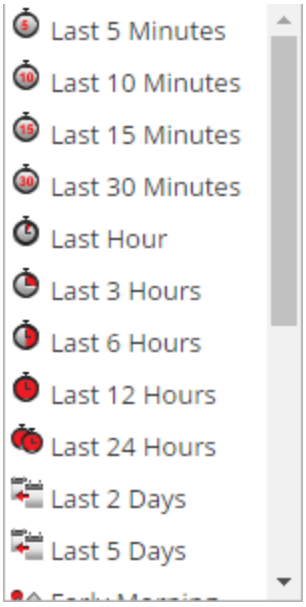
- Une période relative à la collection. Les plages relatives à la collection sont basées sur la dernière heure de collecte pour les données.
- Une période relative au calendrier.
- Une période personnalisée.
- Toutes les données.

La période sélectionnée est affichée dans la barre d'outils de la vue Naviguer en tant que libellé Plage horaire ; par défaut, le libellé est **3 dernières heures**. L'affichage Période dans la bannière de la chronologie affiche les premier et dernier horodatages pour la période utilisée pour les métadonnées.

Remarque : La période est basée sur le fuseau horaire configuré dans le panneau Préférences du profil, comme indiqué dans « Définir les préférences utilisateur » dans le *Guide de NetWitness Platformmise en route de RSA*.

Pour sélectionner une plage horaire intégrée :

1. Cliquez sur l'option **Période** dans la barre d'outils de la vue Naviguer. La période par défaut est **3 dernières heures**, mais une valeur différente de la liste de sélection, par exemple **Toutes les données** ou **Dernière heure**, peut déjà être sélectionnée et utilisée en tant que libellé dans le panneau Options.
   La liste de sélection Période s'affiche.



2. Exécutez l'une des opérations suivantes :
   - Si vous souhaitez afficher toutes les données, sélectionnez **Toutes les données**.
   - Si vous souhaitez définir une période en minutes, heures ou jours relative à la collection, sélectionnez une valeur telle que **10 dernières minutes**, **3 dernières heures** ou **5 derniers jours**.
   - Sélectionnez **Hier**, **Cette semaine**(Version 11.1), **La semaine dernière** (Version 11.1), **Toute la journée** ou une partie de la journée, telle que **Début de matinée**, **Matin**, **Après-midi** ou **Soir**.
   - Si vous souhaitez définir une période unique, sélectionnez **Personnalisé** dans le menu **Période** et suivez la procédure ci-dessous.
     La période sélectionnée est appliquée aux résultats en cours dans le panneau Valeurs.

Pour spécifier une période personnalisée :

1. Sélectionnez **Personnalisé** dans le menu **Période**.
   Les options de sélection de date s'affichent dans la barre d'outils.

2. Dans les champs **Date de début** et **Date de fin**, procédez comme suit pour spécifier la date et l'heure :

a. Cliquez sur une date dans le calendrier.

b. (Facultatif) Sélectionnez l'heure dans les champs Heure et Minute, ou cliquez sur **Maintenant**. La sélection de l'heure est l'heure actuelle par défaut.

Remarque : L'heure de début en secondes a toujours la valeur par défaut :00, alors que l'heure de fin en secondes a toujours la valeur par défaut :59. Par exemple, si vous utilisez une valeur temporelle pour effectuer une recherche verticale d'un problème, l'heure de recherche est interprétée sous la forme suivante : « HH:MM:00 -HH:MM:59 ».

3. Pour appliquer la plage, cliquez sur **OK**.
   La période sélectionnée est appliquée aux résultats en cours dans le panneau Valeurs.

Définir la méthode de quantification et trier la séquence des résultats de clé méta

Cette rubrique fournit une procédure pour sélectionner la façon dont les résultats de chaque clé méta sont quantifiés et séquencés dans la vue Naviguer.

Remarque : Si des entités méta (version 11.1 ou supérieure) sont utilisées dans les groupes méta, les résultats afficheront les 20 valeurs qui correspondent le mieux aux clés méta contenues dans l'entité méta.

Chaque section de clé méta dans la vue Naviguer contient une liste classée des valeurs qui affichent chaque valeur de clé méta (Valeur) et son nombre (Total). Vous pouvez indiquer si :

- Les résultats de chaque section de clé méta sont triés selon la Valeur ou le Total.
- Les résultats sont triés en ordre croissant ou décroissant.
- Les valeurs affichées pour chaque clé méta sont quantifiées par le nombre de paquets (Nombre de paquets), le nombre de sessions ou de logs (Quantifier par nombre d'événements) ou la taille des événements (Quantifier par taille d'événement).

Remarque : Si vous possédez un décodeur de log et un décodeur de paquet pour lequel vous affichez les métadonnées, le calcul des éléments réellement comptés dépend du type de clé. Si vous sélectionnez Quantifier par nombre de paquets et observez les logs, la sortie de la vue Parcourir est identique à celle que vous auriez obtenue en sélectionnant Quantifier par nombre d'événements (voir Vue Naviguer pour plus de détails).

Cette image montre la clé méta `Event Type` présentée selon le **Total** dans l'ordre **Décroissant**. La valeur possédant le plus grand nombre de correspondances est présentée en premier. La valeur `failure audit` possède 71 correspondances et est répertoriée en premier. La valeur `logon` ne possède qu'une correspondance et est présentée en dernier. La méthode de quantification est **Décompte d'événements**.

Cette image montre les clés méta `Event Type` présentées selon la **Valeur** dans l'ordre **Décroissant**. Les noms de valeur sont présentés par ordre alphabétique, en commençant par la fin de l'alphabet. La valeur `success audit` est répertoriée en premier. La valeur `connect` est présentée en dernier. La méthode de quantification est **Décompte d'événements**.

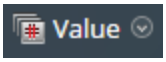
Pour sélectionner la méthode de quantification du nombre de clés méta et l'ordre des résultats de clé méta affichés dans la vue Naviguer :

1. Dans la barre d'outils, sélectionnez **Décompte d'événements**, **Taille des événements** ou **Nombre de paquets** et choisissez l'une des options de quantification dans le menu déroulant. Le libellé du menu affiche l'option sélectionnée.

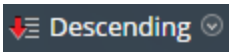
   L'affichage actuel est rechargé selon votre sélection.

2. Dans la barre d'outils, sélectionnez **Total** ou **Valeur** et choisissez l'une des méthodes de classement dans le menu déroulant. Le libellé du menu affiche l'option sélectionnée.

   L'affichage actuel est rechargé selon votre sélection.

3. Dans la barre d'outils, sélectionnez **Croissant** ou **Décroissant** et choisissez l'une des options d'ordre de tri dans le menu déroulant. Le libellé du menu affiche l'option sélectionnée.
   L'affichage actuel est rechargé selon votre sélection.

Gérer et appliquer des clés méta par défaut dans une procédure d'enquête

Lorsque les analystes mènent une procédure d'enquête sur les données capturées, un ensemble de clés méta par défaut est chargé et affiché dans une séquence par défaut dans la vue Naviguer > panneau Valeurs. Le contenu par défaut et la séquence sont basés sur les clés méta pour le service en cours d'étude. Les analystes peuvent spécifier les clés méta à afficher pendant la navigation en sélectionnant les clés méta par défaut ou en sélectionnant un groupe de clés méta définies par l'utilisateur, ce qui offre une grande souplesse pour définir les clés méta. Cela peut aider à approfondir la recherche des données souhaitées et à réduire le temps de chargement en empêchant le chargement des méta qui n'ont pas d'intérêt pour la procédure d'enquête en cours.

Remarque : Dans la version 11.1 ou supérieure, chaque fois que les clés méta sont utilisées, vous pouvez également utiliser des entités méta configurées.

Si aucun groupe de méta personnalisé n'est effectif, la vue Naviguer est affichée avec la visibilité des clés méta spécifiées dans la boîte de dialogue Clés méta par défaut. Pour optimiser le chargement des clés méta dans la vue Naviguer > panneau Valeurs, NetWitness Platform n'ouvre pas les clés méta non indexées par défaut. Lorsque vous ouvrez une clé méta non indexée dans la vue Valeurs, NetWitness Platform commence à charger les valeurs de cette clé méta. Si le temps de chargement est excessif, un message d'expiration met fin au chargement de la clé méta. Les titres, les valeurs et les nombres des clés méta non indexées ne sont pas accessibles dans le panneau Valeurs. Un étiquetage supplémentaire dans la procédure d'enquête identifie les clés méta non indexées.

Pour sélectionner les clés méta à appliquer à votre procédure d'enquête, vous pouvez :

- Sélectionner les clés méta par défaut.
- Sélectionner un ensemble de clés méta, appelé métagroupe.

Remarque : L'enquête comporte des méta-groupes intégrés et des méta-groupes définis par l'utilisateur. Une fois créés, les métagroupes définis par l'utilisateur peuvent être modifiés, supprimés, importés pour être utilisés sur d'autres services, et importés dans le service concerné par la procédure d'enquête. Toutes ces procédures sont fournies dans une rubrique distincte : Gérer les groupes méta.

La boîte de dialogue Clés méta par défaut vous permet de spécifier la vue par défaut et la séquence d'affichage des clés méta pendant la navigation dans Enquêter > vue Naviguer pour un service spécifique. Pour chaque clé ou pour toutes les clés, vous pouvez définir la vue par défaut :

- Masqué : Les résultats d'une clé méta par défaut sont masqués et ne peuvent pas être chargés.
- Ouvert : Les résultats d'une clé méta par défaut sont ouverts avec toutes les valeurs et les nombres affichés.
- Fermé : Les résultats d'une clé méta par défaut sont fermés avec uniquement le nom du méta visible.
- Auto : Le chargement des clés méta par défaut doit être indexé par la valeur, autrement dit, il est contrôlé par le niveau d'index.

Lorsque vous utilisez les clés méta par défaut, sachez qu'elles peuvent être modifiées pour les différents services, et qu'il se peut que vous ne visualisiez pas le même ensemble de clés méta par défaut lors de la navigation à un point de recherche verticale sur les différents services. Si vous ne voyez pas les données souhaitées, vous devrez peut-être modifier l'affichage initial des clés méta par défaut.

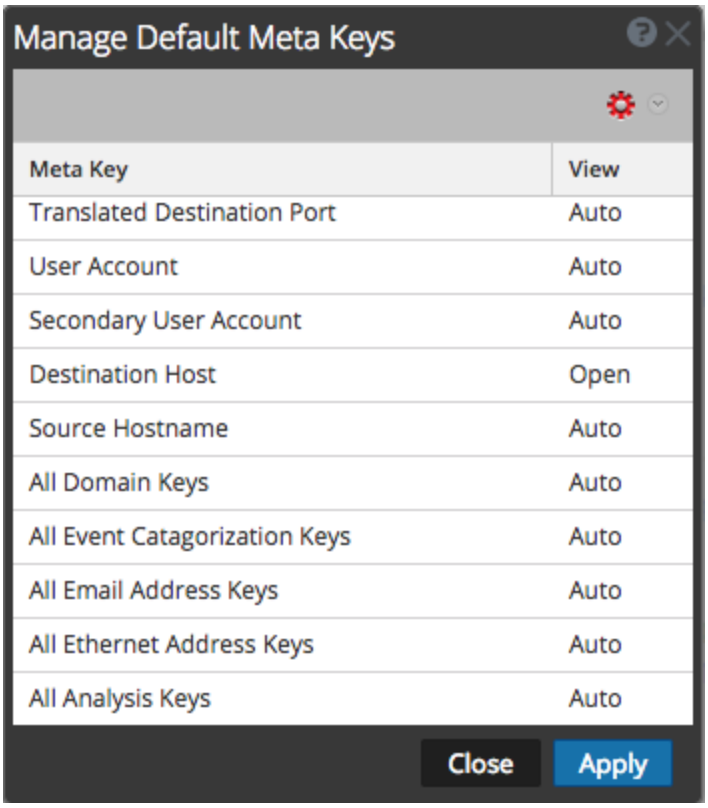
Lorsque vous modifiez l'état initial des clés méta par défaut à partir de la vue Naviguer, la modification reste appliquée à ce service. Lorsque de nouvelles clés sont ajoutées au fichier d'index personnalisé pour un service Core (par exemple, `concentrator-custom-index.xml` ou `decoder-custom-index.xml`), les nouvelles clés sont ajoutées à la liste des clés méta par défaut. Les modifications apportées à la vue Naviguer s'appliquent uniquement au service actif.

Pour spécifier que la vue Naviguer initiale s'ouvre à l'aide des clés méta par défaut :

1. Accédez à **ENQUÊTER** > Naviguer**.**
2. Sélectionnez un service puis **Naviguer**.
3. Dans le menu **Méta**, sélectionnez **Utiliser les clés méta par défaut**.
   Si une procédure d'enquête est déjà en cours, les données seront rechargées dans la vue active et une icône mettra en évidence l'option sélectionnée. Si aucune donnée n'est encore chargée, les clés méta par défaut seront utilisées pour le chargement suivant.

Pour configurer la vue par défaut des clés méta dans la vue Naviguer :

1. Dans la barre d'outils de la vue **Naviguer**, sélectionnez **Méta** > **Gérer les clés méta par défaut**.
   La boîte de dialogue Gérer les clés méta par défaut s'affiche avec la liste des clés méta disponibles pour le service.



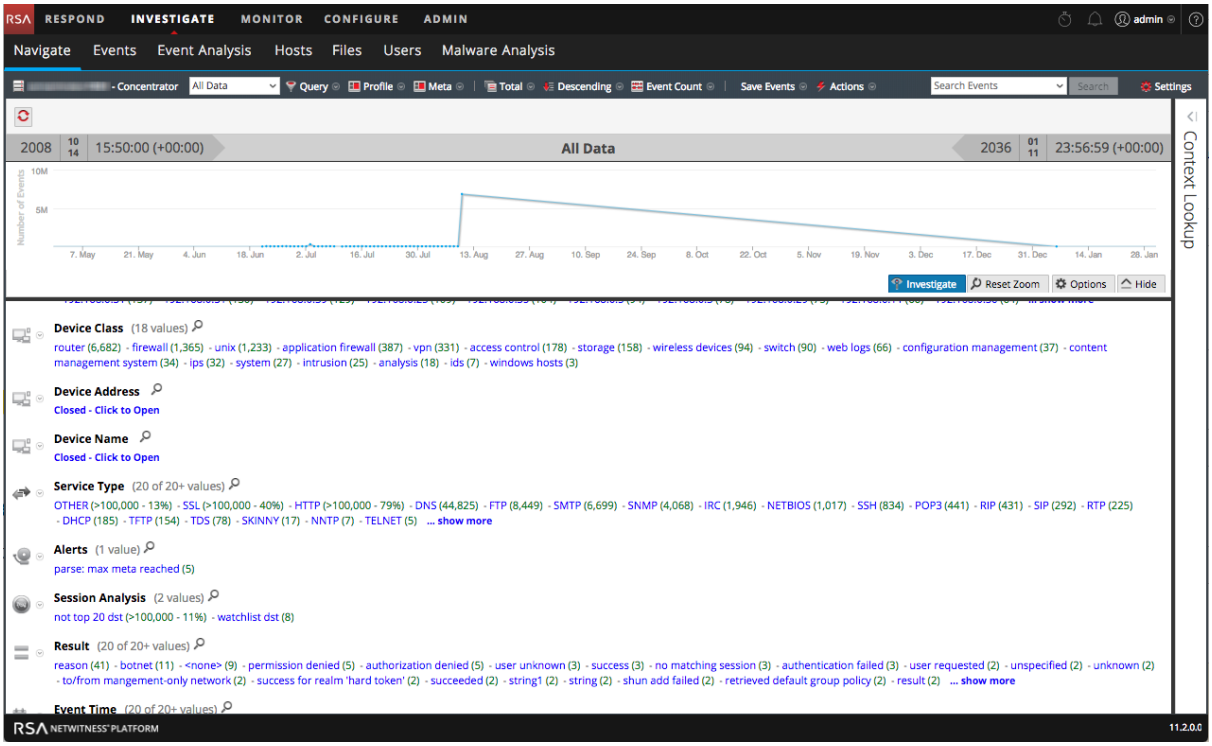
2. (Facultatif) Pour modifier l'ordre des clés, sélectionnez une ou plusieurs clés, puis faites glisser les valeurs de la liste des clés vers le haut ou vers le bas.
3. Exécutez l'une des opérations suivantes :
   - (Facultatif) Pour modifier l'affichage par défaut pour toutes les clés méta, assurez-vous qu'aucune clé n'est sélectionnée, puis dans la barre d'outils, sélectionnez .
   - (Facultatif) Pour modifier l'affichage par défaut pour une ou plusieurs clés, sélectionnez les clés et dans la barre d'outils, sélectionnez .
     Un menu déroulant des vues initiales possibles pour toutes les clés méta par défaut s'affiche.
   - (Facultatif) Pour restaurer la vue par défaut des clés méta comme spécifié dans le fichier d'index du service, vérifiez qu'aucune clé n'est sélectionnée, puis dans la barre d'outils sélectionnez > **Auto**.
     Lorsque vous modifiez la vue par défaut pour une clé méta non indexée, vous ne pouvez pas définir la clé sur OUVERT. Si vous modifiez la vue par défaut d'un groupe de clés méta sur OUVERT et si certaines des clés méta ne sont pas indexées, ces dernières reprennent la valeur AUTO. La clé méta est donc automatiquement chargée uniquement si elle est indexée, et les clés méta non indexées adoptent l'état FERMÉ jusqu'à ce qu'elles soient ouvertes manuellement.
4. Sélectionnez l'une des vues.
5. Pour enregistrer les modifications, cliquez sur **Appliquer**.
   Les clés méta affichées dans la vue Naviguer sont définies en fonction de vos spécifications. Si les clés méta par défaut sont masquées, leurs valeurs n'apparaîtront pas du tout dans la procédure

d'enquête. Si les clés méta par défaut sont fermées, leurs valeurs ne seront pas chargées par défaut, mais vous pourrez les charger individuellement et manuellement dans la vue Naviguer.

Effectuer une recherche verticale dans les données au sein du graphique chronologique de la vue Naviguer

La visualisation Graphique chronologique permet aux analystes de visualiser l'activité dans le temps. Vous pouvez explorer les données en sélectionnant une période et l'option Examiner. Vous pouvez ensuite réinitialiser la navigation à la période effective avant l'analyse.

1. Accédez à **ENQUÊTER > Naviguer**.
   Le graphique chronologique pour le point d'extraction actuel et la période sélectionnée s'affiche.



2. Pour mettre en surbrillance une période sur le graphique chronologique, cliquez sur la période souhaitée et faites glisser la souris.
   Le graphique chronologique est redessiné pour la période sélectionnée, mais les valeurs méta restent inchangées.
3. Pour effectuer une recherche verticale dans les données pour la plage sélectionnée, cliquez sur **Examiner**.
   L'URL est mise à jour pour refléter le changement de période et le panneau des options de procédure d'enquête est mis à jour pour refléter la période personnalisée. Le graphique chronologique est redessiné et les métavaleurs sont chargées pour la période sélectionnée.
4. Pour réinitialiser le graphique chronologique à la période d'origine, cliquez sur **Réinitialiser le zoom**.
   L'URL est mise à jour pour refléter l'URL d'origine avant l'analyse des données et le panneau des options de procédure d'enquête est mis à jour pour refléter la période sélectionnée avant l'analyse. Le

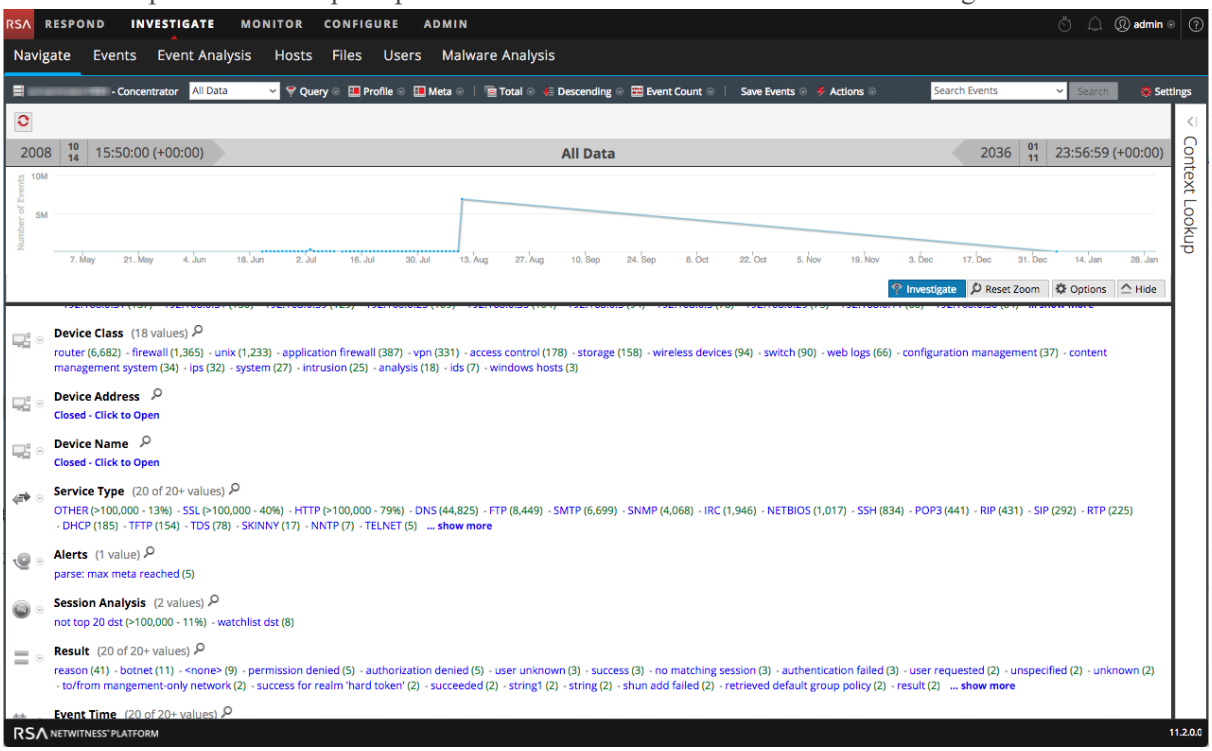
graphique chronologique est redessiné pour la période sélectionnée et les métavaleurs sont chargées pour cette période.

Effectuer une recherche verticale dans les données dans le panneau Valeurs

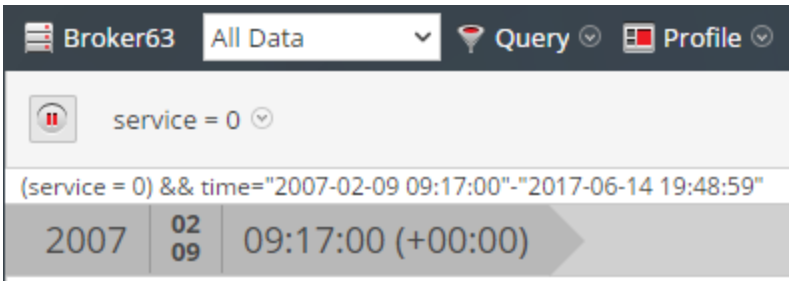
NetWitness Platform affiche l'activité et les valeurs du service sélectionné dans la vue Procédure d'enquête > Naviguer. Pour rechercher des données, les analystes effectuent une recherche verticale dans les données en cliquant sur une clé méta ou une valeur méta, qui est traitée comme une requête. Dans le panneau Valeurs, chaque requête est ajoutée aux données du fil d'Ariane. Cela entraîne l'affichage d'un fil d'Ariane en haut avec un fil pour chaque requête. Vous pouvez modifier le fil d'Ariane pour insérer ou supprimer une requête.

Effectuer une recherche verticale dans un sous-ensemble de métadonnées :

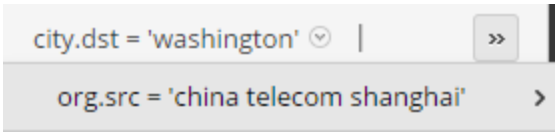
1. Lancez une procédure d'enquête pour afficher les métadonnées dans la vue Naviguer.



2. Pour effectuer une recherche verticale dans les métadonnées, effectuez une ou plusieurs des opérations suivantes :
   a. Cliquez sur une **clé méta**, par exemple, **Type de service**.
   b. Cliquez sur une **valeur méta**, le texte en bleu dans les résultats. Par exemple, **AUTRE**.
   Chaque fois que vous cliquez sur une clé méta ou une valeur méta, la requête de procédure d'enquête pivote vers un point focal ou un point de recherche verticale rétréci, au sein des données. À chaque point de recherche verticale, le panneau Valeurs est mis à jour et le nouveau point de recherche verticale s'affiche dans le fil d'Ariane. Voici un exemple du premier fil.



Ceci est l'exemple d'un long fil d'Ariane qui ne rentre pas dans la barre d'outils. La dernière requête qui s'insère est suivie d'un menu déroulant qui répertorie les requêtes supplémentaires. Pour sélectionner un point de recherche verticale dans le dépassement de capacité, cliquez sur l'icône correspondante et sur une requête dans la liste déroulante.

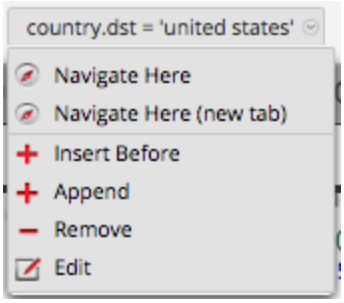


Pour ajouter une requête au fil d'Ariane :

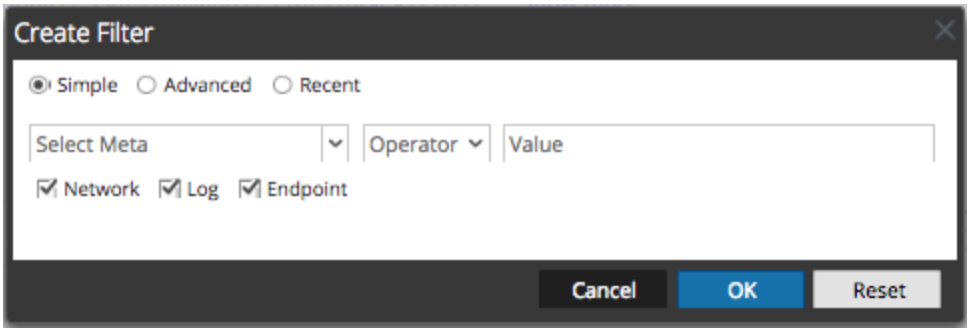
Dans le fil d'Ariane, vous pouvez cliquer sur l'un des fils pour afficher le menu Requête. Vous pouvez insérer une nouvelle requête avant un fil et en ajouter une nouvelle à la fin d'un fil. Après chaque modification dans le fil, NetWitness Platform actualise les résultats.

Pour ajouter une requête au fil d'Ariane :

1. Cliquez sur un fil.
   Le menu Fil d'Ariane s'affiche.



2. Pour ajouter une requête au fil d'Ariane, sélectionnez **Ajouter** ou **Insérer avant**.
   La boîte de dialogue Créer un filtre s'affiche.



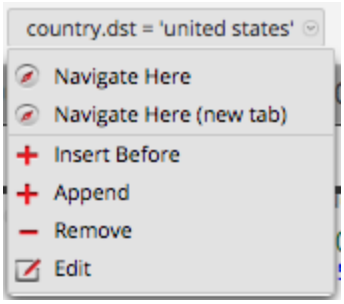
3. Créez la requête comme décrit dans la rubrique Créer une requête personnalisée.

Pour modifier une requête dans le fil d'Ariane :

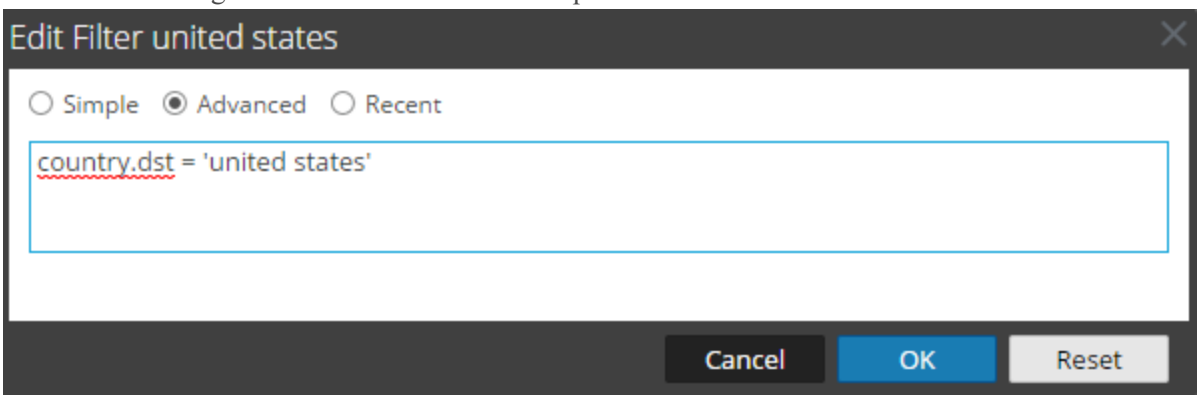
Dans le fil d'Ariane, vous pouvez cliquer sur l'un des fils pour afficher le menu Requête. Vous pouvez supprimer un fil et modifier une requête dans un fil. Après chaque modification dans le fil, NetWitness Platform actualise les résultats.

Pour utiliser les requêtes dans le fil d'Ariane :

1. Cliquez sur un fil.
   Le menu Fil d'Ariane s'affiche.



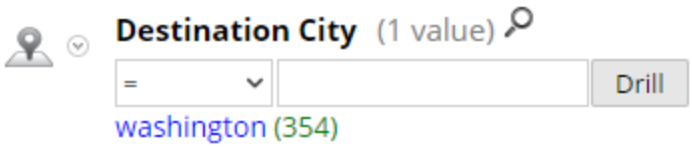
2. Pour modifier une requête dans le fil d'Ariane, sélectionnez **Modifier**.
   La boîte de dialogue Créer s'affiche avec la requête sélectionnée ouverte à des fins de modification.



3. Modifiez les champs comme décrit dans la rubrique Créer une requête personnalisée.

Pour effectuer une recherche rapide dans une clé méta :

1. Déplacez la souris sur une section de clé méta, puis cliquez sur la loupe.
   Le formulaire Recherche rapide, qui contient un comparateur et un opérande facultatif pour la recherche, s'affiche.



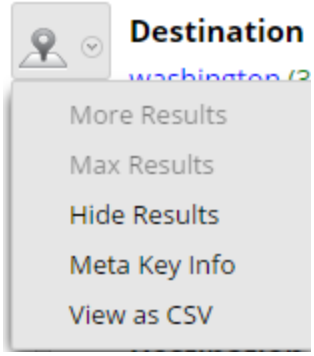
2. (Facultatif) Si vous souhaitez fermer le formulaire de recherche, cliquez de nouveau sur la loupe.
3. Sélectionnez l'opération dans la liste déroulante située à gauche, puis saisissez la valeur du texte à rechercher. Ensuite, cliquez sur **Recherche verticale** pour effectuer l'opération.

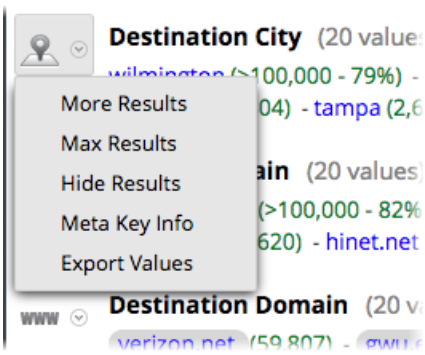
Les métadonnées de cette clé méta servent à effectuer une recherche verticale dans les métadonnées actuelles.

Pour afficher des informations sur la clé méta :

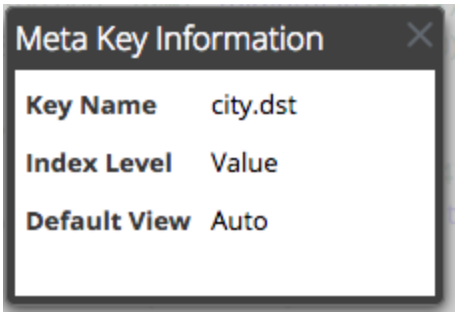
Pour consulter les détails relatifs à une clé méta, en particulier le nom de la clé, le niveau d'index défini pour afficher la clé méta, ainsi que la vue par défaut définie pour la clé méta :

1. Cliquez sur le menu déroulant en regard de la clé méta. Ces deux chiffres affichent le menu déroulant pour la version 11.0.0.x et 11.1 ou supérieure.



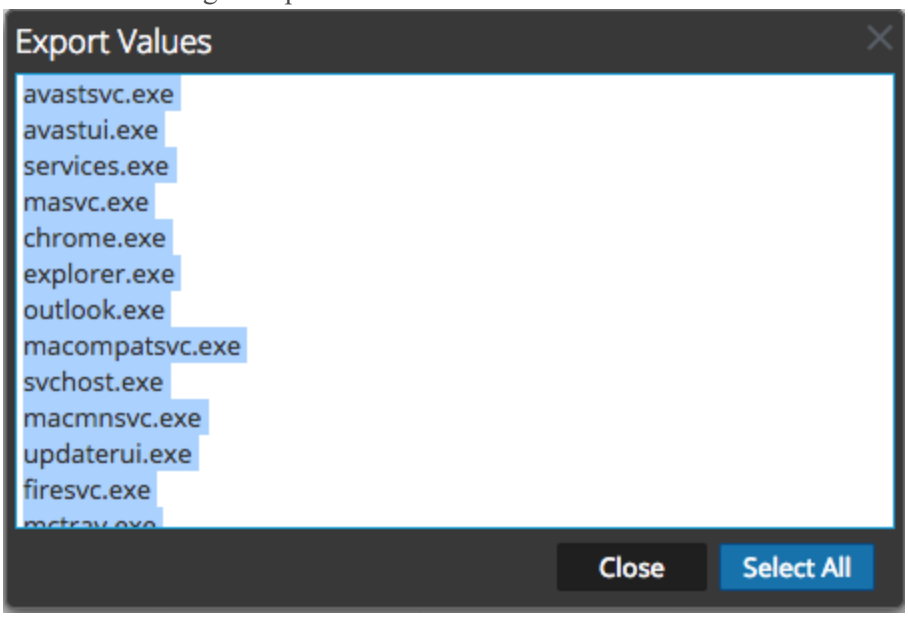
et


2. Sélectionnez **Info sur la clé méta**.
   La boîte de dialogue Info sur la clé méta s'affiche.



3. Lorsque vous avez terminé de la consulter, cliquez sur ■.
4. (Facultatif pour la version 11.0) Pour afficher les noms des méta trouvés pour la clé méta sous la forme d'une liste de valeurs séparées par des virgules, cliquez sur le menu déroulant en regard de la clé méta et sélectionnez **Afficher comme CSV**.
   La boîte de dialogue Affichage des valeurs au format CSV s'affiche. Lorsque vous avez terminé de la consulter, cliquez sur **Fermer**.
5. (Facultatif pour la version 11.1) Pour afficher les noms des méta trouvés pour la clé méta sous la forme d'une liste, cliquez sur le menu déroulant en regard de la clé méta et sélectionnez **Exporter des valeurs**.

La boîte de dialogue Exporter des valeurs s'affiche.



6. (Facultatif) Si vous souhaitez masquer les résultats de la clé méta au niveau du point de recherche verticale actif, cliquez sur le menu déroulant en regard de la clé méta, puis cliquez sur **Masquer les résultats**.

Pour afficher des événements associés à une valeur méta :

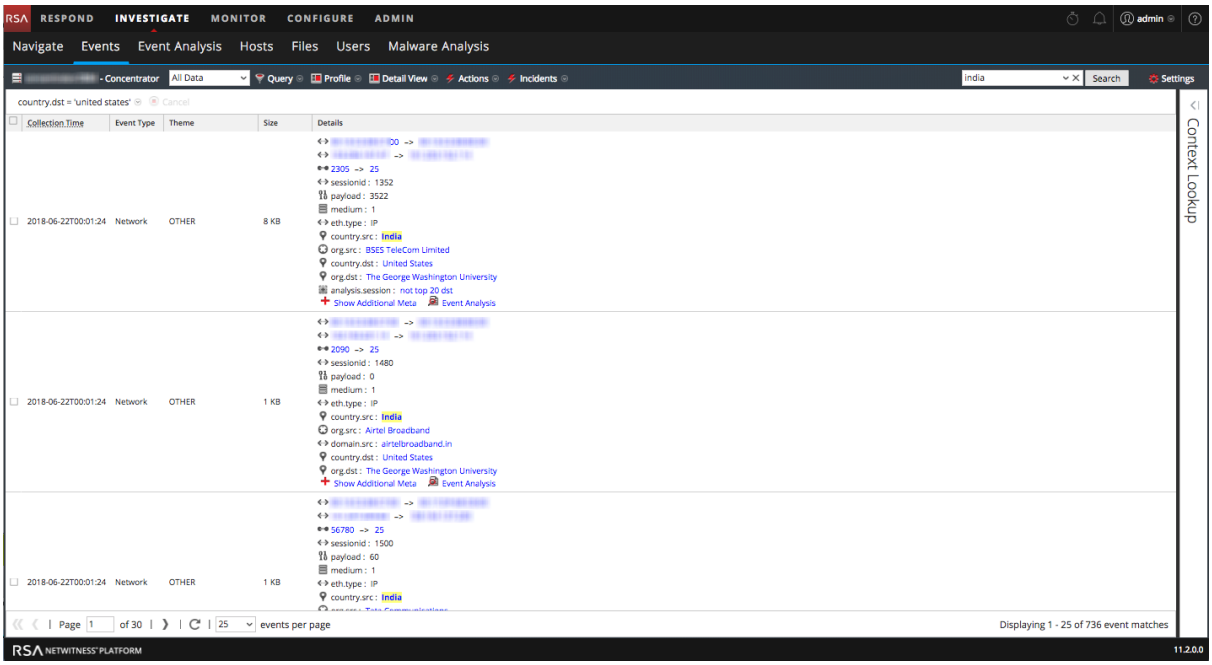
La vue Événements fournit des détails supplémentaires sur un événement en deux points de vue différents : Liste des événements et vue Détails.

1. Dans la vue Naviguer, effectuez une recherche verticale dans les métadonnées sur lesquelles votre procédure d'enquête est axée.
2. Cliquez sur le nombre (en vert) en regard de la valeur méta bleue.
   La vue Événements correspondant au point de recherche verticale actif s'affiche.
   Les opérations que vous pouvez effectuer dans la vue Événements sont décrites dans Examiner les événements bruts dans la vue Événements.

Pour rechercher des événements spécifiques associés à une valeur méta :

1. Dans la vue Naviguer, effectuez une recherche verticale dans les métadonnées qui font l'objet de votre investigation (cliquez sur une valeur méta ou ajoutez une requête).
2. Saisissez une chaîne de recherche dans le champ Rechercher et appuyez sur **Entrée** ou cliquez sur **Rechercher**.
   Vous pouvez également sélectionner et définir des préférences pour le mode de recherche. Consultez Rechercher des modèles de texte pour obtenir des informations détaillées sur la recherche.
   La vue Événements s'ouvre dans un nouvel onglet et affiche les résultats de la recherche. Si vous ne voyez pas le terme de recherche mis en surbrillance, cliquez sur **Afficher les méta supplémentaires**. Votre sélection de période et vos recherches verticales (requêtes) sont reportées

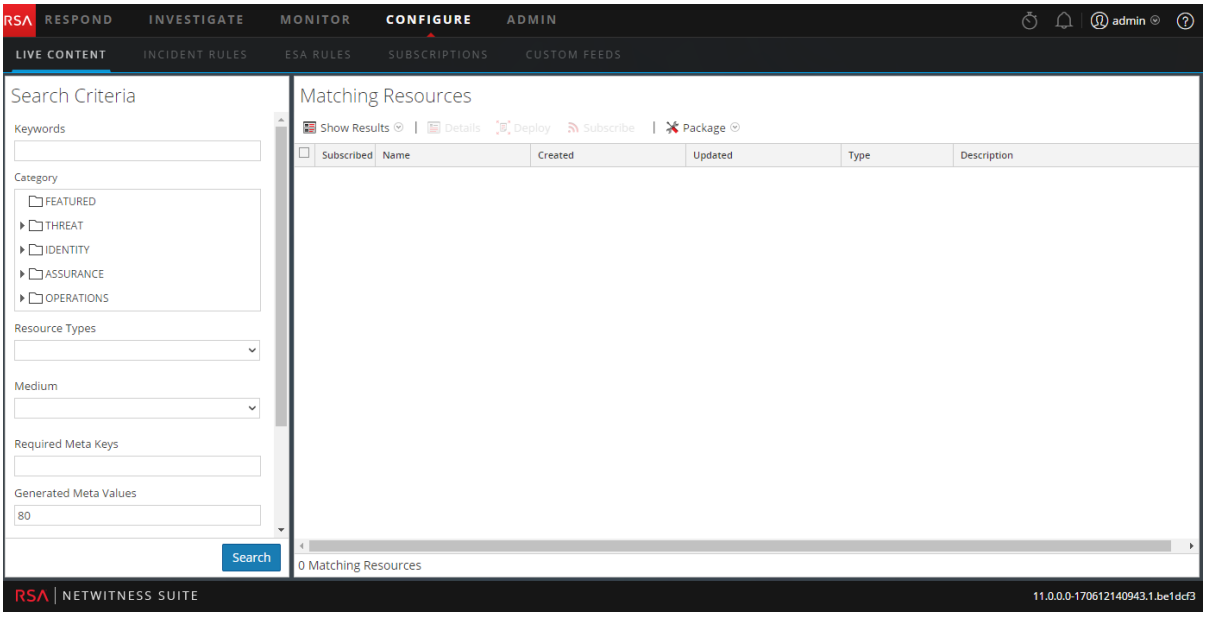
dans la vue Événements.



Pour afficher une valeur méta sélectionnée dans RSA Live :

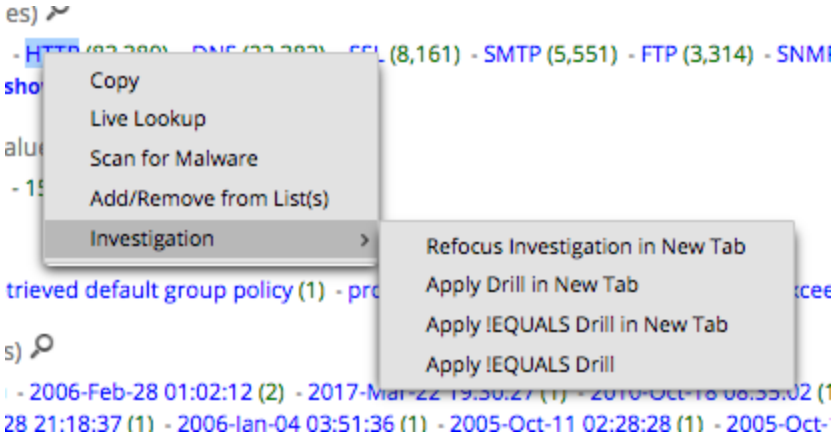
1. Dans la vue Naviguer, effectuez une recherche verticale dans les métadonnées sur lesquelles votre procédure d'enquête est axée.
2. Cliquez avec le bouton droit de la souris sur une valeur méta (le texte en bleu).
   Le menu déroulant Valeur méta s'affiche.

3. Pour rechercher la métavaleur dans RSA Live, sélectionnez **Recherche dans Live**.
   La vue Live Search s'affiche avec la valeur méta saisie dans le champ Valeurs méta générées ; elle est prête pour une recherche.



Pour recentrer la procédure d'enquête sur un point de recherche verticale :

1. Cliquez avec le bouton droit de la souris sur une valeur méta (le texte en bleu).
   Le menu déroulant Valeur méta s'affiche.

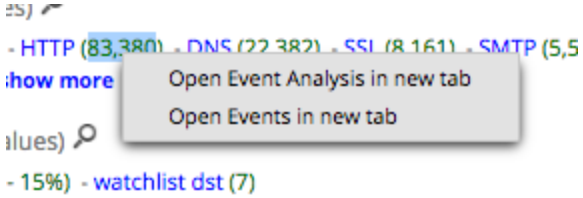


2. Choisissez l'une des options de recentrage.
   La recherche verticale est recentrée en fonction de votre choix.

Pour rechercher un nombre spécifique dans un nouvel onglet :

Pour afficher un nombre pour une valeur Meta dans la vue Événements ou la vue Analyse d'événements, cliquez avec le bouton droit sur un nombre pour une valeur Meta (le numéro vert suivant la valeur Meta bleue).

Le menu contextuel s'affiche.



Gérer les groupes méta

Un groupe méta associe les clés méta sélectionnées en un groupe pour afficher uniquement les données dans lesquelles les clés méta et entités méta ont été trouvées.

Remarque : Dans la version 11.1 ou supérieure, vous pouvez également utiliser des entités méta configurées en groupes méta.

Dans la vue Enquêter > Naviguer, vous pouvez définir des groupes méta afin de filtrer les données affichées dans une procédure d'enquête. Une nouvelle installation de NetWitness Platform inclut les groupes méta prêts à l'emploi pour vous aider à trouver des jeux de données intéressants dans Investigate. Les groupes méta prêts à l'emploi sont précédés de RSA pour leur identification. Ils peuvent être dupliqués, mais pas modifiés ou supprimés. Vous pouvez créer vos propres groupes et dupliquer et modifier un groupe prêt à l'emploi pour créer un groupe personnalisé.

Avec un groupe méta en vigueur au cours d'une procédure d'enquête, les informations contenues dans le panneau Valeurs affichent uniquement les clés méta du groupe sélectionné. Lorsque vous ouvrez une visualisation de coordonnées parallèles, les clés méta et entités méta d'un groupe apparaissent sous la forme d'axes de gauche à droite. Il peut s'avérer utile de créer deux versions de chaque groupe méta personnalisé ; une version pour l'analyse des valeurs méta et une autre pour la création d'un graphique de coordonnées parallèles en s'attachant à un sous-ensemble de plus petite taille pour le même cas d'utilisation.

Les métagroupes personnalisés sont visibles par tous les utilisateurs d'un service et peuvent être exportés à des fins d'importation vers n'importe quel service, avec une limitation par les clés méta disponibles pour ce service.

Remarque : Lorsqu'un administrateur ajoute des métagroupes personnalisés manuellement en modifiant le fichier d'index personnalisé d'un service, les nouveaux groupes deviennent disponibles pour la procédure d'enquête après le redémarrage du service.

Cette section décrit comment ajouter, modifier, importer, exporter et supprimer des métagroupes personnalisés à utiliser lors de la navigation sur un service spécifique.

Groupes méta prêts à l'emploi

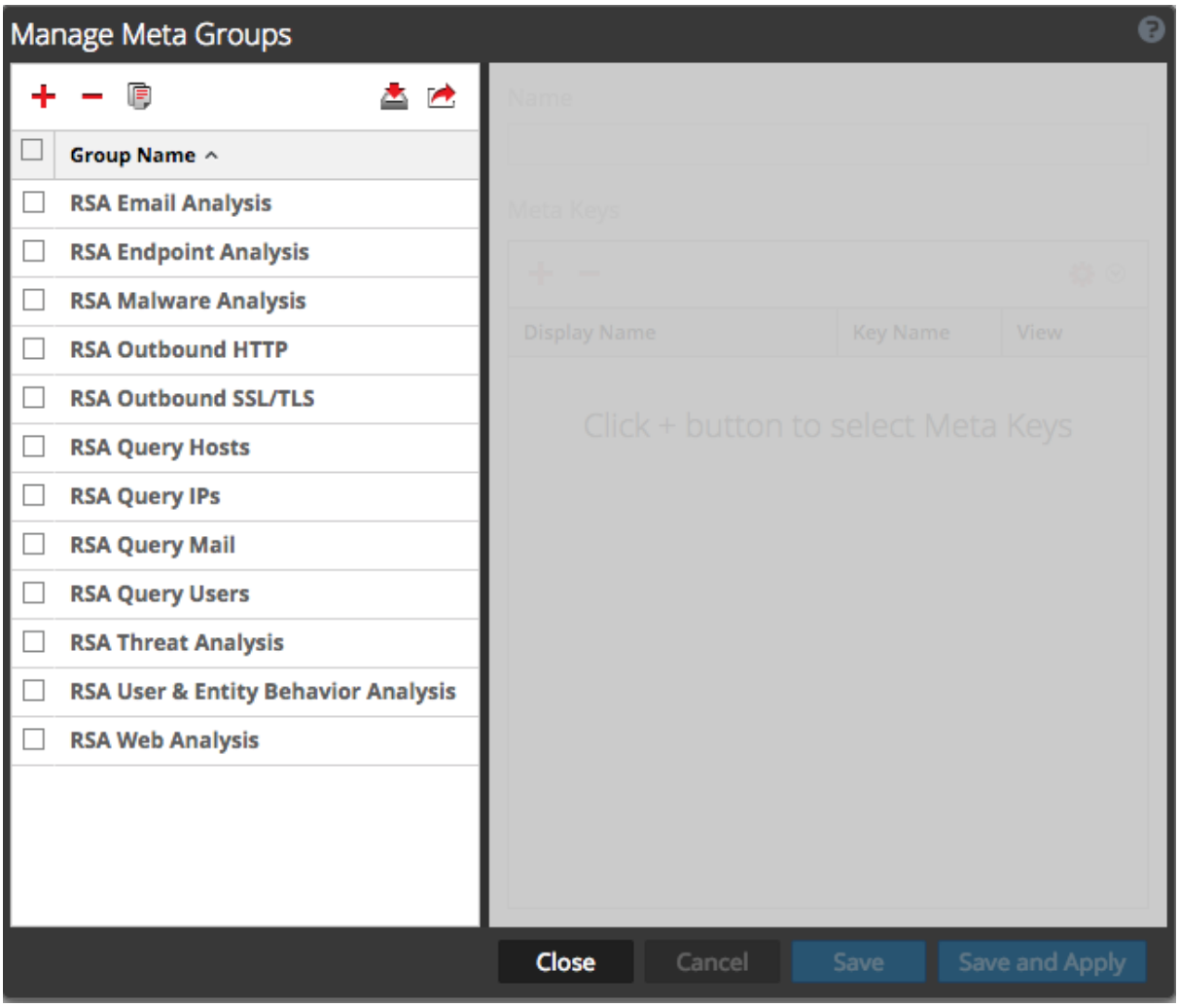
Les méta-groupes prêts à l'emploi sont intégrés à RSA NetWitness Platform. Les groupes méta prêts à l'emploi par défaut sont utiles pour concentrer une procédure d'enquête sur les exemples d'utilisation courants et pour prendre en charge la détection des menaces à l'aide de RSA Hunting Pack. Voici les groupes méta prêts à l'emploi :

- RSA Email Analysis comprend des clés méta qui présentent des interactions d'e-mail.
- RSA Endpoint Analysis contient des clés méta qui fournissent des informations sur les processus, les fichiers, les utilisateurs et les connexions à partir des hôtes NetWitness Endpoint (NWE).
- RSA Malware Analysis comprend des clés méta qui marquent les indicateurs de compromission dans les fichiers contenus dans les événements.
- RSA Outbound HTTP comprend des clés méta qui améliorent la visibilité du trafic web sortant.
- RSA Outbound SSL/TLS comprend des clés méta qui se concentrent sur le trafic web chiffré.

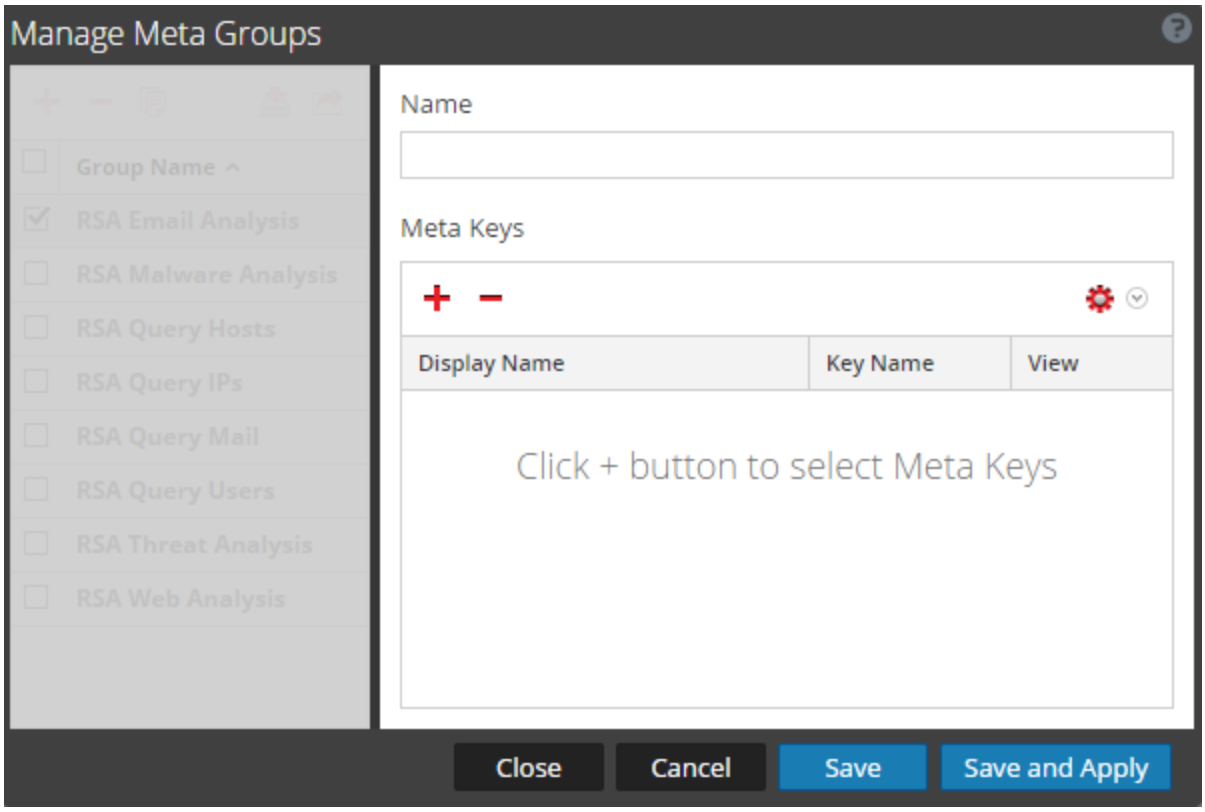
- RSA Query Hosts comprend des clés méta qui incluent toutes les clés méta pour rechercher des hôtes.
- RSA Query IPs comprend des clés méta qui incluent toutes les clés méta pour rechercher des adresses IP.
- RSA Query Mail comprend des clés méta qui incluent toutes les clés méta pour rechercher des e-mails.
- RSA Query Users comprend des clés méta qui incluent toutes les clés méta pour rechercher des utilisateurs.
- RSA Threat Analysis comprend des clés méta qui marquent les menaces potentielles du jeu de données.
- L'analyse des comportements des utilisateurs et des entités RSA inclut des clés méta qui englobent toutes les méta clés pour analyser le comportement des utilisateurs et des entités.
- RSA Web Analysis comprend des clés méta qui marquent des anomalies dans le trafic web.

Créer un groupe méta et ajouter des clés méta

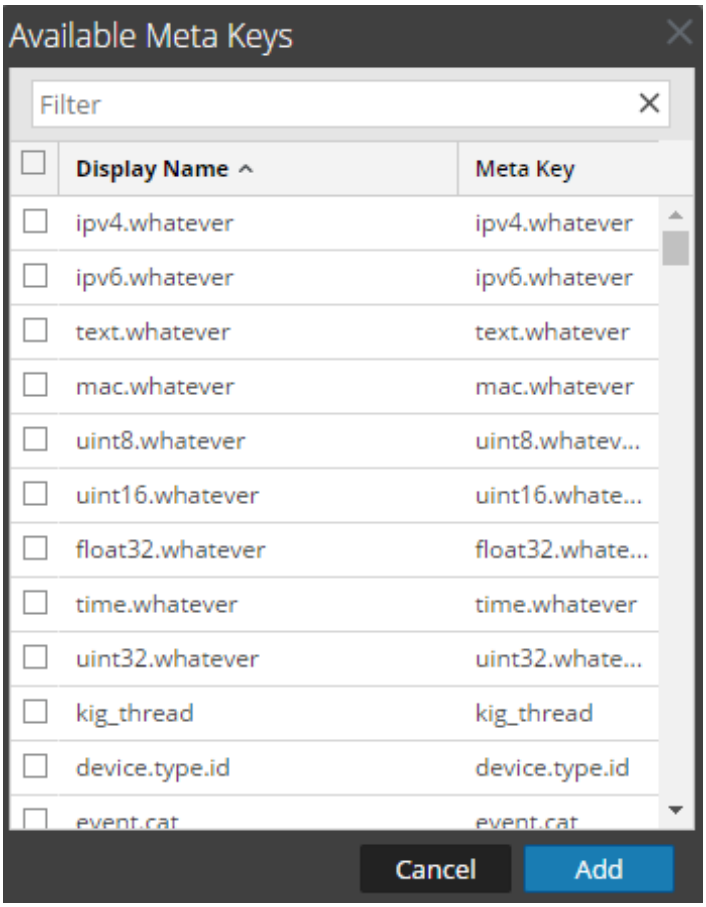
1. Lors de la procédure d'enquête menée sur un service, dans la vue **Enquêter > Naviguer**, sélectionnez **Méta > Gérer les groupes méta** dans la barre d'outils.
   La boîte de dialogue Gérer les groupes méta s'affiche. Initialement, seuls les groupes prêts à l'emploi sont configurés pour un service et répertoriés sous Nom du groupe. Si d'autres groupes personnalisés ont été configurés, ils apparaissent également sous le nom du groupe.



2. Dans la barre d'outils située en haut de liste des groupes méta, cliquez sur +.
   Une nouvelle ligne est insérée en haut de la liste Groupes méta.
3. Saisissez un nom pour le nouveau groupe méta, puis appuyez sur la touche **Entrée**.
   Le formulaire à droite s'ouvre pour édition.



4. (Facultatif) Si vous souhaitez modifier le nom du groupe méta, saisissez une nouvelle valeur dans le champ **Nom**.
5. Dans la barre d'outils **Clés méta**, cliquez sur +.
   La boîte de dialogue Clés méta disponibles s'affiche avec les clés classées par ordre alphabétique.



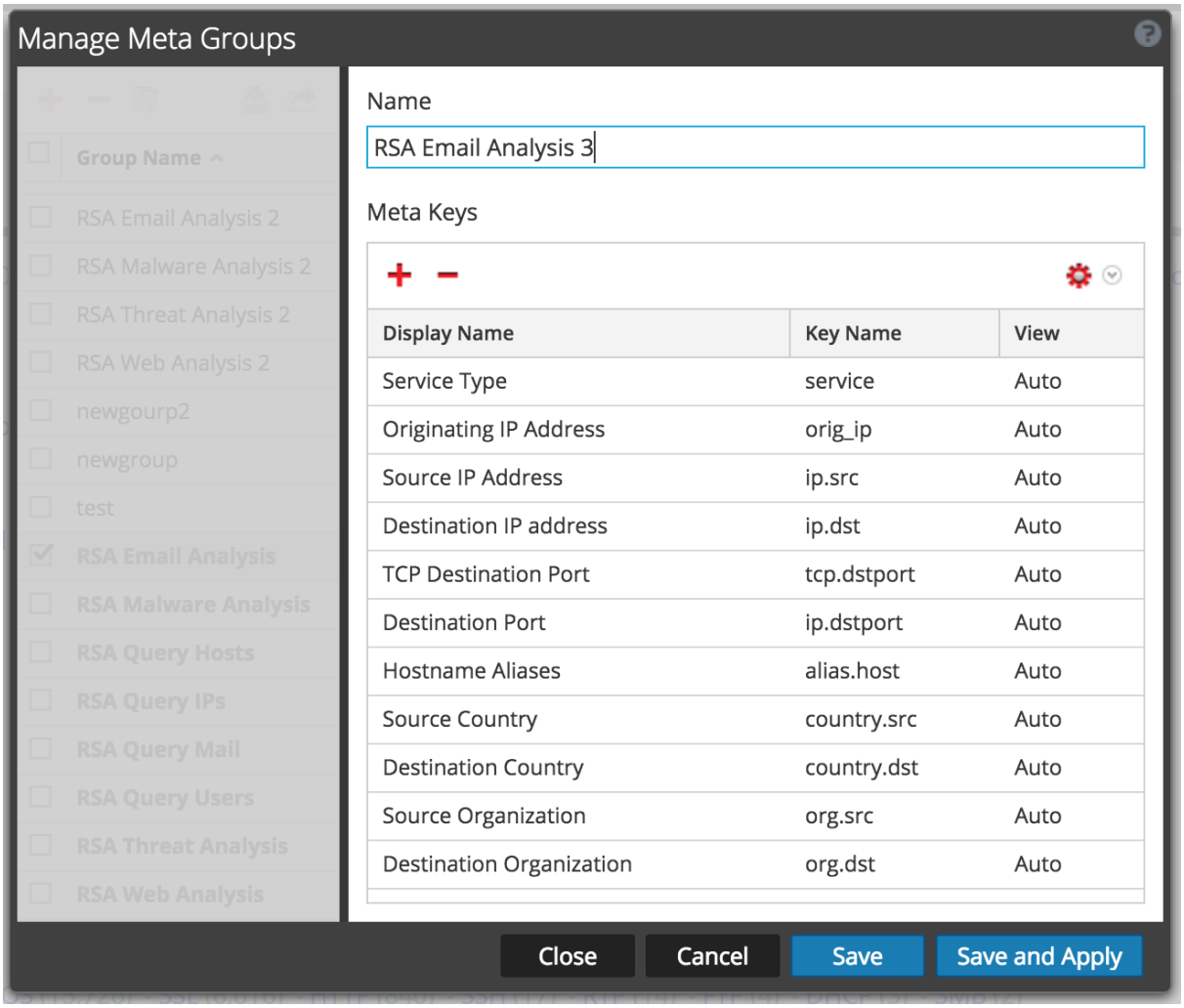
6. Pour filtrer la liste des clés méta, saisissez un mot ou une phrase dans le champ **Filtrer**, puis appuyez sur **Entrée**.
   La liste affiche les correspondances de clés méta trouvées par la recherche insensible à la casse. Supprimez le texte du filtre et appuyez sur **Entrée** pour retirer le filtre.
7. Pour sélectionner les clés métas à ajouter au métagroupe, activez les cases à cocher correspondantes. Pour sélectionner toutes les clés méta, activez la case à cocher dans la barre de titre, puis cliquez sur **Ajouter**.
   Les clés méta sont ajoutées à la liste des clés méta.
8. (Facultatif) Si vous souhaitez changer l'ordre dans lequel les clés méta sont chargées et répertoriées dans la procédure d'enquête, cliquez sur une ou plusieurs clés méta et faites-les glisser vers une nouvelle position.
9. Pour terminer la création du métagroupe, procédez de l'une des manières suivantes :
   a. Pour enregistrer le groupe méta, cliquez sur **Enregistrer**.
      Le groupe est créé et disponible à l'utilisation.
   b. Pour enregistrer et appliquer le groupe méta dans la vue Procédure d'enquête active, cliquez sur **Enregistrer et appliquer**.
      Le groupe est créé et appliqué immédiatement à la vue Procédure d'enquête active.
10. Cliquez sur **Fermer.**

Dupliquer et modifier un groupe méta prêt à l'emploi

Si vous souhaitez personnaliser un groupe méta prêt à l'emploi, vous devez dupliquer le groupe, puis modifier la duplication.

1. Sélectionnez un groupe méta prêt à l'emploi dans la liste Gérer les groupes méta, puis cliquez sur .

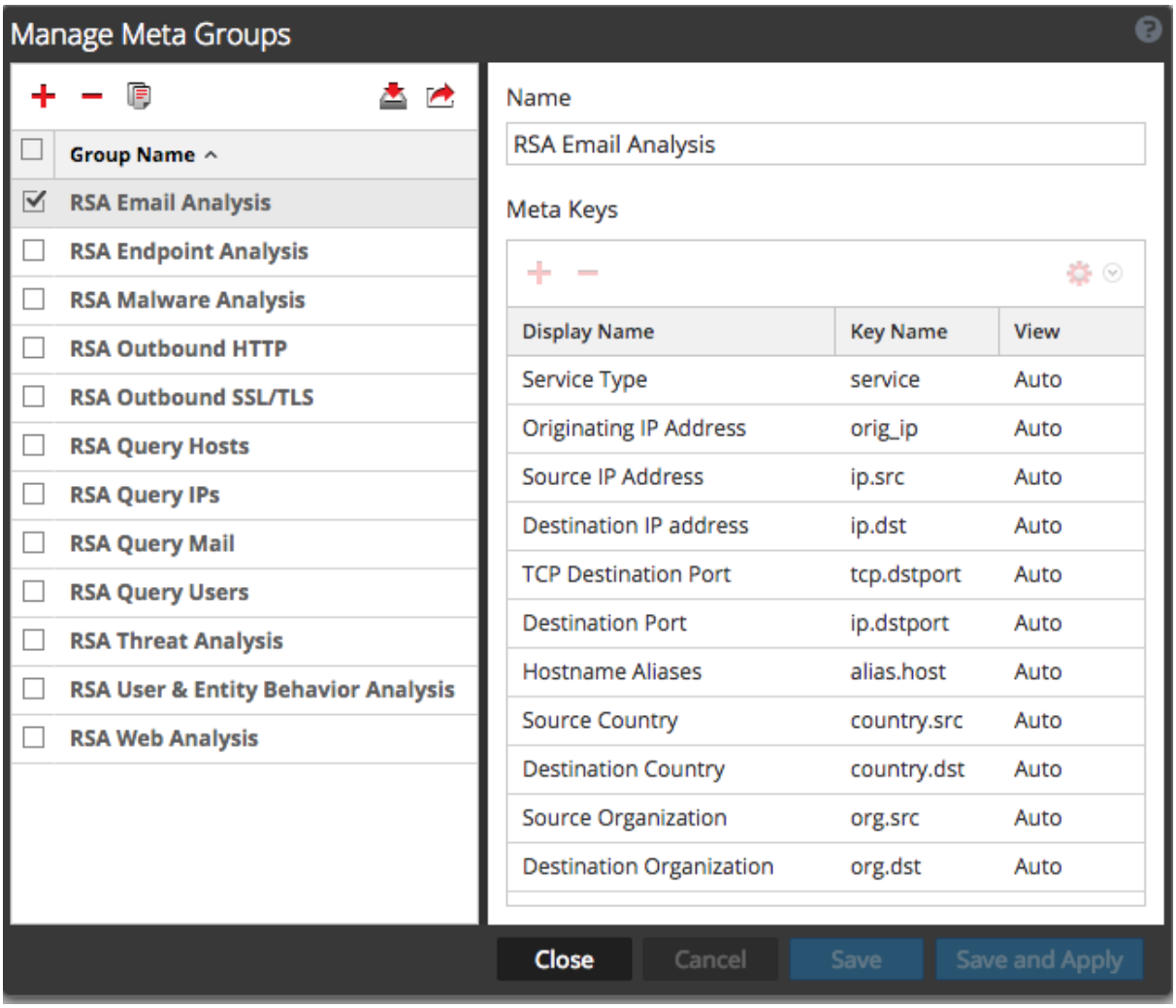
   Le formulaire à droite s'ouvre pour modification avec toutes les clés méta telles qu'elles sont dans le groupe prêt à l'emploi.



2. Entrez un nom pour le nouveau groupe et continuez la modification comme décrit dans « Modifier un groupe méta » ci-dessous.

Modifier un métagroupe

1. Sélectionnez un groupe dans la liste **Groupes méta**.
   Le formulaire à droite s'ouvre pour édition.



2. (Facultatif) Modifiez le nom du groupe.
3. Facultatif) Ajoutez de nouvelles clés méta, comme décrit ci-dessus dans la rubrique Créer un groupe méta et ajouter des clés méta.
4. (Facultatif) Pour définir l'ordre des clés, faites glisser-déplacer une ou plusieurs clés.
5. (Facultatif) Pour modifier la vue initiale d'une clé méta, cliquez sur et choisissez l'une des vues possibles.
   Lorsque vous modifiez le métagroupe, vous ne pouvez pas définir la clé sur OUVERT. Si vous modifiez la vue par défaut d'un groupe de clés méta sur OUVERT et si certaines des clés méta ne sont pas indexées, ces dernières reprennent la valeur AUTO. La clé méta est donc automatiquement chargée uniquement si elle est indexée, et les clés méta non indexées adoptent l'état FERMÉ jusqu'à ce qu'elles soient ouvertes manuellement.
   La valeur de la vue initiale s'affiche dans la colonne Vue.
6. Pour enregistrer les modifications, cliquez sur **Enregistrer**.
7. Pour appliquer les modifications à la vue Naviguer active, cliquez sur **Enregistrer et appliquer**.

Supprimer un métagroupe

1. Dans la liste **Groupes méta**, sélectionnez le groupe à supprimer.
2. Cliquez sur .
   Une fenêtre de confirmation vous permet d'annuler ou d'exécuter la demande.
3. Cliquez sur **OK**.
   Le métagroupe est supprimé. Lorsque vous fermez la fenêtre, si le groupe supprimé était le métagroupe actif, il sera supprimé et les clés méta par défaut seront utilisées pour créer la vue.

Exporter un métagroupe

Les métagroupes définis par l'utilisateur sont créés sur les services individuels. Pour créer des métagroupes disponibles sur un autre service, vous devez les exporter vers votre système de fichiers local. Pour exporter un ou plusieurs groupes méta.

1. Dans la liste **Groupes méta**, sélectionnez un ou plusieurs groupes à exporter.
2. Cliquez sur .
   Les groupes sélectionnés sont téléchargés sur votre système de fichiers local sous la forme d'un **fichier MetaGroups.jsn**. Chaque téléchargement de métagroupes porte le même nom avec un numéro joint pour éviter d'écraser les téléchargements précédents.

Importer un métagroupe

Pour rendre les métagroupes personnalisés disponibles sur le service actif faisant l'objet d'une procédure d'enquête, importez le fichier `MetaGroups.jsn` à partir du système de fichiers local. Lors de l'importation de groupes méta, un message d'erreur s'affiche si l'un des groupes existe déjà. Pour importer un groupe qui est un réplica, vous devez d'abord supprimer le groupe existant. Si vous souhaitez supprimer un groupe méta, il ne peut pas être utilisé par un profil.

Pour importer des métagroupes :

1. Dans la liste **Groupes méta**, sélectionnez un fichier à importer et cliquez sur .
   La boîte de dialogue de sélection s'affiche.

2. Cliquez sur **Parcourir** et accédez au répertoire sur votre système de fichiers local où sont stockés les fichiers `MetaGroups.jsn` téléchargés. Sélectionnez un fichier, puis cliquez sur **Ouvrir**.
   Le nom du fichier s'affiche dans le champ Télécharger le fichier.

3. Cliquez sur **Télécharger**.
   Le processus de téléchargement commence, puis un message indique la réussite de l'opération. Les métagroupes sont ajoutés à la liste Groupe méta. Si le fichier est un doublon d'un métagroupe existant, une fenêtre vous indique que le métagroupe existe déjà.

Visualiser des métadonnées en tant que coordonnées parallèles

Les analystes peuvent utiliser la visualisation de coordonnées parallèles dans la vue Naviguer pour concentrer la procédure d'enquête sur des associations de clés et valeurs méta qui peuvent indiquer que des événements sont anormaux et méritent une procédure d'enquête.

Remarque : Dans la version 11.1 ou supérieure, chaque fois que les clés méta sont utilisées, vous pouvez également utiliser des entités méta configurées.

Le graphique de coordonnées parallèles est une façon de visualiser le point actuel de recherche verticale dans Enquêter afin d'examiner plus de deux clés méta de manière simultanée. Visualiser plusieurs clés méta simultanément peut aider à identifier les problèmes de sécurité associés aux modèles et comparaisons à plusieurs variantes, comme lorsque les valeurs et clés méta ne posent pas de problème de manière individuelle mais présentent une relation ou un modèle anormal lorsqu'elles sont combinées. Les groupes méta (reportez-vous à la section Gérer les groupes méta) peuvent être utilisés efficacement pour définir une collection de clés méta que vous souhaitez visualiser en tant que coordonnées parallèles.

Bonnes pratiques pour des graphiques de coordonnées parallèles efficaces

Pour créer des graphiques de coordonnées parallèles efficaces, suivez ces recommandations :

- Commencez à partir d'un point de recherche verticale, plutôt que d'essayer de visualiser toutes les données.
- Limitez la période si nécessaire.
- Choisissez l'ensemble utile de clés méta le plus réduit pour afficher en tant qu'axes.
- Spécifiez la séquence d'axes pour souligner les anomalies entre les valeurs méta alors que vous suivez une ligne dans le graphique.
- Vous pouvez identifier un ensemble utile de clés méta et une séquence, et créer un groupe méta personnalisé à utiliser lors de procédures d'enquête futures. Par exemple, vous pouvez créer un groupe méta personnalisé pour le type de fichiers Exécutables Windows.
- Utilisez les groupes méta prêts à l'emploi RSA qui sont inclus dans une nouvelle installation.
- Réutilisez et partagez des groupes méta personnalisés en important et exportant des groupes en tant que fichiers `.jsn`.
- Il s'avère utile de créer deux versions de chaque groupe méta personnalisé. Une version pour l'analyse des métavaleurs et une autre pour la création d'un graphique de coordonnées parallèles en s'attachant à un sous-ensemble de plus petite taille pour le même cas d'utilisation.

Remarque : Lors de l'importation de groupes méta, un message d'erreur s'affiche si l'un des groupes existe déjà. Pour importer un groupe qui est un réplica, vous devez d'abord supprimer le groupe existant. Si vous souhaitez supprimer un groupe méta, il ne peut pas être utilisé par un profil.

Pour vous aider à élaborer des graphiques de coordonnées parallèles de meilleure qualité, NetWitness Platform et versions supérieures comprend plusieurs optimisations.

- Les analystes peuvent spécifier que le graphique n'illustre que les sessions contenant toutes les clés méta.
- L'administrateur peut augmenter le nombre de métavaleurs affichées dans les Paramètres de coordonnées parallèles, dans la vue Système d'administration > Panneau Investigation > Onglet Naviguer.

Groupes méta RSA pour des exemples d'utilisation de coordonnées parallèles

Un ensemble de groupes méta prédéfinis est inclus avec NetWitness Platform. Si vous souhaitez obtenir la dernière version, vous pouvez importer le fichier de groupes méta, `MetaGroups_ootb_w_query.jsn`, dans la boîte de dialogue Gérer les groupes méta. Voici certaines des activités ciblées se prêtant bien aux visualisations de coordonnées parallèles :

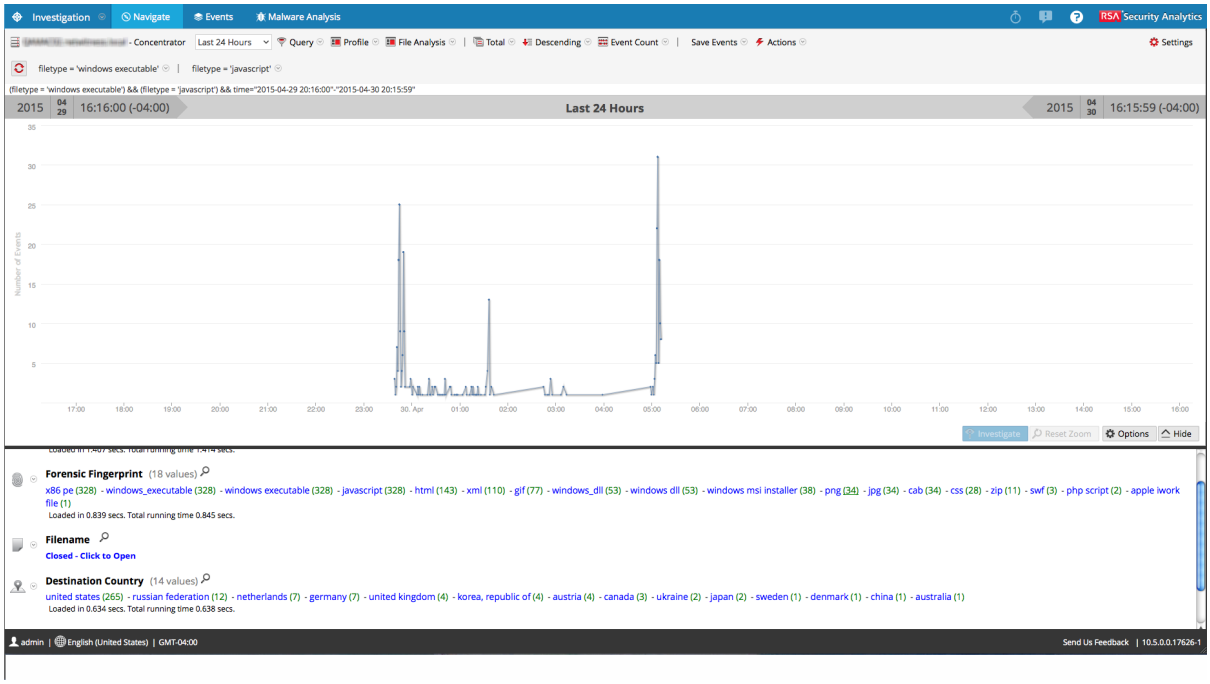
- Balisage de botnets
- Canaux de conversion
- E-mail
- Sessions chiffrées
- Analyse des points de terminaison
- Analyse de fichiers
- Malware Analysis
- Trafic HTTP sortant
- Trafic SSL/TLS sortant
- Attaques d'injection SQL
- Analyse des menaces
- Analyse Web

Afficher la visualisation des coordonnées parallèles

À partir d'une procédure d'enquête dans Enquêter > vue Naviguer :

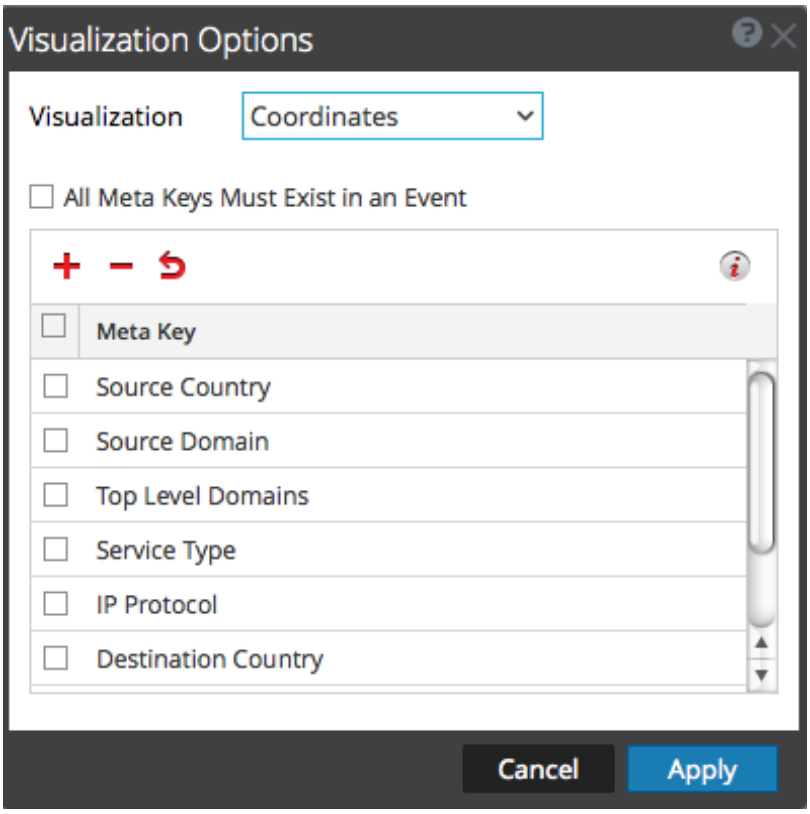
1. Si le panneau Visualisation, au-dessus du panneau Valeurs, est fermé, sélectionnez **Visualisation**.
2. Dans la barre d'outils, sélectionnez **Méta** > **> Utiliser le groupe méta > Analyse de fichiers (Malware)**.
3. Dans le panneau **Valeurs**, dans la clé méta **Empreinte approfondie**, cliquez sur `windows_executable`, puis sur `x86 pe` pour lire le fil d'Ariane `filetype = 'windows_executable' | filetype = 'x86 pe'`.

4. La visualisation par défaut pour le point actuel de recherche verticale s'affiche sous forme de chronologie.

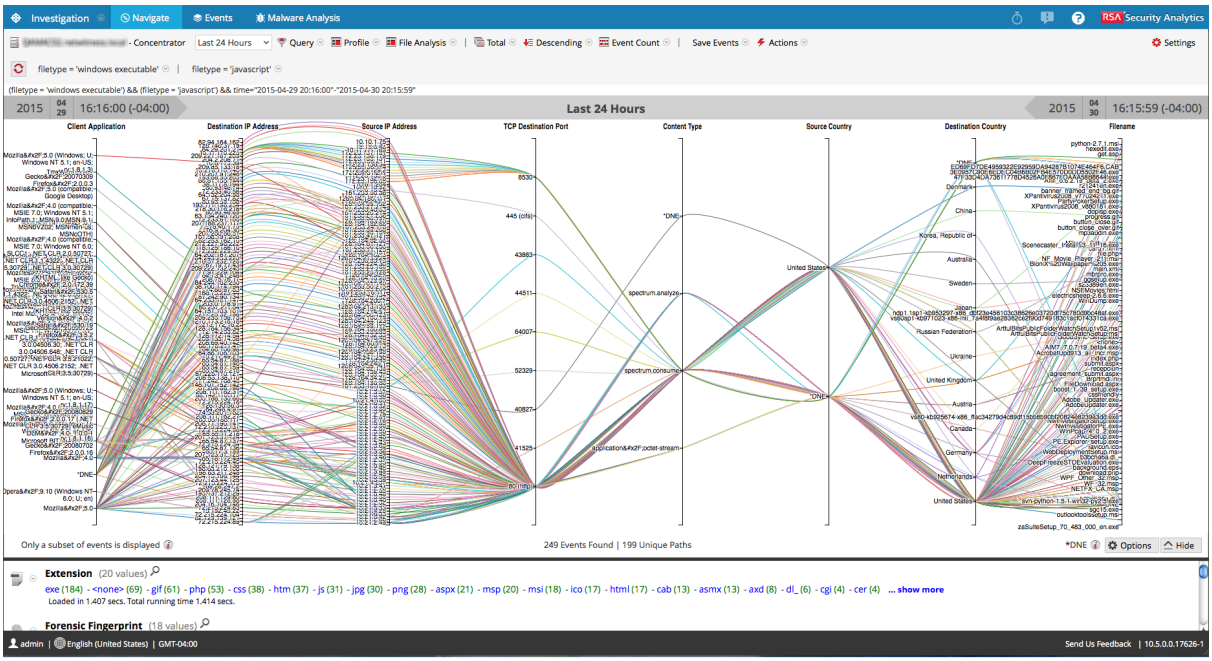


5. Dans le panneau **Visualisation**, sélectionnez **Options**.
La boîte de dialogue Options de visualisation s'affiche.

6. Dans la liste déroulante **Visualisation**, sélectionnez **Coordonnées** et cliquez sur **Appliquer**.



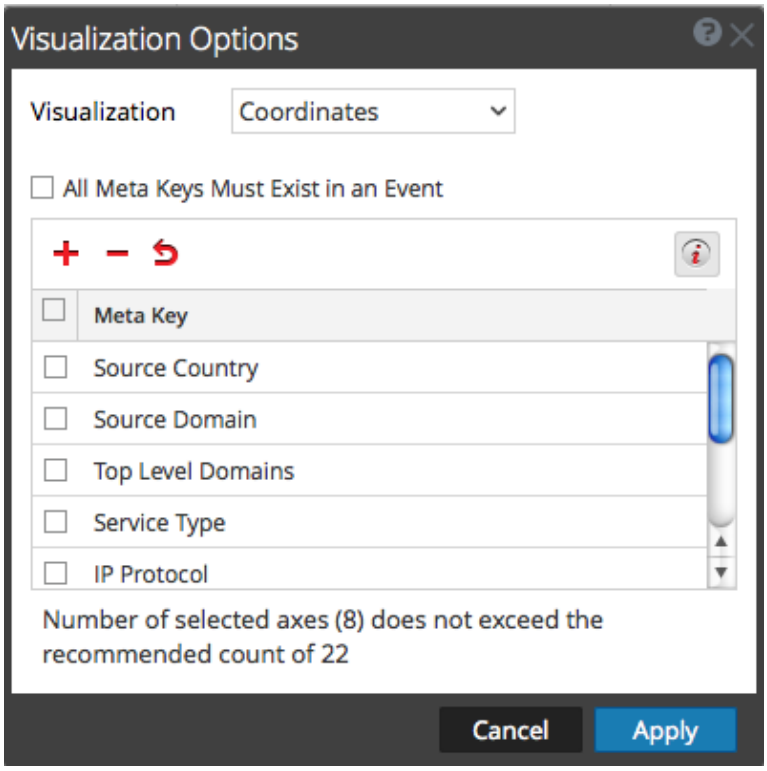
La visualisation est chargée. Dans cet exemple, 249 événements sont trouvés et 199 chemins uniques sont visualisés.



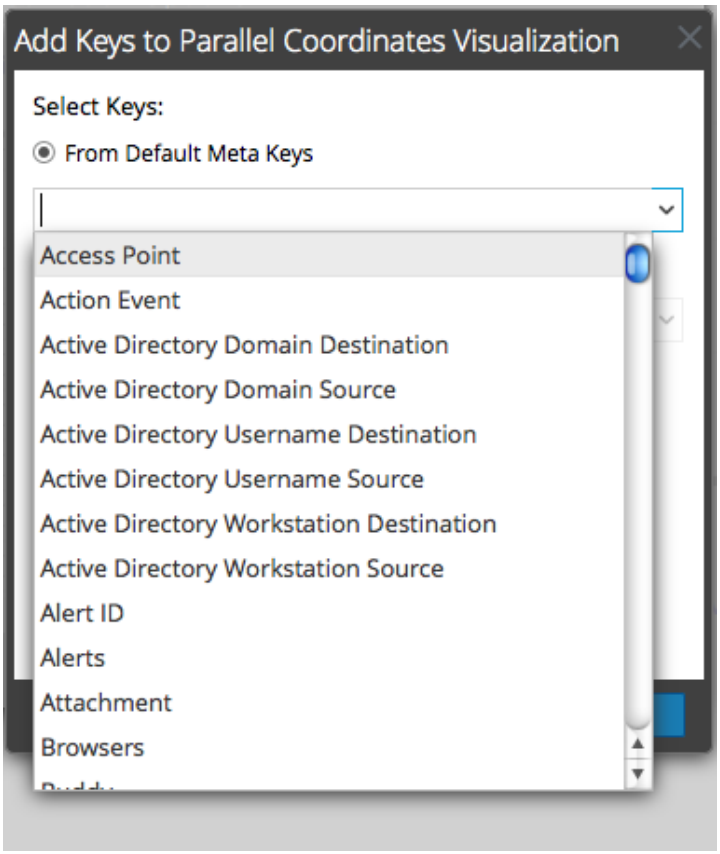
Sélectionner des clés méta pour la visualisation de coordonnées parallèles

Lorsque la visualisation de coordonnées parallèles est ouverte, procédez comme suit :

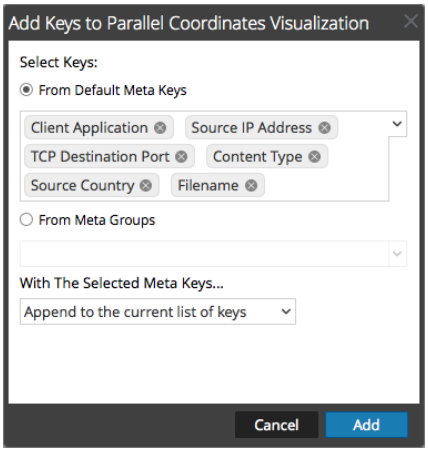
1. Dans le panneau Visualisation, sélectionnez **Options**.
   La boîte de dialogue Options de visualisation s'affiche. Dans la barre d'outils, cliquez sur pour afficher le nombre d'axes recommandé afin que la visualisation soit lisible. Lorsque le nombre recommandé de clés s'affiche, le nombre change en fonction de la taille de la fenêtre du navigateur. Si vous élargissez la fenêtre du navigateur, le nombre recommandé augmente.



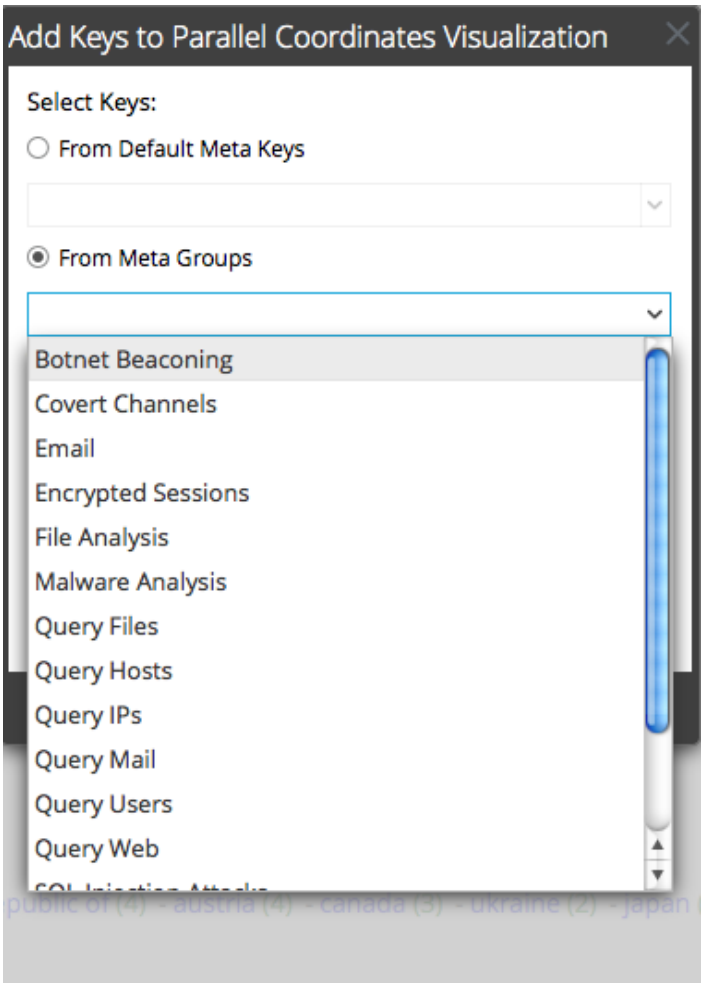
2. Si vous souhaitez modifier la séquence des clés méta, faites glisser les clés méta vers le haut ou vers le bas, selon la séquence souhaitée.
3. Si vous souhaitez supprimer des clés méta, cliquez dans la boîte de sélection, puis cliquez sur .
   Les clés méta sont supprimées, mais la modification n'a pas été appliquée.
4. Si vous souhaitez retrouver l'état précédent, cliquez sur .
   Toutes les clés méta que vous avez supprimées sont restaurées et tous les changements que vous avez réalisés sont supprimés.
5. Pour sélectionner différentes clés méta, cliquez sur , sélectionnez **À partir des clés méta par défaut**, et, dans la liste déroulante, sélectionnez les clés méta.



Les clés sélectionnées sont répertoriées.

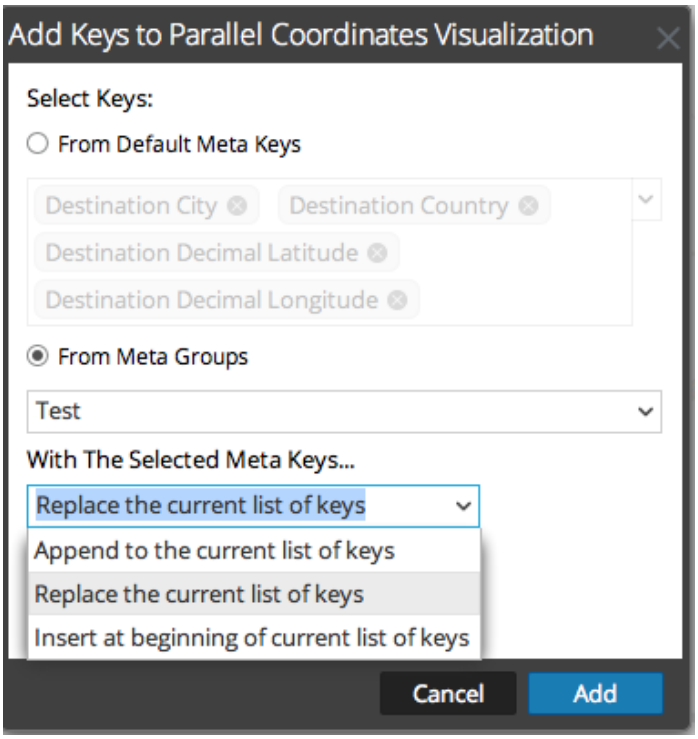


6. Si vous souhaitez ajouter toutes les clés au groupe méta, vous ne pouvez pas ajouter de clés méta individuelles. Sélectionnez **À partir des groupes méta**, et sélectionnez un groupe dans la liste déroulante.

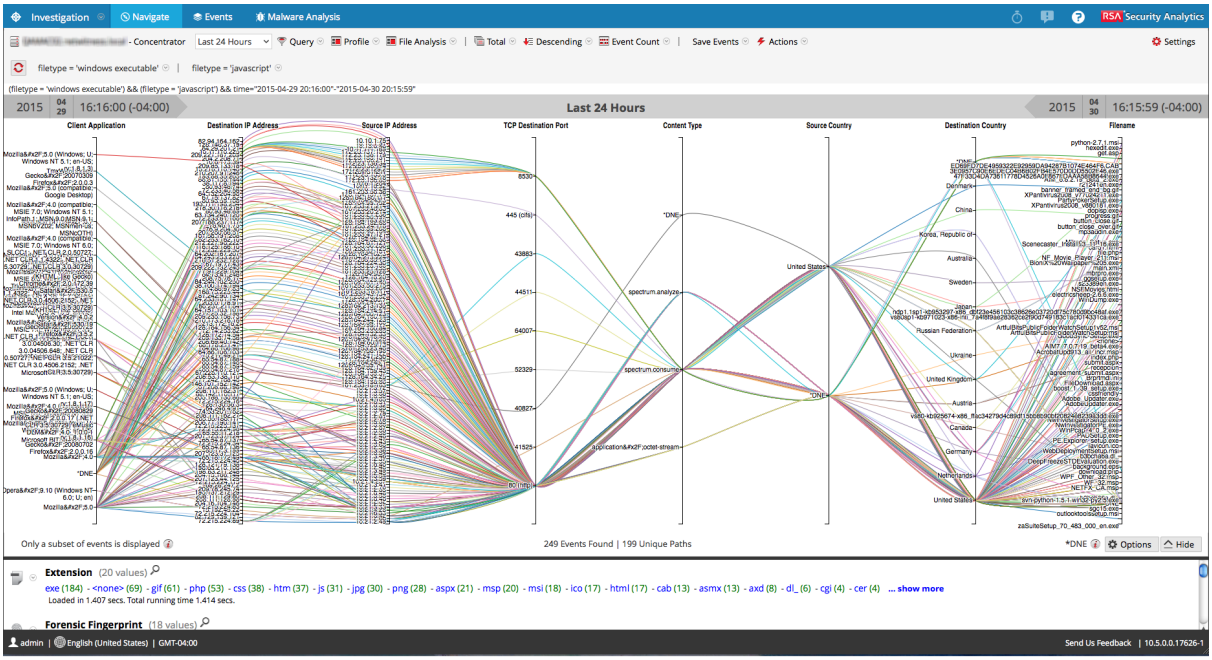


Les groupes méta sélectionnés sont répertoriés dans le champ.

7. Sélectionnez la méthode pour l'ajout de clés ou groupes: Vous pouvez utiliser les options **Remplacer la liste actuelle de clés**, **Ajouter à la liste actuelle de clés** (à la fin) ou **Insérer au début de la liste de clés actuelle.**

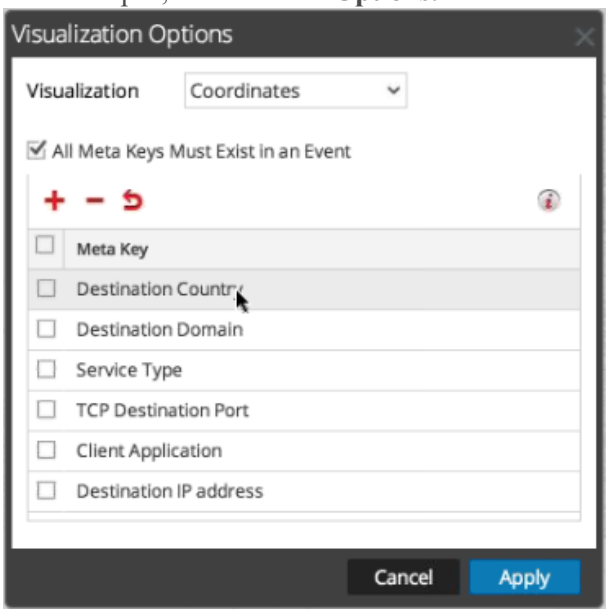


8. Pour terminer la procédure, cliquez sur **Ajouter**.
   La boîte de dialogue Options de visualisation s'affiche avec les clés méta ou groupes que vous avez sélectionnés.
9. Pour afficher le nouveau graphique de visualisation, cliquez sur **Appliquer**.

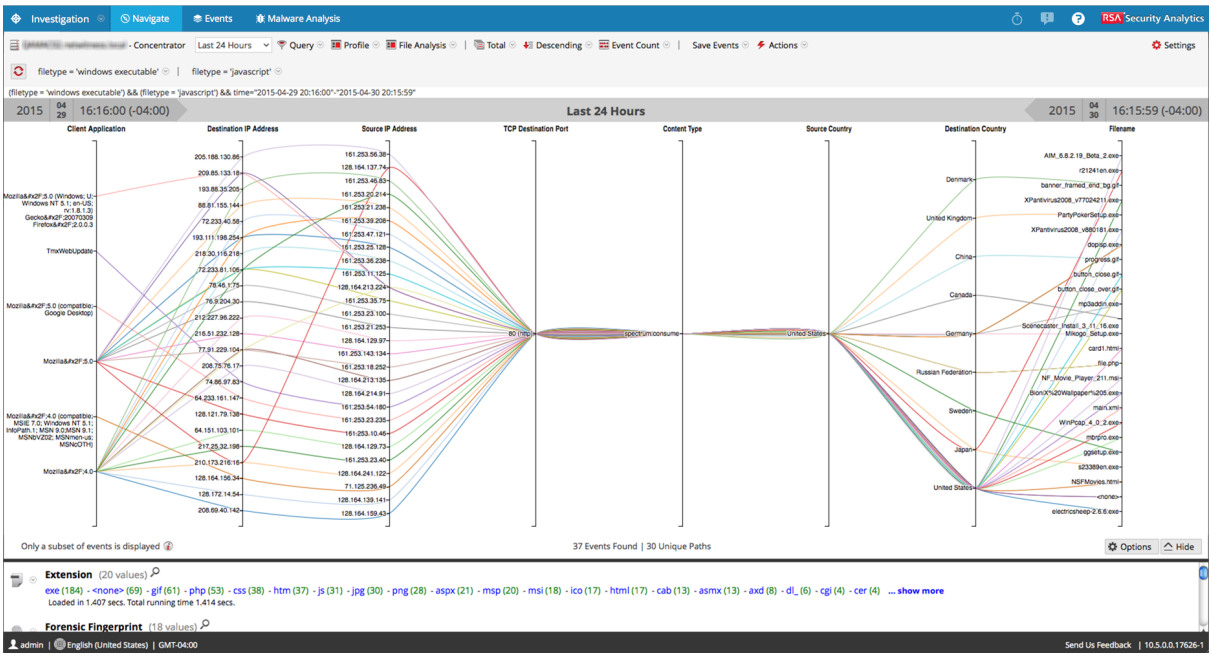


Optimiser la visualisation des coordonnées parallèles

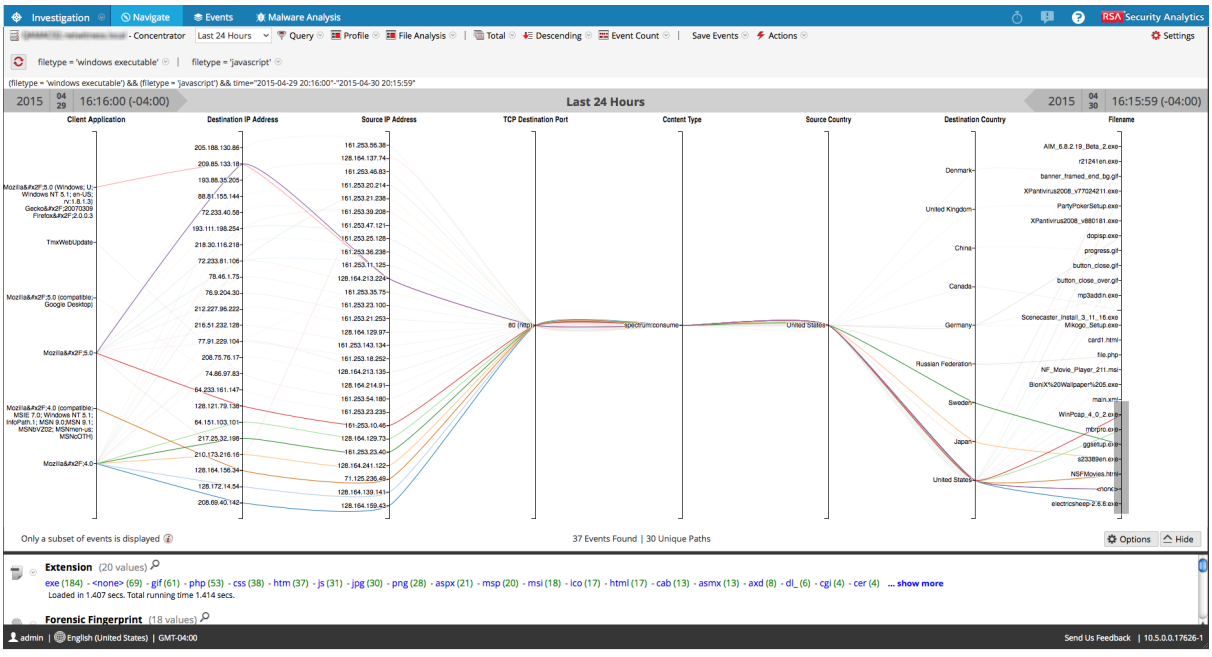
1. Pour optimiser la visualisation en supprimant des événements pour lesquels toutes les clés méta n'existent pas, sélectionnez **Options.**



2. La boîte de dialogue Options de visualisation, sélectionnez **Toutes les clés méta doivent exister dans un événement**. Cliquez sur **Appliquer**.
   Le graphique qui en résulte est plus lisible et utile, et il contient moins de chemins uniques.



3. Si vous souhaitez mettre en surbrillance un petit ensemble de points pour afficher le chemin de la ligne, de droite à gauche, cliquez sur un axe. Le curseur se change en réticule, que vous pouvez faire glisser pour sélectionner une ou plusieurs valeurs. Lorsque vous relâchez la souris, les lignes sont mises en surbrillance. Dans l'exemple ci-dessous, le type de service SLL est mis en surbrillance grâce à la zone grise.



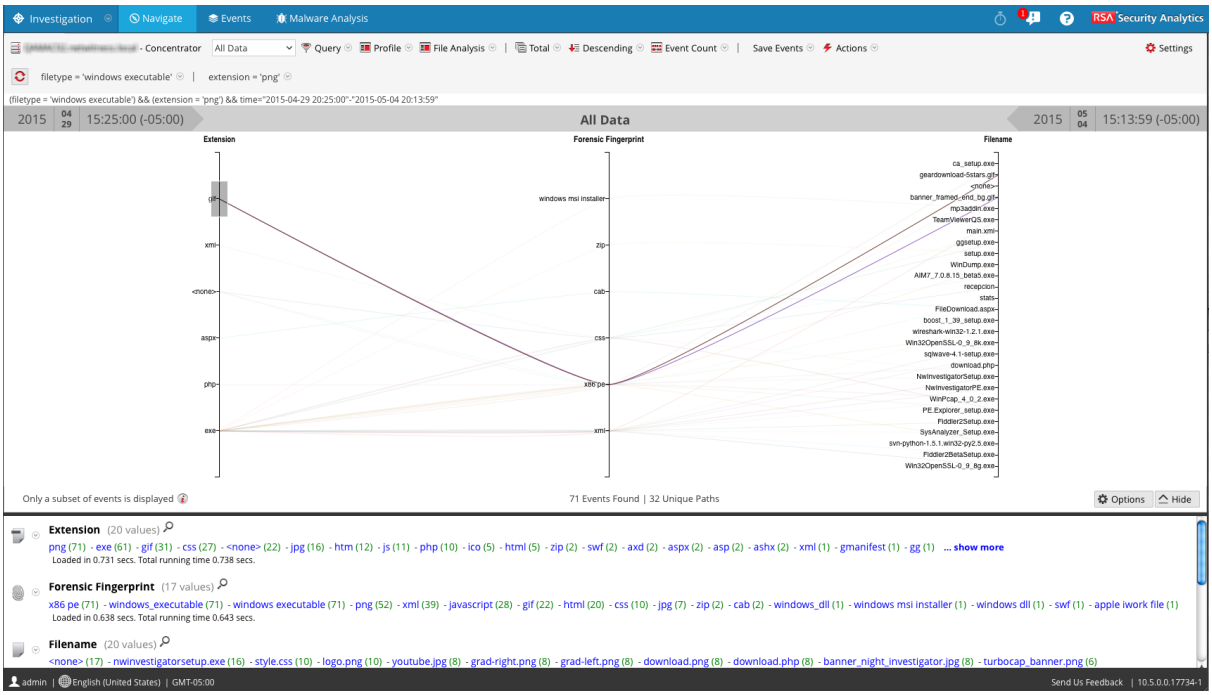
4. Si vous souhaitez agrandir la visualisation, faites glisser le bord inférieur du panneau vers le bas, et agrandissez la fenêtre du navigateur en faisant glisser le bord droit.

Exemple de cas d'utilisation

Voici un exemple de visualisation des coordonnées parallèles des clés méta représentant des métadonnées de fichier dans une session. Il existe trois clés méta ou axes, de gauche à droite : Extensions, Empreinte approfondie et Nom de fichier avec des valeurs répertoriées le long de chaque axe. Les valeurs de l'axe Extension affichent l'extension du fichier et les valeurs de l'axe Empreinte approfondie sont des exécutables Windows. Généralement, le type de fichier correspond à l'empreinte approfondie attendue. Toutefois, il n'est pas normal qu'un fichier de type `gif` soit combiné à une empreinte exécutable Windows. Le type de fichier `gif` est sélectionné pour souligner les corrélations entre ce type de fichiers (`x86pe`) et deux noms de fichiers dans le troisième axe, de façon à ce que l'analyste puisse identifier rapidement les fichiers devant faire l'objet d'une procédure d'enquête.

Pour atteindre cette vue :

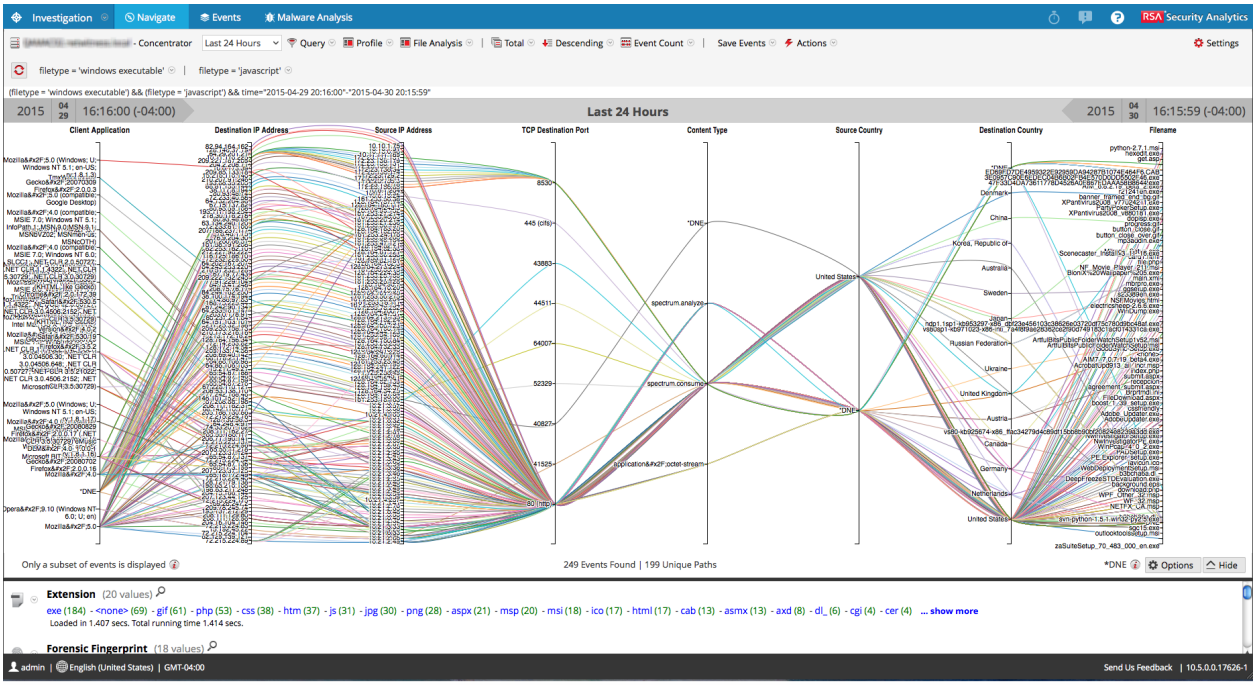
1. Classer par valeur et Trier par ordre croissant.
2. Appliquez deux filtres (file type = 'windows executable' and extension = 'gif') dans la vue Naviguer pour limiter la quantité de données.
3. Configurez un graphique de coordonnées parallèles en choisissant trois axes : `file extension`, `forensic fingerprint` et `filename`.



Exemple de visualisation d'un ensemble étendu de données

Cet exemple de visualisation de coordonnées parallèles, appliqué à un ensemble plus important de données, illustre plusieurs messages pouvant aider l'analyste à comprendre la représentation du graphique.

- Pour créer un graphique, NetWitness Platform commence par analyser les valeurs méta et renvoyer des résultats. Une période type peut contenir jusqu'à 10 000 000 métavaleurs. Lorsque le nombre de valeurs méta renvoyées atteint la Limite de résultat de valeurs méta, le graphique est généré même si NetWitness Platform n'a pas analysé un nombre de valeurs méta équivalent à la Limite d'analyse de valeurs méta.
- Il existe une limite fixe pour la quantité de données qui peut être affichée sous la forme d'un graphique de coordonnées parallèles. Dans NetWitness Platform 10.4 et versions antérieures, la limite se base sur le nombre d'axes, multiplié par les valeurs des données : 1 000 x le nombre d'axes pour protéger les performances, mais dans NetWitness Platform 10.5 et versions supérieures, l'administrateur configure les limites de coordonnées parallèles dans les paramètres d'Investigation, sous Administration vue Système.



Avec un ensemble important de données, le traitement du graphique de coordonnées parallèles est plus long que l'ensemble réduit de données et clés méta. Pour préserver les performances, NetWitness Platform génère les métavaleurs à partir du panneau Valeurs ci-dessous jusqu'à ce que les limites fixées par l'administrateur soient atteintes. Un message d'information indique : **Seul un sous-ensemble d'événements s'affiche.**

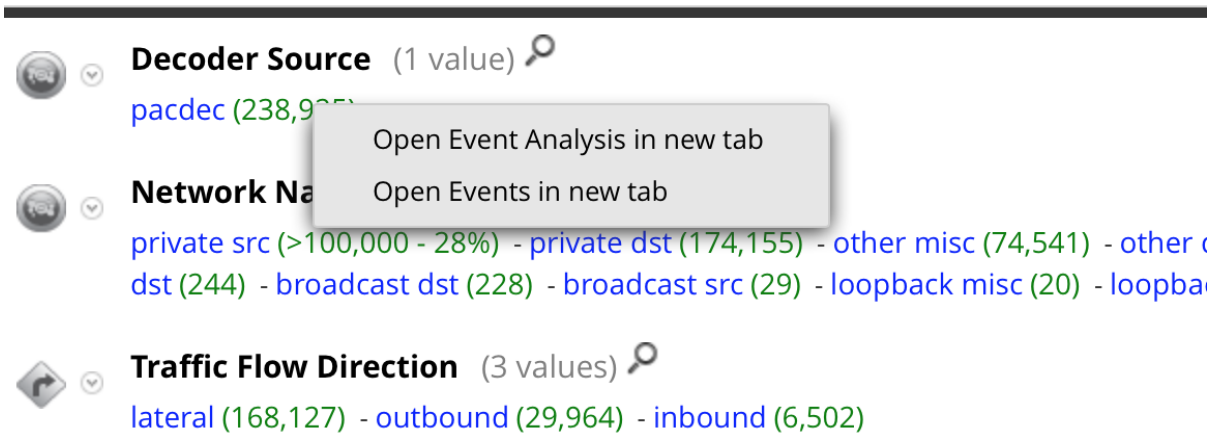
Sur toutes les données visualisées pour 249 événements, il n'y a eu que 199 chemins de coordonnées parallèles uniques. Certains événements sont inclus bien qu'ils ne contiennent pas certaines clés méta. Le libellé **Inexistant** indique que les méta n'existent pas dans cet événement.

Ouvrir un événement de la liste Événements

Une liste d'événements associée à une session est disponible dans Enquêter > vue Événements ou dans la vue Analyse d'événements.

Pour afficher des événements dans la vue Événements, procédez de l'une des façons suivantes :

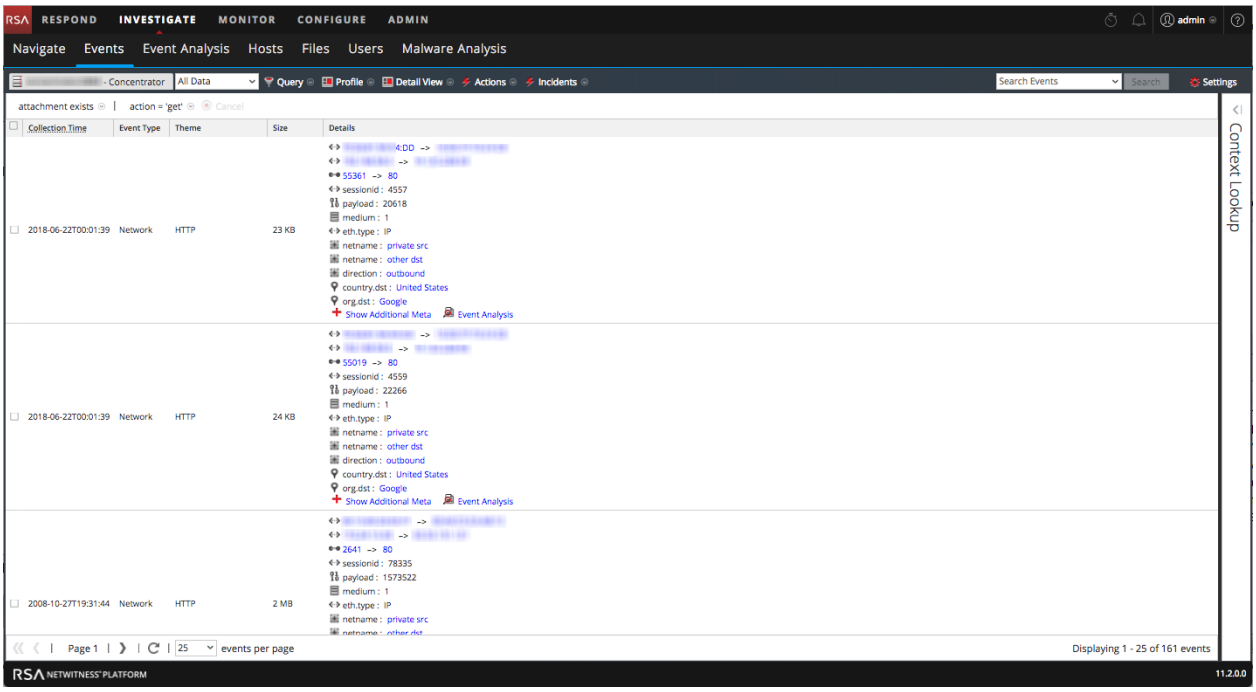
1. Pour utiliser la requête par défaut pour le service par défaut, accédez à **ENQUÊTER** > **Événements**.
   NetWitness Platform exécute une requête par défaut sur les trois dernières heures pour le service par défaut (si un service est défini) ou affiche une boîte de dialogue dans laquelle vous pouvez sélectionner un service, puis exécute la requête par défaut. La requête par défaut sélectionne tous les événements et la vue Événements affiche des événements sur le service sélectionné, avec les événements les plus anciens en premier.
2. Pour afficher les événements correspondant à une métavaleur spécifique, accédez à **ENQUÊTER** > **Naviguer** et lorsque le chargement des événements dans le panneau Valeurs est terminé, cliquez sur un métanombre (en vert). Vous pouvez également cliquer avec le bouton droit de la souris sur le nombre de métadonnées pour une valeur méta. Lorsque le menu contextuel s'affiche, cliquez sur **Ouvrir les événements dans un nouvel onglet**. (L'option Ouvrir l'analyse d'événements dans un nouvel onglet est disponible dans la version 11.1 ou supérieure).



   La vue Événements affiche les événements de la valeur méta sélectionnée.

La vue Événements fournit trois présentations intégrées des données d'événement : la vue Détails, la vue Liste et la vue Log.

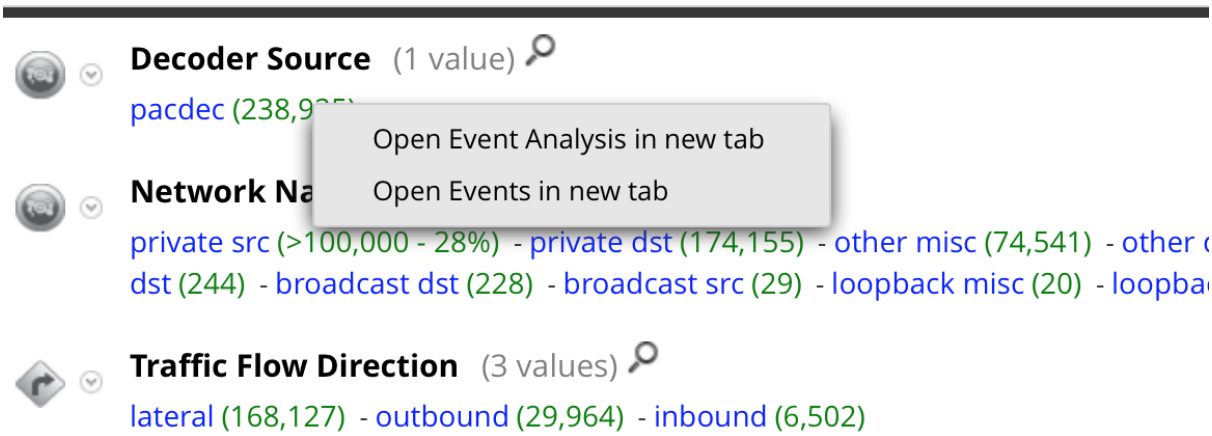
Voici un exemple de la vue Détails.



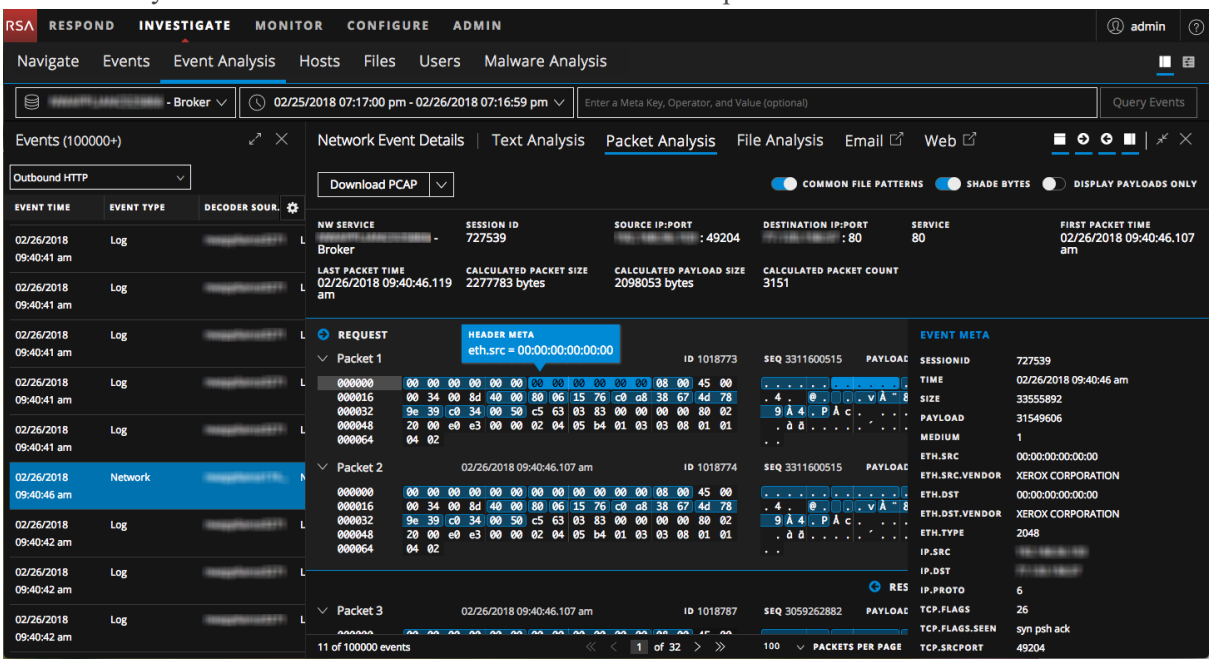
Vous pouvez utiliser des requêtes, le paramètre de plage temporelle et les profils pour filtrer les événements répertoriés dans la vue Événements. Depuis tous les types de vue dans la vue Événements, vous pouvez extraire des fichiers, exporter des événements, exporter des logs et ouvrir le panneau Reconstruction d'événement en double-cliquant sur un événement. Reportez-vous à la rubrique Examiner les événements bruts dans la vue Événements pour consulter des informations détaillées sur ces fonctionnalités.

Pour afficher des événements dans la vue Analyse d'événements, procédez de l'une des façons suivantes :

1. Dans la version 11.0 et versions ultérieures, accédez à **ENQUÊTER > Naviguer**, cliquez avec le bouton droit sur le métanombre (en vert) d'une métavaleur. Lorsque le menu contextuel s'affiche, sélectionnez **Ouvrir Analyse d'événements** dans un nouvel onglet.



La vue Analyse d'événements affiche les événements correspondant à la métavaleur sélectionnée.



Pour obtenir des informations détaillées sur les types d'analyse que vous pouvez utiliser dans cette vue, reportez-vous à la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements.

Exporter ou imprimer un point d'extraction

Dans NetWitness Enquêter, lorsque les données d'un point d'extraction s'affichent dans la vue Naviguer, vous pouvez :

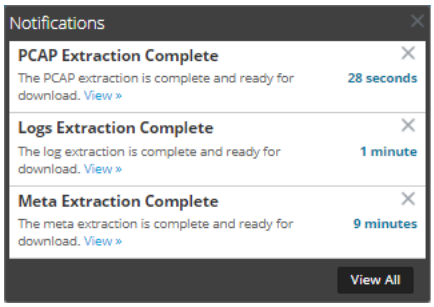
- Extraire des fichiers d'une session et choisir le type de fichier à extraire : archives, BitTorrent audio, documents, exécutable, images, autre, vidéo et web.
- Exporter le point d'extraction en tant que fichier de capture de paquet (PCAP), fichier log ou fichier de données méta.
- Imprimer le point d'extraction.

Les détails exportés sont affectés par la plage temporelle et le point d'extraction au moment de l'exportation.

Remarque : Lorsque vous exportez le point d'extraction en tant que fichier log, seules les sessions de log sont exportées. Le message de la file d'attente des tâches fait référence au nombre total de sessions dans le point d'extraction au lieu du nombre de logs. Par exemple, si le point d'extraction compte 505 sessions et seulement cinq sessions de log, le message de la file d'attente des tâches indique que NetWitness Platform extrait les logs de 505 sessions.

Pour exporter un point d'extraction à partir de la vue Naviguer :

1. Menez une procédure d'enquête jusqu'à ce que vous atteigniez le point d'extraction souhaité.
2. Dans la version 11.0, dans la barre d'outils, sélectionnez **Actions > Exporter** et sélectionnez l'une des options d'exportation : **PCAP**, **Logs** ou **Méta**.
   Le point d'extraction est extrait et un message de planification de la tâche s'affiche. Vous pouvez consulter la page des tâches pour vérifier l'état.
3. Dans la version 11.1, dans la barre d'outils, sélectionnez **Enregistrer les événements** > et sélectionnez l'une des options d'exportation : **PCAP**, **Logs**, **Files** ou **Meta**.
   Une boîte de dialogue vous donne la possibilité de modifier le nom de fichier par défaut pour le fichier. La valeur par défaut est dans le formulaire `investigation-Feb-21-15-44-33`. Lorsque vous exportez un PCAP, le fichier est exporté sans choix de formats. Si vous utilisez l'une des autres options d'exportation, une boîte de dialogue s'affiche.
4. Dans la boîte de dialogue, sélectionnez :
   - Format du log d'exportation : **Text**, **XML**, **CSV** ou **JSON**.
   - Le type de fichier à exporter : Archives, Audio, BitTorrent, Documents, Executables, Images, Autre, Vidéo et Web.
   - Le format Meta : **Text**, **CSV**, **TSV**, **JSON**.
5. Lorsque l'extraction du fichier planifié est terminée, un message s'affiche dans la barre d'état Notifications de tâche.



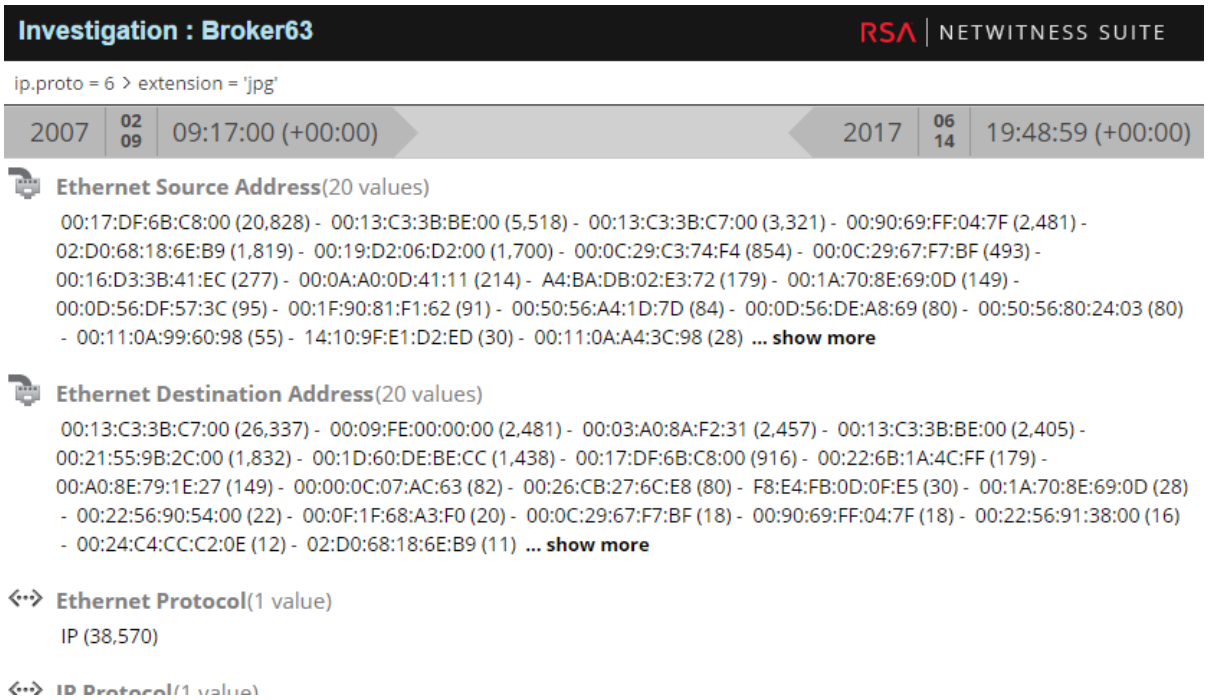
6. Cliquez sur le lien **Afficher** dans la barre d'état Tâches et téléchargez le fichier d'extraction spécifique demandé.

Pour imprimer le point de recherche verticale actuel :

Dans la vue Naviguer, vous pouvez afficher le contenu du point de recherche vertical actuel sous un format imprimable dans la fenêtre du navigateur.

Pour afficher le point de recherche verticale actuel dans l'aperçu avant impression :

1. Avec un point de recherche verticale ouvert dans la vue **Naviguer**, sélectionnez **Actions** > **Imprimer** dans la barre d'outils.
   Un nouvel onglet est créé avec l'aperçu avant impression du point de recherche verticale actuel.



2. Utilisez l'option d'impression de votre navigateur pour envoyer une version imprimable à l'imprimante.

Lancer la recherche externe d'une clé méta

Cette rubrique fournit des instructions pour l'utilisation de plug-ins Procédure d'enquête prêts à l'emploi pour lancer une recherche externe de clés méta spécifiques à l'aide d'outils externes à NetWitness Platform lors de la procédure d'enquête sur des données dans la vue Naviguer ou Événements.

Les analystes peuvent utiliser des recherches externes NetWitness Platform Investigation prêtes à l'emploi pour gagner du temps pendant les procédures d'enquête. Pour accéder aux recherches prêtes à l'emploi, l'utilisateur doit cliquer avec le bouton droit de la souris sur l'une de ces métaclés : Adresse IP (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, et `file-hash`.

Pour toutes les clés méta `IP` et `host`, les recherches suivantes sont intégrées à NetWitness Platform :

- Google Malware : Ouvre une recherche Google Malware dans un nouvel onglet.
- Historique SANS IP : Ouvre une recherche Historique SANS IP dans un nouvel onglet.
- McAfee SiteAdvisor : Ouvre une recherche McAfee SiteAdvisor dans un nouvel onglet.
- Recherche dans le client Endpoint Thick : Ouvre une recherche dans le client NetWitness Endpoint Thick Client dans un nouvel onglet.
- Collecte DNS passive BFK : Ouvre une recherche de collection DNS passive BFK dans un nouvel onglet
- CentralOps Whois pour adresses IP et noms d'hôte : Ouvre une recherche CentralOps Whois pour adresses IP et noms d'hôte dans un nouvel onglet.
- Recherche Malwaredomainlist.com : Ouvre une recherche Malwaredomainlist.com dans un nouvel onglet
- Recherche d'adresses IP Robtex : Ouvre une recherche RobtexIP dans un nouvel onglet
- Recherche ThreatExpert : Ouvre une recherche ThreatExpert dans un nouvel onglet
- Recherche IPVoid : Ouvre une recherche UrlVoid dans un nouvel onglet

Pour les métaclés `file-hash` et `alias-host`, la recherche Google ouvre une recherche Google dans un nouvel onglet.

Pour la métaclé `client`, l'option NetWitness Endpoint Lookup ouvre un client Endpoint Thick Client dans un nouvel onglet si le client est installé sur le même système que celui sur lequel le navigateur est utilisé.

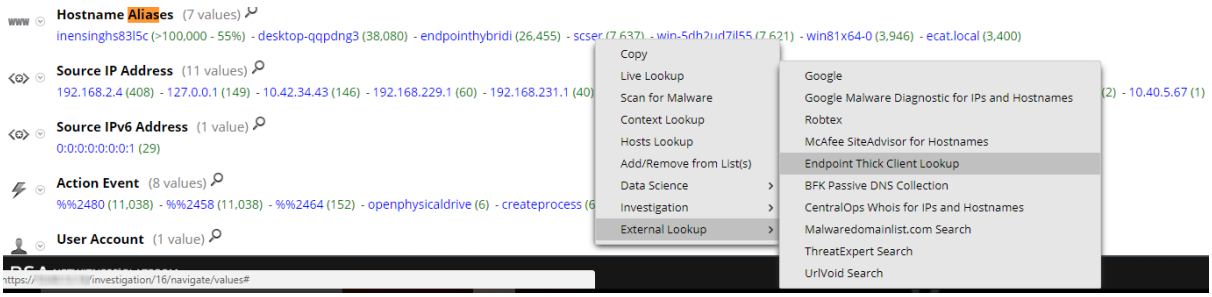
Les administrateurs peuvent ajouter des recherches externes supplémentaires et d'autres actions personnalisées, comme décrit dans « Ajouter des actions de menu contextuel personnalisées » dans le *Guide de configuration système*.

Lancer une recherche dans le client Endpoint Thick :

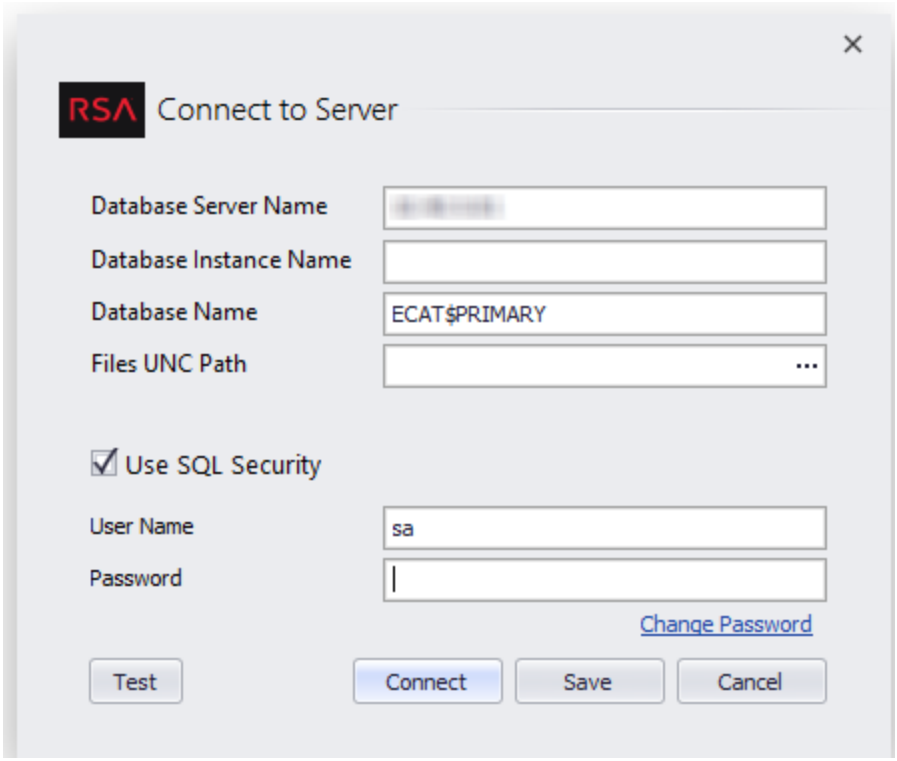
Pour lancer une recherche dans le client Endpoint Thick à partir de la vue Naviguer :

1. Cliquez avec le bouton droit de la souris sur une valeur méta pour l'une des clés méta suivantes : `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`

2. Sélectionnez **Recherche externe** dans le menu contextuel.
   Un sous-menu des options de recherche externes s'affiche.

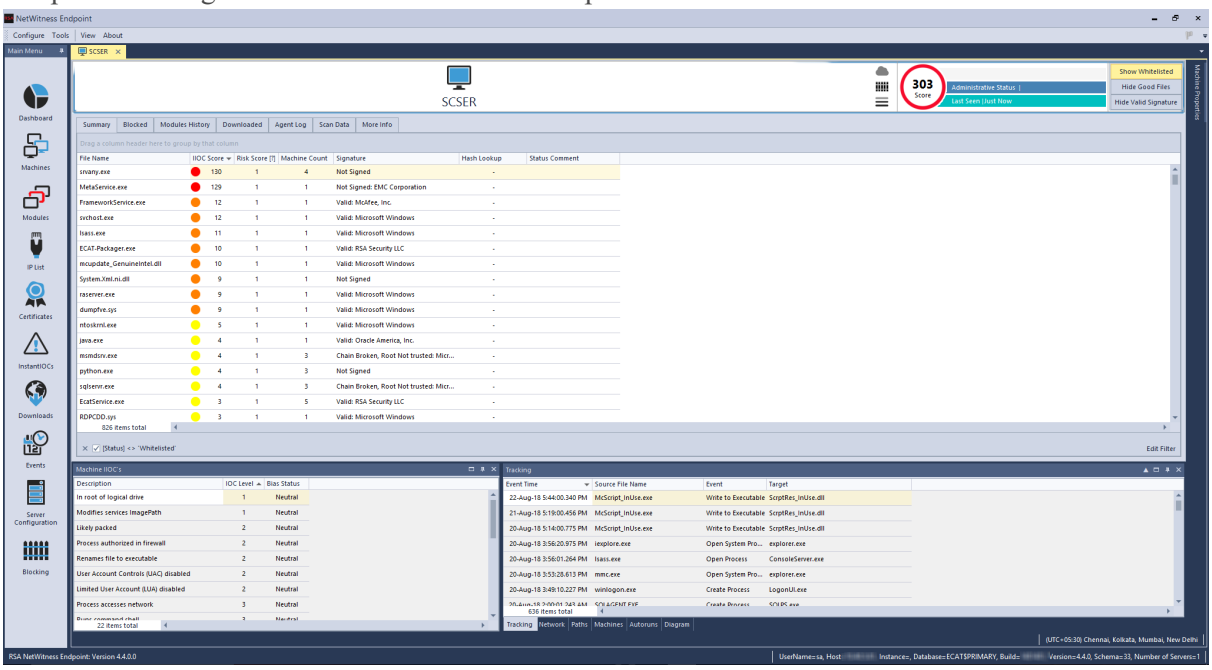


3. Sélectionnez **Recherche dans le client Endpoint Thicke**.
   La boîte de dialogue Se connecter au serveur.



4. Saisissez le nom d'utilisateur et le mot de passe requis pour vous connecter au client Endpoint Thick Client, puis cliquez sur **Se connecter.**

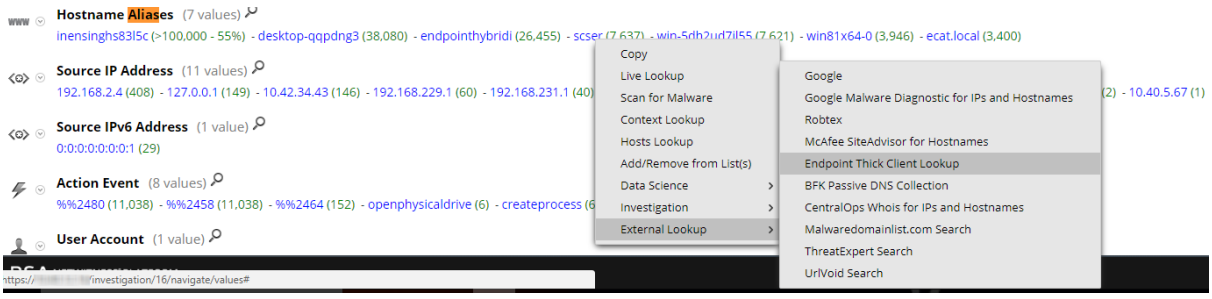
Le point de forage s'ouvre dans NetWitness Endpoint.



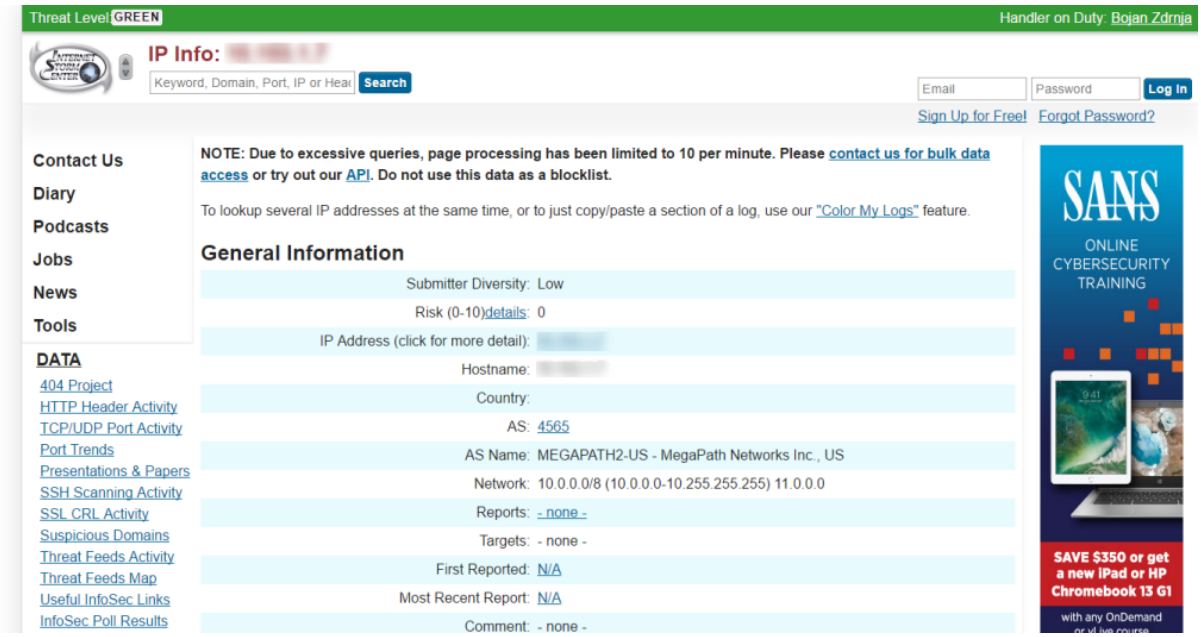
Lancer d'autres recherches externes

Pour lancer une recherche externe (autre que la recherche NetWitness Endpoint Thick Client) des données de la vue Naviguer :

1. Cliquez avec le bouton droit de la souris sur une valeur méta pour l'une des clés méta suivantes : `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`
2. Sélectionnez **Recherche externe** dans le menu contextuel.
   Un sous-menu des options de recherche externes s'affiche.



3. Sélectionnez l'une des options de recherche.
   La valeur méta sélectionnée s'ouvre dans la recherche sélectionnée. Par exemple, si vous avez sélectionné Historique SANS IP, les informations du point de recherche verticale s'affichent dans SANS Internet Storm Center.

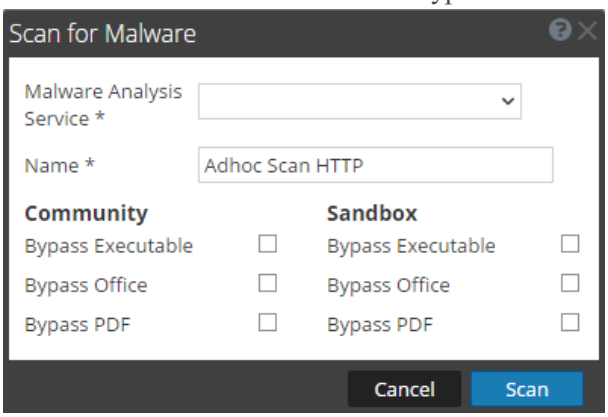

Threat Level GREEN
Handler on Duty: Bojan Zdrnja
IP Info:
Keyword, Domain, Port, IP or Hea
Search
Email
Password
Log In
Sign Up for Free!
Forgot Password?
Contact Us
Diary
Podcasts
Jobs
News
Tools
DATA
404 Project
HTTP Header Activity
TCP/UDP Port Activity
Port Trends
Presentations & Papers
SSH Scanning Activity
SSL CRL Activity
Suspicious Domains
Threat Feeds Activity
Threat Feeds Map
Useful InfoSec Links
InfoSec Poll Results
NOTE: Due to excessive queries, page processing has been limited to 10 per minute. Please contact us for bulk data access or try out our API. Do not use this data as a blocklist.
To lookup several IP addresses at the same time, or to just copy/paste a section of a log, use our "Color My Logs" feature.
General Information
Submitter Diversity: Low
Risk (0-10)details: 0
IP Address (click for more detail):
Hostname:
Country:
AS: 4565
AS Name: MEGAPATH2-US - MegaPath Networks Inc., US
Network: 10.0.0.0/8 (10.0.0.0-10.255.255.255) 11.0.0.0
Reports: - none -
Targets: - none -
First Reported: N/A
Most Recent Report: N/A
Comment: - none -
SANS
ONLINE CYBERSECURITY TRAINING
SAVE $350 or get a new iPad or HP Chromebook 13 G1
with any OnDemand

Lancer une analyse Malware Analysis à partir de la vue Naviguer

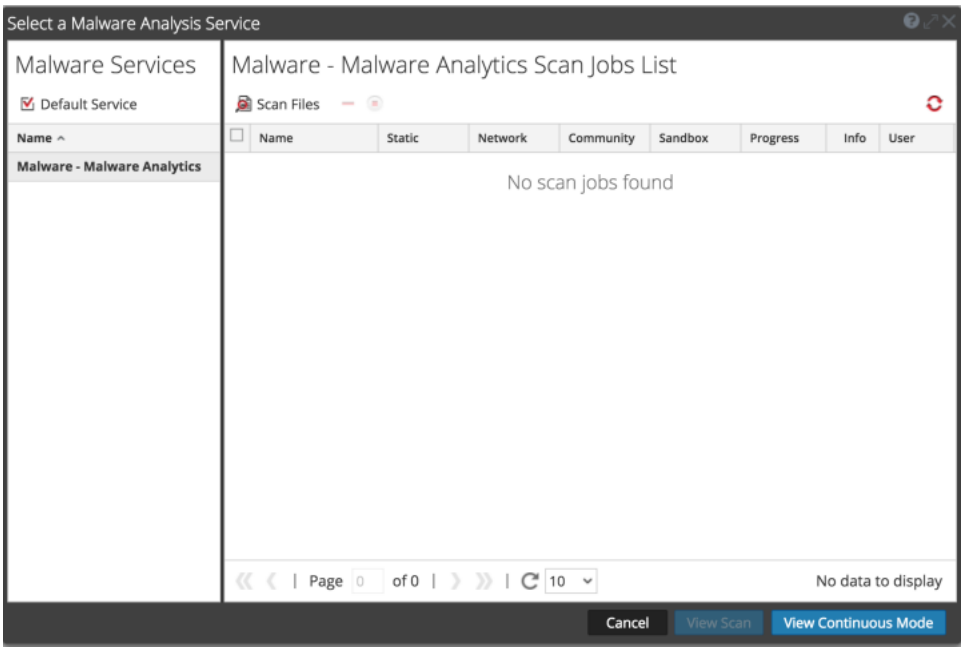
À partir de la Procédure d'enquête, les analystes peuvent lancer une analyse Malware Analysis à la demande en sélectionnant un service et une valeur méta, puis en choisissant une option dans le menu contextuel. Lorsque l'interrogation est terminée, les données analysées sont disponibles pour l'analyse de malware.

Pour lancer une analyse de données Malware Analysis à partir de la vue Enquêter > Naviguer :

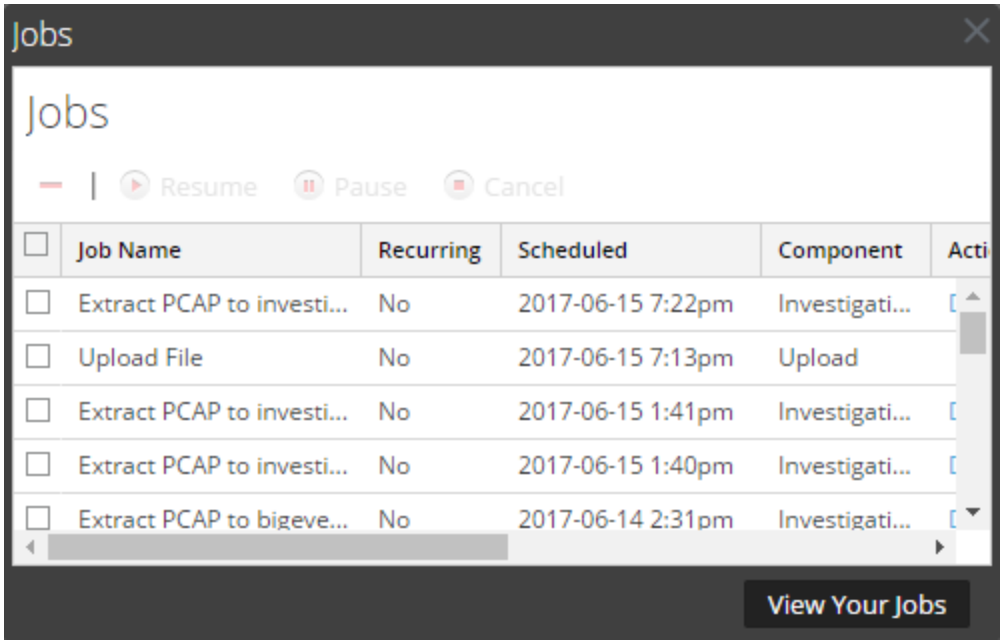
1. Cliquez avec le bouton droit de la souris sur une valeur méta (par exemple, OTHER, DNS ou FTP) et sélectionnez **Analyser les malwares** dans le menu contextuel.
   La boîte de dialogue Analyser les malwares s'affiche avec un nom suggéré pour l'analyse à la demande et aucun service sélectionné.
2. Dans la boîte de dialogue Analyser les malwares, sélectionnez un service pour effectuer l'analyse, modifiez le nom et sélectionnez les types de fichiers à ignorer sous Communauté et Sandbox.



3. Cliquez sur **Analyse**.
   La demande d'analyse est ajoutée au dashlet Liste des tâches d'analyse et à la barre d'état Tâches. Les paramètres de contournement de cette boîte de dialogue remplacent les paramètres par défaut dans les paramètres de configuration Malware Analysis de base.
4. Pour afficher les tâches, procédez de l'une des façons suivantes :
   a. Accédez à la liste des tâches d'analyse dans la vue Malware Analysis ou dans le tableau de bord Unified. Double-cliquez sur une analyse pour l'afficher.



b. Pour afficher la tâche dans la barre d'état Tâches, cliquez sur  dans la barre d'outils NetWitness Platform. Une fois la tâche terminée, faites défiler l'affichage vers la gauche et cliquez sur **Afficher**.



Le Récapitulatif des événements de malware pour l'analyse sélectionnée s'affiche. L'analyse est également ajoutée à la liste des analyses disponibles dans la boîte de dialogue de sélection des analyses dans la vue Investigation > onglet Malware.

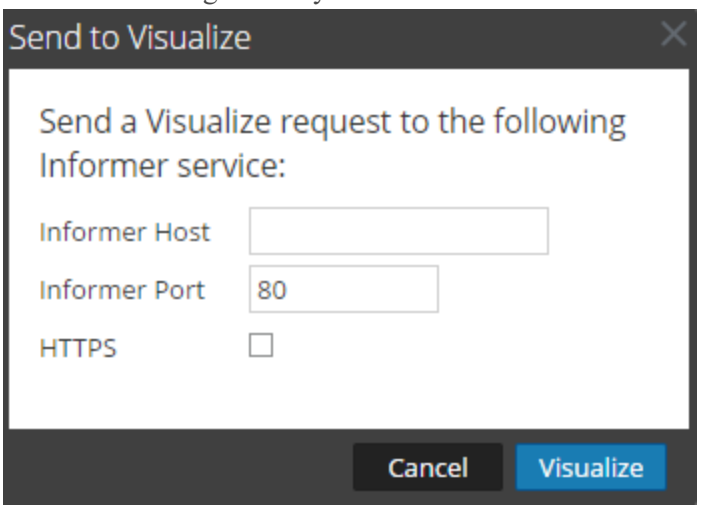
Visualiser le point d'extraction verticale actuel dans Informer

Cette rubrique fournit des instructions pour l'envoi d'un point d'extraction verticale dans la vue Naviguer vers une visualisation Informateur.

Informer doit être installé sur votre réseau et accessible par le service qui fait l'objet d'une enquête. Vous devez fournir le nom d'hôte et le port utilisés sur l'hôte Informer pour communiquer avec NetWitness Platform.

Pour afficher une visualisation du point d'extraction actuel dans Informer :

1. Avec un point d'extraction ouvert dans la vue Naviguer, cliquez sur **Actions > Visualiser**.
   La boîte de dialogue Envoyer à Visualize s'affiche.



2. Saisissez le nom d'hôte ou l'adresse IP Informer et vérifiez le port du serveur NetWitness Platform utilisé pour communiquer avec l'hôte Informer.
3. (Facultatif) Sélectionnez l'option HTTPS si l'hôte Informer utilise les communications sécurisées.
4. Cliquez sur **Visualiser**.
   La visualisation s'affiche dans un nouvel onglet.

Examiner les événements bruts dans la vue Événements

Les analystes qui mènent l'enquête sur les données dans Enquêter peuvent afficher et reconstruire des événements associés à une session.

- Les analystes effectuant une analyse à l'aide de NetWitness Platform Enquêter et disposant des rôles et autorisations système appropriés configurés pour leurs comptes utilisateur peuvent accéder depuis un point de recherche verticale de la vue Naviguer à la vue Événements.
- Ceux n'ayant pas accès à la vue Naviguer ou souhaitant parvenir directement à la vue Événements peuvent ouvrir des sessions et examiner les événements qui composent la session dans la vue Événements.
- Les analystes peuvent sélectionner les requêtes à partir de leur fenêtre « Historique de requêtes ».

Des rubriques distinctes décrivent les méthodes d'utilisation de la vue Événements :

- Résultats du filtrage et de la recherche dans la vue Événements
- Gérer des groupes de colonnes dans la vue Événements
- Exporter les événements dans la vue Événements
- Ajouter des événements à un incident pour obtenir une réponse
- Associer des événements à partir de sessions partagées

En outre, vous pouvez utiliser ces méthodes pour interroger des données et agir sur les résultats communs à la vue Naviguer et à la vue Événements.

- Rechercher des modèles de texte
- Créer une requête personnalisée
- Afficher et modifier des requêtes avec l'intégration URL
- Utiliser des profils pour encapsuler les vues personnalisées
- Gérer Listes Context Hub et Valeurs de la liste dans les vues Naviguer et Événements
- Rechercher un contexte supplémentaire dans les vues Naviguer et Événements
- Reconstruire un événement

Résultats du filtrage et de la recherche dans la vue Événements

Les analystes peuvent filtrer les résultats dans la vue Événements, en recherchant les événements ou sélectionnant le service pour lequel afficher les événements, définir la période et interroger les métadonnées.

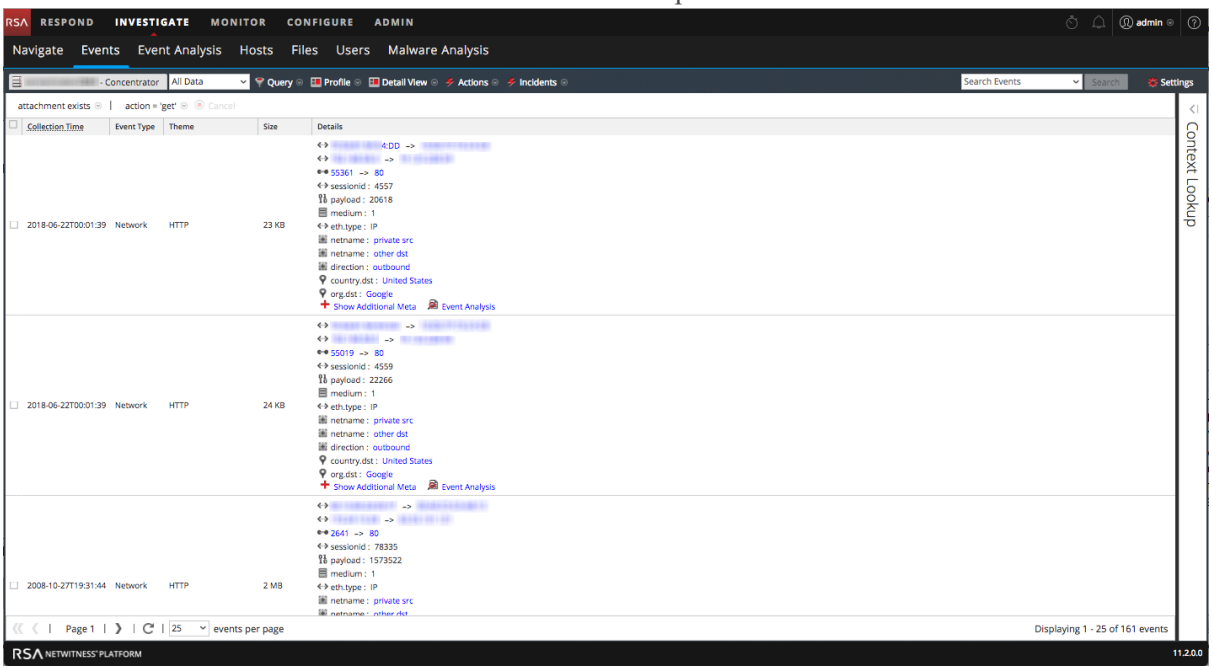
Si vous avez ouvert la vue Événements à partir d'un point de recherche verticale de la vue Naviguer, la vue détaillée des événements s'ouvre par défaut. Les analystes qui ne disposent pas des autorisations pour utiliser la vue Naviguer peuvent interroger les services directement à partir de la vue Événements. Il existe plusieurs options de configuration pour filtrer les informations affichées dans la vue Événements.

Remarque : Lorsqu'un service Archiver est le service actif dans la vue Événements et que vous êtes à la recherche d'un Broker ou Concentrator, l'opération est plus lente que la recherche d'un Broker ou Concentrator car les données du service Archiver sont compressées et qu'il y a généralement plus de données.

Filtrer les événements affichés dans la vue Événements

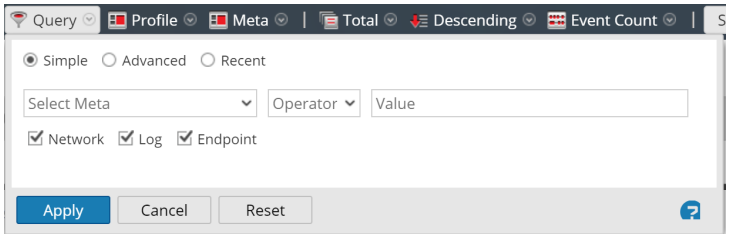
Pour filtrer les données affichées dans la vue Événements :

1. Go to **ENQUÊTER** > **Événements**.
   La vue Événements s'affiche en affichant la vue Détail par défaut.

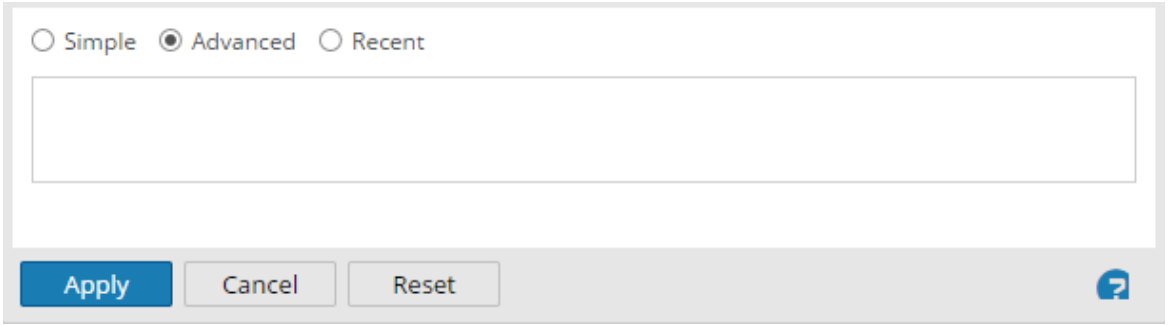


2. Pour sélectionner une autre période que la période par défaut, (**3 dernières heures**), dans la barre d'outils, cliquez sur le champ de la période et sélectionnez une valeur. Par exemple, **Dernière heure**.
   La vue Événements s'actualise avec la période sélectionnée.

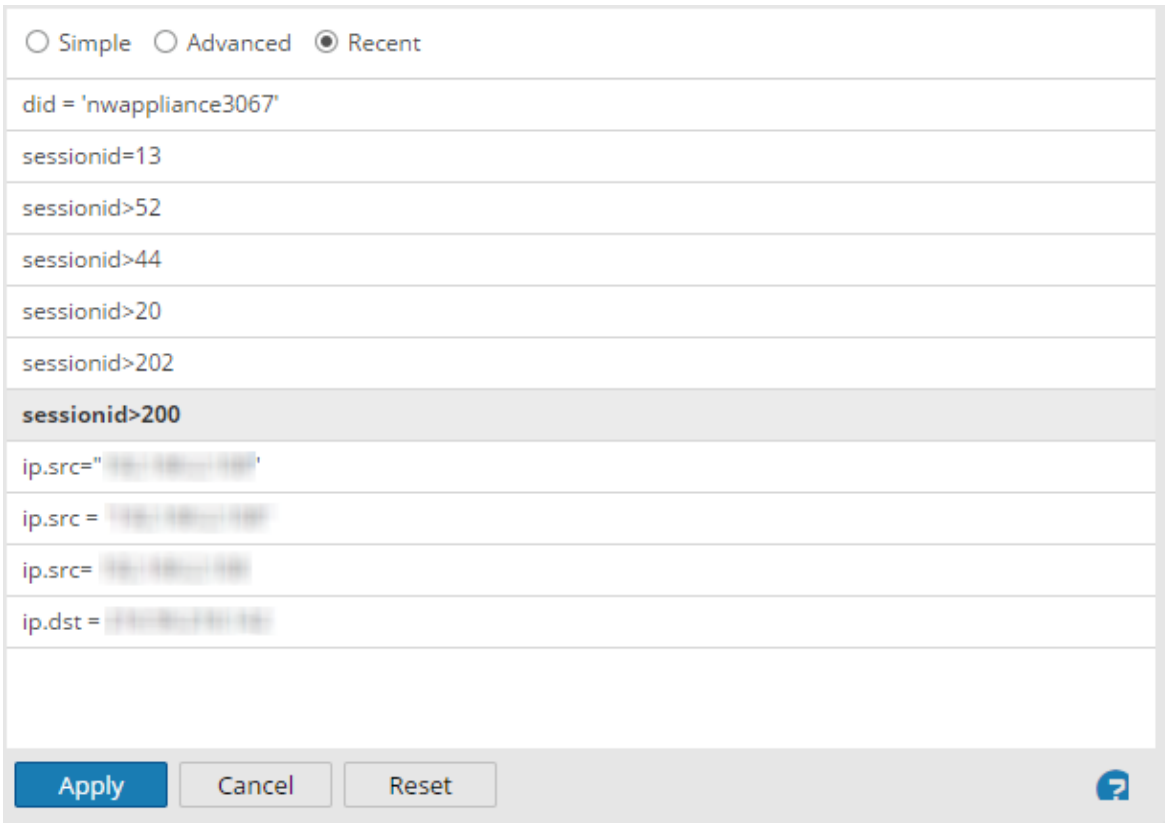
3. Pour saisir une requête pour le service et la période sélectionnés, cliquez sur **Requête** dans la barre d'outils.
   La boîte de dialogue Requête simple s'affiche.



4. Si vous souhaitez saisir une requête simple à l'aide de la fonction de remplissage automatique pour sélectionner les méta et les opérateurs, procédez de l'une des manières suivantes :
   a. Cliquez dans le champ **Sélectionner les méta**, puis sélectionnez une clé méta dans la liste déroulante.
   b. Sélectionnez un opérateur dans la liste déroulante sous le champ **Opérateur**.
   c. Saisissez une valeur de correspondance dans le champ **Valeur**.
   d. Sélectionnez les données **Réseau, Log** ou **Point de terminaison**, puis cliquez sur **Appliquer**.
      Les données correspondantes s'affichent dans la vue Événements.
5. Pour saisir une requête plus complexe basée sur vos connaissances des métas et des opérateurs :
   a. Cliquez sur **Avancée**.
      La boîte de dialogue Requête avancée s'affiche.



   b. Saisissez une requête. Au fur et à mesure que vous saisissez la requête, commençant par la clé méta, les listes déroulantes des clés méta et des opérateurs disponibles s'affichent. Une fois terminé, cliquez sur **Appliquer**.
6. Si vous souhaitez sélectionner une requête dans liste des requêtes récentes :
   a. Sélectionnez **Récente**.
      La boîte de dialogue Requête récente s'affiche.



b. Sélectionnez une requête, puis cliquez sur **Appliquer**.
Les résultats correspondants pour la requête sont affichés dans la vue Détails sous la vue Événements. Le fil d'Ariane reflète la requête.

c. Dans le fil d'Ariane, vous pouvez cliquer sur l'un des fils pour afficher le menu Requête. Vous pouvez insérer une nouvelle requête avant un fil et en ajouter une nouvelle à la fin d'un fil. Après chaque modification dans le fil, NetWitness Platform actualise les résultats.

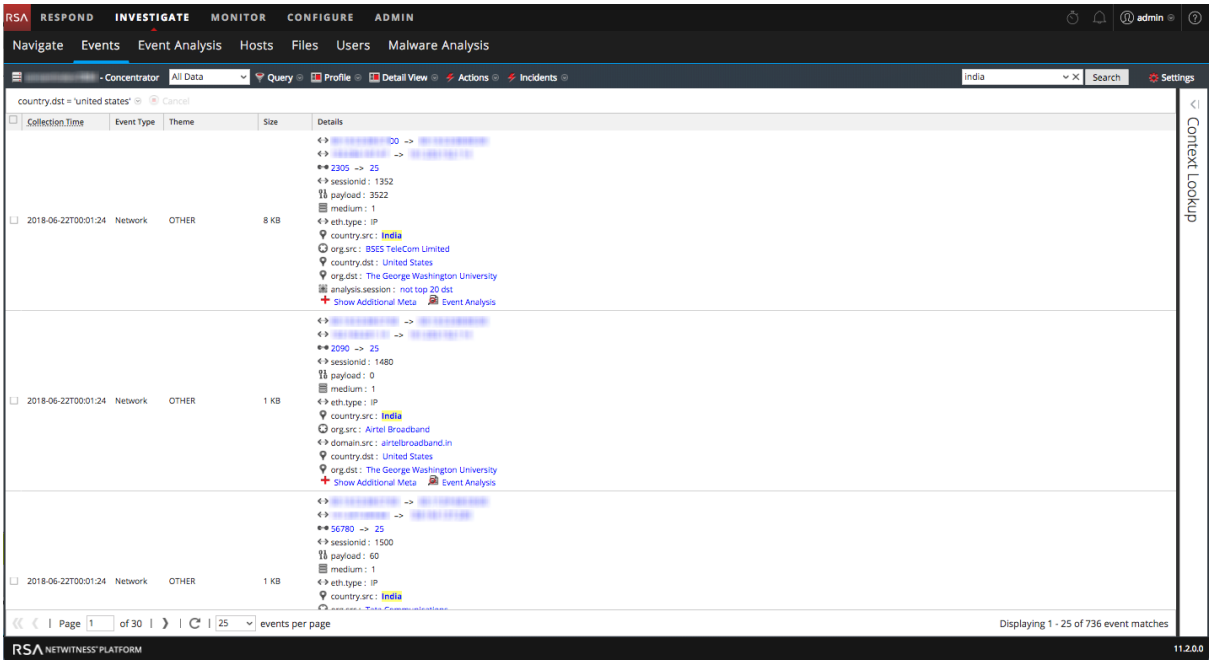
Rechercher des événements dans la vue Événements

Vous pouvez rechercher les données actives affichées dans la vue Événements en saisissant une chaîne de recherche dans le champ de recherche. La chaîne de recherche peut être une regex (expression régulière) ou une recherche de texte simple. fournit des informations détaillées sur ces types de recherche.

Pour effectuer une recherche dans les données affichées dans la vue Événements :

1. Pour exécuter la recherche, placez le curseur dans la zone de recherche, saisissez une chaîne de recherche, puis appuyez sur la touche **Entrée** ou cliquez sur **Rechercher**.
Les résultats de la recherche s'affichent dans la vue Événements. Les événements qui correspondent aux critères de recherche s'affichent dans la grille de la vue Événements. Dans la vue Détails et la vue Liste, les correspondances sont mises en surbrillance dans la colonne Détails. De plus, lors de la recherche des données BRUTES, les correspondances sont mises en surbrillance dans la vue Log - colonne Logs. Voici un exemple des résultats de la recherche du terme **India** dans la vue Détails des

événements. Notez que les correspondances de recherche ne sont pas mises en surbrillance dans une reconstruction d'événement.



2. Si vous souhaitez affiner la recherche, modifiez la requête et l'heure, comme décrit ci-dessus dans la rubrique Filtrer les événements affichés dans la vue Événements.
3. Si vous souhaitez arrêter la recherche et revenir à la vue Événements, cliquez sur **Annuler**.
   Les résultats déjà affichés restent à l'écran.
4. Pour effacer la zone de recherche et revenir à la vue Événements normale, cliquez sur **X** dans la zone de recherche.

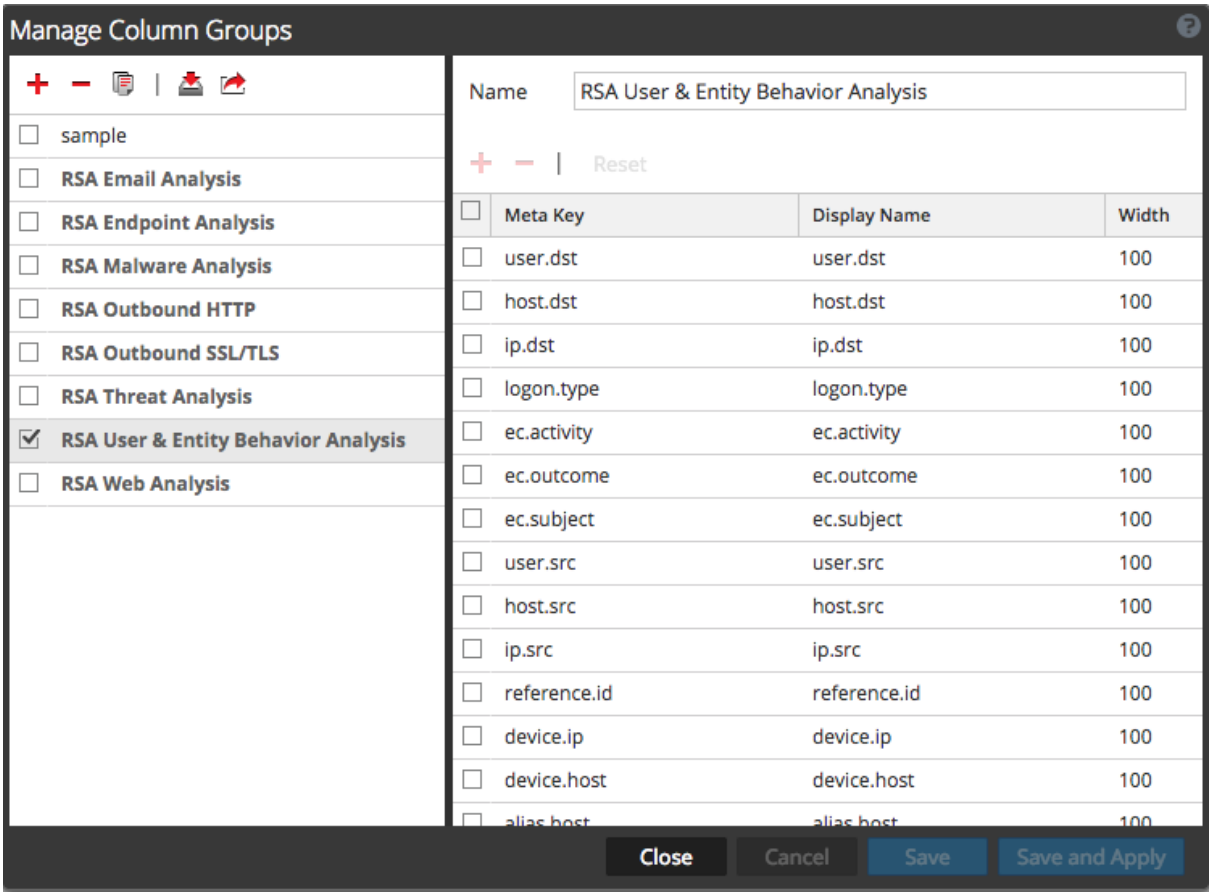
Gérer des groupes de colonnes dans la vue Événements

Lors de l'affichage d'une liste d'événements dans la vue Événements, vous pouvez personnaliser la façon dont les données s'affichent en définissant l'affichage des clés méta dans une colonne, la position de la colonne dans la grille et la largeur par défaut de la colonne.

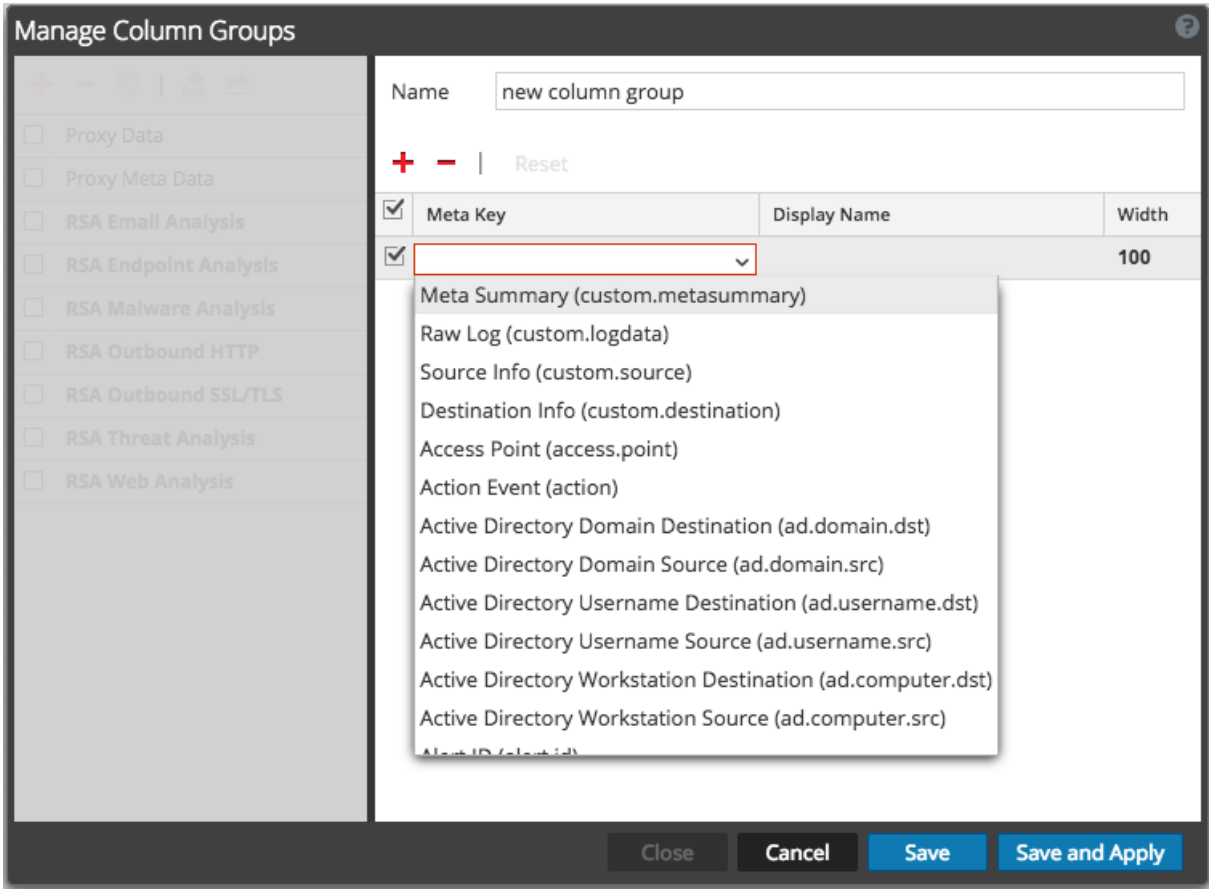
Remarque : Dans la version 11.1 ou supérieure, chaque fois que les clés méta sont utilisées, vous pouvez également utiliser des entités méta configurées.
Les profils Enquêter peuvent inclure des groupes de colonnes personnalisés. Si un groupe de colonnes personnalisé est utilisé dans un profil et si vous affichez des événements dans la vue Événements avec un groupe de colonnes personnalisé, vous ne pouvez pas modifier le type de vue (Détails, Liste ou Log).

Créer un groupe de colonnes personnalisé

1. Go to **NAVIGUER** > **Événements**.
2. Sélectionnez **Gérer les groupes de colonnes** dans le menu déroulant **Vue**. L'option Vue porte le nom de la valeur en cours, par exemple, Vue Détails, Vue Liste, Vue Log ou le groupe de colonnes sélectionné.
   La boîte de dialogue Gérer les groupes de colonnes s'affiche.

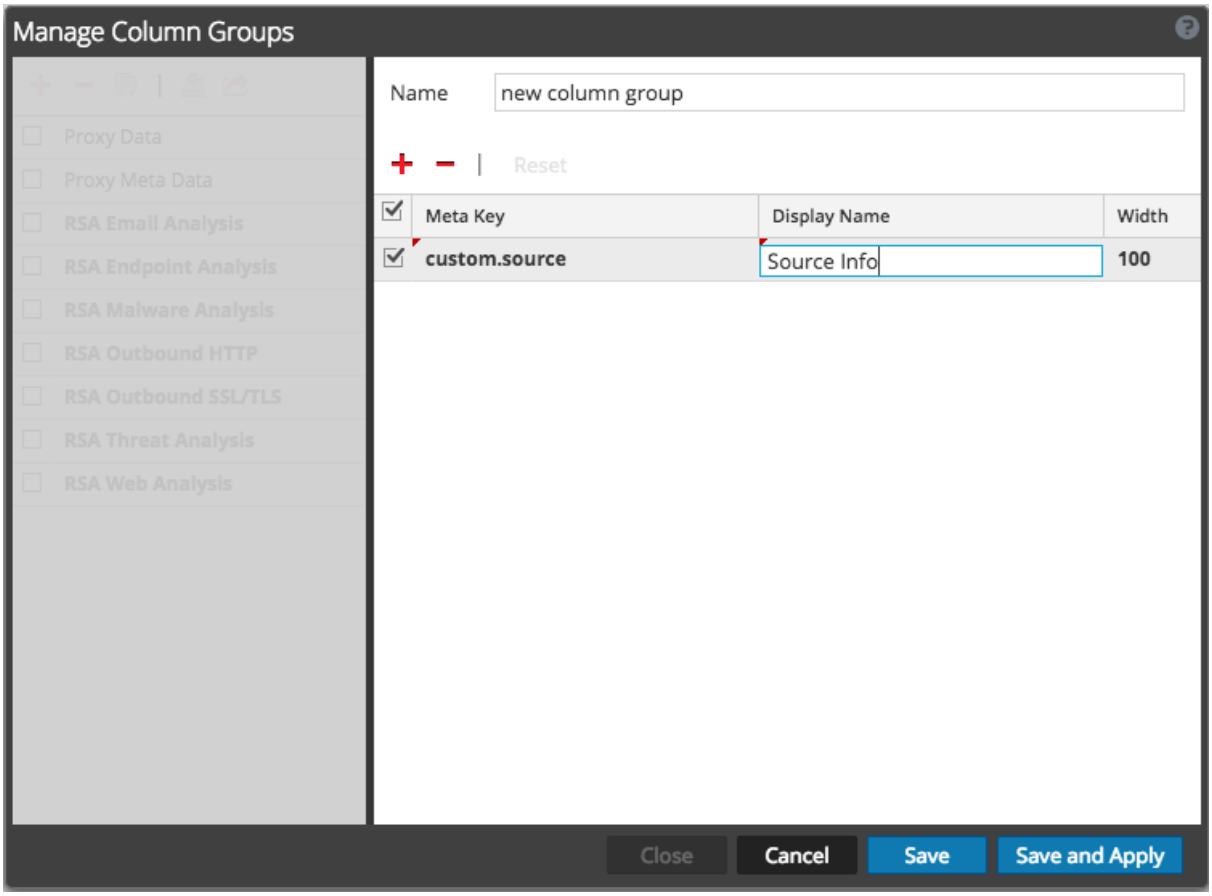


3. Pour ajouter un nouveau groupe de colonnes dans le panneau Groupe de colonnes, cliquez sur + et saisissez le nom du nouveau groupe dans le champ qui en résulte.
   Le panneau de définition de colonne s'ouvre sur la droite avec le nom de groupe rempli. Vous pouvez modifier ce dernier.
4. Pour ajouter une colonne au groupe, cliquez sur + et cliquez dans le champ **Clé méta** vide pour afficher la liste déroulante **Clé méta**. Sélectionnez un champ de clé méta dans la liste et répétez cette étape jusqu'à ce que l'ensemble de colonnes soit terminé.



5. (Facultatif) Pour supprimer une clé méta du groupe de colonnes, cliquez sur −.
6. (Facultatif) Pour réorganiser l'ordre dans lequel les colonnes apparaissent dans la liste Événements, faites glisser les clés méta à l'emplacement souhaité.

7. (Facultatif) Pour définir la largeur par défaut pour une colonne, cliquez sur la valeur correspondante dans la colonne **Largeur** et saisissez une nouvelle largeur de colonne.

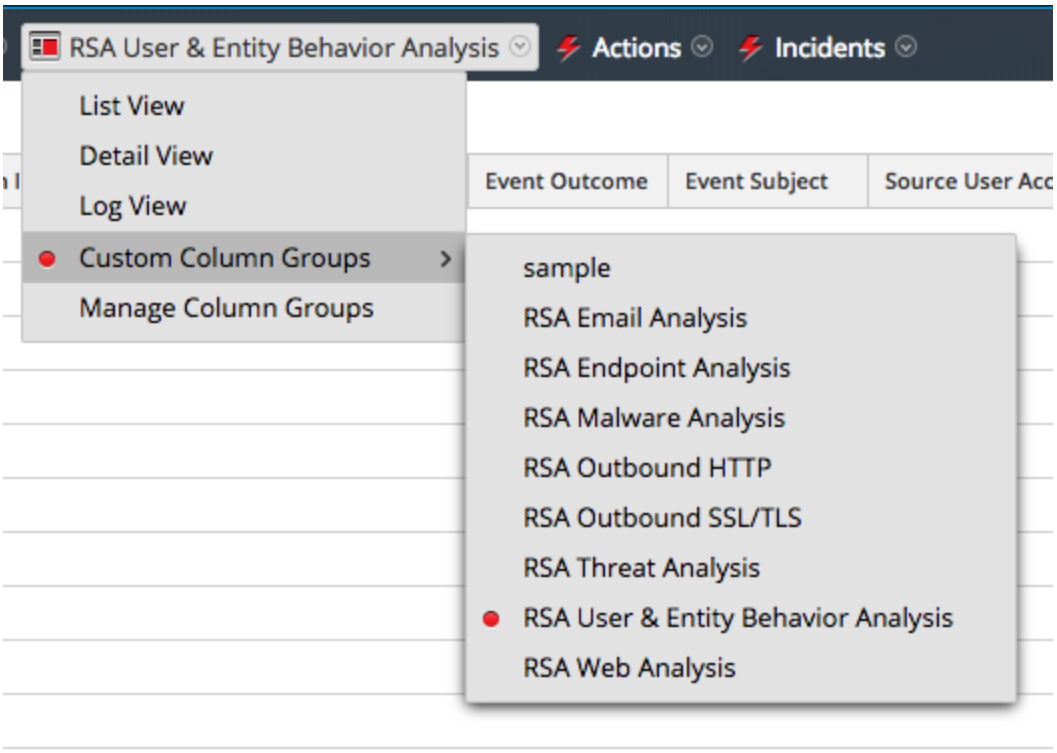


8. (Facultatif) Pour rétablir les paramètres précédents pour le groupe de colonnes et annuler toutes vos modifications, cliquez sur **Réinitialiser**.
9. Lorsque vous êtes prêt à sauvegarder, procédez de l'une des manières suivantes :
   a. Pour enregistrer le groupe de colonnes modifié et actualiser la vue Événements avec les paramètres du groupe de colonnes, cliquez sur **Enregistrer et appliquer**.
   b. Pour enregistrer le groupe de colonnes modifié sans actualiser la vue Événements, cliquez sur **Enregistrer**.

Sélectionner un groupe de colonnes

Pour sélectionner un groupe de colonnes :

1. Dans la vue Événements ouverte, sélectionnez **Groupes de colonnes personnalisées** dans le menu déroulant **Vue**. Le nom de l'option est la valeur par défaut (vue Détails ou valeur actuelle).



2. Sélectionnez l'un des groupes de colonnes dans le sous-menu.
   La vue Événements est actualisée pour refléter le groupe de colonnes personnalisé.

Exporter les événements dans la vue Événements

Dans la vue Événements, le menu Actions comporte une option pour exporter des événements à partir de l'événement consulté vers une archive.

Remarque : Vous ne pouvez exporter que les fichiers sur lesquels vous disposez de droits d'accès ou d'affichage.

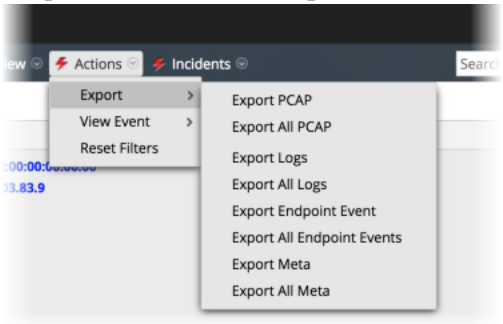
La fonction d'exportation recherche dans le service toutes les sessions comprises dans la période et le point d'extraction sélectionnés afin d'extraire le contenu de chaque session. Les détails exportés sont affectés par la plage temporelle et le point d'extraction au moment de l'exportation. Dans la boîte de dialogue Extraction de fichier, vous pouvez choisir d'exporter :

- Des PCAP
- Des logs
- Un événement NetWitness Endpoint
- Des valeurs méta

Le format de l'archive exportée : Fichier ZIP ou GZIP. Une fois la requête envoyée, une tâche est planifiée. Vous pouvez alors la suivre dans la barre d'état Tâches. En cas de problème de récupération du journal ou du fichier PCAP auprès du service, NetWitness Platform affiche une notification d'erreur.

Pour extraire les fichiers d'un événement :

1. Dans la **vue Événement**, cliquez sur un événement.
2. Cliquez sur **Actions** > **Exporter**.



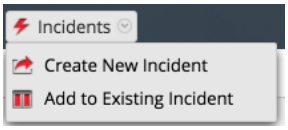
3. Sélectionnez l'option d'exportation et le format du fichier.
   Un message vous informe que les données sélectionnées sont en cours de téléchargement.

Ajouter des événements à un incident pour obtenir une réponse

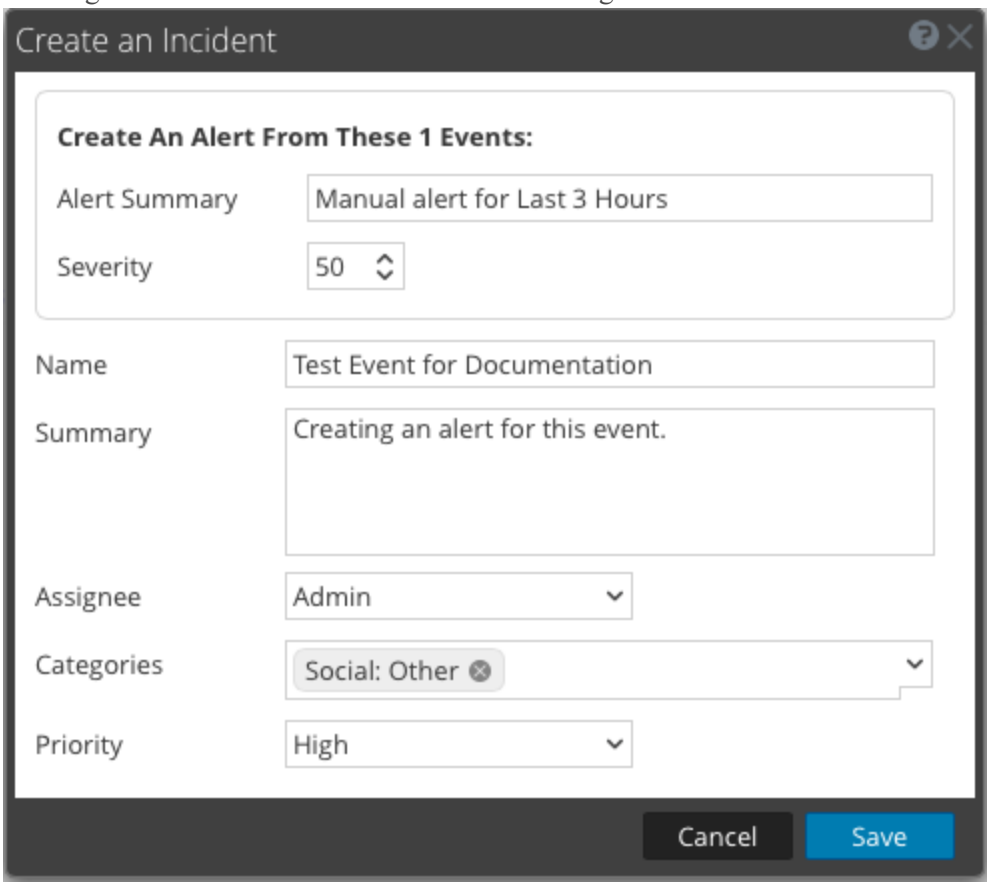
Lors d'une procédure d'enquête dans Vue Événements, vous pouvez sélectionner un ou plusieurs événements et créer un incident qui est disponible pour les responsables de la réponse aux incidents dans Répondre. Vous pouvez également ajouter des événements à un incident existant dans Répondre, auquel vous avez accès.

Remarque : Un administrateur doit configurer les rôles et autorisations appropriés, comme indiqué dans « Autorisations du rôle » et « Gérer les utilisateurs avec des rôles et des autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

1. Accédez à **ENQUÊTER** > **Événements**.
2. Dans la vue Événements, sélectionnez un ou plusieurs événements, puis **Incidents** > **Créer un nouvel incident**.



3. Renseignez les informations dans la boîte de dialogue Créer un incident.



a. Sélectionnez le niveau de gravité, un entier compris entre 1 et 100, 100 étant le plus élevé.

b. Saisissez le nom de l'incident et décrivez-le dans le champ **Récapitulatif**.

c. Dans la liste déroulante, sélectionnez une personne affectée pour l'incident. Cette liste répertorie les rôles intégrés qui ont accès à Répondre, ainsi que des rôles personnalisés qui ont été ajoutés à votre système. Par exemple, cette liste peut inclure des rôles d'administrateur, analyste, dpo, opérateur et rôles pour les responsables de la réponse aux incidents.

d. À partir de la liste déroulante **Catégories**, sélectionnez une ou plusieurs catégories d'alertes qui s'appliquent à cet incident.

e. À partir de la liste déroulante **Priorités**, sélectionnez une catégorie pour l'incident. Par exemple, un incident peut avoir une priorité critique, élevée, moyenne ou faible.

f. Cliquez sur **Enregistrer**.
Le nouvel incident est créé et est disponible immédiatement dans les files d'attente d'incident pour le rôle sélectionné dans Répondre.

4. Pour ajouter un ou plusieurs événements à un incident, sélectionnez un ou plusieurs événements, puis **Incidents > Ajouter à un incident existant**.

5. Dans la boîte de dialogue Ajouter des événements à un incident, sélectionnez la gravité et sélectionnez un ou plusieurs incidents auxquels les événements seront ajoutés. Vous pouvez rechercher un incident existant par ID d'incident ou nom d'incident. Lorsque vous êtes prêt, cliquez sur **Ajouter à l'incident**.
Les événements sont ajoutés aux incidents sélectionnés et mis à jour dans Répondre.

Associer des événements à partir de sessions partagées

Les analystes peuvent identifier les sessions qui ont été fractionnées en raison de leur taille dans la vue Événements, et de combiner les sessions fragmentées de sorte que la session complète soit visible sous la forme d'un résultat de requête unique dans la vue Événements. Lorsque des sessions partagées sont rassemblées, une exportation de paquet de la session dans la vue Événements comprend tous les fragments de session.

La version 10.4 et les versions antérieures des composants Decoder sont configurées avec une taille de session par défaut de 32 Mo. Lorsqu'une session dépasse la limite de 32 Mo, le Decoder fragmente la session pour que tous les paquets suivants fassent partie d'une nouvelle session, ce qui fragmente réellement la session réseau en plusieurs sessions Decoder. Les sessions fractionnées sont analysées sans tenir compte du fait qu'il s'agit d'un fragment de la plus grande session réseau, entraînant parfois des fragments de session avec des adresses et des ports source et de destination inversés et avec des protocoles d'application non identifiés. L'autre conséquence des sessions fractionnées peut être la difficulté à afficher tous les fragments de session sous la forme d'un résultat de requête unique, ou de créer un export de paquet unique de tous les fragments de session.

Les améliorations apportées au Decoder dans NetWitness Platform 10.5 fournissent un meilleur traitement des sessions fragmentées :

- Analyse contextuelle des fragments.
- Mise en évidence des fragments de session.
- Recherche des fragments de session.
- Exportation de tous les paquets sous forme de fichier PCAP unique.

Analyse contextuelle des fragments

Le Decoder effectue l'analyse de la session avant de la fractionner en fonction de la taille de session maximale configurée (32 Mo) ou du délai d'attente configuré (60 secondes). Une fois l'analyse terminée, les résultats obtenus indiquent la direction d'adresse et le protocole d'application appropriés, qui sont propagés à chaque fragment de session suivant pour assurer la cohérence avec la session de réseau logique qu'ils représentent.

Remarque : Tous les paramètres de configuration correspondants du Decoder sont modifiés lors de la mise à niveau vers la version 10.5. Cependant, le paramètre Rechercher des fragments de session exige que les clés méta des ports source tcp et udp (tcp.srcport et udp.srcport) soient entièrement indexés, ce qui n'était pas la configuration par défaut dans les versions antérieures à SA 10.5. Cela limite de manière fonctionnelle la capacité à rechercher des fragments de session dans les sessions capturées après la mise à niveau du Decoder vers la version 10.5.

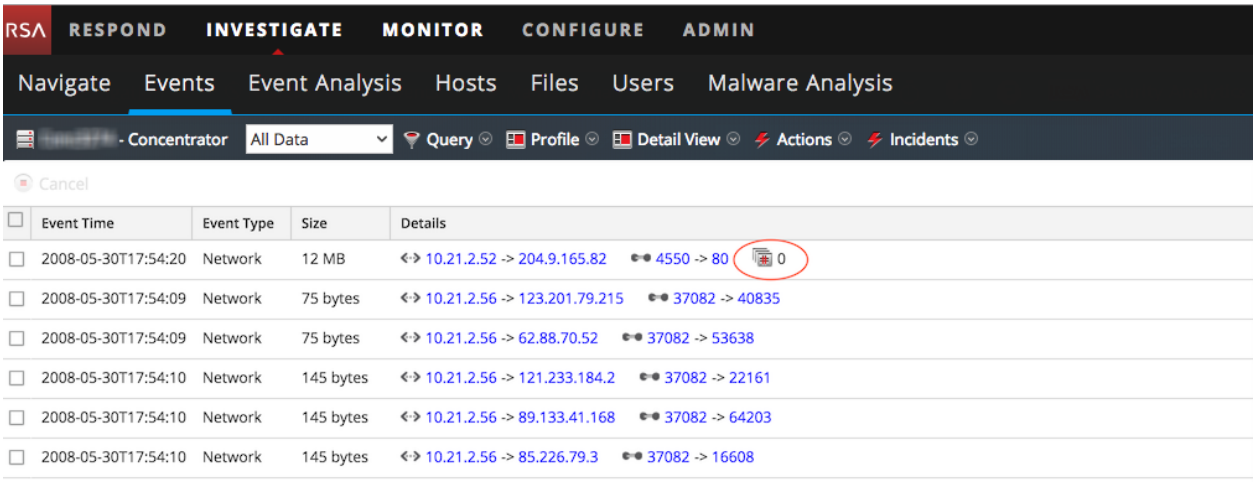
Mise en évidence des fragments de session

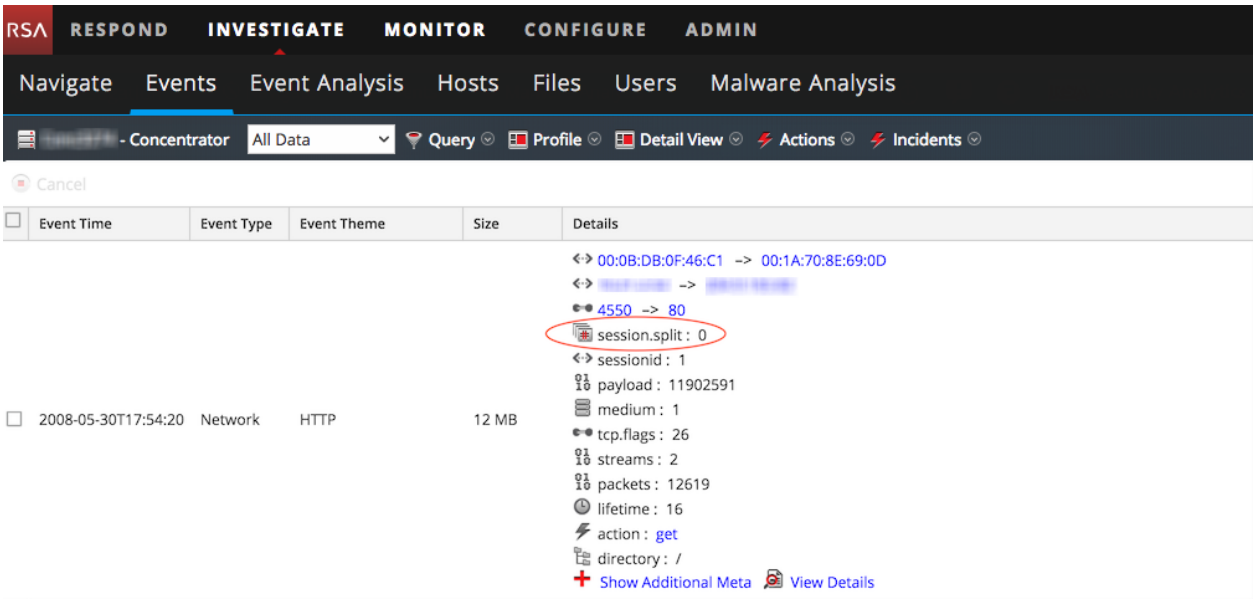
Chaque fragment de session dispose d'un élément méta supplémentaire, `session.split`. La valeur de l'élément méta `session.split` pour un fragment de session donné indique le nombre de fragments qui précèdent ce fragment. Lors de l'affichage des sessions dans la vue Événements, l'élément méta `session.split` identifie clairement les sessions qui sont des fragments dans la vue Liste des événements et la vue Détails des événements.

Le fractionnement de la session se produit lorsque le Decoder configuré `assembler.size.max` ou `assembler.timeout.session` (latence entre les sessions) est atteint. Le premier fragment est la session 0 et les sessions avec un horodatage ultérieur sont numérotées de manière incrémentielle : 1, 2, 3, etc. Le méta `session.split` indique le nombre de fragments de sessions précédents ; cependant, cela ne signifie pas toujours qu'il y a des fragments de session ultérieurs, même avec une valeur 0. Il est également possible que le premier fragment de la session n'ait pas de l'élément méta `session.split` si la session est analysée avant de dépasser la taille maximale de session.

En affichant les fragments de session, vous pouvez déterminer la taille maximale de la session ou la temporisation de session nécessaire pour l'analyse en vue de combiner les sessions fractionnées en une seule session. Par exemple, si vous avez quatre fragments de 32 Mo, vous devez configurer votre Decoder de test (généralement une machine virtuelle configurée distincte du service de production principal) avec une taille maximale de session supérieure à 128 Mo. Les étapes sont les mêmes que pour la recherche des fragments basée sur un délai d'expiration de session. Les figures ci-dessous montrent la vue Liste des événements et la vue Détails des événements avec des informations de sessions fragmentées en surbrillance.

Remarque : Une taille de session de 12 Mo maximum a été configurée au moment de la création des captures d'écran ci-dessous.





Les métadonnées `session.split` sont toujours affichées immédiatement après les métadonnées d'adresse et de port dans la vue Détails. Elles ne sont jamais masquées en tant que métadonnées supplémentaires. Ces améliorations permettent d'effectuer les opérations suivantes rapidement :

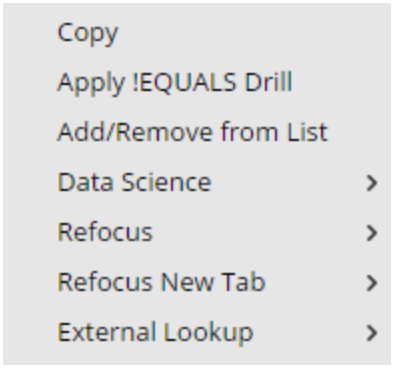
- Identifier les sessions qui sont des fragments de sessions réseau.
- Afficher tous les fragments de session d'une session réseau avec un fragment de session unique.
- Exporter les paquets de toute la session réseau sous forme de fichier PCAP unique.

Rechercher et associer des fragments

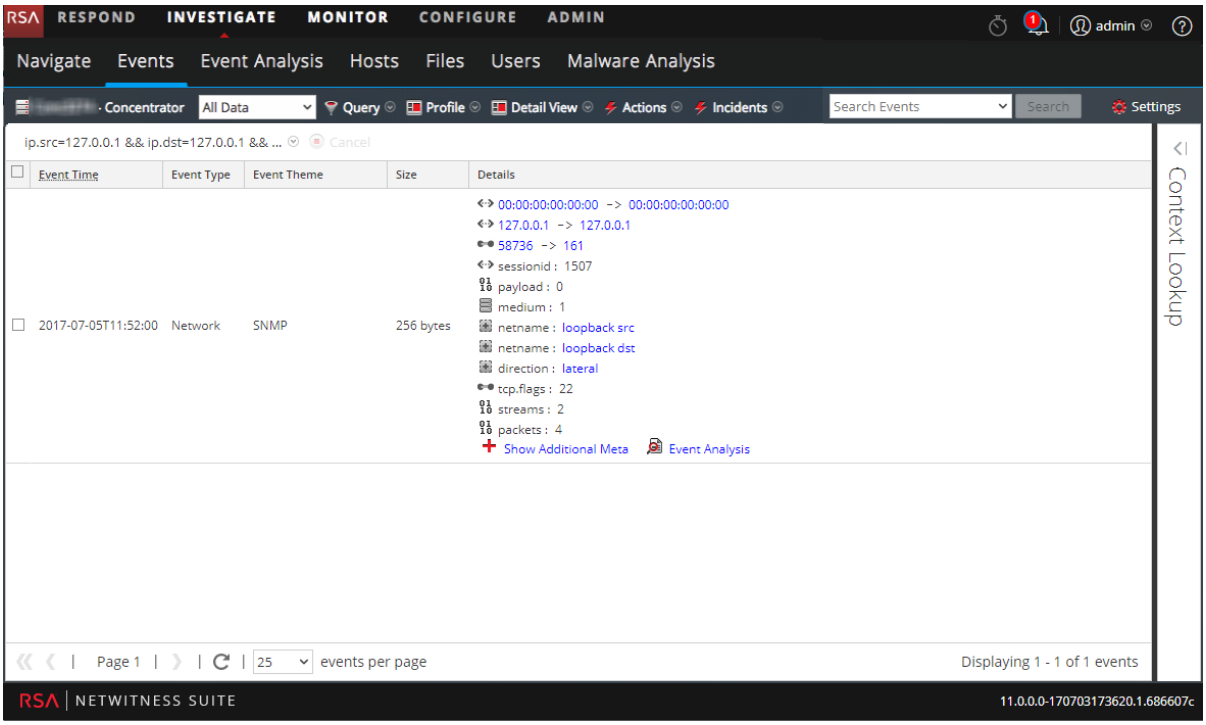
Depuis la vue Événements, vous pouvez trouver les fragments d'une session en utilisant l'option du menu contextuel Recentrer > Rechercher des fragments de session. NetWitness Platform crée une requête en utilisant les ports et les adresses source et de destination de la session sélectionnée, et affiche toutes les sessions qui correspondent à cette requête pendant la période en cours.

Pour rechercher des fragments de session :

1. Dans la vue **Événements**, cliquez avec le bouton droit sur l'une des valeurs d'adresses et de ports source et de destination : `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport` et `udp.dstport`), ainsi que sur les valeurs `session.split`.
   Le menu contextuel s'affiche.



2. Sélectionnez **Recentrer > Rechercher des fragments de session** ou **Recentrer le nouvel onglet > Rechercher des fragments de session**.
   NetWitness Platform remplit la liste des événements avec des fragments de session pour une session unique au sein de la période en cours. Selon l'option que vous avez sélectionnée, le recentrage remplace l'affichage en cours ou s'ouvre dans un nouvel onglet. (Toutes les données sont utilisées dans ces exemples, mais elles ne sont pas recommandées sur les systèmes de production).



3. Si nécessaire, ajustez la période pour inclure des fragments de session qui peuvent précéder ou suivre la période en cours. Vous pouvez définir que la période doit être étendue si les fragments se produisent à la limite du temps imparti, surtout si le premier fragment visible n'a pas la valeur de fraction 0 (aucune). Autrement, l'inspection des paquets de la dernière session visible peut vous amener à croire que la session continue. Voici un exemple :

   a. Si vous êtes à la recherche de fragments qui ne sont évidemment pas le premier fragment, par exemple, 1, 2, 3 et 4 entre 10:30 et 10:35, il devrait y avoir un fragment 0. Vous pouvez augmenter la période pour commencer plus tôt (dans ce cas, 10:25) pour trouver le fragment supplémentaire.

   b. Si la taille de la session du dernier fragment est proche de la taille maximale de session (12 Mo dans cet exemple), recherchez les fragments supplémentaires en augmentant la période en vue de repousser l'heure (dans cet exemple, 10:40).
      Lorsque tous les fragments de session d'une session réseau sont inclus dans une liste d'événements unique, la liste peut s'étendre sur plusieurs pages.

4. (Facultatif) Pour exporter les paquets de chaque fragment de session sous forme de fichier PCAP unique, sélectionnez **Actions > Exporter tous les PCAP**.

Un message vous informe que le PCAP est en cours de téléchargement. Lorsque le téléchargement est terminé, le fichier PCAP comprend toute la session réseau qui a été fragmentée.

Interrogation et action sur les données dans les vues Naviguer et Événements

Cette rubrique décrit les modes d'interrogation de données et d'action sur les résultats communs dans la vue Naviguer et la vue Événements. Les analystes peuvent :

- Rechercher des modèles de texte
- Créer une requête personnalisée
- Afficher et modifier des requêtes avec l'intégration URL
- Utiliser des profils pour encapsuler les vues personnalisées
- Gérer Listes Context Hub et Valeurs de la liste dans les vues Naviguer et Événements
- Rechercher un contexte supplémentaire dans les vues Naviguer et Événements
- Reconstruire un événement

Créer une requête personnalisée

Dans la vue Enquêter > Naviguer ou Événements, vous pouvez créer une requête au lieu de cliquer sur les clés méta et les valeurs pour accéder jusqu'aux métadonnées. Les boîtes de dialogue pour créer une requête offrent une aide à la syntaxe grâce à des listes déroulantes de clés méta applicables et d'opérateurs. Lors de l'affichage de la liste déroulante, vous pouvez développer et réduire chaque métagroupe pour afficher ou masquer les clés métas individuelles de ce groupe.

Remarque : Dans la version 11.1 ou supérieure, vous pouvez effectuer des requêtes sur les entités méta, ainsi que les clés méta.

Lorsque vous sélectionnez un groupe méta, NetWitness Platform génère une requête complexe équivalant à une requête contenant toutes les clés méta regroupées dans ce groupe avec l'opérateur OR. Par conséquent, si un groupe méta contient `ip.src` et `ip.dst`, la requête générée est `ip.src = <value> OR ip.dst = <value>`. Si le groupe méta contient des clés méta qui comportent différents types de métavaleurs, l'entrée de la valeur est désactivée et la requête utilise des instructions `exists`. Par exemple, un groupe méta qui contient `ip.src`, `ip.dst` et `alias.host` inclut des clés méta qui comportent différents types de valeurs ; `ip.src` et `ip.dst` sont des adresses IP et `alias.host` est du texte. La requête générée est `ip.src exists OR ip.dst exists OR alias.host exists`.

Une requête de base se présente sous la forme suivante :

```
<metakey> <operator> [<metavalue>]
```

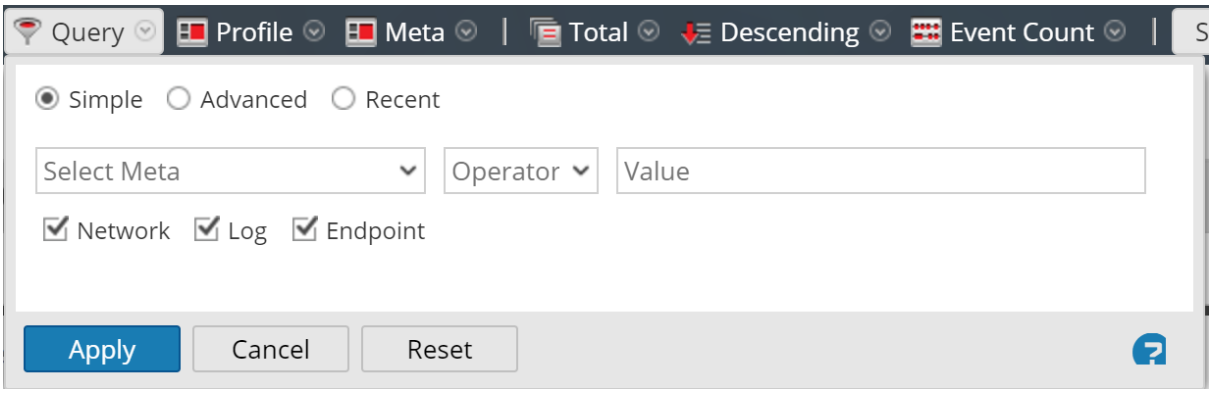
Voici quelques exemples :

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Créer une requête en utilisant la méthode de base

Lorsque vous créez une requête en utilisant la méthode de base, NetWitness Platform fournit des listes déroulantes de métadonnées et d'opérateurs.

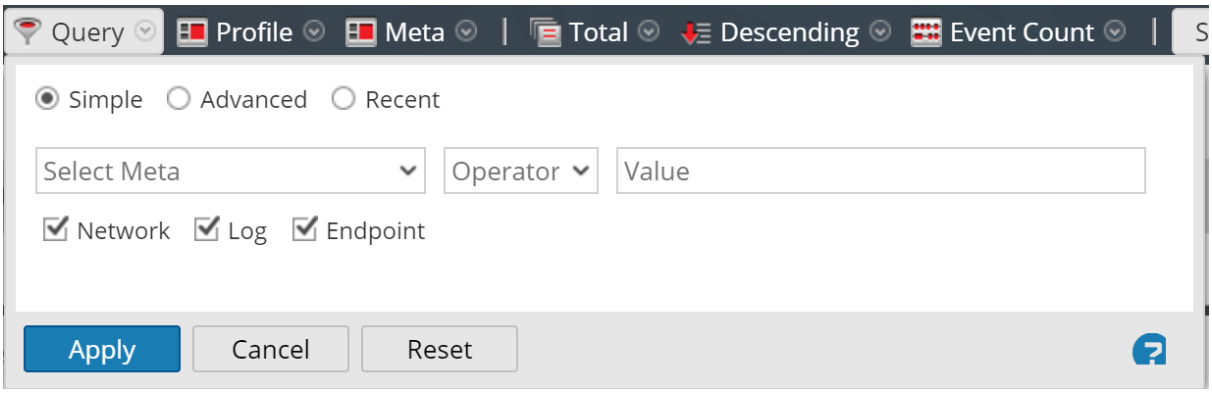
1. Dans la barre d'outils de la **vue Naviguer**ou de la **Vue Événements**, sélectionnez **Requête.**
   La boîte de dialogue Requête s'affiche avec l'option Simple sélectionnée.



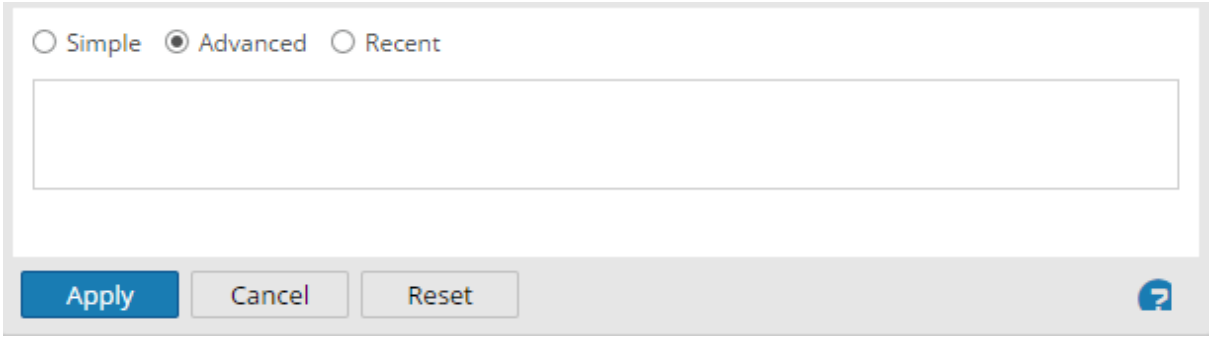
2. Dans le champ **Sélectionner les méta**, cliquez pour afficher la liste déroulante. La liste déroulante comporte deux sections : Groupes méta et Toutes les méta.
3. Sélectionnez une clé méta unique dans **Toutes les méta** ou sélectionnez un groupe méta dans **Groupes méta**. Vous pouvez également saisir une clé méta ou un métagroupe dans le champ.
4. Dans le champ **Opérateur**, saisissez un opérateur ou cliquez sur la liste déroulante pour sélectionner un opérateur valide.
5. (Facultatif) Si vous avez sélectionné un opérateur qui nécessite une valeur, par exemple, begins dans le troisième champ, saisissez la valeur de la clé méta.
6. Dans les cases à cocher Réseau, Log et Point de terminaison, choisissez le type de données à interroger. Exécutez l'une des opérations suivantes :
   a. Pour limiter la requête aux paquets, sélectionnez **Réseau** et désélectionnez **Log** et **Point de terminaison**.
   b. Pour limiter la requête aux logs, sélectionnez **Log** et désélectionnez **Réseau** et **Point de terminaison**.
   c. Pour limiter la requête aux événements de point de terminaison, sélectionnez **Point de terminaison** et désélectionnez **Réseau** et **Point de terminaison**.
   d. Pour appliquer la requête aux paquets, aux logs et aux points de terminaison, sélectionnez **Réseau**, **Log** et **Point de terminaison**.
7. Exécutez l'une des opérations suivantes :
   a. Cliquez sur **Apply**.
   La fenêtre est fermée et la vue est mise à jour avec les résultats de la nouvelle requête. La requête s'affiche dans le fil d'Ariane.
   b. Cliquez sur **Annuler**.
   La fenêtre est fermée et aucun changement n'est apporté à la vue ou à la requête en cours.

Créer une requête en utilisant la méthode avancée

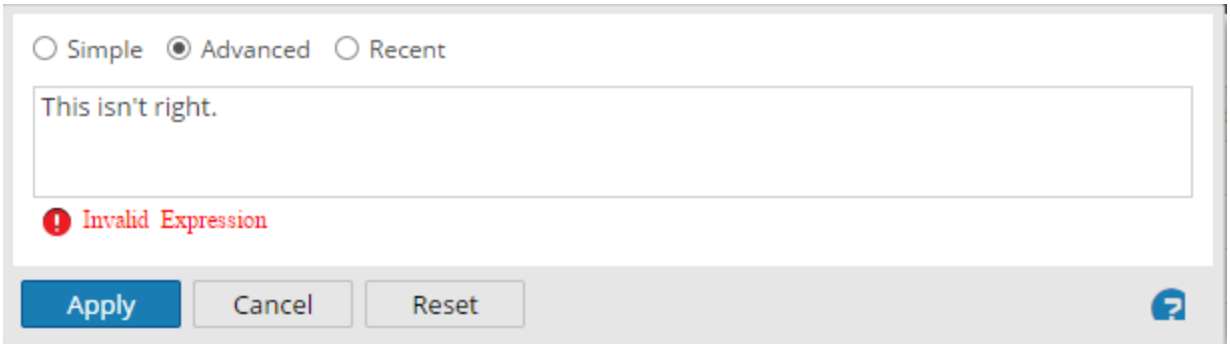
1. Dans la barre d'outils de la **vue Naviguer** ou de la vue Événements, sélectionnez **Requête.**
   La boîte de dialogue Requête s'affiche.



2. Sélectionnez **Avancée**.
   Le champ Requête avancée s'affiche.



3. Dans le champ, créez une requête qui peut inclure la clé méta, l'opérateur et la valeur. Lorsque vous commencez à saisir une clé méta dans le champ, une liste déroulante des clés métas disponibles du service sélectionné s'affiche.
4. Sélectionnez la clé méta pour votre requête.
   L'affichage se met à jour. Si l'expression n'est pas encore terminée, l'état indique que la requête n'est pas valide.
5. Continuez avec un opérateur, dans la liste déroulante, puis une valeur si nécessaire. L'affichage se met à jour pendant que vous continuez à saisir la requête. Si vous saisissez un opérateur, comme **exists** ou **!exists**, qui n'utilise pas le champ Valeur, celui-ci est désactivé et l'état non valide est effacé. Si vous saisissez un opérateur, comme =, qui exige le champ Valeur, l'état reste défini sur non valide jusqu'à ce que vous entriez une valeur. Lorsque la requête est valide, l'état non valide ne s'affiche plus.

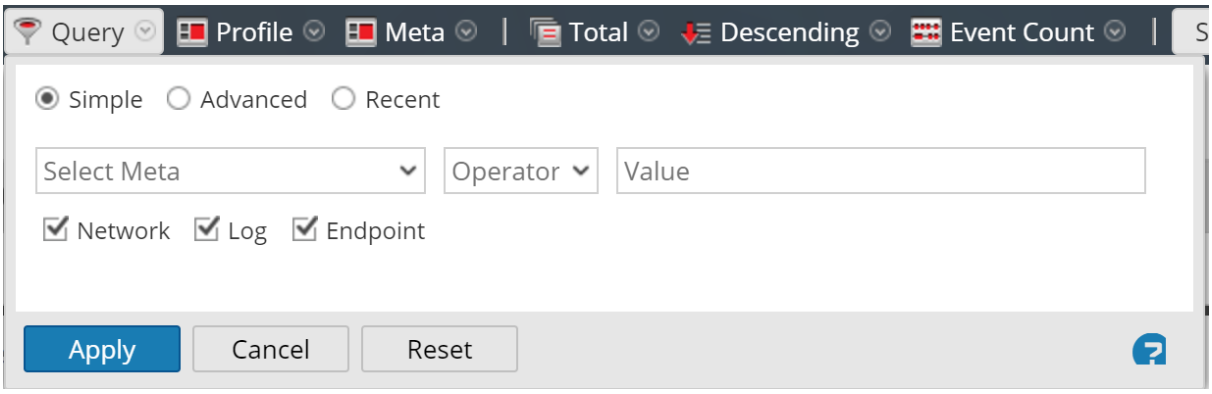


6. Exécutez l'une des opérations suivantes :
   - Cliquez sur **Apply**.
     La fenêtre est fermée et la vue est mise à jour avec les résultats de la nouvelle requête. La requête s'affiche dans le fil d'Ariane.
   - Cliquez sur **Annuler**.
     La fenêtre est fermée et aucun changement n'est apporté à la vue ou à la requête en cours.

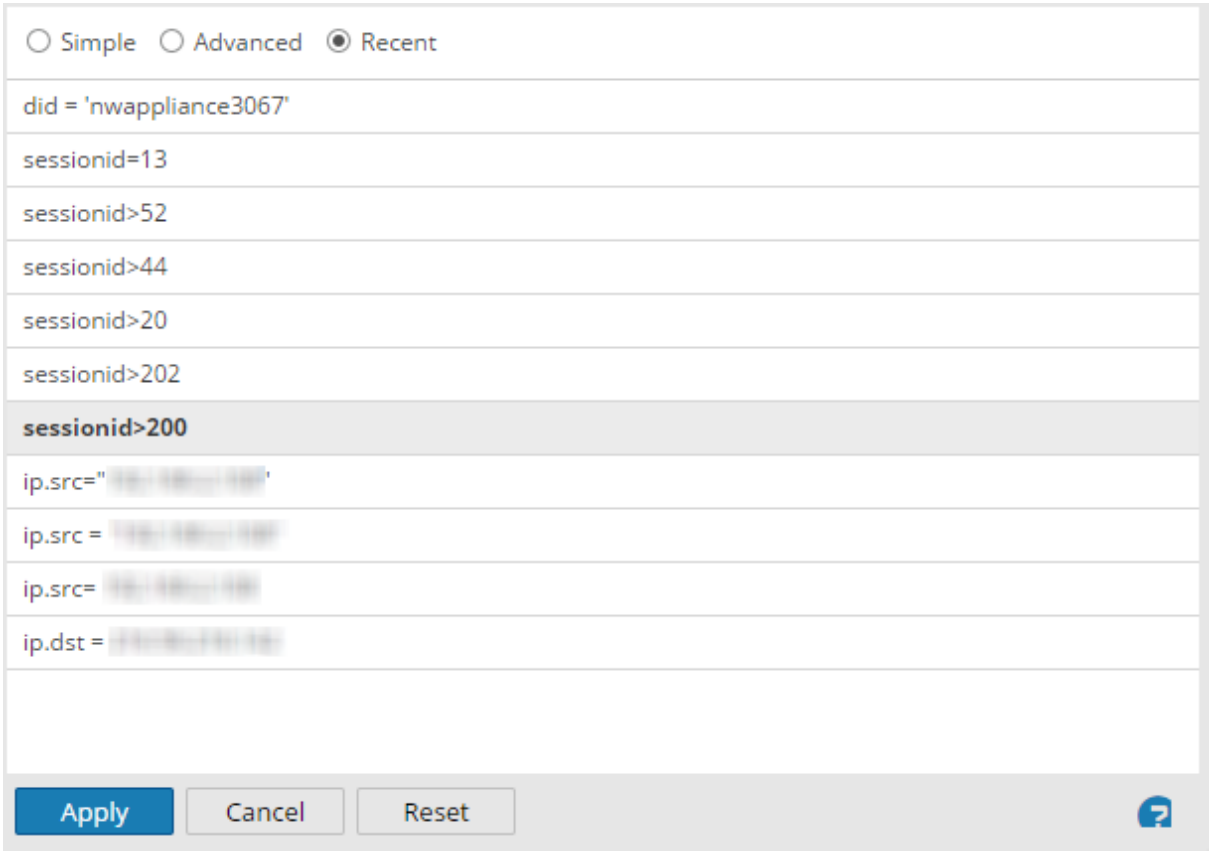
Appliquer une requête récente

Vous pouvez afficher les requêtes récentes et en sélectionner une à appliquer au service actuel à l'étude. Pour sélectionner une requête récente :

1. Dans la barre d'outils de la **vue Naviguer** ou de la vue Événements, sélectionnez **Requête.**
   La boîte de dialogue Requête s'affiche avec l'option Simple sélectionnée.



2. Sélectionnez l'option **Récente**.
   La liste des requêtes récentes s'affiche dans la partie inférieure de la boîte de dialogue.



3. Dans la liste des requêtes récentes, cliquez sur une requête pour la sélectionner.
4. Exécutez l'une des opérations suivantes :
   - Double-cliquez sur une requête.
   - Sélectionnez une requête, puis cliquez sur **Appliquer**.
     La fenêtre est fermée et la vue est mise à jour avec les résultats de la nouvelle requête. La requête s'affiche dans le fil d'Ariane.
   - Cliquez sur **Annuler**.
     La fenêtre est fermée et aucun changement n'est apporté à la vue ou à la requête en cours.

Gérer Listes Context Hub et Valeurs de la liste dans les vues Naviguer et Événements

Les analystes peuvent ajouter des listes et des valeurs de liste pour l'enrichissement de Context Hub dans les vues Naviguer et Événements. (Dans la version 11.2 et versions ultérieures, les analystes peuvent ajouter des listes et des valeurs de listes dans la vue Rechercher un contexte supplémentaire dans la vue d'analyse d'événement.)

Lorsque le service Context Hub est activé et configuré, NetWitness Platform fournit des données d'enrichissement à partir d'Incident Management, des listes personnalisées et d'NetWitness Endpoint, directement dans la vue Naviguer et la vue Événements. Un repère visuel met en surbrillance les métavaleurs pour lesquelles des données d'enrichissement sont disponibles dans les vues Enquêter. Vous pouvez cliquer sur la valeur en surbrillance pour rechercher les informations de contexte et les renseignements supplémentaires.

En outre, à partir du panneau Valeurs de la vue Naviguer et de la vue Événements, vous pouvez afficher des listes, modifier les valeurs méta d'une liste existante ou créer une liste. Lorsque vous ajoutez des métavaleurs à une liste, vous pouvez enquêter sur ces métavaleurs à l'aide de l'option de recherche contextuelle.

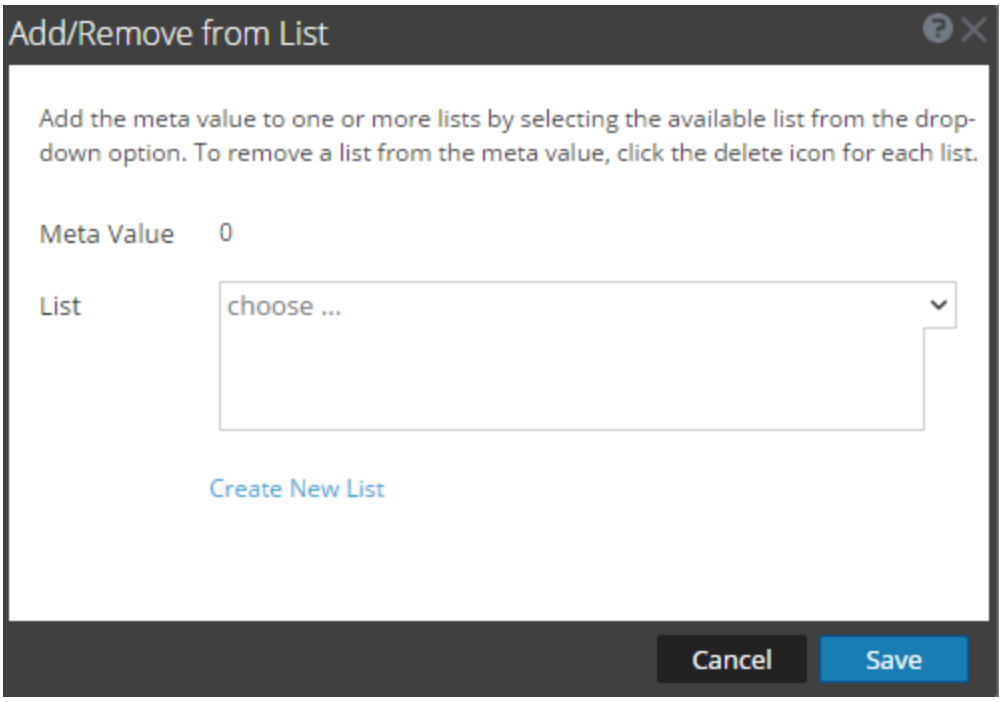
Pour permettre à un analyste de gérer des listes dans Enquêter, l'administrateur doit :

- Activer le service Context Hub.
- Attribuez un rôle d'analyste avec l'autorisation `Manage List from Investigation` à l'utilisateur qui effectue une recherche contextuelle depuis les vues Investigation.
- Configurez les rôles et autorisations appropriés, comme indiqué dans « Autorisations du rôle » et « Gérer les utilisateurs avec des rôles et des autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Ajouter des métavaleurs à une liste existante

Pour ajouter une valeur méta à une liste existante dans Context Hub :

1. Lorsque vous enquêtez sur un service dans la vue **Naviguer** ou **Événements**, cliquez avec le bouton droit de la souris sur une valeur méta (par exemple les valeurs situées sous IP Source, IP de destination ou Nom d'utilisateur), puis sélectionnez **Ajouter à la liste/Supprimer de la liste** dans le menu contextuel.
   La boîte de dialogue Ajouter à la liste/Supprimer de la liste s'affiche.



2. Dans le champ **Liste**, sélectionnez dans l'option déroulante une ou plusieurs listes auxquelles la valeur méta doit être ajoutée.
3. Cliquez sur **Enregistrer**.
   La valeur méta est ajoutée aux listes sélectionnées.

Supprimer une valeur méta d'une liste Context Hub

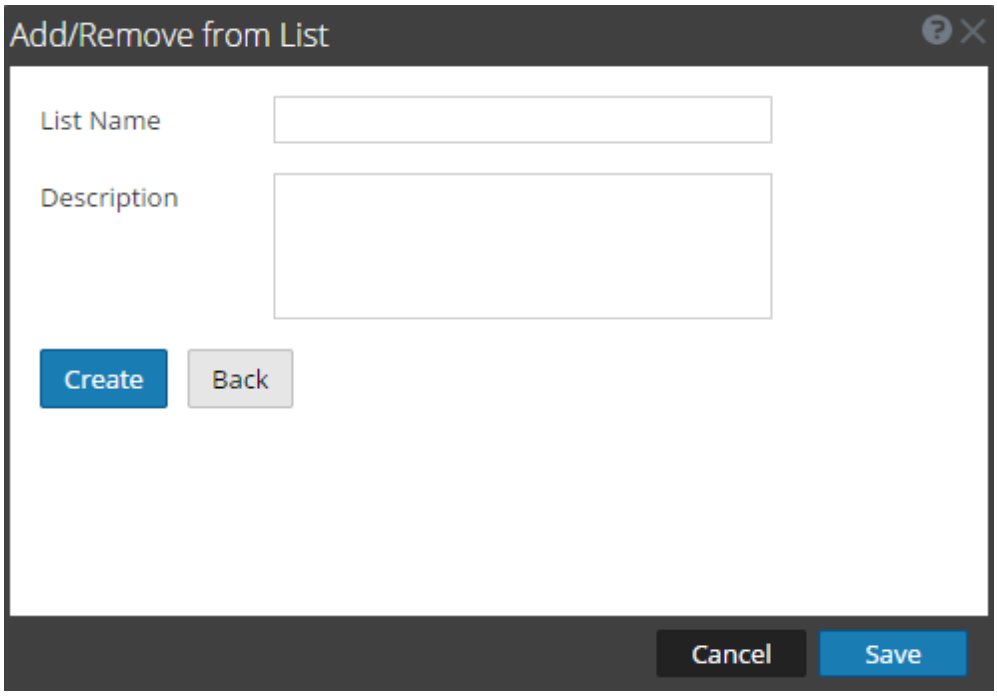
Pour supprimer une valeur méta d'une liste :

1. Dans la boîte de dialogue **Ajouter à la liste/Supprimer de la liste**, dans le champ **Liste**, affichez les listes qui comportent la valeur méta.
2. Cliquez sur l'icône de suppression (x) pour chaque liste ne devant pas inclure la valeur méta.
3. Cliquez sur **Enregistrer**.
   La valeur méta est retirée de la liste supprimée.

Créer une nouvelle liste

Pour créer une liste Context Hub dans Enquêter :

1. Dans la boîte de dialogue **Ajouter à la liste/Supprimer de la liste**, cliquez sur **Créer une nouvelle liste**.



2. Dans le champ **Nom de la liste**, saisissez un nom unique pour la liste.
3. Dans le champ **Description**, saisissez la description de la liste.
4. Cliquez sur **Créer** pour créer la liste.
5. Cliquez sur **Enregistrer** pour ajouter la valeur méta à la liste créée.
   Ces listes sont considérées comme des sources de données permettant de récupérer des informations de contexte.

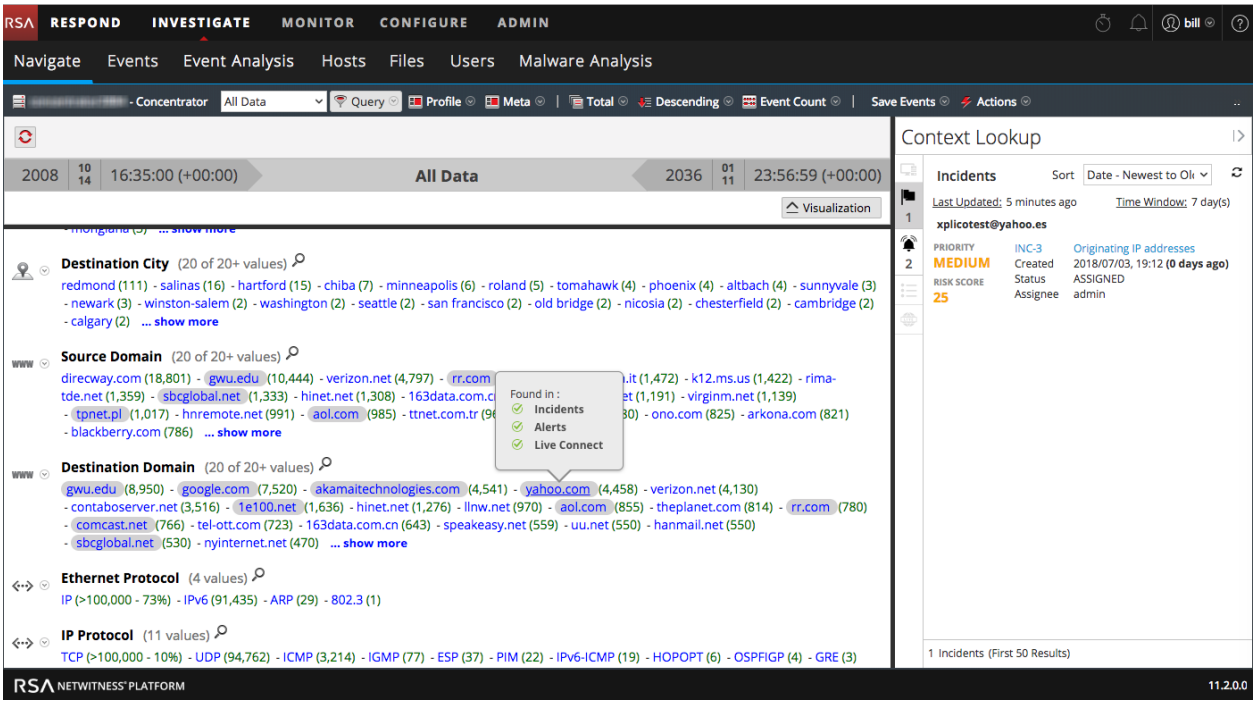
Rechercher un contexte supplémentaire dans les vues Naviguer et Événements

À partir de la vue événements et la vue Naviguer, vous pouvez consulter les détails et les renseignements sur les éléments associés à un événement dans le service Context Hub. (Dans la version 11.2 et versions ultérieures, vous pouvez également rechercher un contexte supplémentaire dans la vue Analyse d'événements, comme décrit dans Rechercher un contexte supplémentaire dans la vue d'analyse d'événement). Ces éléments, ou entités, sont des identifiants, tels qu'une adresse IP, un nom d'utilisateur, un nom d'hôte, un nom de domaine, un nom de fichier ou un hachage de fichier. Les données issues de sources configurées, comme RSA NetWitness Endpoint, peuvent vous aider à comprendre ce qui se passe.

Remarque : Pour activer l'affichage des informations contextuelles, votre administrateur doit ajouter le service Context Hub dans la plate-forme RSA NetWitness et configurer les sources de données pour le service Context Hub comme décrit dans le *guide de configuration de Context Hub*. L'analyste dispose également d'un rôle disposant de l'autorisation `Context Lookup`, comme décrit dans « Autorisations du rôle » et « Gérer les utilisateurs avec les rôles et autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Le service Context Hub est un service centralisé qui agrège les données sur les entités de plusieurs sources de données configurables. Ces données peuvent étendre votre procédure d'enquête avec un contexte supplémentaire au-delà des résultats immédiats d'une requête spécifique. Par exemple, le service Context Hub peut vous indiquer si une entité donnée a été mentionnée dans des incidents, alertes, flux ou publications de renseignements de la communauté.

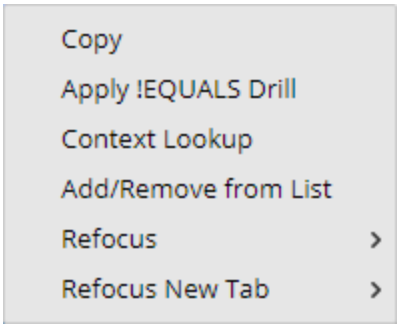
Dans la vue Naviguer et Événements, les entités ayant des données de contexte associées disponibles sont mises en surbrillance avec un arrière-plan gris ; passez sur la souris sur une entité pour afficher un récapitulatif des données disponibles. Lorsque vous cliquez avec le bouton droit sur l'entité, Context Hub interroge les sources de données configurées pour les informations pertinentes, et le panneau Recherche contextuelle s'ouvre à partir du côté droit de la fenêtre du navigateur. Le panneau Recherche contextuelle est renseigné avec les informations du service Context Hub dès que possible. Pour effectuer une autre recherche, cliquez avec le bouton droit sur une autre entité. Le panneau Recherche contextuelle est mis à jour avec les informations de cette entité.



Dans le panneau Recherche contextuelle, vous pouvez visualiser et explorer des sources de données pour approfondir la procédure d'enquête. Pour une description détaillée des informations affichées dans chaque source de données, consultez Panneau Recherche contextuelle.

Pour afficher des informations dans le panneau Recherche contextuelle dans la vue Naviguer ou dans la vue Événements :

1. Pointez sur différentes méta-valeurs pour voir les sources de données pour lesquelles des données sont disponibles.
   Une zone de pointage affiche une liste des sources de données dont les données de contexte sont disponibles pour la valeur méta. Les sources de données possibles sont les suivantes : NetWitness Endpoint, Incidents, Alertes, Hôtes, Fichiers, Flux et Live Connect.
2. Cliquez avec le bouton droit sur une valeur méta, puis cliquez sur **Contexte** Recherche dans le menu déroulant pour ouvrir le panneau Recherche contextuelle.

   Le panneau Recherche contextuelle s'ouvre depuis le côté droit de la fenêtre du navigateur. Le panneau Recherche contextuelle est renseigné avec les informations du service Context Hub dès que possible.
3. Pour effectuer des actions à partir du panneau Recherche contextuelle, cliquez sur une entité, comme l'adresse IP.
   Les options suivantes sont disponibles : Ouvrir le lien dans un nouvel onglet, Requête dans Enquêter, Copier le lien, Coller, Recherche Google, Recherche total de virus et Requête dans le point de terminaison.
4. Pour fermer le panneau Recherche contextuelle, cliquez sur ■.

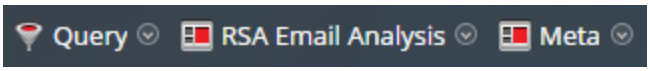
Utiliser des profils pour encapsuler les vues personnalisées

L'utilisation de profils est un moyen simple et rapide de personnaliser les données qui sont affichées dans les vue Naviguer et Événements. La boîte de dialogue Gérer les profils vous permet d'utiliser un profil pour spécifier les métagroupes et les groupes de colonnes affichés par défaut, pour ajouter une procédure d'enquête, et pour importer et exporter des profils.

Remarque : Les profils sont partagés entre les utilisateurs sur le même réseau NetWitness Platform. Si un utilisateur modifie ou supprime un profil, cela aura une répercussion sur les éléments disponibles aux autres utilisateurs.

Si vous disposez de plusieurs profils, vous pouvez basculer entre eux pour modifier rapidement les préférences du profil sélectionné. Si un profil est actuellement actif, le titre du menu Profil est remplacé par le nom du profil.

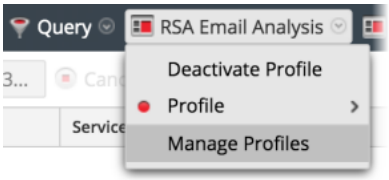
La figure suivante l'illustre dans la vue Naviguer. Le nom du profil s'affiche à droite de l'option Requête. Cela est également vrai pour la vue Événements.



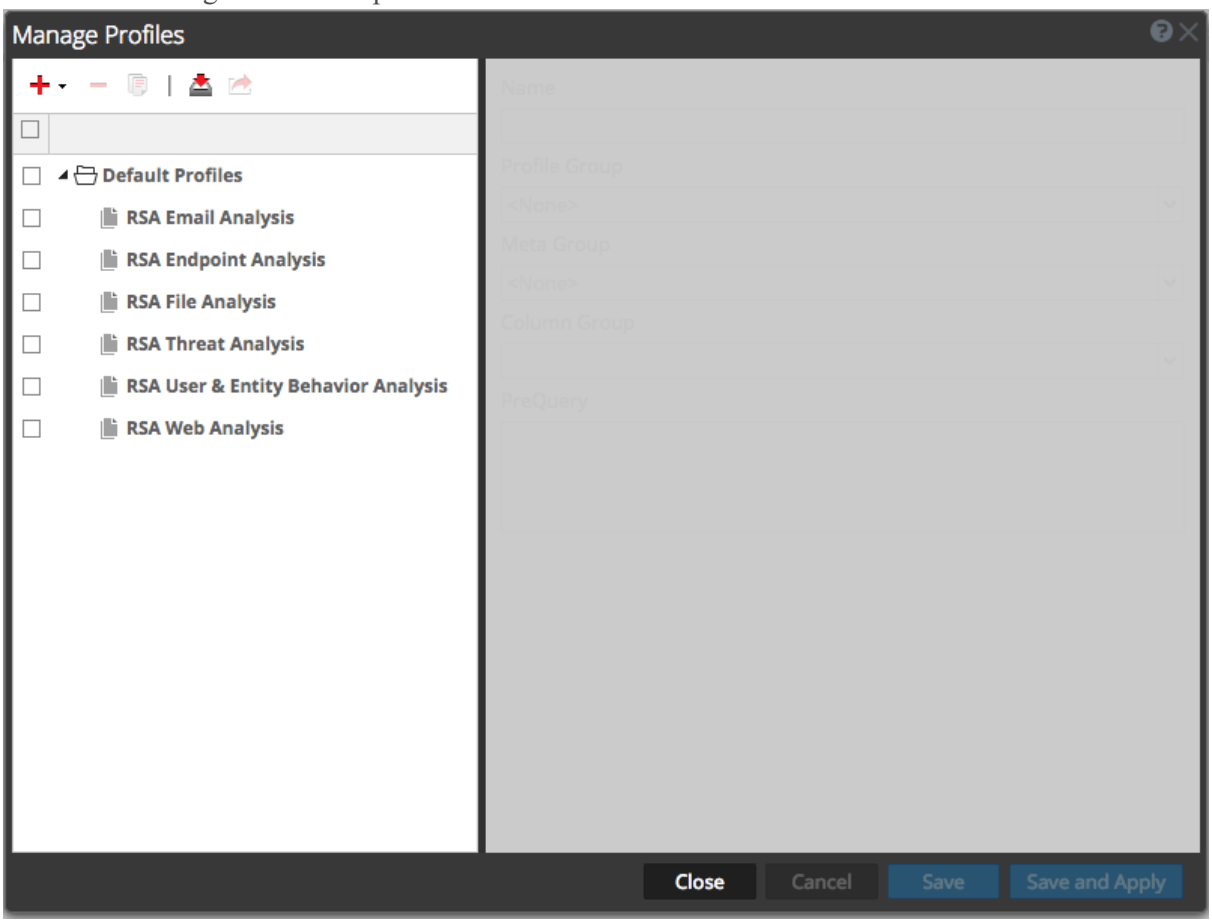
À partir de la version 11.2, les profils sont organisés en groupes de profil. Les profils intégrés se trouvent dans le groupe Profils par défaut, qui ne peut pas être modifié. Les analystes peuvent créer de nouveaux groupes de profils, que n'importe qui peut utiliser. Une fois créé, vous pouvez modifier un groupe de profils pour ajouter, supprimer ou déplacer des profils d'un groupe à un autre. Lorsque vous créez un profil, celui-ci n'est pas ajouté à un groupe de profils par défaut. Lors de l'exportation de profils, des informations sur le groupe de profils sont enregistrées et les profils sont importés dans le même groupe à partir duquel ils ont été exportés.

Parcourir la boîte de dialogue Gérer les profils

1. Accédez à ENQUÊTER > **Événements** ou **ENQUÊTER** > **Naviguer**. (Si la boîte de dialogue **Examiner** s'affiche, sélectionnez un service, puis cliquez sur **Naviguer**.)
2. Dans la barre d'outils, sélectionnez **Profil > Gérer les profils**.



La boîte de dialogue Gérer les profils s'affiche.



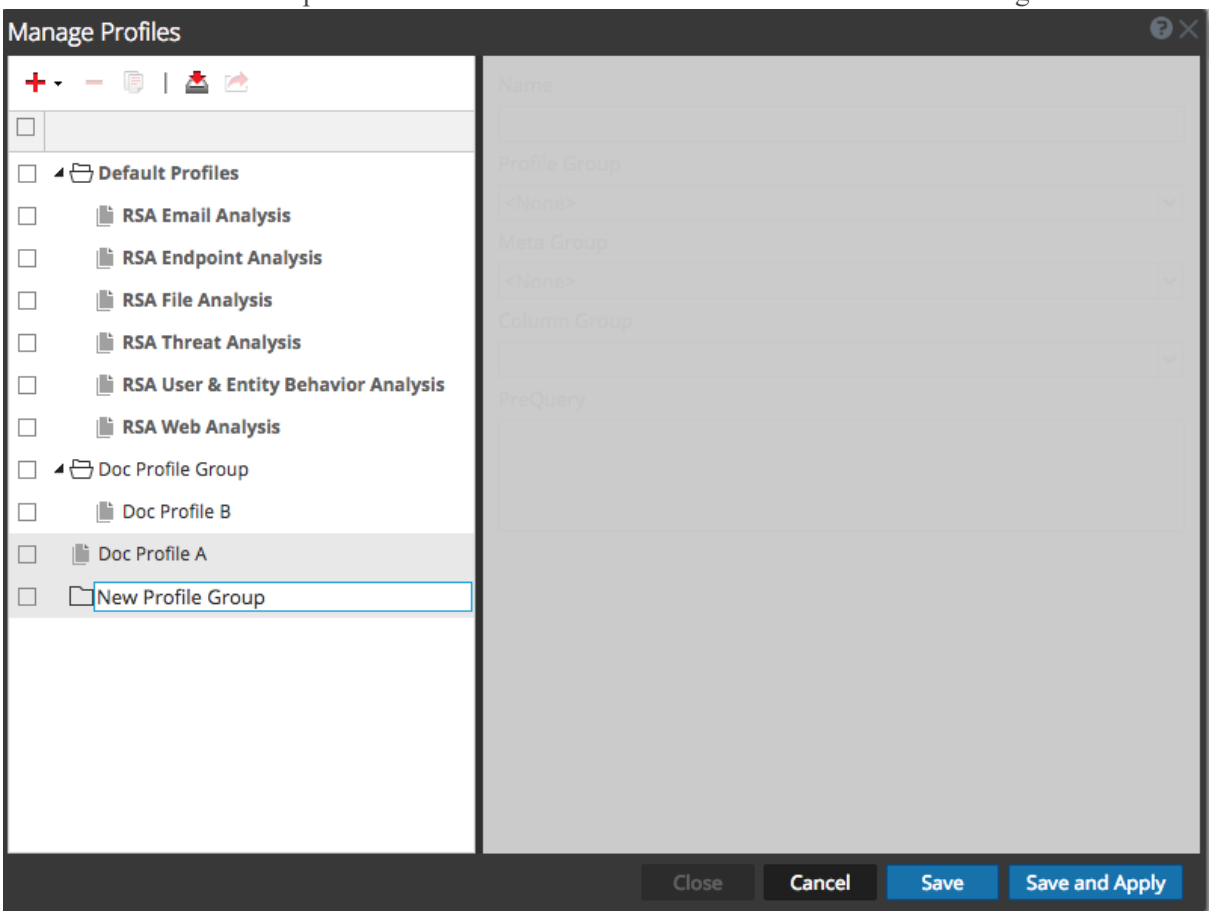
Créer, modifier ou supprimer un groupe de profils (version 11.2 et supérieure)

Vous pouvez créer un groupe de profil personnalisé pour organiser différents profils. Une fois créé, la seule modification que vous pouvez effectuer directement dans un groupe de profils consiste à modifier le nom du groupe de profils. Pour ajouter ou supprimer un profil dans un groupe, modifiez le profil et assignez-le à un autre groupe de profils , comme décrit dans Créer et modifier des profils.

1. Sous l'onglet **Gérer les profils**, exécutez l'une des opérations suivantes :
   - Pour sélectionner un groupe de profils existant à modifier, double-cliquez sur le groupe de profils.
   - Pour ajouter un nouveau groupe de profils, cliquez sur + et sélectionnez **Ajouter un nouveau groupe de profils**.

Remarque : Si vous souhaitez modifier l'un des groupes de profils intégrés, cliquez sur pour créer une copie modifiable.

Un dossier avec un champ vide s'affiche en bas de la liste Profils dans la colonne de gauche.



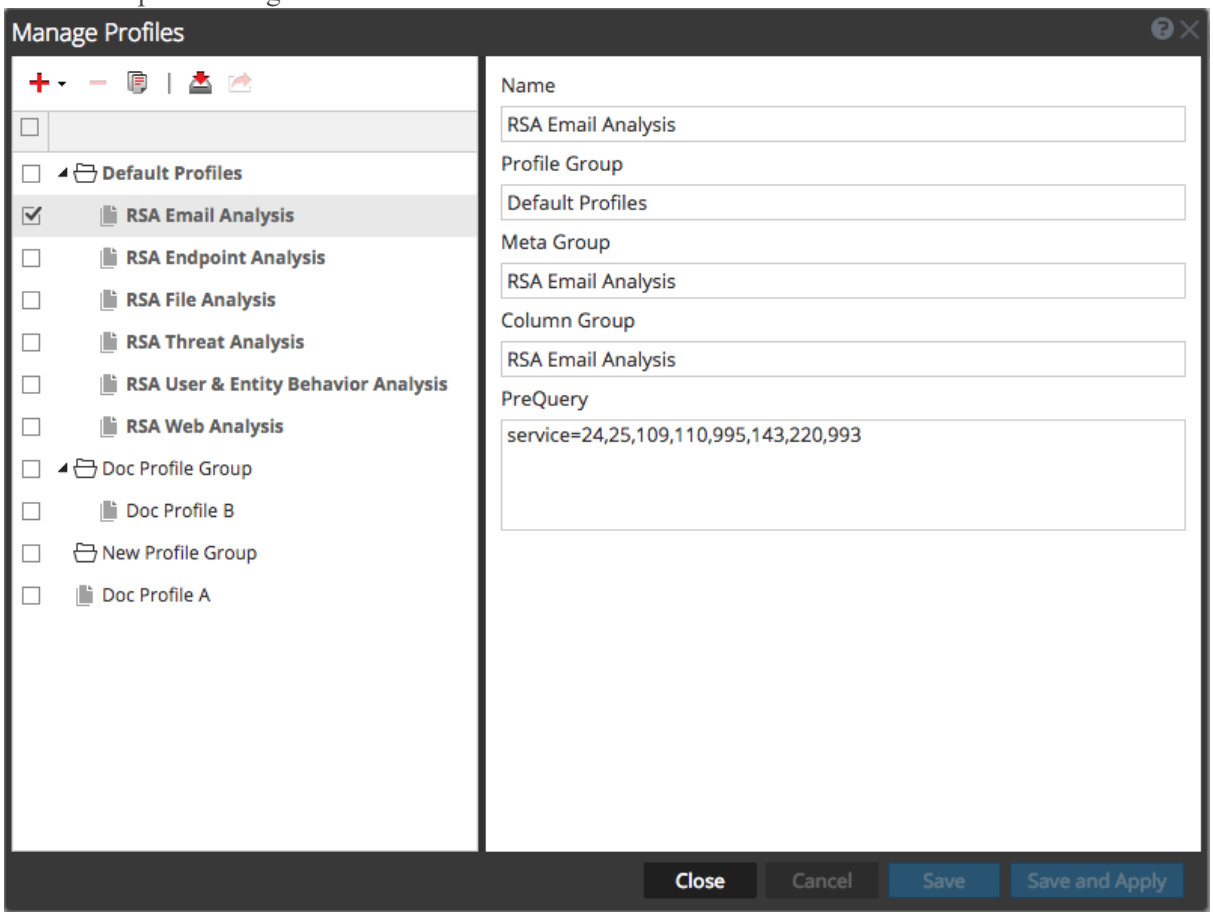
2. Pour modifier ou entrer le nom du groupe de profils, double-cliquez sur le groupe de profils et tapez le champ d'entrée. Ce nom doit comprendre entre 2 et 80 caractères.
   Le nom du groupe de profils est appliqué à un nouveau groupe de profils ou au groupe de profils que vous avez modifié. Le groupe de profils est maintenant disponible lors de la configuration d'un profil.
3. Pour supprimer un groupe de profils, effectuez l'une des opérations suivantes :
   - Si vous souhaitez supprimer un groupe de profils, mais conservez les profils, cochez la case pour sélectionner le groupe, désactivez les cases à cocher des profils du groupe, puis cliquez sur supprimer.
   - Si vous souhaitez supprimer un groupe de profil ainsi que les profils qu'il contient, cochez la case pour sélectionner le groupe et ne désactivez pas les cases à cocher pour les profils que vous souhaitez supprimer.
     Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer le groupe. Si vous n'avez pas désélectionné la case en regard des profils, le groupe et les profils du groupe sont supprimés. Si vous avez désactivé les cases à cocher pour les profils, seul le groupe de profils est supprimé et les profils sont déplacés hors du groupe et peuvent être ajoutés à un autre groupe de profils.

Créer et modifier des profils

1. Sous l'onglet **Gérer les profils**, exécutez l'une des opérations suivantes :
   - Pour sélectionner un profil existant à modifier, cochez la case à côté du nom.
   - Pour ajouter un nouveau profil dans la version 11.2 et ultérieures, cliquez sur + ou cliquez sur la flèche en regard de + et sélectionnez **Ajouter un nouveau profil**.
   - Pour créer un nouveau profil dans les versions antérieures à 11.2, + cliquez sur .

   Remarque : Si vous souhaitez modifier l'un des profils prédéfinis, cliquez sur pour créer une copie, puis modifiez-la.

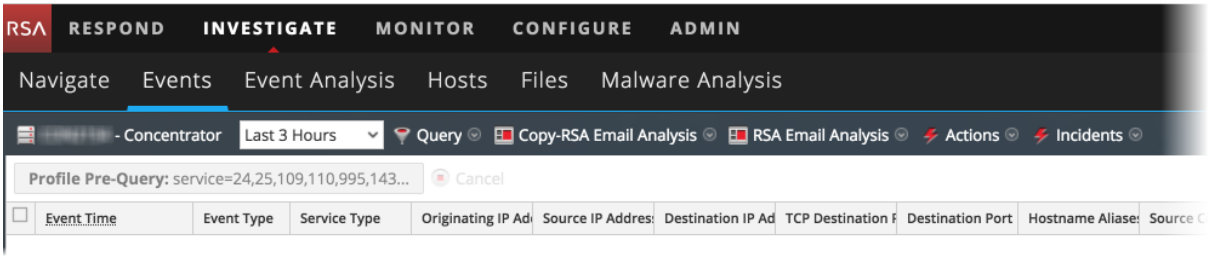
   La définition du profil peut être modifiée dans le panneau de droite. Cette figure illustre la définition de l'un des profils intégrés.



2. Modifiez ou saisissez le nom du profil dans le champ **Nom**. Ce nom doit comprendre entre 2 et 80 caractères.
3. (Facultatif pour la version 11.2 et supérieure) Si vous souhaitez ajouter le profil à un groupe de profils, sélectionnez un groupe de profils dans la liste déroulante **Groupe de profils**.
   Si vous sélectionnez un groupe de profils, le profil est ajouté au groupe lorsque vous enregistrez les

modifications. Si vous ne sélectionnez pas de groupe de profils, le profil ne fait pas partie d'un groupe.

4. Sélectionnez un métagroupe dans la liste déroulante **Groupe méta**. Vous pouvez ajouter des métagroupes personnalisés comme décrit dans la rubrique Gérer les groupes méta.
5. Sélectionnez un groupe de colonnes pour la liste déroulante **Groupe de colonnes**. Vous pouvez personnaliser les groupes de colonnes comme décrits dans la rubrique Gérer des groupes de colonnes dans la vue Événements.
6. Saisissez des requêtes pour filtrer les résultats dans le champ **PreQuery**. PreQuery applique la même syntaxe que le Générateur de requête. Le PreQuery dans la figure utilise un méta-groupe dénommé **service = 24,25,109,110,995,143,220,993**.
7. Cliquez sur **Enregistrer** pour enregistrer le profil sans l'utiliser, ou cliquez sur **Enregistrer et appliquer** pour enregistrer le profil et l'utiliser immédiatement.
   Si vous cliquez sur **Enregistrer et appliquer**, une fenêtre de confirmation s'affiche avant d'appliquer le profil sélectionné. Pour la version 11.2 et les versions précédentes, la PreQuery que vous avez entré dans la boîte de dialogue Gérer les profils s'affiche dans le Fil d'Ariane.



Supprimer un profil

1. Dans la boîte de dialogue **Gérer les profils**, sélectionnez un profil en sélectionnant la case à côté du nom.

   Remarque : Vous ne pouvez pas supprimer les profils intégrés.

2. Cliquez sur .
   Une invite vous demande de confirmer que vous souhaitez supprimer le profil, et le profil est supprimé. Le nom de l'option dans la barre d'outils redevient **Profil** pour afficher qu'aucun profil n'est actif.

Modifier le profil actif

Si vous ne pouvez pas visualiser un certain nombre de résultats ou les résultats appropriés dans les vues Naviguer ou Événements, c'est que vous disposez d'un profil actif qui applique une prérequête. Si vous ne souhaitez pas utiliser de profils, vous pouvez cliquer sur **Désactiver les profils** dans le menu déroulant **Profils**.

Pour utiliser un profil différent :

1. Dans la barre d'outils de la vue **Naviguer** ou **Événements**, ouvrez le menu déroulant **Profils**.
2. Placez le point de la souris sur l'option **Profil** pour afficher la liste déroulante des profils disponibles.
3. Sélectionnez le profil que vous souhaitez utiliser.
   Les paramètres du profil sont appliqués immédiatement.

Si vous souhaitez modifier le profil actif dans la boîte de dialogue Gérer les profils :

1. Dans la barre d'outils de la vue **Naviguer** ou **Événements**, sélectionnez **Profils > Gérer les profils**.
   La boîte de dialogue Gérer les profils s'affiche.
2. Sélectionnez un profil dans le panneau gauche, puis cliquez sur **Enregistrer et appliquer**.
   Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Yes**.
   Les paramètres du profil sont appliqués immédiatement.

Importer les profils

Vous pouvez télécharger en amont ou importer des fichiers `.jsn` qui ont été téléchargés à partir d'un autre service. Lorsque les groupes de profils sont exportés puis importés, le regroupement de profil est maintenu.

1. Dans la boîte de dialogue **Gérer les profils**, cliquez sur  dans la barre d'outils du panneau gauche.
   La boîte de dialogue Importation du profil s'affiche.
2. Cliquez dans le champ **Parcourir** ou **Télécharger le fichier** pour sélectionner un fichier à partir de votre ordinateur.
3. Lorsque le fichier est sélectionné, cliquez sur **Télécharger**.
   Ce profil s'affiche dans le panneau gauche.

Télécharger des profils

Les profils sont téléchargés sous la forme de fichiers .jsn.

1. Dans la boîte de dialogue **Gérer les profils**, sélectionnez un ou plusieurs profils dans le panneau gauche.
2. Dans la barre d'outils du panneau de gauche, cliquez sur  .
   Le téléchargement commence immédiatement.

Rechercher des modèles de texte

Vous pouvez rechercher des modèles de texte dans les paramètres actuels d'événements dans les vues Naviguer et Événements. Vous pouvez effectuer une recherche par mot-clé ou mettre en correspondance des expressions régulières. Dans la vue Naviguer, vous pouvez cliquer sur une valeur méta, par exemple HTTP, pour explorer les données, puis saisir une chaîne de recherche dans le champ Rechercher pour rechercher des événements dans ce sous-ensemble de données. La recherche ouvre un onglet dans la vue Événements, met en évidence l'étendue et l'heure de votre recherche verticale, et affiche les résultats de votre recherche. Vous pouvez également effectuer une recherche verticale dans les données à l'aide des requêtes avant de démarrer une recherche. Pour exécuter la recherche, entrez une chaîns de recherche dans la zone de recherche, puis appuyez sur la touche **Entrée** ou cliquez sur **Rechercher**.

Recherche de texte par mot-clé

La recherche de texte fournit les fonctionnalités suivantes :

- Chaque mot séparé par un espace est relié par l'opérateur ET, pour que chaque mot soit trouvé, mais l'ordre ou la position par rapport aux autres mots est sans importance. Par exemple, si vous effectuez une recherche sur `Mark Albert`, Mark et Albert doivent être trouvés dans la session, mais ils doivent être ensemble ou dans un ordre spécifique.
- Le mot OU est spécial. Si vous recherchez `Mark OR Albert`, Mark ou Albert doivent être trouvés dans la session pour correspondre ; les deux ne sont pas nécessaires.
- Vous pouvez associer les opérateurs implicites ET et OU dans la chaîne de recherche. L'opérateur OU explicite a une priorité supérieure à l'opérateur ET implicite (espace blanc). Les exemples suivants ont la même instruction logique, qui exige que les deux termes fromage et boulettes soient présents dans une occurrence avec le terme grille-pain :
  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```
- Vous pouvez exclure des mots des résultats de la recherche en utilisant l'opérateur `-`. Par exemple, une recherche effectuée avec `cheese -toast` ne retournera aucun résultat contenant le mot fromage, sauf si le mot toast est également présent.
- La recherche par mot-clé peut trouver des occurrences de métadonnées stockées dans les modèles suivants :
  - **Adresses IPv4 et IPv6**. Tout terme pouvant être reconnu comme étant une adresse IP sera converti au format de métadonnée natif pour pouvoir être trouvé dans les données indexées.
  - **Plages d'adresses IPv4 CIDR**. Vous pouvez utiliser la notation CIDR pour trouver des adresses IPv4 dans une plage d'adresses.
  - **Horodatages**. Les horodatages sont mis en correspondance avec le méta de temps natif et tous les autres champs de métadonnées de temps stockés avec le type Time.
  - **Nombres**. La fonction de recherche tentera automatiquement d'identifier les termes de recherche décimaux et de les mettre en correspondance avec les champs de métadonnées numériques.

Options de contrôle du comportement de recherche

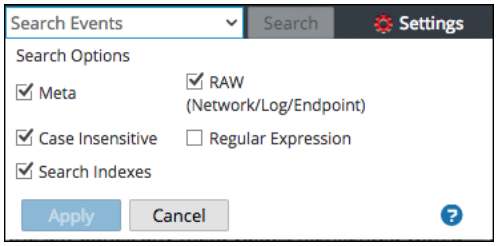
Pour accéder à la zone de recherche et aux options de recherche dans les vues Naviguer ou Événements :

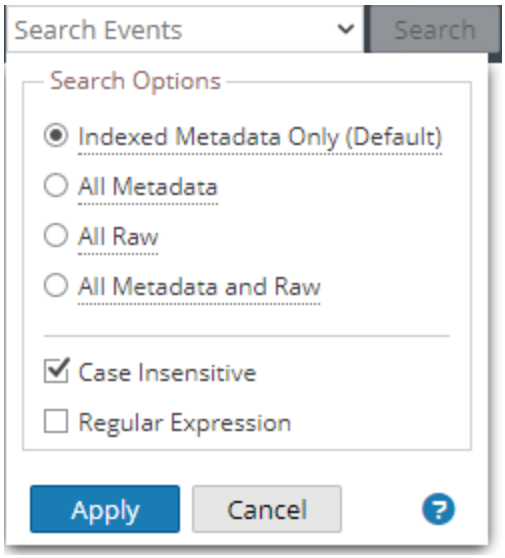
1. Le champ Rechercher des événements s'affiche dans la barre d'outils.

   Résolution des problèmes : Si vous ne voyez pas le champ Rechercher des événements dans la barre d'outils, cliquez sur » sur le côté droit de la barre d'outils.

2. Cliquez dans le champ de recherche pour afficher le menu déroulant Options de recherche. Dans la version 11.2 et versions ultérieures, les options de menu sont légèrement différentes. La première figure illustre le menu pour la version 11.1 et versions antérieures ; la deuxième figure illustre le menu pour la version 11.2 et versions ultérieures.

Les options sélectionnées dans cette zone modifient la manière dont la recherche et exécutée. Le mode de recherche par défaut consiste à rechercher des index pour les métadonnées indexées et les données brutes uniquement.

Remarque : Étant donné que la case à cocher Rechercher dans les index ou dans les métadonnées indexées uniquement est sélectionnée par défaut, la recherche renvoie des résultats en fonction des données qui sont indexées. Si vous souhaitez rechercher un ensemble complet de métadonnées ou de données brutes, activez ces cases à cocher et désactivez la case à cocher Rechercher dans les index ou dans les métadonnées indexées uniquement (paramètre par défaut). Ce type de recherche est plus long, mais celle-ci contiendra un ensemble plus complet de données.

Le tableau suivant décrit les options de recherche dans Procédure d'enquête.

Fonction	Description
Case à cocher **Métadonnées indexées uniquement (par défaut)** uniquement (version 11.2) Bouton radio **Index** (version 11.1)	La recherche ne renvoie que les résultats obtenus avec les données indexées. Rechercher dans l'index est le moyen le plus rapide de trouver des mots-clés dans un ensemble de données volumineux. La recherche dans l'index exploite les index appropriés présents dans votre collection de données. **Attention :** Les occurrences de sous-chaînes ne sont pas trouvées par les recherches dans les index. Pour trouver des occurrences de sous-chaînes, désélectionnez cette case à cocher et recherchez autrement que dans les index.
Bouton radio **Toutes les métadonnées** (version 11.2) Case à cocher **Méta** (version 11.1)	Recherche dans les métadonnées. Votre mot-clé ou votre modèle Regex est mis en correspondance avec les métadonnées analysées.
Bouton radio **Toutes les données brutes** (version 11.2) Case à cocher **RAW** (Réseau/Log/Point de terminaison) (Version 11.1)	Recherche le réseau, le journal et le texte de l'événement du point de terminaison. Chaque événement est décodé et le contenu est exploré pour y rechercher des occurrences à l'aide du mot-clé ou du modèle Regex. Si vous sélectionnez toutes les données sans filtres sur un Archiver, la durée d'exécution peut être excessive et un avertissement peut s'afficher. **Attention :** La recherche dans les sessions réseau de recherche provoque le décodage des sessions, lequel est très long. Vous pouvez désactiver les recherches brutes lorsque vous examinez les collections réseau uniquement.
Bouton radio **Toutes les métadonnées et données brutes** (version 11.2)	Recherche les métadonnées et le texte du journal ou de l'événement. Cette option est une combinaison de deux options dans la version 11.1 : Métadonnées et données brutes (Réseau/Log/Point de terminaison), que vous pouvez sélectionner ensemble. Dans la version 11.2, vous ne pouvez sélectionner qu'un seul bouton radio.
Non sensible à la casse	Ignore la casse lors de la recherche.
Expression régulière	Recherche avec une expression régulière Perl au lieu de texte. Par défaut, exécute une recherche de texte. Pour exécuter une recherche d'expression régulière, sélectionnez l'option Expression régulière. **Attention :** - Les recherches d'expression régulière peuvent être très lentes. - Lorsque les expressions régulières et les options de recherche dans les index sont combinées, le modèle de l'expression régulière est mis en correspondance avec des valeurs d'index spécifiques au lieu de valeurs méta. Cela accélère l'obtention des résultats, mais il ne s'agit pas d'une recherche exhaustive de toutes les métadonnées ou données brutes.

Fonction	Description
Appliquer	Définit les options de recherche par défaut à appliquer à une recherche dans les vues naviguer et Événements. Cette option met aussi à jour les préférences de procédure d'enquête dans votre profil (Profil > Préférences > onglet Investigation). Les préférences sont enregistrées et effectives immédiatement. Vous pouvez sélectionner les options de recherche à utiliser pour une recherche sans modifier vos préférences de recherche par défaut.

Syntaxe de recherche d'une expression régulière

La recherche d'une expression régulière utilise la syntaxe d'expression régulière Perl, qui est documentée en détail dans la page http://perldoc.perl.org/perlre.html.

Recherche par mot-clé de texte brut

Le Log Decoder peut créer un index de texte brut pour événements de log non analysés. Cette fonctionnalité crée les éléments de métadonnées qui forment un index en texte intégral sur les services en aval tels que les Concentrators et les Archivers. Lorsque vous activez l'option Rechercher dans les index dans vos préférences de recherche, votre recherche utilise automatiquement l'index de texte. Notez que l'index de texte produit des éléments de métadonnées dotés d'une granularité grossière. Par exemple, la configuration de l'indexeur de texte tronque les termes d'un texte. En comparant les occurrences de l'index avec les données brutes, le moteur de recherche trouvera les résultats exacts de votre recherche. Cependant, vous pouvez améliorer les temps de recherche en désactivant la case à cocher de la recherche brute. Ainsi, les résultats seront renvoyés plus rapidement, mais vous pourrez constater des occurrences de faux positifs dans les résultats de la recherche.

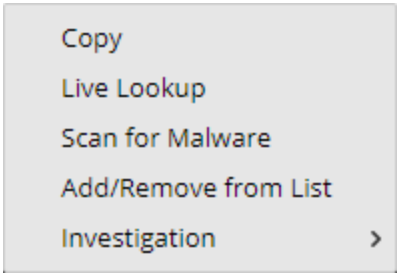
Exemples de recherche

Les exemples suivants illustrent les recherches effectuées dans les vues Naviguer et Événements.

Recherche dans la vue Naviguer

Pour effectuer une recherche dans les données affichées dans la vue Naviguer, procédez comme suit :

1. Pour explorer les données, cliquez sur une métavaleur, par exemple HTTP, dans le panneau Valeurs.



2. Saisissez une chaîne de recherche dans le champ Rechercher et appuyez sur **Entrée** ou cliquez sur **Rechercher**.
3. Pour effacer la zone de recherche et revenir à la vue Événements normale, cliquez sur le **X** dans la zone de recherche.

Recherche dans la vue Événements

Pour effectuer une recherche dans les données affichées dans la vue Événements :

1. Saisissez une chaîne de recherche dans le champ Rechercher et appuyez sur **Entrée** ou cliquez sur **Rechercher**.
   Les résultats de la recherche s'affichent dans la vue Événements. Les événements qui correspondent aux critères de recherche s'affichent dans la liste d'événements. Dans la vue Détails et la vue Liste, les correspondances sont mises en surbrillance dans la colonne Détails. De plus, lors de la recherche des données BRUTES, les correspondances sont mises en surbrillance dans la vue Log - colonne Logs.
2. Pour limiter la recherche, modifiez la requête et l'heure.
3. Si vous souhaitez arrêter la recherche et revenir à la vue Événements, cliquez sur **Annuler**.
   Les résultats déjà affichés restent à l'écran.
4. Pour effacer la zone de recherche et revenir à la vue Événements normale, cliquez sur **X** dans la zone de recherche.

Afficher et modifier des requêtes avec l'intégration URL

NetWitness Investigate comprend une fonction d'intégration d'URL externe qui facilite les intégrations aux produits tiers en permettant d'effectuer une recherche en fonction de l'architecture NetWitness Platform. En utilisant une requête dans un URI, vous pouvez pivoter directement d'un produit qui autorise les liens personnalisés vers un point de recherche verticale spécifique dans la vue Enquêter. Cette intégration fournit une présentation interne de la requête de l'utilisateur.

L'intégration d'URL permet à l'utilisateur d'identifier le service soit à l'aide de l'ID de l'hôte, soit à l'aide du service et du port, comme défini dans NetWitness Platform. Si NetWitness Platform ne peut pas résoudre le service, l'analyste est redirigé vers la vue Naviguer, qui contient la boîte de dialogue Sélection de service. Une fois que le service est sélectionné, la vue Naviguer est chargée avec le point de recherche verticale, défini par la requête.

ID de service connu

Lorsque l'ID du service à utiliser dans le cadre de la procédure d'enquête est connu, le format de saisie d'un URI à l'aide d'une requête chiffrée au format URL est le suivant :

```
http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

où

- `<sa host: port>` est l'adresse IP ou DNS, avec ou sans port selon le cas (ssl ou non). Cette désignation est nécessaire uniquement si l'accès est configuré sur un port non standard via un proxy.
- `<deviceId>` est l'ID de service interne dans l'instance NetWitness Platform du service sur lequel effectuer la requête. L'ID de service ne peut être représenté que sous la forme d'un nombre entier. Vous pouvez visualiser l'ID de service approprié à partir de l'URL dans la vue Procédure d'enquête de NetWitness Platform. Cette valeur change en fonction du service à analyser.
- `<encoded query>` est la requête NetWitness Platform codée par URL. La longueur de la requête est limitée par les restrictions d'URL HTML.
- `<start date>` et `<end date>` définissent la période pour la requête. Le format est `<yyyy-mm-dd>T<hh:mm:ss>Z.`. Les dates de début et de fin sont obligatoires. Si aucune date n'est fournie, les valeurs par défaut de l'utilisateur pour ce service sont utilisées. Les plages relatives (par exemple, Dernière heure) ne sont pas prises en charge. Toutes les heures sont exécutées au format UTC.
  Par exemple :
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Hôte et port connus

Lorsque l'hôte et le port du service à utiliser dans le cadre de la procédure d'enquête sont connus, le format de saisie d'un URI à l'aide d'une requête chiffrée au format URL est le suivant :

```
http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

où

- <sa host: port> est l'adresse IP ou DNS, avec ou sans port selon le cas (ssl ou non). Cette désignation est nécessaire uniquement si l'accès est configuré sur un port non standard via un proxy.
- <device host:port> est l'hôte et le port d'un service défini dans l'instance NetWitness Platform que le service peut interroger. NetWitness Platform tente de résoudre l'hôte et le port en tant qu'ID de service défini dans NetWitness Platform.
- <encoded query> est la requête NetWitness Platform codée par URL. La longueur de la requête est limitée par les restrictions d'URL HTML.
- <start date> and <end date> définissent la période pour la requête. Le format est <yyyy-mm-dd>T<hh:mm:ss>Z. Les dates de début et de fin sont obligatoires. Si aucune date n'est fournie, les valeurs par défaut de l'utilisateur pour ce service sont utilisées. Les plages relatives (par exemple, Dernière heure) ne sont pas prises en charge dans cette version. Toutes les heures sont exécutées au format UTC.
  Par exemple :
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Exemples

Voici des exemples de requêtes où le serveur NetWitness correspond à 192.168.1.10 et où deviceID est identifié par la valeur 2.

Toute l'activité du 03/12/2013 entre 05:00 et 06:00 avec un nom d'hôte enregistré

- Pivot personnalisé : `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

Toute l'activité du 03/12/2013 entre 17:00 et 17:10 avec trafic http vers et à partir de l'adresse IP 10.10.10.3

- Pivot personnalisé : `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Encoded Pivot Dissected:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Remarques supplémentaires

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

Reconstruire un événement

Lors de l'affichage d'une liste d'événements dans la vue Événements, vous pouvez créer une reconstruction de l'événement sous une forme lisible qui corresponde à l'originale. Par défaut, la vue initiale d'un événement reconstruit est le format le plus adapté (Meilleure reconstruction). Par exemple, un contenu Web est reconstruit sous la forme d'une page Web ; une conversation de messagerie instantanée (IM) est affichée avec les deux parties de la conversation. Chaque utilisateur peut sélectionner une reconstruction par défaut différente dans la vue Profil > Préférences.

Vous pouvez également ouvrir une reconstruction à partir de la vue Naviguer si vous connaissez l'ID de l'événement.

Dans la reconstruction, vous pouvez :

- Sélectionner les informations relatives aux événements à afficher. Les valeurs possibles sont : les données de demande, les données de réponse, les données de demande et de réponse.
- Sélectionner le type de reconstruction : détails, texte, hex, paquets, Web, Courrier électronique ou IM.
- Exporter des logs bruts.
- Exporter un événement au format de fichier PCAP.
- Extraire les fichiers disponibles dans l'événement.
- Extraire toutes les métadonnées associées à l'événement.

  Attention : Soyez vigilant(e) lorsque vous cliquez sur un lien vers un fichier au cours de la reconstruction. Si votre système dispose d'une application associée au fichier, ou que le navigateur est capable d'ouvrir les pièces jointes et qu'elles sont malveillantes, celles-ci peuvent nuire à votre système.

- Afficher l'événement dans une fenêtre ou un onglet séparé (selon la configuration de votre navigateur).
- En cas de prévisualisation de la reconstruction dans la vue active, faites défiler les événements (dans les deux sens) à l'aide des boutons de navigation situés dans le coin inférieur gauche.

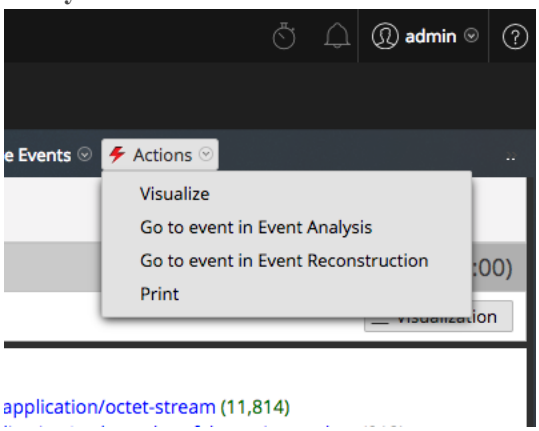
Remarque : Les paramètres de reconstruction et les paramètres du cache de reconstruction permettent à un administrateur de gérer les performances de l'application dans le cadre d'une procédure d'enquête. Lorsque les analystes reconstruisent les sessions qu'ils inspectent, deux situations peuvent affecter les performances et les résultats.
- Certains événements peuvent être très importants et contenir plusieurs milliers de paquets source. Reconstruire ces types de sessions peut dégrader les performances de l'application.
- Dans certains cas, le cache de reconstruction peut présenter un contenu incorrect ; pour cette raison, NetWitness Platform nettoie le cache toutes les 24 heures. Entre les nettoyages de cache quotidiens, certaines actions peuvent entraîner l'utilisation du cache obsolète pour la reconstruction, et dans ce cas, les administrateurs ont la possibilité d'effacer manuellement le cache pour un ou plusieurs services qui sont connectés au NetWitness Server actif.

Reconstruire un événement à partir de la vue Naviguer

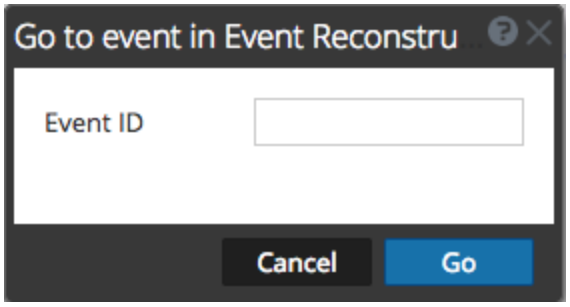
Vous pouvez reconstruire un événement directement à partir de la vue Naviguer avec un ID d'événement connu. Vous pouvez utiliser cette option sans exécuter de requête, comme vous le faites habituellement au début d'une procédure d'enquête. Un service et une période doivent être sélectionnés pour être en mesure d'accéder directement à un événement en utilisant simplement son `eventid`.

Pour afficher une analyse de reconstruction ou d'événement directement à partir de la vue Naviguer :

1. Accédez à **ENQUÊTER** > **Parcourir** et sélectionnez **Actions** > **Accéder à un événement dans Analyse d'événements** ou **Accéder à un événement dans Reconstruction d'événement**.



La boîte de dialogue Accéder à l'événement s'ouvre. Deux boîtes de dialogue sont disponibles, l'une pour Analyse d'événements et l'autre pour Reconstruction d'événement. Toutes deux invitent à indiquer l'ID de l'événement.

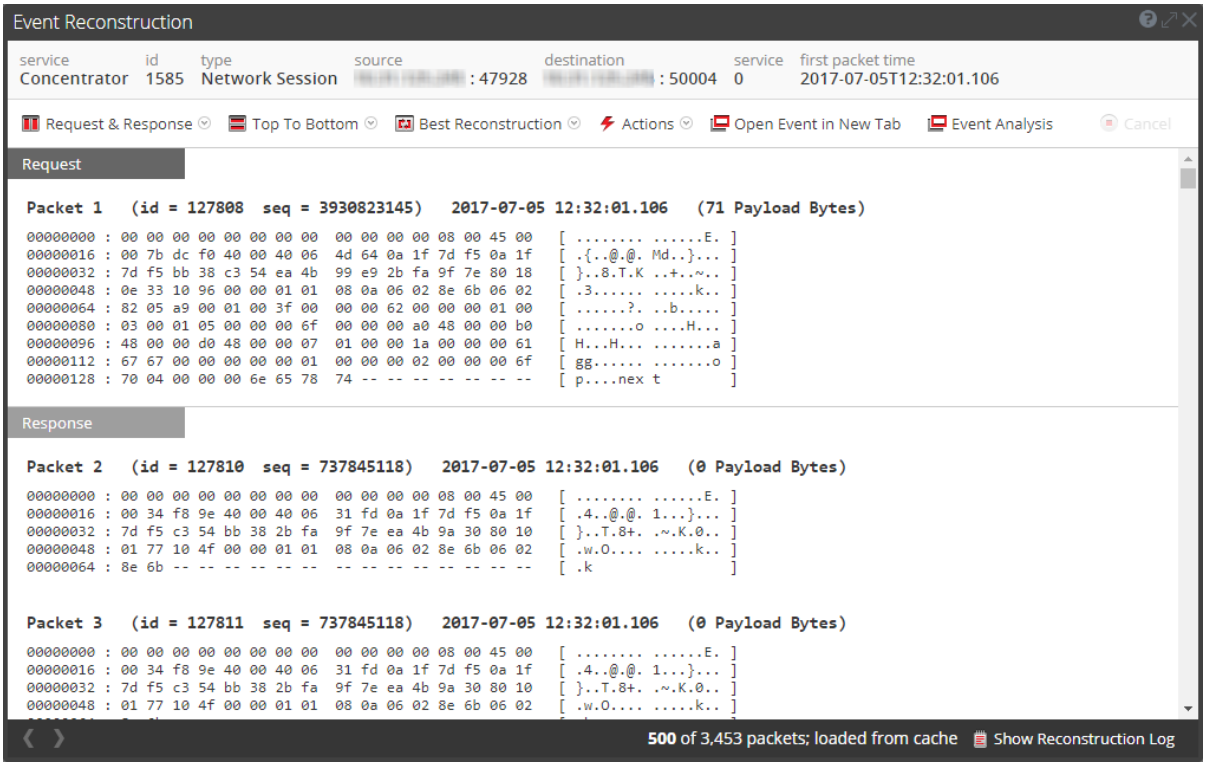


2. Dans le champ **ID d'événement**, saisissez l'ID et cliquez sur **Atteindre**.
   L'événement spécifié est reconstruit dans la vue Reconstruction d'événement ou la vue de Analyse d'événements.

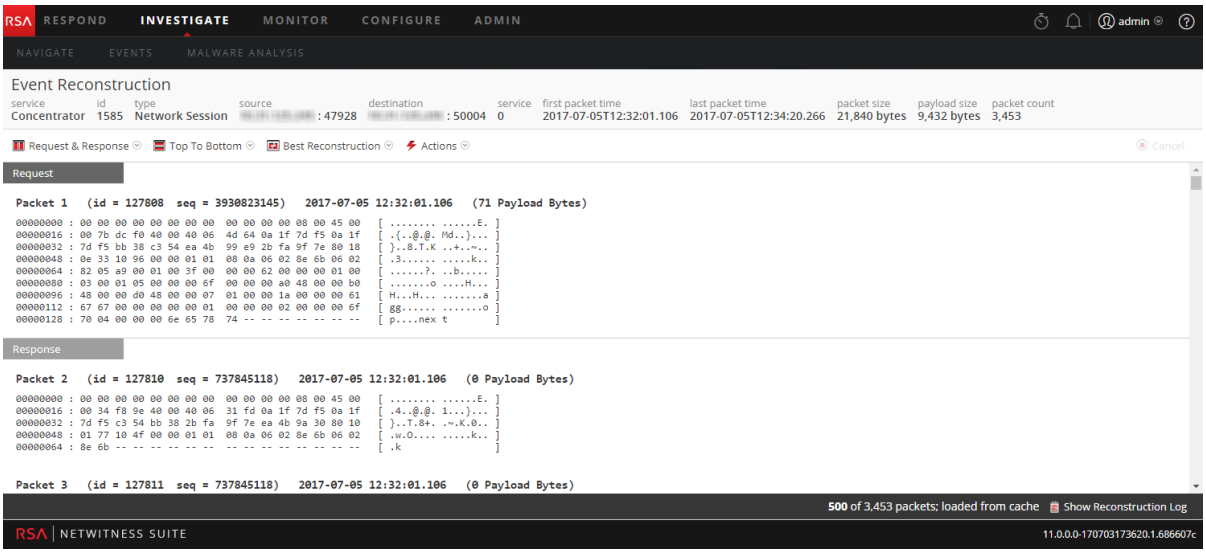
Reconstruire un événement à partir de la vue Événements.

1. Ouvrez un point de recherche verticale dans la vue **Événements**.
2. Pour afficher toutes les métadonnées, cliquez sur + Show Additional Meta .
3. Pour ouvrir une reconstruction d'événement dans la vue actuelle, sélectionnez un événement à reconstruire, puis choisissez **Actions** > **Afficher l'événement** > **Aperçu à la volée**.
   La Reconstruction d'événement s'ouvre dans une fenêtre contextuelle au sein de la même vue. Par défaut, NetWitness Platform affiche la meilleure reconstruction pour l'événement déterminée par son

contenu ou la reconstruction que vous avez sélectionnée dans le paramètre Vue Session par défaut pour la Procédure d'enquête.Définir un serveur de notification syslog Vous pouvez utiliser les options de la barre d'outils Reconstruction d'événement pour modifier la méthode de reconstruction, afficher les résultats côte à côte, exporter un événement, ouvrir la pièce jointe d'un e-mail, extraire des fichiers et ouvrir l'événement dans un nouvel onglet. Les options de la barre d'outils varient en fonction du type d'événement en cours de reconstruction (événement de réseau, événement de log ou événement de point de terminaison). Cette figure est un exemple de reconstruction d'un événement de réseau.



4. Pour avoir un aperçu d'une reconstruction de l'événement suivant, cliquez sur ❯ ou pour l'événement précédent sur ❮.
5. Pour ouvrir une reconstruction d'événement dans un nouvel onglet, effectuez ce qui suit :
   a. Dans la vue **Événement**, sélectionnez l'événement à reconstruire, puis choisissez **Actions** > **Afficher l'événement** > **Ouvrir dans un nouvel onglet**.
   b. Dans la barre d'outils **Reconstruction d'événement** de la reconstruction prévisualisée, cliquez sur **Ouvrir l'événement dans un nouvel onglet**.
      La Reconstruction d'événement s'ouvre dans un nouvel onglet.



Afficher côte à côte ou du haut vers le bas

Pour sélectionner le mode d'affichage des demandes et des réponses relatives à un événement :

1. Dans la barre d'outils **Reconstruction d'événement**, cliquez sur **Du haut vers le bas** ou **Côte à côte**.
2. Dans le menu déroulant, sélectionnez les informations que vous souhaitez afficher dans l'événement : **Côte à côte** ou **De haut en bas.**
   La reconstruction est actualisée avec les informations sélectionnées.

Sélectionner les informations relatives aux événements à afficher.

Pour sélectionner les informations liées aux événements à afficher :

1. Dans la barre d'outils **Reconstruction d'événement**, cliquez sur **Requête et réponse**.
2. Dans le menu déroulant, sélectionnez les informations que vous souhaitez afficher dans l'événement : **Requête et réponse**, **Requête** ou **Réponse**.
   La reconstruction est actualisée avec les informations sélectionnées.

Sélectionner le type de reconstruction d'événement

Pour sélectionner le type de reconstruction pour un événement :

1. Dans la barre d'outils **Reconstruction d'événement**, cliquez sur **Meilleure reconstruction**.
2. Dans le menu contextuel, sélectionnez le type de reconstruction à afficher : **méta**, **texte**, **hex**, **paquets**, **web**, **courrier électronique** ou **fichiers**.
   La reconstruction est actualisée avec le type de reconstruction sélectionné.

Ouvrir ou télécharger une pièce jointe à un e-mail

Lors de l'affichage de la reconstruction d'un e-mail contenant des pièces jointes, vous pouvez ouvrir les types de fichiers pris en charge ou télécharger les fichiers sur le système local.

Attention : Soyez vigilant(e) lors de la sélection des pièces jointes. Si votre système dispose d'une application associée aux fichiers joints, ou si le navigateur est capable d'ouvrir les pièces jointes et qu'elles sont malveillantes, elles peuvent nuire à votre système.

Pour ouvrir ou télécharger les pièces jointes aux e-mails :

1. Dans la barre d'outils de **Reconstruction d'événement**, sélectionnez la liste déroulante **Vue**, puis sélectionnez **Afficher la messagerie**.
   La vue Reconstruction d'événement s'affiche.
2. Dans la section **Reconstruction d'événement** de l'e-mail, cliquez sur Pièce jointe.
   Si le type de fichier est pris en charge par le navigateur, la pièce jointe s'ouvrira dans un nouvel onglet.
   Si le type de fichier n'est pas pris en charge, la boîte de dialogue Télécharger s'affichera pour vous permettre de télécharger la pièce jointe.

Exporter un événement au format de fichier PCAP

L'option Exporter un PCAP permet de télécharger les sessions de la période en cours et un point de recherche verticale dans un fichier PCAP. Pour exporter un événement au format de fichier PCAP :

1. Dans la barre d'outils **Reconstruction d'événement**, cliquez sur **Actions**.
2. Cliquez sur **Exporter un PCAP**.
3. Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **OK**.
   La tâche est planifiée et une fois l'opération terminée, le fichier PCAP est téléchargé sur le système de fichiers local. Sous Profil > onglet Tâches, vous pouvez télécharger le fichier PCAP.

Extraire des fichiers d'un événement reconstruit

L'option Extraire des fichiers permet d'extraire et de télécharger les fichiers associés à l'événement. Pour extraire les fichiers :

1. Dans la barre d'outils **Reconstruction d'événement**, cliquez sur **Actions**.
2. Cliquez sur **Extraire des fichiers**.
   La boîte de dialogue d'extraction de fichiers s'affiche.
3. Sélectionnez les types de fichiers à extraire, puis cliquez sur **OK**.
4. La tâche est planifiée et une fois l'opération terminée, les types de fichiers sélectionnés sont téléchargés sur le système de fichiers local. Sous Profil > onglet Tâches, vous pouvez télécharger les fichiers.

Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements

L'analyse des événements bruts et des données dans la même vue est possible lorsque vous travaillez dans la vue Analyse d'événements. Après avoir pris connaissance de la section Types de reconstruction dans la vue Analyse d'événements, vous pouvez :

- Filtrer les résultats dans la vue Analyse d'événements
- Examiner les événements dans la vue Analyse d'événements
- Rechercher un contexte supplémentaire dans la vue d'analyse d'événement
- Télécharger des données dans la vue Analyse d'événements
- Agir sur les données dans la vue Analyse d'événements

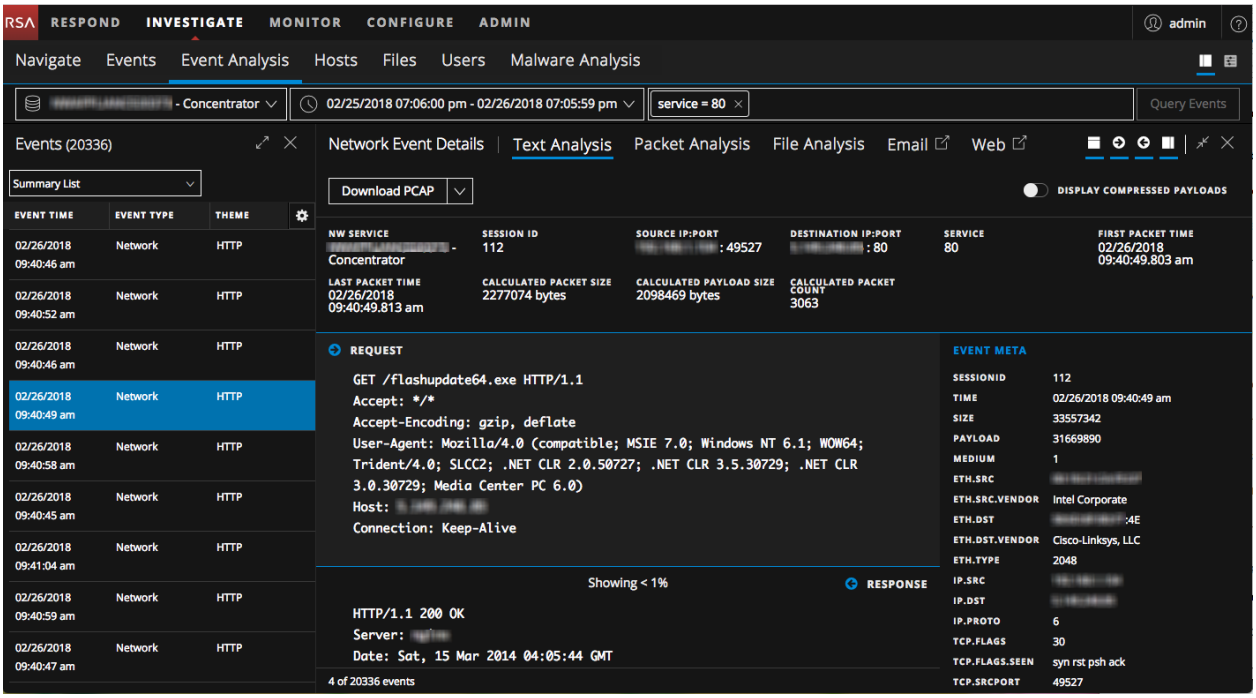
Types de reconstruction dans la vue Analyse d'événements

Lors de la chasse aux menaces possibles dans les données de réseau capturées, vous pouvez accéder à différents points d'intérêt dans les données. Si une session donnée contient des événements suspects, vous pouvez examiner la liste des événements pour la session et afficher également en toute sécurité d'une reconstruction de l'événement, avec des fonctions qui permettent d'identifier des tendances. (Reportez-vous à la section Commencer une procédure d'enquête pour connaître les différentes méthodes d'accès à la vue Analyse d'événements.)

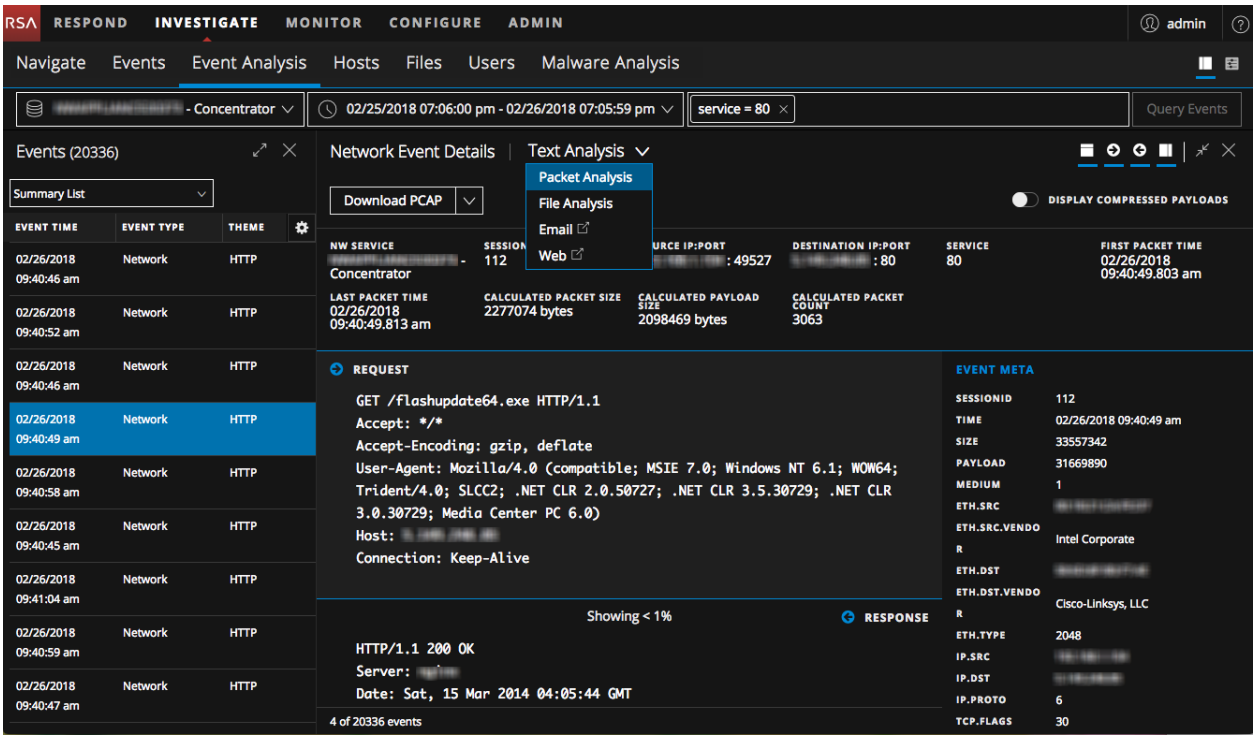
Remarque : Si vous analysez des événements sur un service 10.6.x ou 11.0.0.x à partir d'un serveur NetWitness 11.1 ou 11.2, le comportement de téléchargement dans la vue Analyse d'événements varie pour les fichiers, PCAP, logs, charges utiles et valeurs méta. Vous pouvez voir la charge utile d'un événement sur un service 10.6.x ou 11.0.0.x pour lequel vous n'avez pas d'autorisation, mais vous ne serez pas en mesure de télécharger des fichiers ou des charges utiles.

Dans la vue Analyse d'événements, vous pouvez sélectionner le format de la reconstruction : Analyse de paquets, Analyse de fichiers, ou Analyse de texte, **E-mail** (version 11.1 ou supérieure), et **Web** (version 11.1 ou supérieure). Lorsque la clé méta `medium` étiquette un événement en tant qu'événement de log ou de point de terminaison, seule l'analyse Analyse de texte est disponible. La reconstruction par défaut des événements de réseau est Analyse de texte ; toutefois, pour un événement de réseau, le dernier format de reconstruction ouvert remplace la valeur par défaut. Les reconstructions Email et Web ouvrent l'événement dans la vue Événements et sont décrits dans « Sélectionner le type d'analyse d'événement » dans Examiner les événements dans la vue Analyse d'événements

La figure suivante est un exemple de Détails des événements réseau : un panneau Analyse de texte dans une fenêtre de navigateur Web suffisamment large pour afficher les options de format de reconstruction en une ligne.



Lorsque la fenêtre du navigateur est trop étroite pour afficher toutes les options d'affichage horizontalement, les options sont présentées dans une liste déroulante.



Au sein de chaque type d'analyse, des paramètres sont disponibles afin d'améliorer votre analyse. Si vous modifiez un paramètre, ce dernier est conservé entre les actualisations de navigateur et les connexions au sein du même navigateur. Les paramètres conservés sont les suivants :

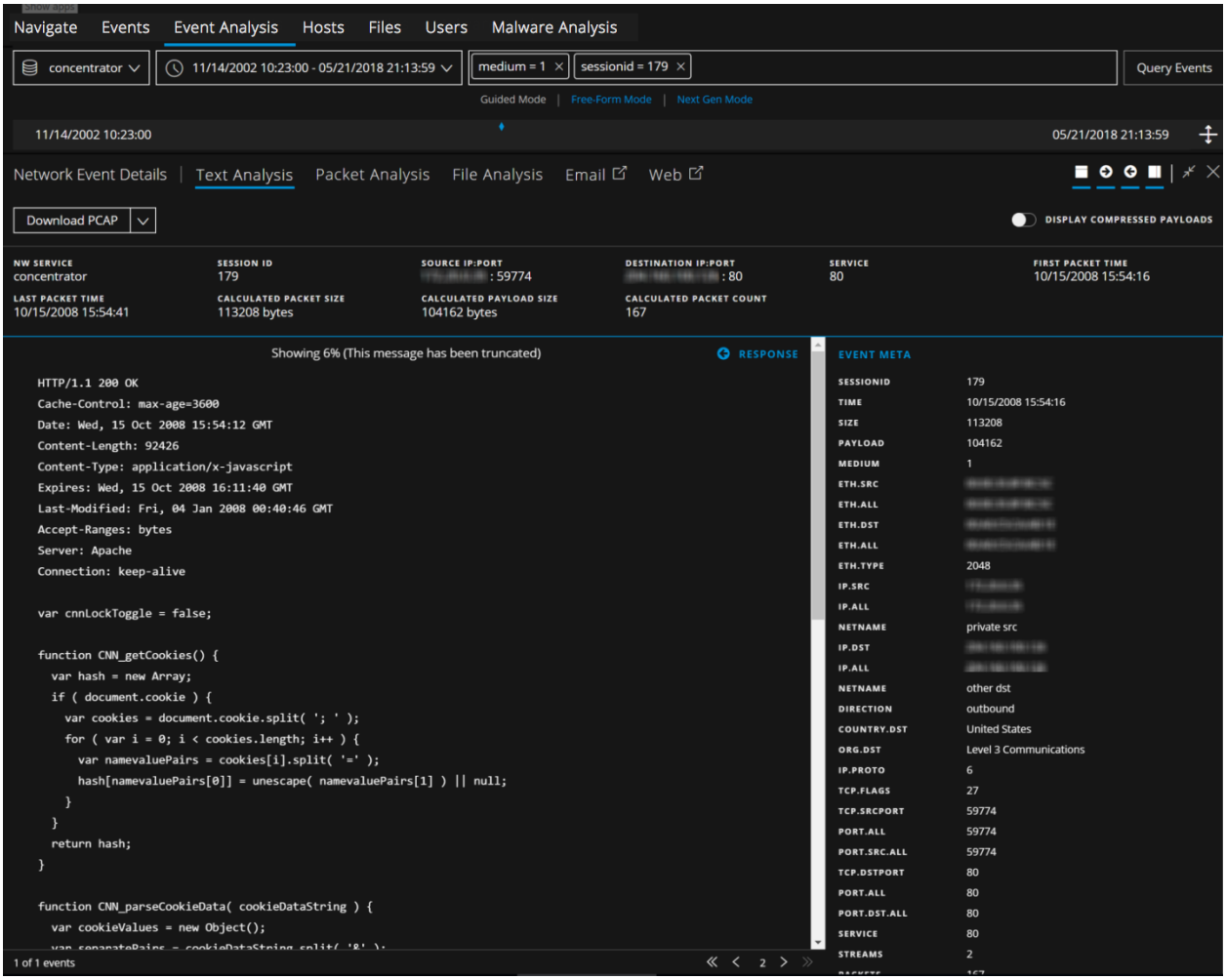
- La reconstruction sélectionnée actuelle : Analyse de texte, Analyse de paquets ou Analyse de fichiers.
- Si le Panneau Méta de l'événement est ouvert ou fermé.
- Si l'en-tête d'événement est ouvert ou fermé.
- Si la demande ou réponse ou les deux sont affichés.
- Si les charges utiles des paquets sont affichées dans le panneau Analyse de paquets.
- Si les octets d'ombrage sont affichés dans le panneau Analyse de paquets.
- Si les autres types de fichiers communs sont mis en surbrillance dans le panneau Analyse de paquets.
- Nombre de paquets par page dans le panneau Analyse de paquets.
- Si le texte compressé ou décompressé s'affiche dans le panneau Analyse de texte.
- Le paramètre de décodage de texte dans le panneau Analyse de texte d'un événement de réseau.

Le panneau d'analyse de texte

Vous pouvez afficher tous les types d'événements (événements de réseau, événements de log et événements de point de terminaison) dans leur format de texte d'origine dans le panneau Analyse de texte. Les contrôles de pagination ajoutent de la souplesse lors de la pagination via le texte reconstruit d'un événement.

Remarque : Il est possible de réaliser une procédure d'enquête sur des événements de point de terminaison dans la version 11.1 ou supérieure. Les contrôles de pagination sont disponibles dans la version 11.2 et versions ultérieures.

Le panneau Analyse de texte pour certains événements de réseau peut être très volumineux. Pour assurer un rendu optimal, une charge utile excessivement volumineuse est tronquée à l'échelle. Si une seule requête ou réponse reconstruite dans l'événement reconstruit dépasse le nombre maximal d'octets, l'en-tête indique que le message a été tronqué. Cette figure illustre une réponse unique qui a été tronquée car elle dépasse le nombre maximal d'octets (version 11.2).



La version 11.1 traite les charges utiles volumineuses différemment ; la charge utile pour un seul événement est limitée à 2 500 paquets. Lorsque la limite de paquets est atteinte, un avertissement dans le pied de page indique que la limite a été atteinte et fournit le nombre total de paquets dans l'événement. Cette figure illustre l'info-bulle qui s'affiche lorsque vous pointez sur l'avertissement.

Remarque : L'option Afficher plus est toujours disponible pour les messages tronqués, toutefois, l'intégralité du texte du message n'est pas visible sans télécharger la charge utile brute.

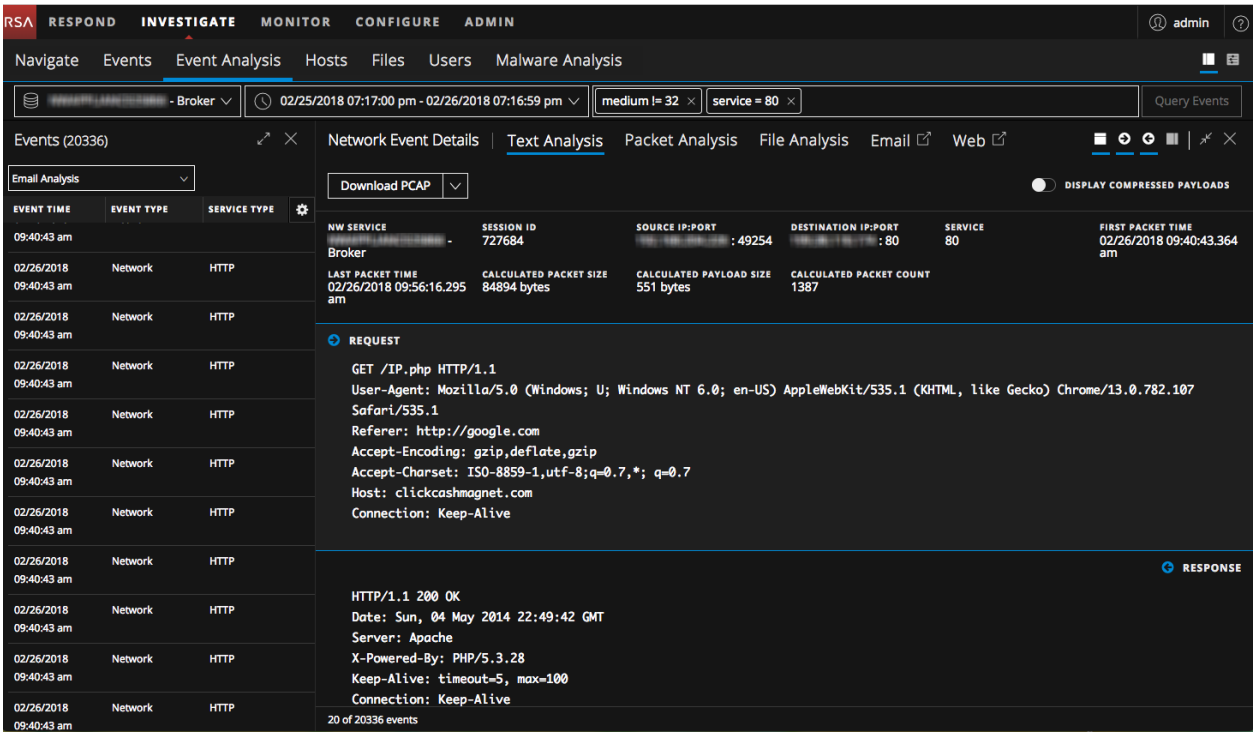
Dans le panneau Analyse de texte, les événements de réseau, les événements de log et les événements de point de terminaison sont présentés différemment.

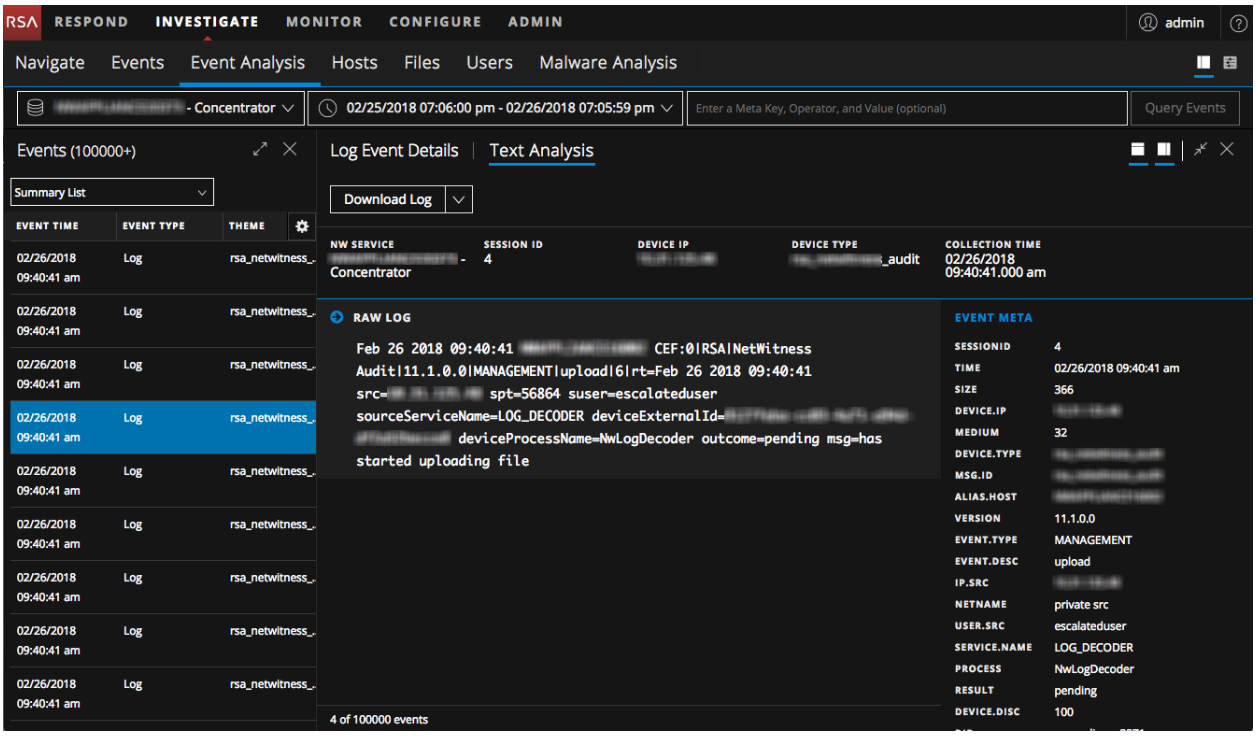
- Pour les événements de réseau, la vue Enquêter affiche l'orientation du paquet (demande ou réponse) et le contenu de chaque paquet au format texte. Si vous reconstruisez un événement de réseau, le panneau Analyse de texte est déroulant. Lorsque vous faites défiler la liste, les informations relatives au texte d'identification ainsi que les libellés de requête et de réponse restent visibles, au lieu de quitter l'affichage.
- Les événements de log et les événements de point de terminaison ne présentent pas de requête ou de réponse. Seul l'événement brut s'affiche dans le panneau Analyse de texte.

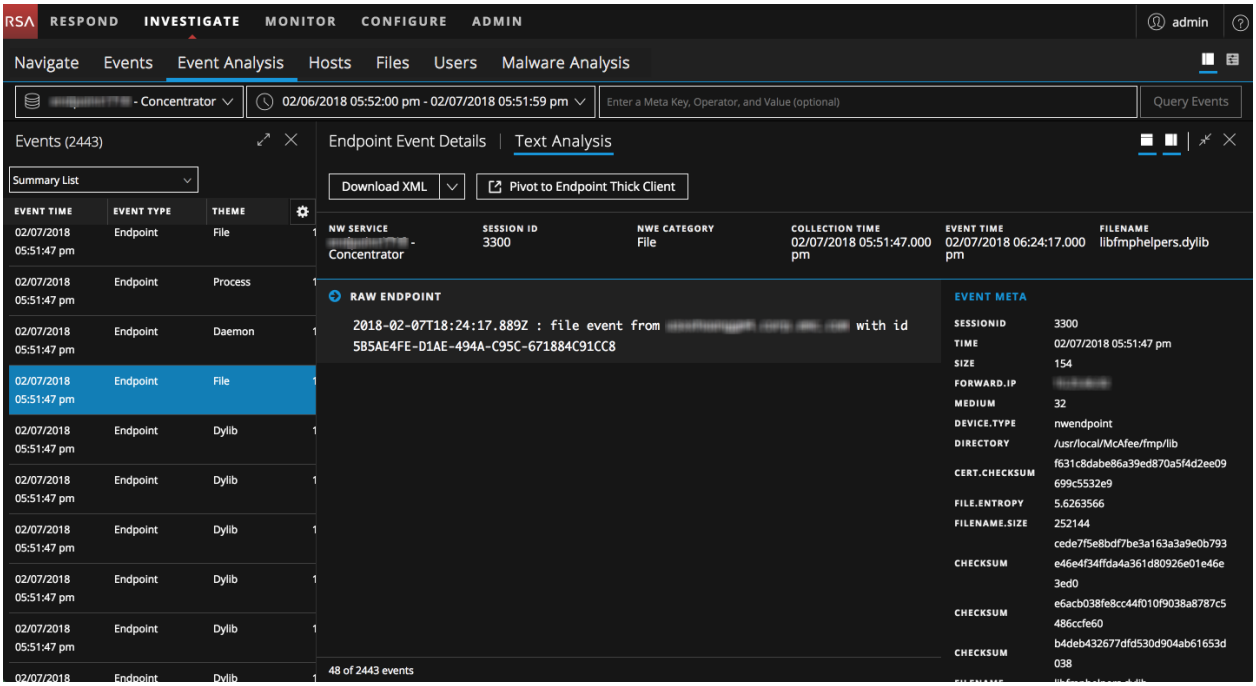
Pour chaque type d'événement (réseau, log ou point de terminaison), il existe plusieurs différences :

- L'en-tête Événement comprend des informations pertinentes pour chaque type d'événement.
- Il existe plusieurs options pour l'exportation.

Voici un exemple du panneau Analyse de texte pour chaque type d'événement, un événement de réseau, un événement de log et un événement de point de terminaison.



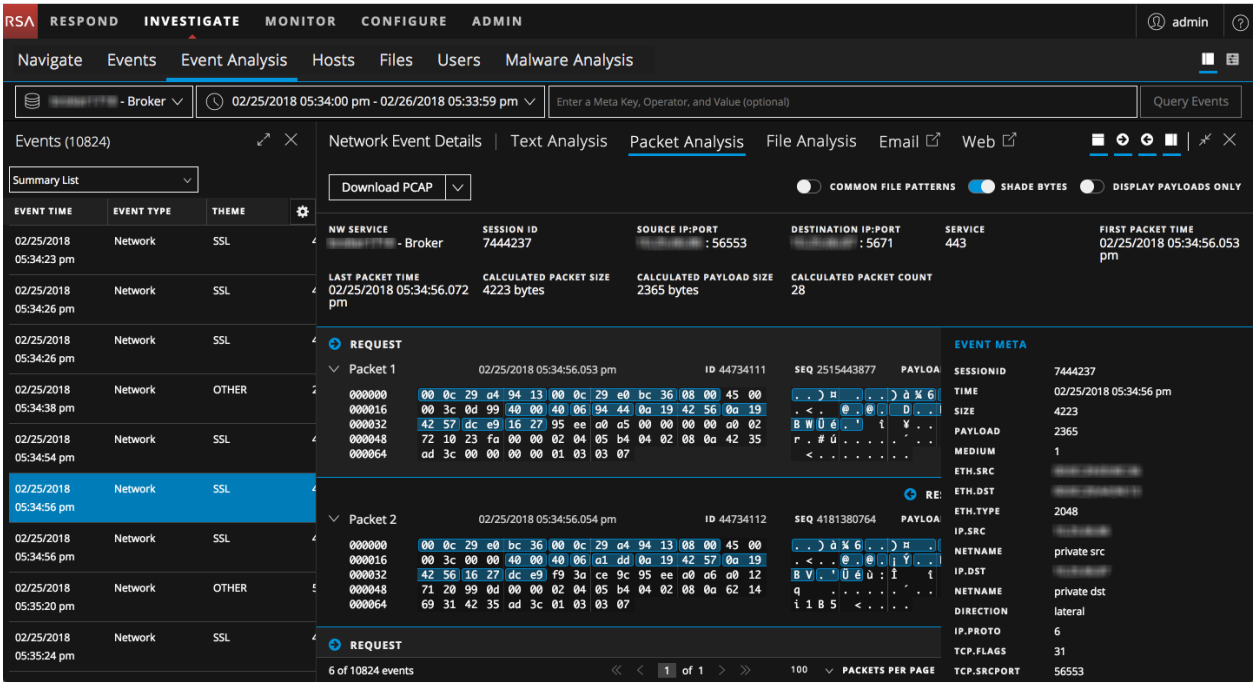




Remarque : Le nombre de paquets calculé, la taille de paquets calculée et la taille de charge utile calculée dans l'en-tête Événement peut être différente des mêmes statistiques dans le Panneau Méta de l'événement car les métadonnées sont parfois écrites avant la fin de l'analyse des événements et peuvent inclure des doublons de paquets.

Le panneau d'analyse des paquets

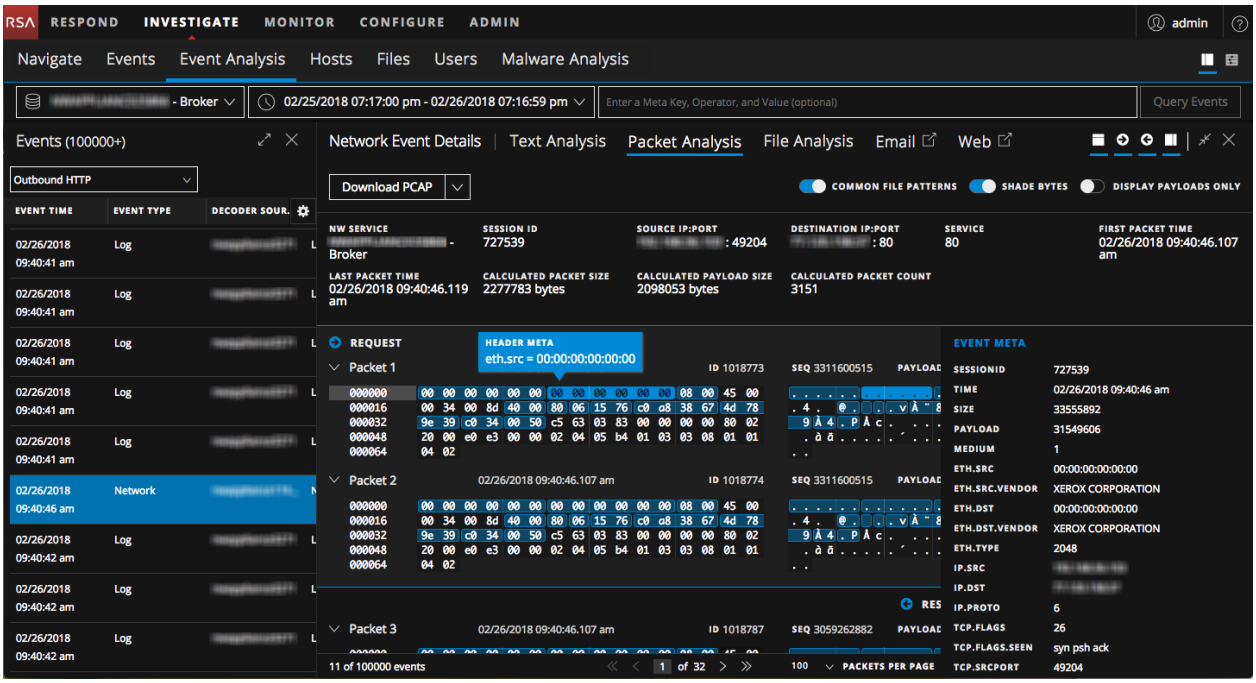
Le panneau Analyse de paquets concerne uniquement les événements de réseau. Le panneau Analyse de paquets peut défiler et les informations d'identification du paquet, ainsi que les libellés de requête et de réponse, restent visibles, au lieu de quitter l'affichage.



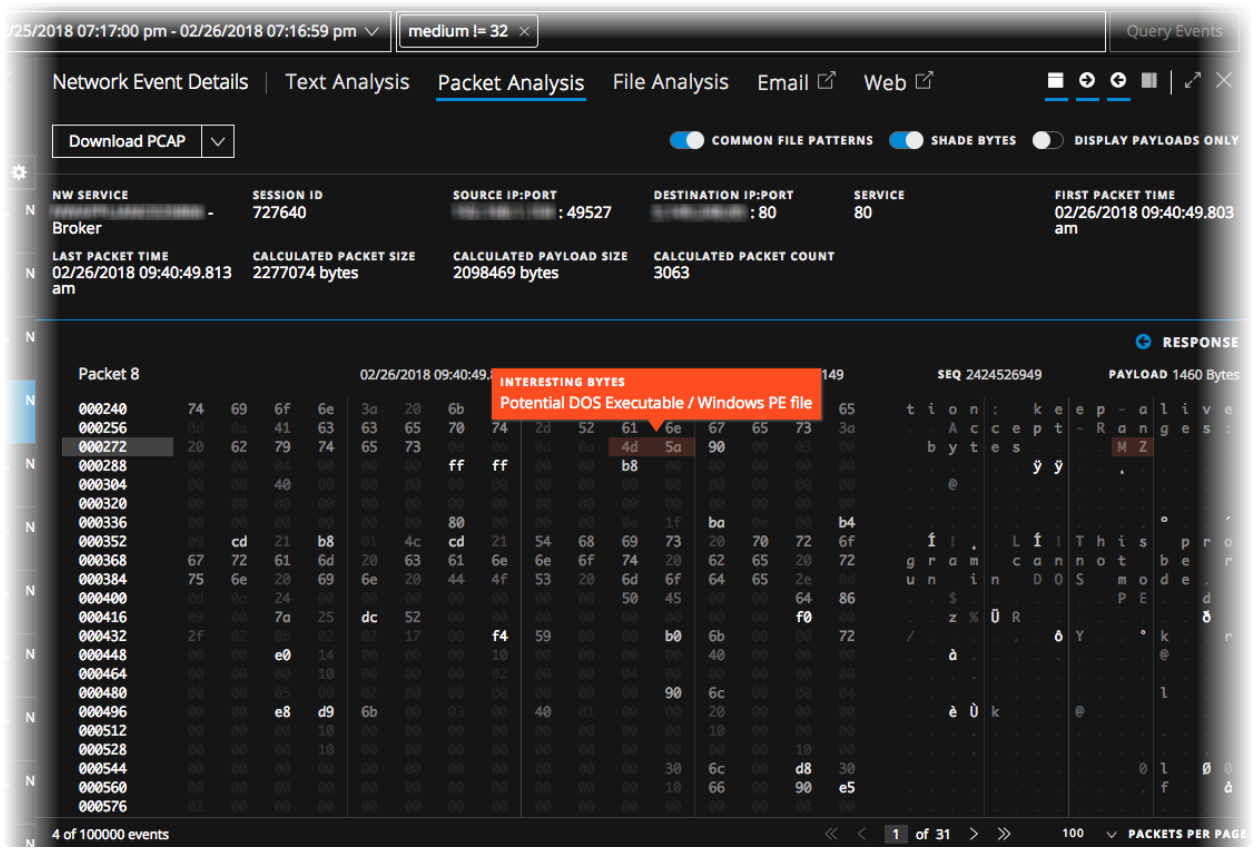
Dans le panneau Analyse de paquets, les en-têtes fournissent la direction du paquet (demande ou réponse), le nombre de paquets, l'heure de début du paquet, l'ID de paquet et la séquence, ainsi que la taille de la charge utile. Tous les paquets commencent par un en-tête, et certains paquets ont un pied de page. Certains paquets ont une charge utile.

Dans la version 11.1, les commandes de pagination ajoutent de la flexibilité pour parcourir les paquets.

Les métadonnées au format hexadécimal et les données ASCII sont mis en surbrillance en bleu ; lorsque vous placez le curseur sur les métadonnées en surbrillance, les informations de valeur de clé méta/méta s'affichent dans une zone de survol.

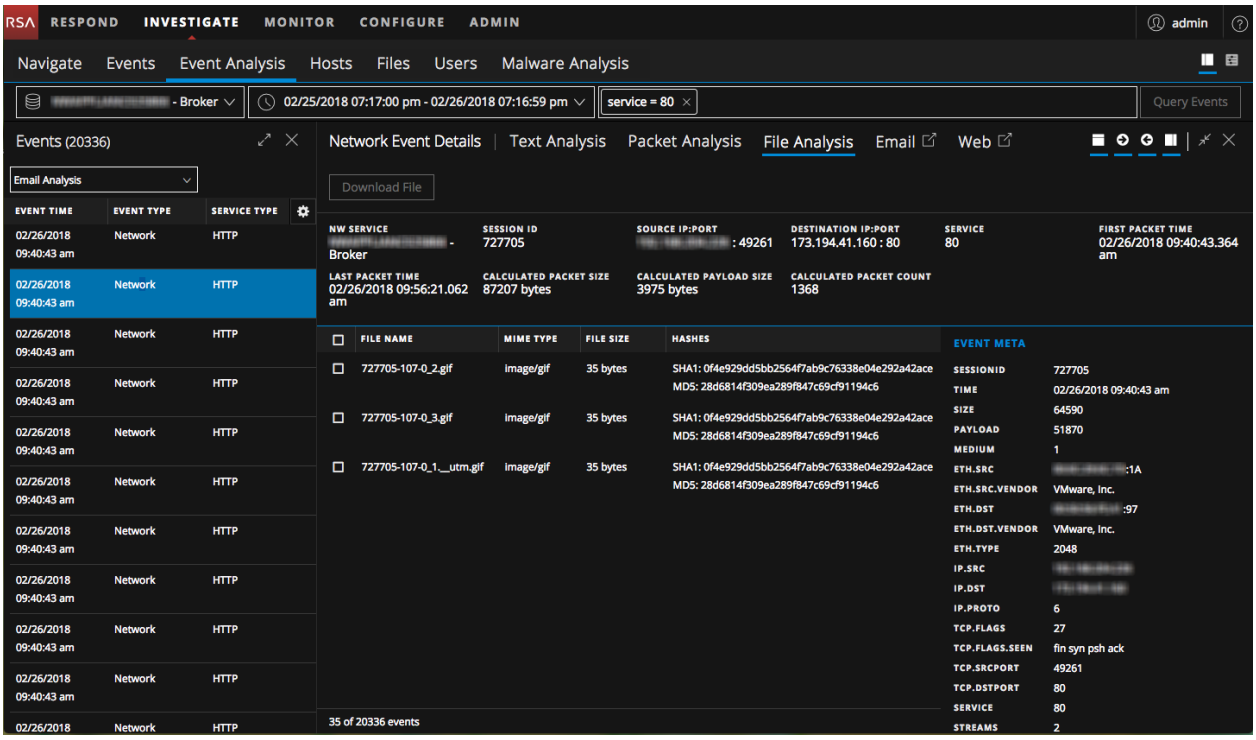


Les signatures de fichiers courants sont mises en surbrillance en orange. Lorsque vous placez le curseur sur le texte en surbrillance, la description du type de fichier s'affiche dans une zone de survol.

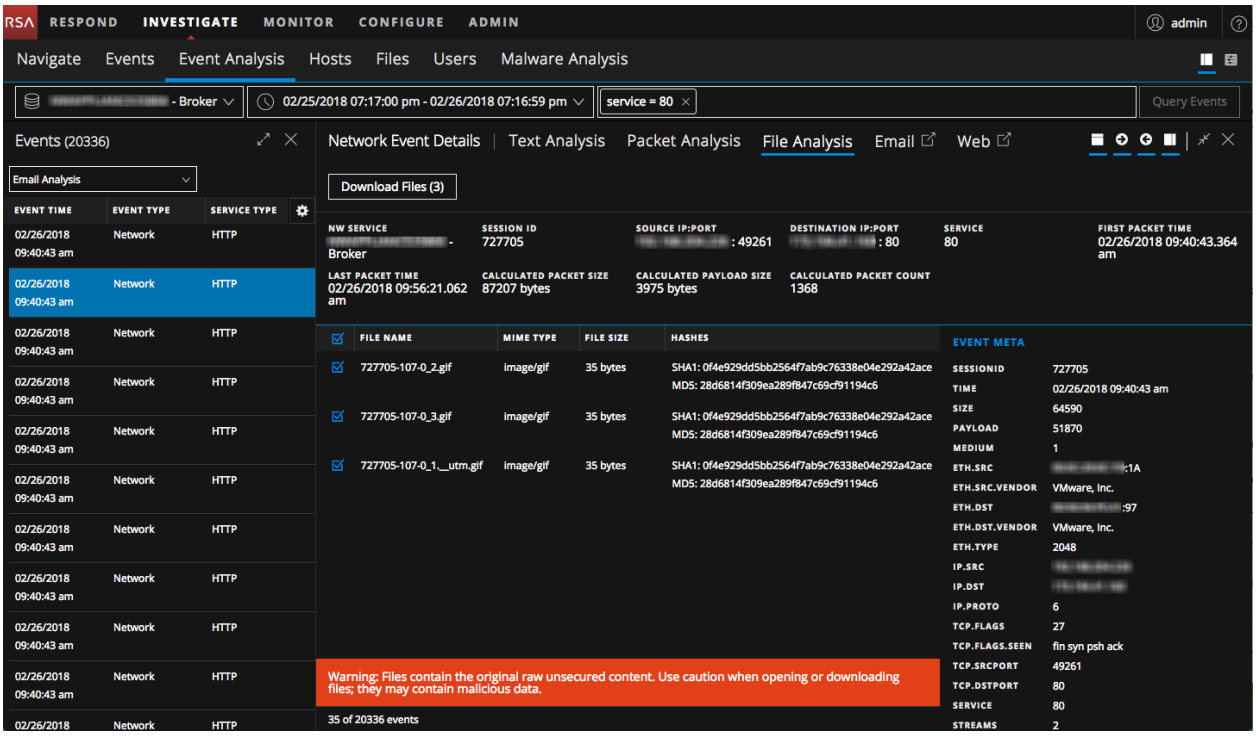


Le panneau Analyse de fichiers

Le panneau Analyse de fichiers présente une liste de fichiers associés à l'événement de réseau sélectionné. Voici un exemple du panneau Analyse de fichiers.



Vous pouvez sélectionner un seul fichier, un ou plusieurs fichiers ou tous les fichiers à exporter vers votre système de fichiers local. Lorsque des fichiers sont sélectionnés, le bouton Exporter les fichiers devient actif et reflète le nombre de fichiers sélectionnés.



Attention : Procédez avec prudence lors de la décompression et de l'ouverture de fichiers qui sont associés à une application par défaut ; par exemple, une feuille de calcul Excel peut automatiquement s'ouvrir dans Excel avant de vous permettre d'avoir le temps de vérifier qu'elle ne présente aucun risque.

Outils d'analyse pour chaque type d'analyse d'événements

Les outils d'analyse dans la vue Analyse d'événements sont conçus pour aider les analystes à trouver les informations pertinentes pour les différents types d'événements (événement de réseau, événement de log et événement de point de terminaison). Ce tableau répertorie les actions que vous pouvez entreprendre par type d'événement. Le reste de cette section fournit des procédures pour effectuer les actions.

Action	Événement réseau	Consignation d'événements	Événement de point de terminaison
Afficher le panneau Analyse de texte	✓	✓	✓
Afficher le panneau Analyse de fichiers	✓		
Afficher le panneau Analyse des paquets	✓		
Ouvrir, fermer et ajuster la taille des panneaux	✓	✓	✓
Régler l'affichage des demandes et réponses	✓		

Action	Événement réseau	Consignation d'événements	Événement de point de terminaison
Afficher ou masquer l'en-tête d'événement dans le panneau Analyse de texte	✓	✓	✓
Développer les entrées de texte tronquées dans le panneau Analyse de texte	✓		
Basculez entre une vue compressée et une vue décompressée des charges utiles dans le panneau Analyse de texte	✓		
Afficher les octets mis en surbrillance dans le panneau Analyse des paquets	✓		
Mettre en surbrillance les types de fichiers communs dans le panneau Analyse des paquets	✓		
Afficher uniquement la charge utile dans le panneau Analyse des paquets	✓		
Griser les octets dans le panneau Analyse des paquets lors de l'affichage de la charge utile uniquement	✓		
Effectuer un codage et un décodage URL et Base64 dans le panneau Analyse de texte	✓		
Afficher le texte décompressé pour une session de réseau HTTP dans le panneau Analyse de texte	✓		
Afficher les métadonnées d'événements pour un événement dans le panneau Analyse de texte	✓	✓	✓
Télécharger un événement de réseau (comme un fichier PCAP, charge utile uniquement, demande uniquement ou réponse uniquement) dans le panneau Analyse des paquets ou Analyse de texte	✓		
Exporter des fichiers à partir d'un événement de réseau dans le panneau Analyse de fichiers	✓		
Télécharger le fichier pour un événement de log dans le panneau Analyse de texte		✓	
Télécharger le fichier pour un événement de point de terminaison dans le panneau Analyse de texte			✓

Action	Événement réseau	Consignation d'événements	Événement de point de terminaison
Ouvrir l'événement de point de terminaison actuel dans le panneau Analyse de texte			✓

Filtrer les résultats dans la vue Analyse d'événements

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Dans NetWitness Platform version 11.0, vous envoyez une requête dans la vue Naviguer ou Événements, et lorsque vous accédez à la vue Analyse d'événements, un fil d'Ariane en lecture seule affiche la requête soumise. Vous devez revenir à la vue Vue Événements ou la vue Naviguer si vous souhaitez saisir une requête différente.

Dans la version 11.1 ou supérieure, un générateur de requête renseigne le fil d'Ariane interactif dans la vue Analyse d'événements afin que vous puissiez créer et modifier chaque filtre `<meta key> <operator> <meta value>` dans le fil d'Ariane. En outre, vous pouvez sélectionner un service et une période différente sans revenir à la vue Naviguer ou Événements. Le reste de cette section fournit des informations sur l'utilisation des fonctions du Générateur de requête.

Comment fonctionne le fil d'Ariane ?

Lorsque vous cliquez sur l'option Analyse d'événements sous Enquêter pour ouvrir la vue, le sélecteur de service et de période s'affiche. Par défaut, le premier service est sélectionné automatiquement (sauf si vous avez sélectionné précédemment un service et si le service sélectionné est mémorisé dans le navigateur). Si vous ne sélectionnez pas de période, la période par défaut (3 heures) est utilisée. Le champ Générateur de requête est un champ vide à droite de la période.

Lorsque vous ouvrez la vue Analyse d'événements à partir de la vue Événements ou Naviguer, le service, la période et tous les filtres qui ont été sélectionnés dans la vue Événements ou Naviguer s'affichent dans le fil d'Ariane. Le service, la période et les filtres individuels peuvent être modifiés.

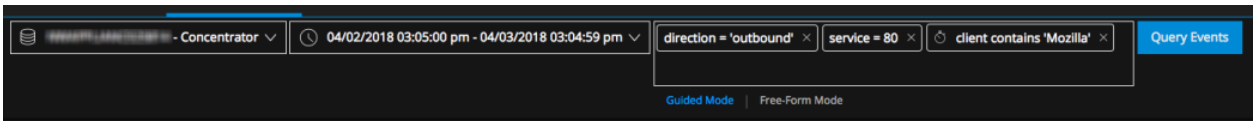
À partir de la version 11.2, en plus de la création d'une requête en mode guidé, les analystes avancés peuvent entrer une requête en mode formulaire libre. Le mode par défaut est le mode guidé, qui inclut les options de suggestion automatique et de validation. Le mode formulaire libre vous permet de saisir une requête complexe ; la validation est effectuée lorsque vous exécutez la requête.

Remarque : Une requête complexe est une requête autre qu'un filtre <meta key> <operator> <value> qui contient des opérateurs `()`, `||`, `&&`, `length`, ou `regex`.

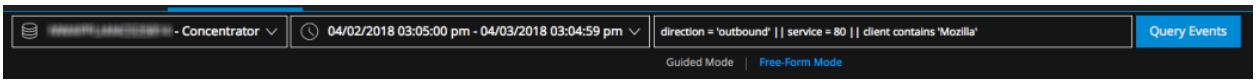
Deux boutons basculent entre les modes et placent un curseur dans la barre de requête afin de créer une requête immédiatement. Si vous avez sélectionné le mode Formulaire libre la dernière fois que vous vous êtes connecté, ce choix reste actif lors de votre connexion suivante.

- Lorsque vous passez du mode Guidé au mode formulaire libre, les filtres que vous avez créés en mode Guidé sont transformés en une requête de texte dans le champ Formulaire libre.
- Lorsque vous passez du mode Formulaire libre au mode Guidé, la requête que vous saisissez est ajoutée au générateur de requêtes sous la forme d'un seul filtre non modifiable.
- Si vous démarrez la création d'une requête avec plusieurs filtres en mode Guidé, puis basculez en mode formulaire libre, puis revenez en mode Guidé sans aucune modification, et les filtres multiples conservent le même état.

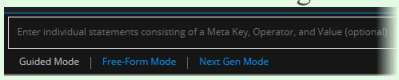
La figure suivante est un exemple de la vue Analyse d'événement avec le générateur de requêtes en mode Guidé en actif.



La figure suivante donne un exemple de la vue Élaborer le formulaire libre de requête.

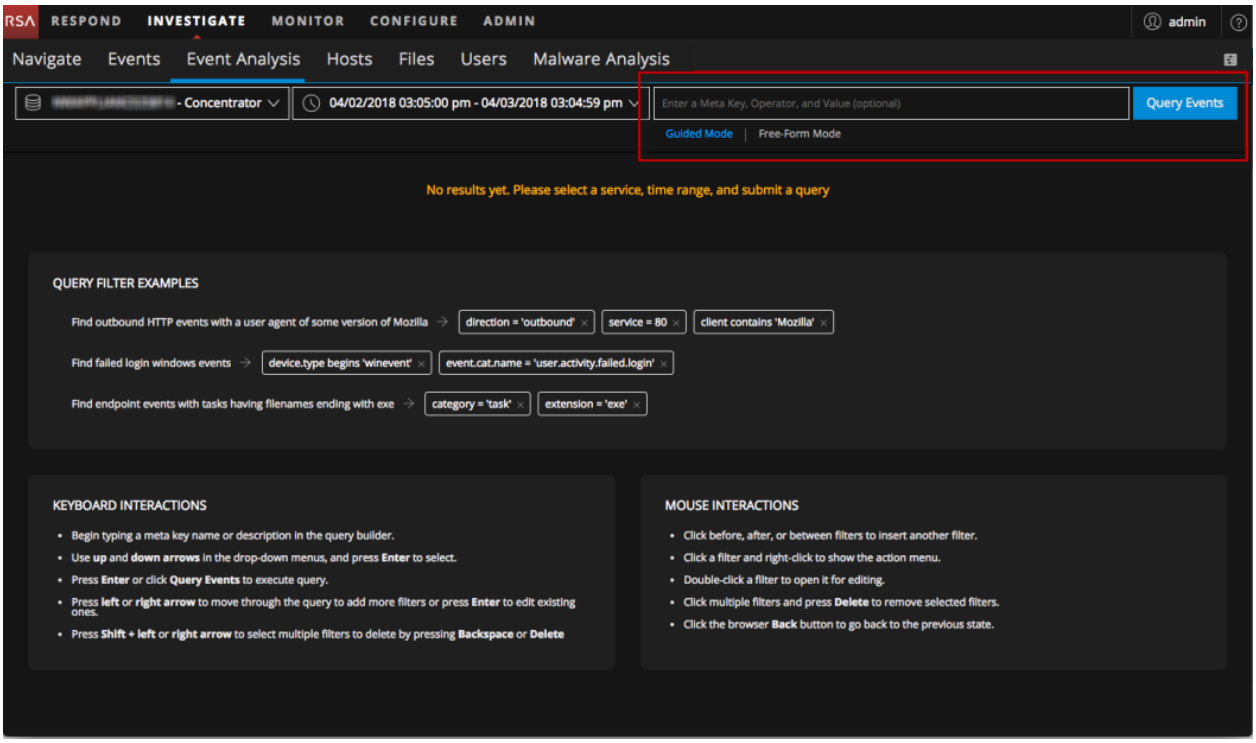


Remarque : La version 11.2 comprenait une fonctionnalité bêta non documentée, appelée mode Next Gen, dans le générateur de requêtes de la vue Analyse d'événements qui était encore en cours de développement et de test. Le mode Next Gen a été désactivé dans le correctif 11.2.0.1. Si vous voyez le mode Next Gen ne l'utilisez pas ; vous devez utiliser uniquement le mode Guidé et le mode Formulaire libre dans le générateur de requêtes pour garantir des résultats cohérents et prévisibles.



Générateur de requêtes en mode Guidé

Le mode Guidé est le moyen le plus simple de créer une requête avec des fonctionnalités permettant aux analystes d'entrer des requêtes valides. La figure suivante illustre la vue initiale Analyse d'événements avec le générateur de requêtes en mode Guidé actif.



Remarque : Le Générateur de requête du mode Guidé ne prend en charge que les filtres simples sous la forme `<meta key><operator><meta value>`. Si la vue Événements ou la vue Naviguer dispose d'un filtre avec plus d'un opérateur `not`, `>`, `<`, `<=`, `>=`, `||`,`&&`, `()`, `REGEX`ou `LENGTH`, le filtre est ajouté, mais la modification n'est pas prise en charge dans la vue Analyse d'événements. Il en va de même pour un filtre introduit à partir du générateur de requêtes du formulaire libre.

Lorsque vous créez des filtres dans le Générateur de requête du mode Guidé, le fil d'Ariane est mis à jour avec chaque filtre dans un champ modifiable. Lorsque vous exécutez la requête, AND est attribué à tous les filtres pour générer les résultats. La requête n'est envoyée que si vous cliquez sur Interroger des événements. Les filtres s'alignent de gauche à droite, selon l'ordre dans lequel ils ont été créés. Chaque filtre est une expression simple sous la forme `<meta key> <operator> <optional value>`. Si plusieurs filtres sont ajoutés et ne peuvent pas être affichés sur une seule ligne, ils s'affichent sur une autre ligne et la zone de saisie s'étend verticalement de façon à ce que tous les filtres soient visibles sans défilement vers la droite.

Lorsque vous créez et modifiez des filtres, vous obtenez une assistance sous forme de suggestions en saisie semi-automatique qui n'affichent que des clés méta et des opérateurs valides dans la liste déroulante. Vous pouvez effectuer une saisie ou une sélection dans la liste déroulante. Dans la liste déroulante, les opérations dont l'exécution prend plus de temps sont accompagnés d'une icône de chronomètre. Les filtres non valides sont encadrés en rouge et si vous passez la souris sur le filtre, une infobulle expliquant l'erreur s'affiche.

Le bouton Interroger des événements se trouve sur le côté droit de la saisie du fil d'Ariane et il devient actif lorsqu'une saisie de requête est nécessaire. Une requête est envoyée lorsque vous cliquez sur Événements de requête ou appuyez sur Entrée après la création d'un filtre. Lorsqu'un jeu de résultats est chargé et que vous modifiez le service, la période ou un filtre, le bouton Interroger des événements devient bleu, ce qui indique que les données de la vue sont désormais obsolètes. Dans la version 11.2 et versions ultérieures, le bouton Événements de requête deviendra également bleu au bout d'une minute car la plage de temps de la requête d'origine ne génère plus le même jeu de résultats.

Remarque : Si vous modifiez le service, un appel réseau de données de reconstructions ou de données supplémentaires dans le panneau Événements (par exemple, Charger davantage) utilise les filtres précédemment utilisés pour le service/période/métadonnées. L'appel de réseau continue d'utiliser les paramètres de la requête précédente jusqu'à ce que vous soumettiez la nouvelle requête.

Actions du clavier à utiliser en mode Guidé

Dans le mode Guidé, le générateur de requête est conçu pour permettre la saisie, la modification et la suppression de filtres à l'aide du clavier, sans avoir à utiliser de pointeur. Bien que l'utilisation du pointeur soit possible, vous pouvez garder les doigts sur le clavier. Ce tableau identifie les actions du clavier disponibles lorsque le curseur se trouve dans la partie du Générateur de requête du mode Guidé du fil d'Ariane. Celles-ci ne s'appliquent pas au sélecteur de service et de période.

Action	Saisie clavier
Envoyer une requête	En pointant le Générateur de requête et sur les filtres qui ne sont pas en attente, appuyez sur **Entrée.**
Sélectionner le filtre situé immédiatement à gauche, s'il existe.	Sans aucune sélection dans le Générateur de requête, appuyez sur la touche de la **flèche vers la gauche**.
Sélectionner le filtre situé immédiatement à droite, s'il existe.	Sans aucune sélection dans le Générateur de requête, appuyez sur la touche de la **flèche vers la droite**.
Insérer un nouveau filtre immédiatement à gauche du filtre sélectionné.	Lorsqu'un filtre est sélectionné, appuyez sur la touche de la **flèche vers la gauche**.

Action	Saisie clavier
Insérer un nouveau filtre immédiatement à droite du filtre sélectionné.	Lorsqu'un filtre est sélectionné, appuyez sur la touche de la **flèche vers la droite**.
Insérer un nouveau filtre immédiatement à droite du filtre sélectionné et l'ouvrir pour le modifier.	Lorsqu'un filtre est sélectionné, appuyez sur les touches **Maj + Flèche vers la gauche**.
Insérer un nouveau filtre immédiatement à droite du filtre sélectionné et l'ouvrir pour le modifier.	Lorsqu'un filtre est sélectionné, appuyez sur les touches **Maj + Flèche vers la droite**.
Sélectionner tous les filtres à droite du filtre actuel.	Lorsqu'un filtre est sélectionné, appuyez sur les touches **Maj + Flèche vers le bas**.
Sélectionner tous les filtres à gauche du filtre actuel.	Lorsqu'un filtre est sélectionné, appuyez sur les touches **Maj + Flèche vers le haut**.
Modifier un filtre sélectionné	Lorsqu'un filtre est sélectionné, appuyez sur la touche **Entrée**.
Désélectionner tous les filtres.	Lorsqu'un filtre est sélectionné, appuyez sur la touche **Échap**.
Supprimer tous les filtres sélectionnés.	Lorsque des filtres sont sélectionnés, **cliquez avec le bouton droit > Supprimer les filtres sélectionnés**, appuyez sur **Supprimer** ou sur **Retour arrière**.
Mettre à jour la requête avec uniquement les filtres sélectionnés.	Lorsque des filtres sont sélectionnés, **cliquez avec le bouton droit > Requête avec des filtres sélectionnés**.
Ouvrir un nouvel onglet avec les filtres sélectionnés.	Lorsque des filtres sont sélectionnés, **cliquez avec le bouton droit > Requête avec des filtres sélectionnés dans un nouvel onglet**.

Rétroaction en mode Guidé

Le mode Guidé fournit des commentaires visuels pendant la création des requêtes. Ce tableau identifie et décrit les commentaires possibles.

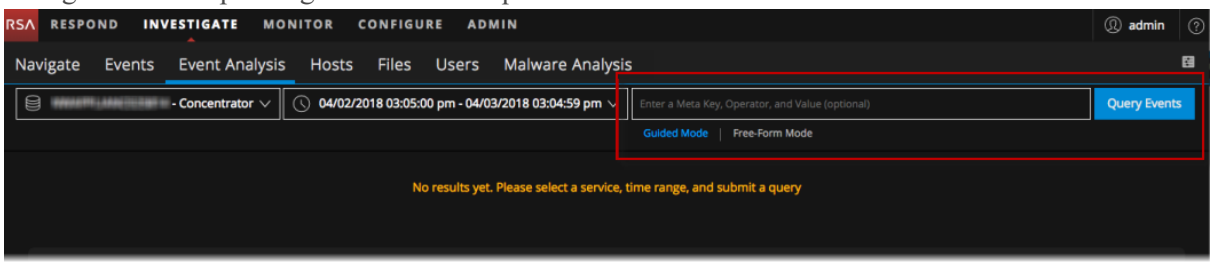
Commentaires	Icône	Description
Cercle vert		Le curseur a été placé entre deux filtres existants. Le fait de cliquer insère un nouveau filtre à cet emplacement.

Commentaires	Icône	Description
Contour rouge d'un filtre		Le type de valeur n'est pas valide pour la clé méta sélectionnée, par exemple, une valeur de chaîne pour une clé méta où un chiffre entier doit être saisi. Une info-bulle expliquant l'erreur qui s'affiche.
Chronomètre		La combinaison clé/opérateur sélectionnée nécessite un délai de traitement supplémentaire. La requête reste exécutable, mais une clé meta ou un opérateur plus efficace est recommandé.

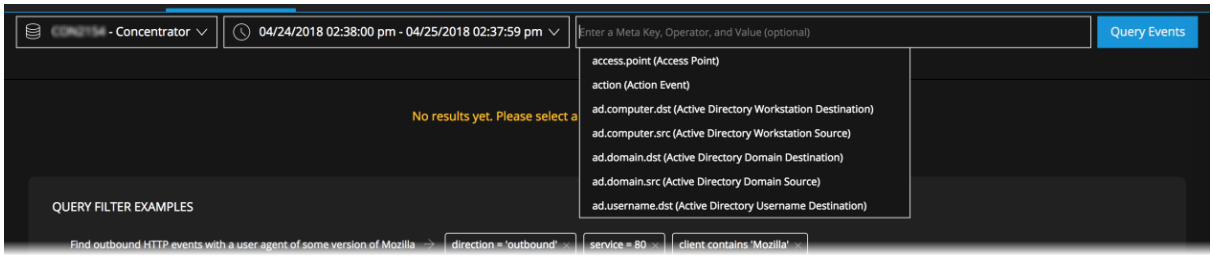
Ajouter un filtre en mode Guidé

Pour filtrer les données affichées dans la vue Analyse d'événements du mode Guidé :

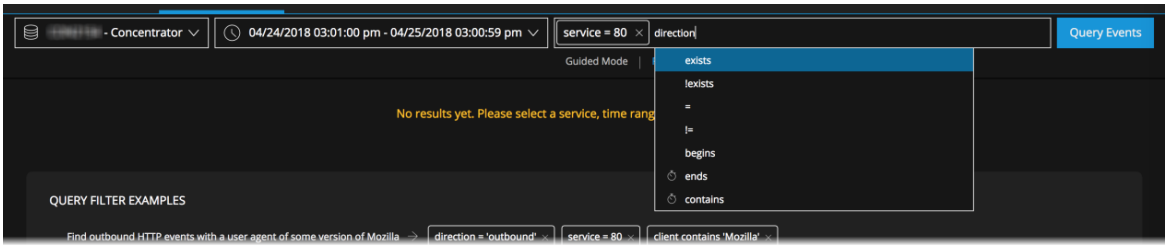
1. Accédez à la vue vue **Analyse d'événements** et sélectionnez le **mode Guidé** sous le générateur de requêtes.
   Il s'agit d'un exemple de générateur de requêtes vide en mode Guidé avant la saisie d'un filtre.



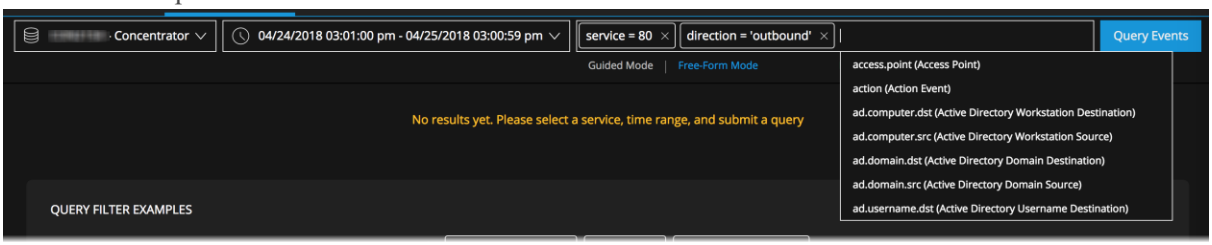
2. Pour insérer un filtre, cliquez dans le champ du Générateur de requête, ou avant ou après un filtre existant.
   Si le point d'insertion se trouve entre deux filtres, un point vert marque le point d'insertion. Si le point d'insertion se trouve à la fin du fil d'Ariane existant, le champ de saisie de filtre s'ouvre et présente un curseur clignotant au point d'entrée. Un menu déroulant répertorie les clés méta disponibles pour le service sélectionné par ordre alphabétique. Les clés méta disponibles sont transmises à partir du service en cours d'investigation, et les clés méta nécessitant plus de temps de traitement sont marquées par une icône de chronomètre.



3. Pour sélectionner une clé méta, effectuez l'une des actions suivantes :
   a. S'il n'existe qu'une seule option dans le menu déroulant, appuyez sur **Entrée**.
   b. S'il existe deux options ou plus dans le menu déroulant, cliquez sur la clé méta ou utilisez la flèche vers le haut/bas et appuyez sur **Entrée**.
   c. Commencez à saisir la clé méta. Lorsque vous saisissez la clé méta, la liste est encore mise à jour. Pour sélectionner la clé méta, appuyez sur **Entrée**.
   d. Si vous souhaitez modifier ou supprimer la clé méta, appuyez sur **Retour arrière** ou **sur**Supprimer.
   Lorsque vous effectuez un retour arrière et supprimez un caractère, la liste déroulante de clés méta est filtrée pour inclure les clés méta qui commencent par ces caractères. Pour sélectionner une clé méta, appuyez sur **Entrée**.
   La clé méta est ajoutée au générateur de requêtes, une liste d'opérateurs valides pour la clé méta sélectionnée s'affiche. Les opérations dont l'exécution prend plus de temps sont accompagnés d'une icône de chronomètre.



4. Pour sélectionner un opérateur, effectuez l'une des actions suivantes :
   a. S'il n'existe qu'une seule option dans le menu déroulant, appuyez sur **Entrée**.
   b. S'il existe deux options ou plus dans le menu déroulant, cliquez sur l'opérateur ou utilisez la flèche vers le haut/bas et appuyez sur **Entrée**.
   c. Saisissez l'opérateur et appuyez sur **Entrée**.
   La liste déroulante se ferme et vous pouvez ajouter une valeur si l'opérateur accepte une valeur.
5. (Facultatif) Saisissez une valeur et appuyez sur **Entrée**.
6. Pour créer le filtre, appuyez sur **Entrée**. Si vous cliquez n'importe où en dehors du cadre avant d'appuyer sur **Entrée**, le filtre n'est pas créé.
   Le nouveau filtre est inséré et le curseur clignotant est recentré après le dernier filtre, puis le menu déroulant des clés méta s'affichent. Si le filtre comporte une erreur, il est signalé en rouge. Vous pouvez passer le curseur sur le filtre pour afficher une infobulle expliquant l'erreur. Cette figure montre une requête en cours de création sans erreurs.



7. Corrigez tous les filtres qui présentent des erreurs.

8. Lorsque vous êtes prêt à exécuter la requête dans le fil d'Ariane, cliquez sur **Interroger des événements**.
9. La Liste d'événements est actualisée pour refléter la requête.

Modifier un filtre en mode Guidé

Avec une requête dans le générateur de requêtes en mode Guidé, vous pouvez modifier un filtre. Pour modifier un filtre :

1. Double-cliquez dessus ou cliquez sur le filtre et appuyez sur **Entrée**.
2. Modifiez le filtre. Lorsque la modification est terminée, appuyez sur **Entrée** pour mettre à jour le filtre.
3. Si vous souhaitez exécuter de nouveau la requête, cliquez sur le bouton **Requête**.
   La Liste d'événements est actualisée pour refléter la mise à jour du filtre.

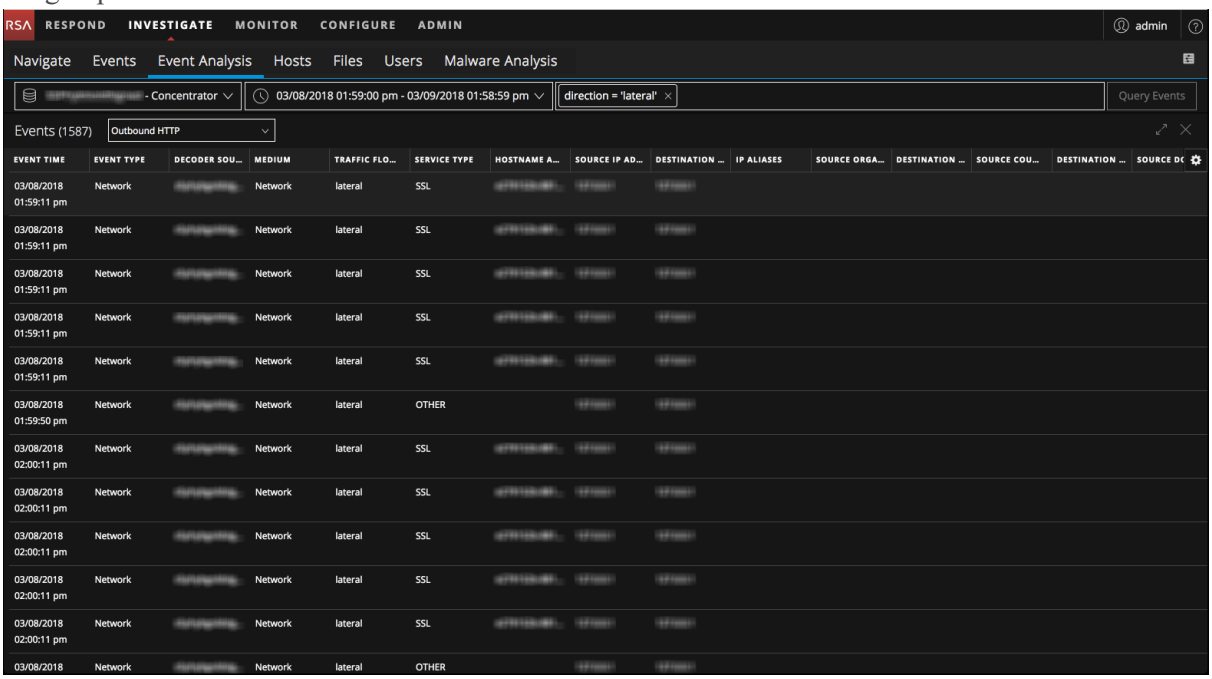
Requête utilisant des filtres sélectionnés en mode Guidé

Lorsque un ou plusieurs filtres dans le générateur de requête du mode Guidé sont appliqués, vous pouvez recentrer la même requête pour inclure uniquement les filtres sélectionnés. Les résultats s'affichent dans l'onglet du navigateur actuel ou dans un nouvel onglet du navigateur. Pour mettre à jour la requête avec uniquement les filtres sélectionnés :

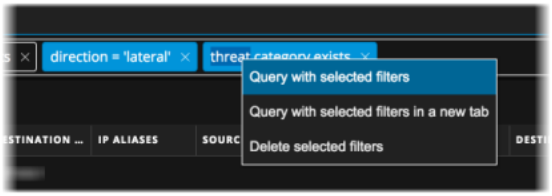
1. Commencez par une requête en mode Guidé incluant un ou plusieurs filtres, par exemple une requête a trois filtres : `risk.info = exists`, `direction ="lateral"` et `threat.category exists`.
2. Pour ouvrir un nouvel onglet avec les filtres sélectionnés, sélectionnez `direction = "lateral"`, cliquez avec le bouton droit sur le filtre et sélectionnez **Requête avec des filtres sélectionnés dans un nouvel onglet** dans le menu déroulant.

   Un nouvel onglet s'ouvre avec les résultats du filtre sélectionné et la requête d'origine est intacte sur

l'onglet précédent.



3. Pour effectuer une requête sur les filtres sélectionnés dans le même onglet, sélectionnez `direction = "lateral"` et `threat.category exists`. Ensuite, cliquez avec le bouton droit et sélectionnez **Requête avec des filtres sélectionnés** dans le menu déroulant.



Une requête avec uniquement les filtres sélectionnés est envoyée et tous les filtres restants sont supprimés.

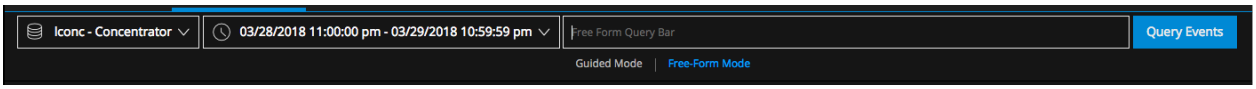
Supprimer un filtre en mode Guidé

Pour supprimer un filtre :

1. Cliquez sur **X** dans un filtre, cliquez sur le filtre pour le sélectionner, puis appuyez sur **Supprimer**, ou cliquez avec le bouton droit sur un ou plusieurs filtres et sélectionnez **Supprimer les filtres sélectionnés** dans le menu déroulant.
2. Si vous souhaitez exécuter de nouveau la requête, cliquez sur le bouton **Requête**.
   Le filtre sélectionné est supprimé et la Liste d'événements est actualisée.

Générateur de requêtes en formulaire libre

Les requêtes de formulaire libre sont plus utiles lorsque vous avez une requête complexe à l'esprit que vous souhaitez entrer rapidement, et que vous connaissez les clés méta, les opérateurs valides et la syntaxe valide pour entrer des valeurs. La figure suivante illustre la vue Analyse d'événement initiale avec le champ de générateur de requêtes de formulaire libre vide.



Le curseur clignotant indique que le système est prêt à entrer une requête. Vous pouvez entrer du texte libre ici. À mesure que plusieurs expressions sont ajoutées et si elles ne peuvent être affichées sur une seule ligne, elles s'affichent sur une autre ligne et la zone de saisie s'étend verticalement de façon à ce que tous les filtres soient visibles sans défilement vers la droite.

Voici quelques exemples de requêtes que vous pouvez saisir en mode forme libre :

Pour rechercher des événements avec un nom d'utilisateur de 8 à 11 caractères semblable à atreeman-72 :

```
user.all length 8-11 && (user.all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')
```

Pour rechercher des événements qui sont des événements de réseau HTTP ou liés aux journaux aix ou ciscoasa :

```
service=80 || (device.type = 'aix','ciscoasa')
```

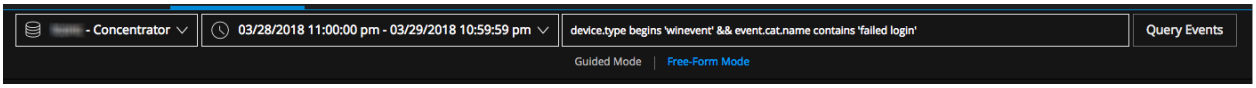
Pour trouver tous les événements sortants qui ne vont pas au Canada ou aux États-Unis :

```
direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')
```

Si vous avez envoyé une requête en mode Guidé, celle-ci est transformée en texte lorsque vous cliquez sur Basculer en mode formulaire libre. Il s'agit d'un exemple de requête soumise en mode Guidé.

Vous pouvez entrer du texte libre ici. Si plusieurs fexpressions sont ajoutées et ne peuvent pas être affichées sur une seule ligne, elles s'affichent sur une autre ligne et la zone de saisie s'étend verticalement de façon à ce que tous les filtres soient visibles sans défilement vers la droite.

Le bouton Interroger des événements se trouve sur le côté droit de la saisie du fil d'Ariane et il apparaît en bleu lorsqu'il est nécessaire de saisir une requête. La requête est appliquée lorsque vous cliquez sur Événements de requête. La requête est alors validée pour afficher les erreurs de syntaxe et de logique.



Les opérations nécessitant un délai de traitement supplémentaire ne sont pas mises en surbrillance car elles sont en mode Guidé, mais ce tableau fournit un résumé des opérations coûteuses, à titre de référence.

Méthode d'index	Valeur non textuelle	Valeur du texte	Opérations régulières	Opérations coûteuses
Par Key	✓		`exists, !exists`	`eq, !eq`

Méthode d'index	Valeur non textuelle	Valeur du texte	Opérations régulières	Opérations coûteuses
Par Key		✓	`exists`, `!exists`	`eq`, `!eq`, `begins`, `ends`, `contains`
Par valeur	✓		`exists`, `!exists`, `eq`, `!eq`	pas d'opérateurs coûteux
Par valeur		✓	`exists`, `!exists`, `eq`, `!eq`, `begins`	`ends`, `contains`
Par None	cas particulier pour`sessionid`		`exist`, `!exits`, `eq`, `!eq`	pas d'opérateurs coûteux

Examiner les événements dans la vue Analyse d'événements

Lorsque vous examinez des métadonnées et événements bruts dans la vue Analyse d'événements, vous pouvez effectuer des ajustements simples dans la visibilité et la taille des panneaux. Dans les panneaux Analyse des paquets et Analyse de texte, des fonctions supplémentaires vous permettent d'ajuster l'affichage de la reconstruction et de révéler des données intéressantes.

Sélectionner le type Analyse d'événements

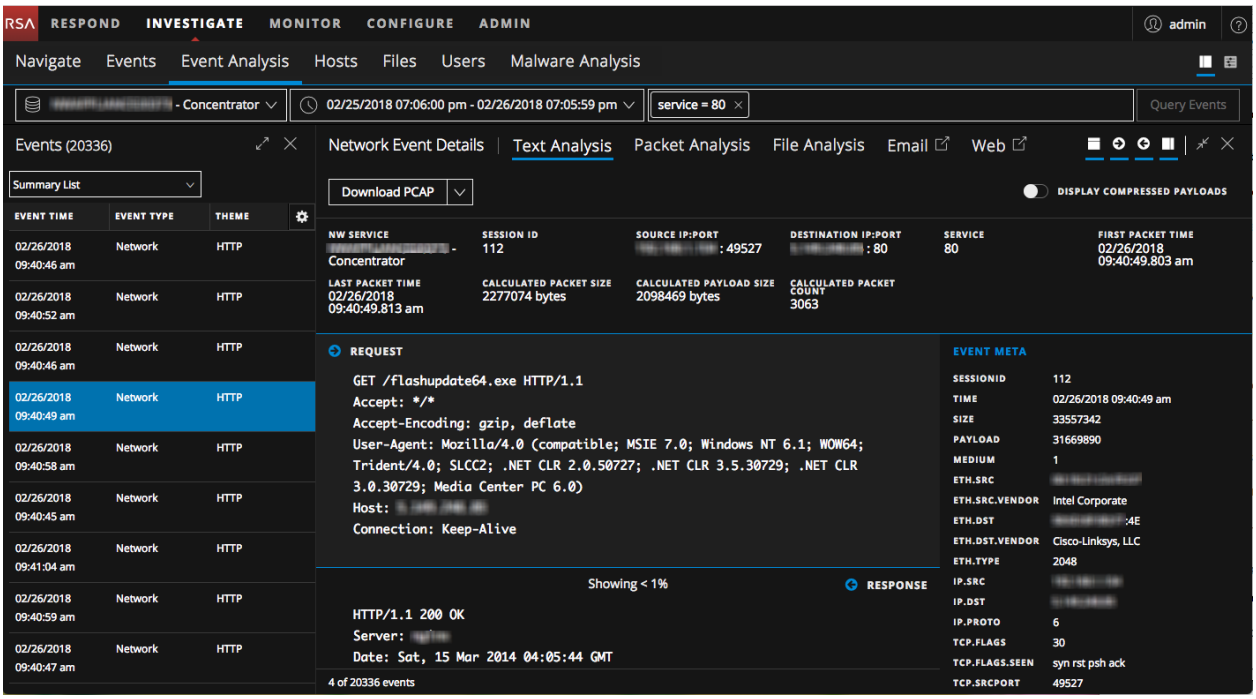
Pour sélectionner le type d'analyse d'événement d'un événement, effectuez l'une des opérations suivantes :

1. Dans la barre d'outils de la **vue Analyse d'événements**, cliquez sur le menu du type d'analyse dans la barre d'outils.
2. Dans le menu déroulant, sélectionnez le type d'analyse : **Analyse de fichiers**, **Analyse de texte**, **Analyse de paquets**, **E-mail** (version 11.1 et supérieure), ou **Web** (version 11.1 et supérieure).
   Si vous avez choisi **Analyse de fichiers**, **Analyse de texte** ou **Analyse de paquets** la vue est actualisée avec le panneau Analyse de paquets, le panneau Analyse de fichiers ou le panneau Analyse de texte ouvert.
   Si vous avez choisi **E-mail** ou **Web**, l'e-mail ou la reconstruction Web de l'événement unique s'ouvre dans nouvel onglet. Il s'agit de la même reconstruction d'e-mail ou de session Web utilisée dans la vue Événements. La vue Événements fournit davantage de fonctionnalités lors de l'affichage d'une reconstruction d'e-mail ou Web, ce qui vous permet de faire défiler les événements dans cette vue au lieu de l'affichage d'un seul événement (reportez-vous à la section Reconstruire un événement).

Remarque : le panneau Analyse de paquets est uniquement disponible pour les événements réseau.

Ouvrir, fermer et ajuster la taille des panneaux dans la vue Analyse d'événements

La vue Analyse d'événements s'ouvre sur la Liste d'événements et aucun événement n'est sélectionné ou reconstruit. Lorsque vous sélectionnez un événement, le panneau Détails des événements réseau, Détails des événements de consignation ou Détails des événements liés aux points de terminaison s'ouvre sur la droite. Au départ, le panneau Détails des événements réseau, Détails des événements de consignation ou Détails des événements liés aux points de terminaison occupe 75 % de la largeur de la fenêtre par défaut.



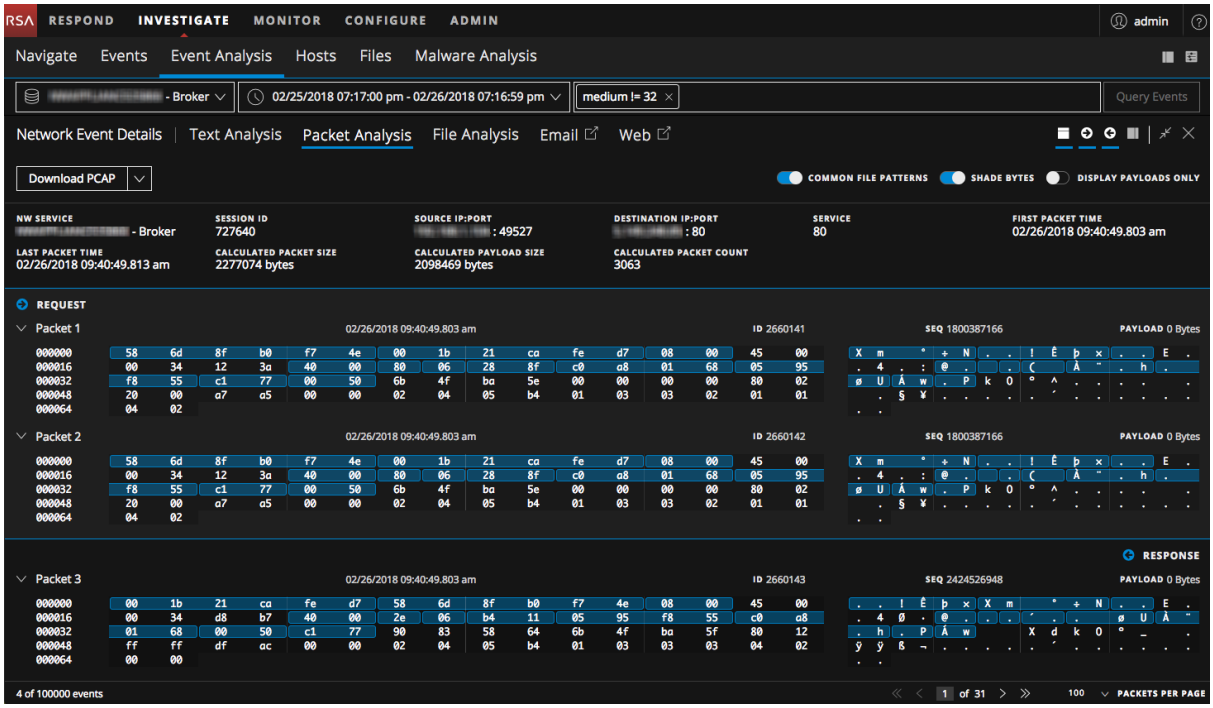
Vous pouvez modifier le rapport de dimensionnement entre les deux panneaux pour améliorer la lisibilité en développant un des panneaux, en en réduisant un ou en fermant un. Vous pouvez rouvrir le panneau après sa fermeture. Le rapport que vous sélectionnez persiste jusqu'à ce que vous modifiiez ou actualisiez le navigateur.

- Pour rouvrir le Panneau Événements, cliquez sur ☐ en haut à droite.

Pour optimiser votre vue :

1. Pour ajuster le rapport de dimensionnement entre les deux panneaux, effectuez l'une des opérations suivantes :
   a. Cliquez sur ◪ dans la barre d'outils du panneau que vous souhaitez étendre.
   b. Cliquez sur ◪ dans la barre d'outils du panneau que vous souhaitez réduire.

2. Pour fermer un panneau et restaurer le panneau ouvert à sa pleine largeur, cliquez sur ▣.
   Il s'agit d'un exemple de la reconstruction affiché sur la largeur totale de la fenêtre du navigateur.



3. Pour rouvrir le Panneau Événements après l'avoir fermé, cliquez sur ◫ en haut à droite de la Vue Naviguer.
   Le Panneau Événements se rouvre avec le dernier état (25%:75% ou 50%:50%).
4. Pour rouvrir le panneau Détails de l'événement, cliquez sur un événement dans le Panneau Événements.

Sélectionnez un Groupe de colonnes et des Colonnes dans l'Analyse d'événements

Dans la version 11.1 ou supérieure, vous pouvez utiliser les groupes de colonnes prédéfinies ou personnalisées dans le panneau Événements. Les groupes de colonnes sont créés et gérés dans la vue Événements (reportez-vous à la section Gérer des groupes de colonnes dans la vue Événements) ; ces groupes sont répercutés dans la vue Analyse d'événements. Lorsque vous modifiez un groupe de colonnes, les modifications que vous y apportez ne s'appliquent qu'à la vue actuelle. Lorsque vous quittez puis revenez à la vue Analyse d'événements, les modifications de colonne ne sont pas conservées dans le panneau Événements.

Voici les groupes de colonnes intégrés.

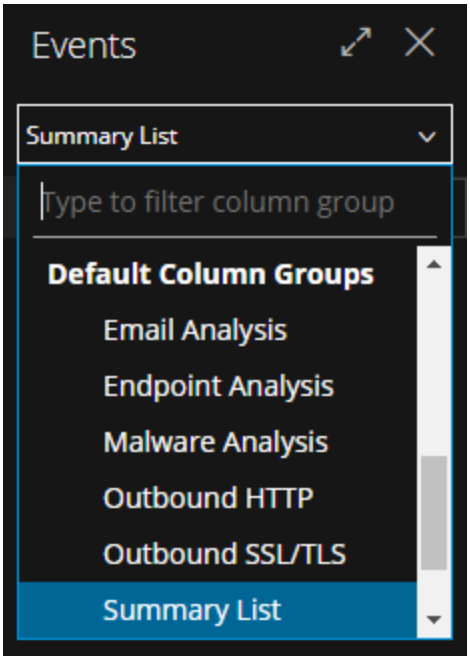
- **Analyse des e-mails** : Comprend les clés méta qui sont utiles lors de la procédure d'enquête sur les métadonnées liées aux e-mail.
- **Analyse des points de terminaison** : Comprend les clés méta qui sont utiles lors de la procédure d'enquête sur les métadonnées liées aux points de terminaison.
- **Malware Analysis** : Comprend les clés méta qui sont utiles lors de la procédure d'enquête sur les métadonnées liées aux programmes malveillants.

- **Trafic HTTP sortant** : Comprend les clés méta qui sont utiles lors de la procédure d'enquête sur les métadonnées liées au Trafic HTTP sortant.
- **Trafic SSL/TLS sortant** : Comprend les clés méta qui sont utiles lors de la procédure d'enquête sur les métadonnées liées à l'analyse du Trafic SSL/TLS sortant.
- **Liste de Résumé** : Comprend les clés méta qui sont utiles dans une procédure générale d'enquête. **Il s'agit du groupe de colonnes par défaut.**
- **Analyse des menaces** : Comprend des clés méta qui marquent les menaces potentielles du jeu de données.
- **Analyse Web** : Comprend des clés méta qui marquent des anomalies dans le trafic web.

Un groupe de colonnes peut contenir plus de colonnes qui sont visibles sans défilement vers la droite. Dans la version 11.1, vous pouvez sélectionner les colonnes qui apparaissent dans la vue Analyse d'événements. L'ordre des colonnes reflète l'ordre dans la vue Événements du groupe de colonnes par défaut. Par défaut, les 15 premiers colonnes s'affichent lorsque vous sélectionnez un groupe de colonnes. Pour une meilleure visualisation, il est conseillé d'afficher uniquement 15 colonnes à la fois. Toutefois, vous pouvez sélectionner des colonnes supplémentaires à afficher et supprimer des colonnes déjà affichées.

Pour sélectionner un groupe de colonnes :

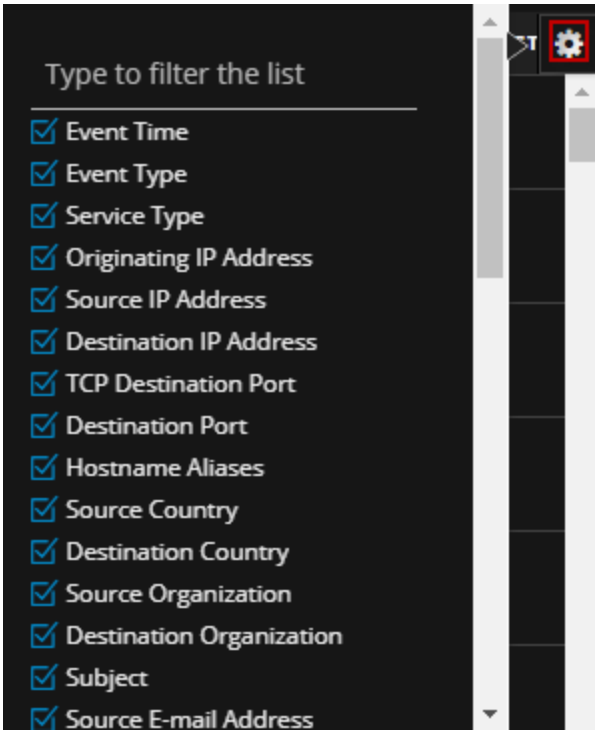
1. Dans le menu déroulant en regard d'Événements, sélectionnez un groupe de colonnes (par exemple, **Liste de Résumé**). Vous pouvez également commencer à saisir le nom du groupe de colonnes et sélectionner un groupe lorsque les groupes apparaissent dans le menu déroulant.



   Le panneau Événements affiche les données dans les colonnes qui appartiennent au groupe de colonnes sélectionné.

Pour sélectionner des colonnes à afficher :

1. Lorsque vous travaillez dans la vue Analyse d'événements avec un groupe de colonnes sélectionné, cliquez sur pour afficher le sélecteur de colonnes.



2. Sélectionnez les clés méta ou saisissez le nom d'une clé méta que vous souhaitez afficher dans des colonnes supplémentaires.
3. Si vous ne souhaitez pas voir une clé méta affichée dans une colonne, désélectionnez la clé méta. Les données sont de nouveau affichées via les colonnes sélectionnées.

Régler l'affichage des demandes et réponses

Pour les types d'événements qui contiennent des demandes et des réponses, vous pouvez apporter plusieurs modifications.

Remarque : si le type d'analyse n'a pas de requêtes ou de réponses, l'option n'est pas sélectionnable. Le panneau Analyse de fichiers est un exemple de type de reconstruction sans demandes ni réponses. Un événement de journal reconstruit dans la vue Texte est un autre exemple.

Pour sélectionner le côté de la conversation à afficher (Demande, Réponse ou les deux), cliquez sur l'une ou l'autre des icônes de direction. La reconstruction est actualisée avec les informations sélectionnées.

Remarque : Si vous ne voyez pas de données, il se peut que vous ayez désélectionné Demande et Réponse. Vous devez sélectionner l'une des deux options pour afficher les données.

Afficher les métadonnées d'événement pour un événement

Lorsque vous examinez les événements dans le panneau Analyse de texte, le panneau Analyse de paquets ou le panneau Analyse de fichiers, vous pouvez cliquer sur pour afficher les métadonnées associées dans un panneau adjacent, le panneau Méta de l'événement.

Lors de l'affichage du panneau Analyse de texte et Méta de l'événement, placez la souris sur les paires de valeurs clé méta/valeur méta pour afficher une paire de jumelles si la valeur méta est consultable dans le texte brut. Il s'agit d'un exemple de l'icône de jumelles lorsque vous survolez la paire de clé méta/valeur méta **Répertoire** et/.

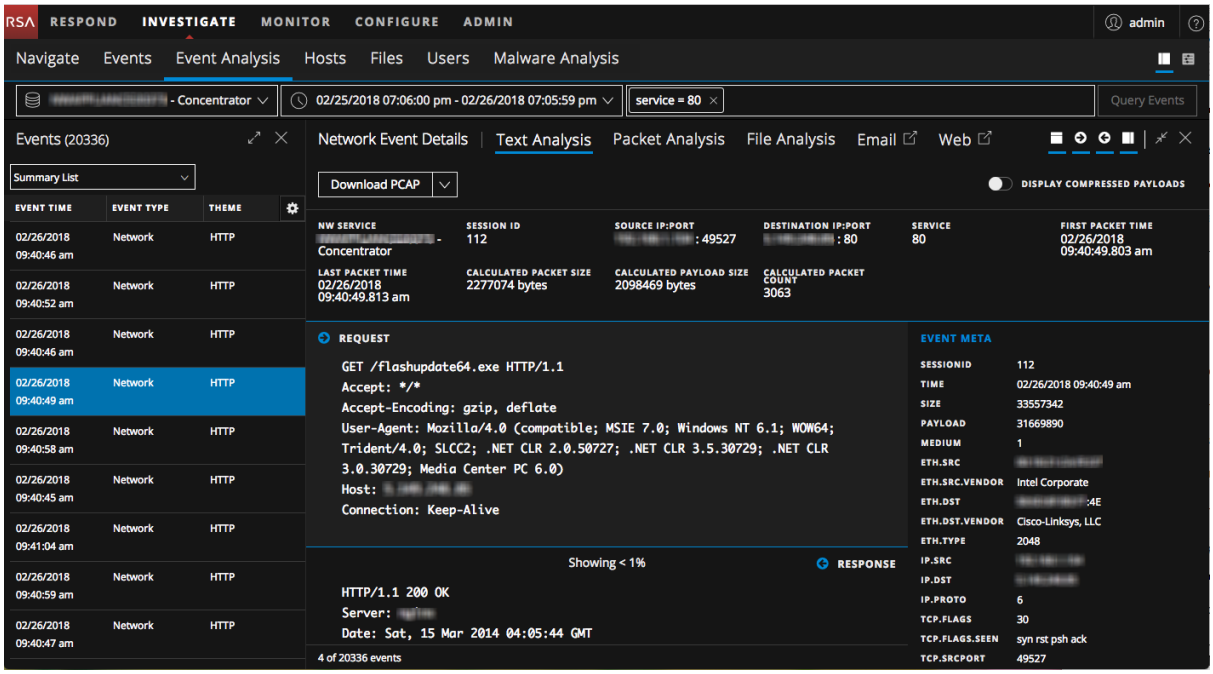
Cliquer sur l'icône déclenche une recherche pour la paire clé méta/valeur méta (non sensible à la casse) dans le panneau Analyse de texte et chaque instance est mise en surbrillance. Dans le Panneau Méta de l'événement, la ligne en surbrillance dispose d'un nombre de résultats et d'une barre de défilement qui vous permettront de trouver rapidement chaque résultat dans le panneau Analyse de texte. Vous pouvez afficher chaque emplacement mis en évidence des données qui a déclenché la génération de la clé méta, avancer pour afficher le prochain et revenir en arrière pour consulter le précédent.

Seules les clés méta qui ont des valeurs pertinentes dans le texte BRUT peuvent être recherchées. Vous pouvez rechercher une seule clé méta à la fois. Si la valeur est actuellement masquée en raison de la troncature d'une entrée de texte avec plus de 3 000 caractères, l'entrée de texte est développée pour afficher la valeur méta trouvée.

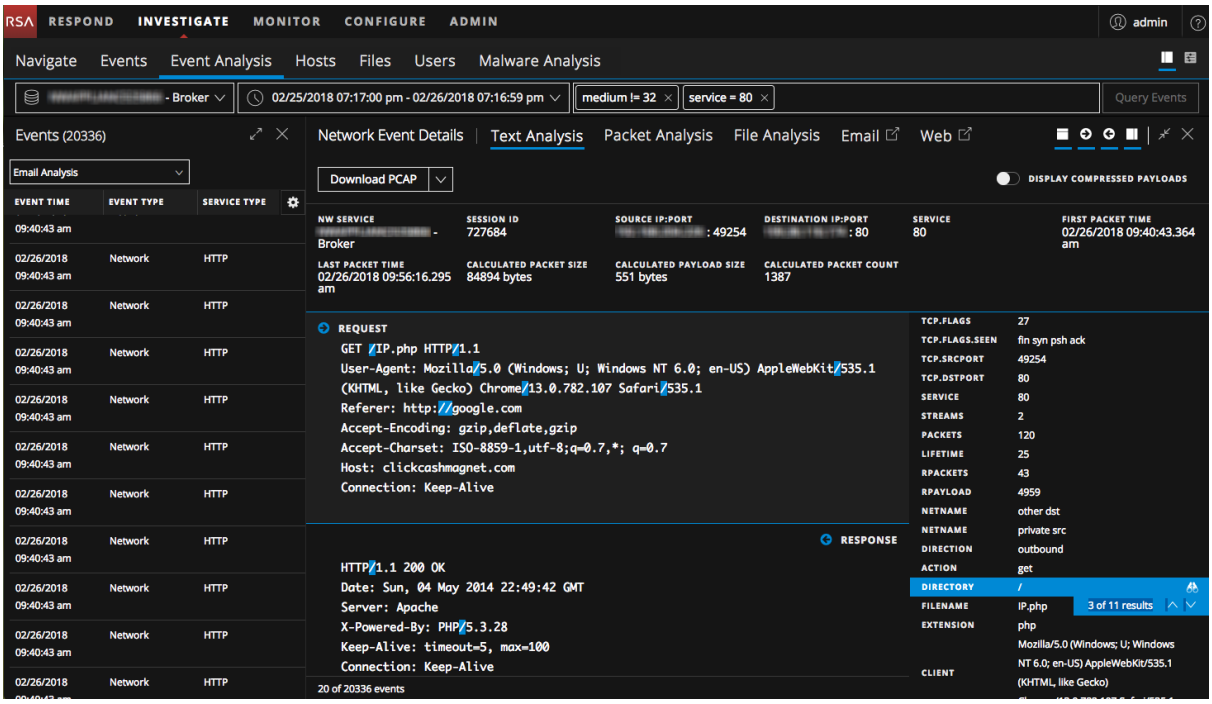
Cliquer sur la même paire clé méta/valeur méta ou une clé méta différente : la paire de valeurs dans le Panneau Méta de l'événement supprime la mise en surbrillance du texte brut. La mise en surbrillance est également supprimée si vous fermez le Panneau Méta de l'événement.

Pour rechercher le texte brut des valeurs méta qui ont déclenché une clé méta :

1. Ouvrez un événement de réseau dans le panneau Analyse de texte.



2. Dans la barre d'outils, cliquez sur pour ouvrir le Panneau Méta de l'événement. Lorsque vous survolez les paires clé méta - valeur méta dans la liste, une icône de jumelles identifie les valeurs qui peuvent être recherchées dans le panneau Analyse de texte.
3. Pour rechercher la valeur dans le texte brut, cliquez sur une ligne qui possède l'icône jumelles, indiquant si elle peut faire l'objet d'une recherche.
   Si aucune occurrence pertinentes de la valeur ne se trouve dans le texte, la valeur que vous recherchez est mise en surbrillance dans le Panneau Méta de l'événement et rien n'est mis en surbrillance dans le panneau Analyse de texte.
   Si une ou plusieurs instances pertinentes de la valeur sont trouvées dans le panneau Analyse de texte, chaque occurrence est mise en surbrillance. La valeur que vous recherchez est mise en surbrillance dans le Panneau Méta de l'événement et la barre de défilement est visible.



4. Pour supprimer la mise en évidence, fermez le Panneau Méta de l'événement, cliquez sur la même paire clé méta/valeur méta dans le Panneau Méta de l'événement ou cliquez sur une paire clé méta/valeur méta différente dans le Panneau Méta de l'événement.
   La mise en surbrillance est supprimée du texte brut.

Afficher ou masquer l'en-tête d'événement

Pour masquer l'en-tête d'événement dans le panneau Analyse de paquets, le panneau Analyse de texte ou le panneau Analyse de fichiers, en fournissant davantage d'espace vertical pour les données, cliquez sur  .

Parcourir les événements dans le panneau Paquets et Analyse de texte.

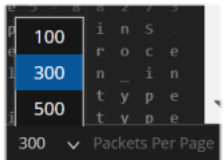
Les commandes de pagination permettent une plus grande flexibilité pour parcourir la liste de paquets ou le texte. Dans le panneau Analyse de paquets, vous pouvez sélectionner le nombre de paquets à afficher par page et votre sélection est conservée d'une connexion à l'autre dans l'application NetWitness. Lorsqu'une commande n'est pas disponible, elle est grisée. Par exemple, lorsque vous affichez la page 1, les commandes  et  sont grisées.

Remarque : Pour l'analyse de paquets, les contrôles de pagination sont disponibles dans la version 11.1 et versions ultérieures. Pour l'Analyse de texte, les contrôles de pagination sont disponibles dans la version 11.2 et versions ultérieures.

Pour utiliser les commandes de pagination :

1. (Analyse de paquets uniquement). Lorsqu'un événement est ouvert dans la vue Analyse d'événements, cliquez sur le nombre actuel de paquets par page (**100**, **300** ou **500**), puis sélectionnez

le nouveau nombre de paquets par page dans le menu contextuel.

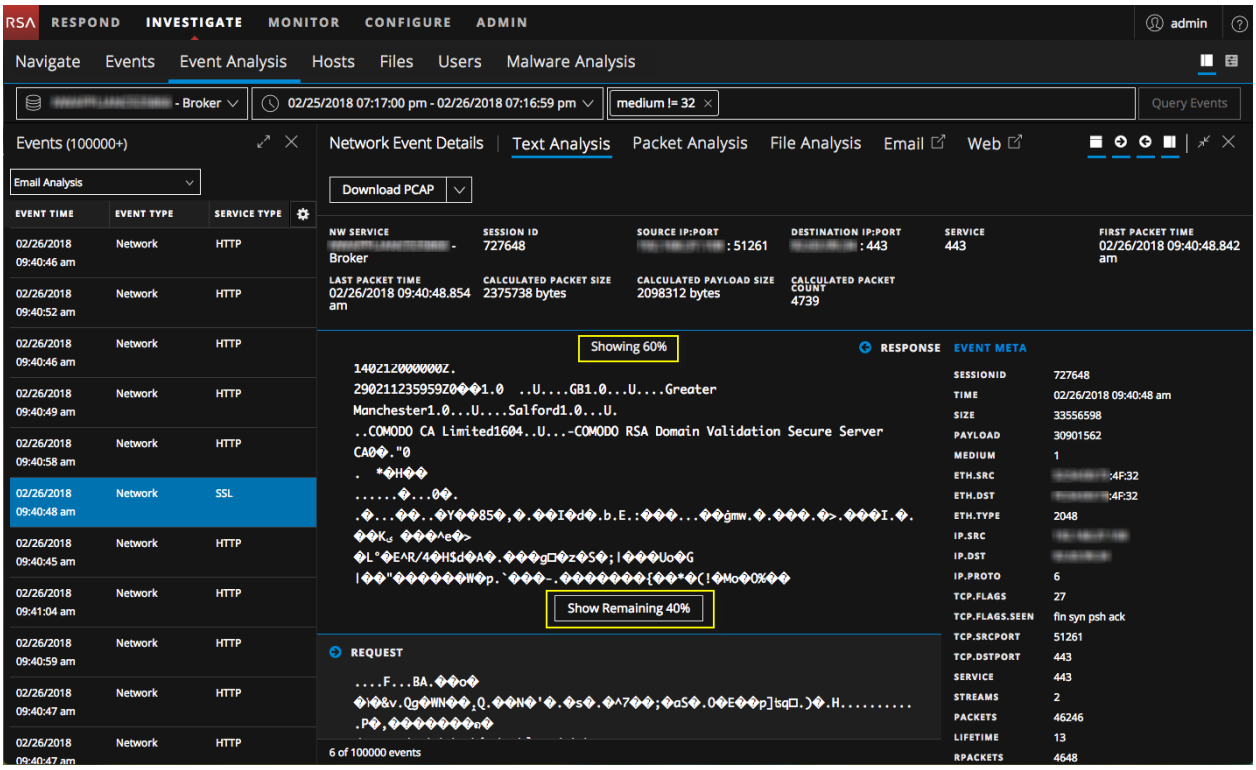


2. Pour avancer ou reculer d'une page, utilisez les icônes des commandes de page :
   Cliquez sur pour passer à la page suivante.
   Cliquez sur pour passer à la dernière page.
   Cliquez sur pour accéder à la page précédente.
   Cliquez sur pour accéder à la première page.
3. (Analyse de paquets uniquement). Pour accéder à une page spécifique, saisissez un numéro de page dans le champ du numéro de page 1 of 206.

Remarque : Lorsque dans le panneau Analyse de texte, vous devez naviguer manuellement vers la dernière page avant que l'icône de contrôle de la dernière page est disponible.

Développer les entrées de texte tronquées dans le panneau Analyse de texte

La reconstruction d'un événement de réseau dans le panneau Analyse de texte peut inclure des demandes et des réponses de plusieurs centaines de milliers de caractères. Parcourir une longue entrée de plus de 6 000 caractères qui ne représentent pas d'intérêt peut constituer une perte de temps. Pour améliorer l'expérience pour les analystes, toutes les entrées de texte contenant plus de 6 000 caractères sont tronquées pour afficher uniquement les 2 000 premiers caractères. Cet exemple montre une entrée qui comporte plus de 2 000 caractères et un message dans l'en-tête indique le pourcentage du nombre total de caractères affichés.



Vous pouvez voir que 60 % des caractères (les 2 000 premiers) s'affichent. Cliquez sur **Afficher les 40 % restants** pour afficher le reste de l'entrée.

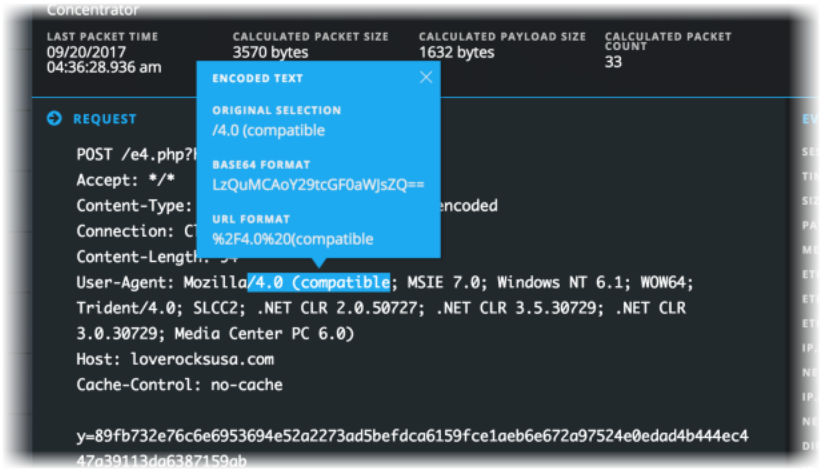
Si vous recherchez des données méta visibles dans le Panneau Méta de l'événement alors que le texte est tronqué dans le panneau Analyse de texte, le texte tronqué est recherché. Si les données méta se trouvent dans du texte masqué, l'entrée de texte se développe pour afficher le texte avec les données méta trouvées.

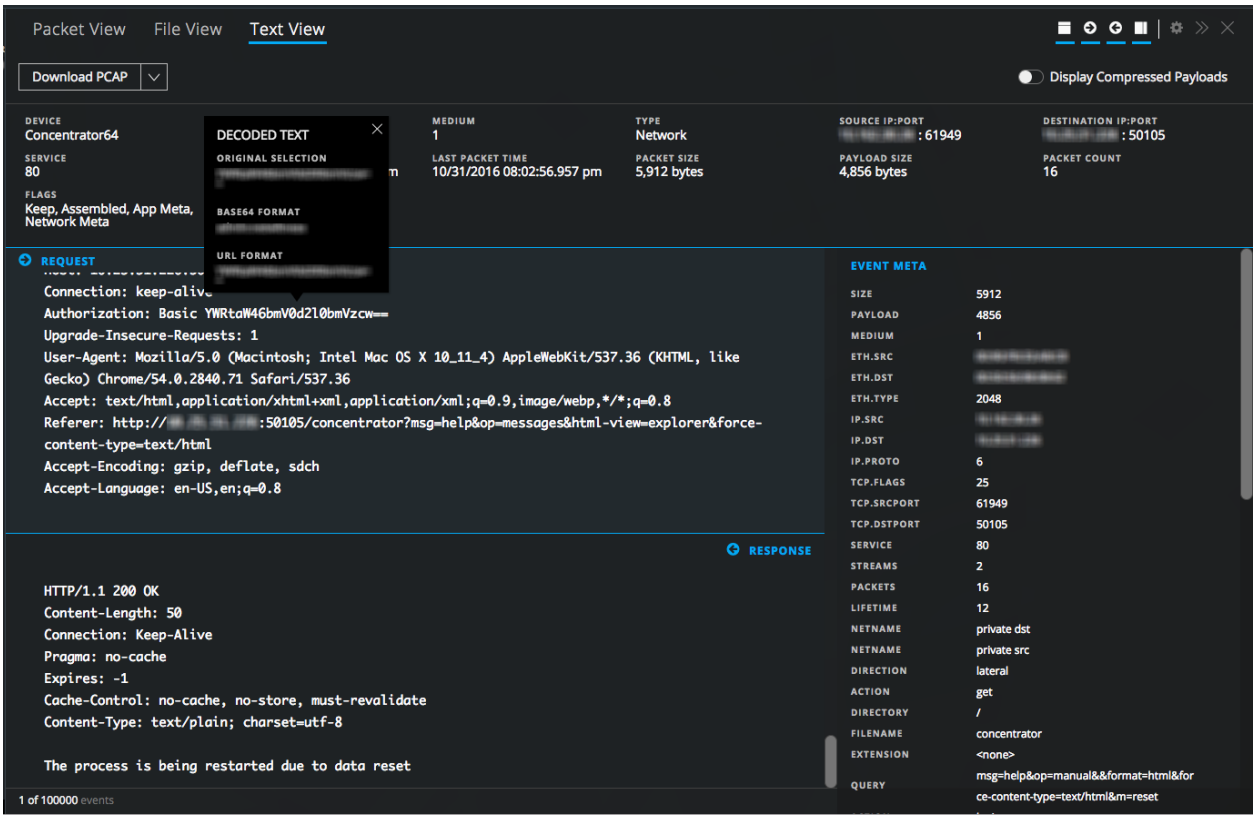
Effectuer un codage et un décodage URL et Base64 dans le panneau Analyse de texte

Si une session réseau en cours de reconstruction dans le panneau Analyse de texte contient des chaînes codées Base64 ou URL, vous pouvez décoder une chaîne pour mieux comprendre la session. Si la session contient des chaînes décodées pour Base64 ou URL, vous pouvez afficher une chaîne dans sa forme codée afin de rechercher des instances supplémentaires du texte codé dans d'autres sessions.

Lors de l'affichage d'une session de réseau qui contient du texte codé dans le panneau Analyse de texte, vous pouvez sélectionner un sous-ensemble du texte dans une Demande ou une Réponse unique à afficher sous forme codée ou décodée. En fonction du contenu chargé sur le Décodeur, il existe des métadonnées supplémentaires indiquant que des données encodées Base64 ou URL se trouvent au sein de la session.

Vous trouverez ci-dessous des exemples d'une zone de survol qui affiche le codage URL et le texte codé Base 64.

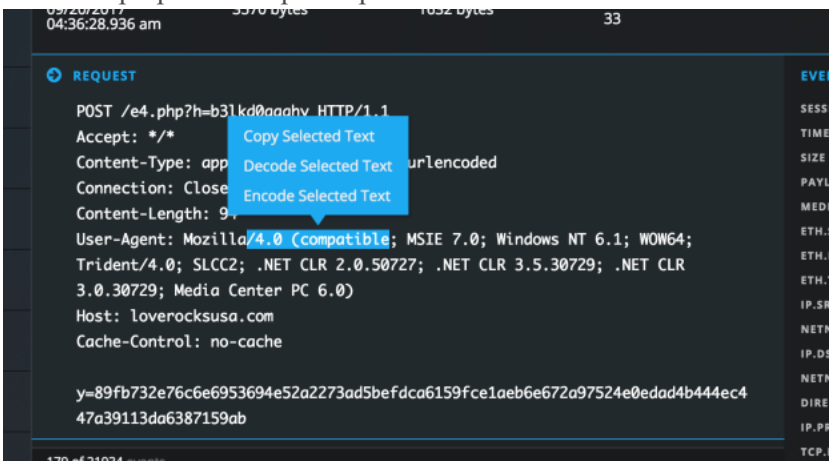




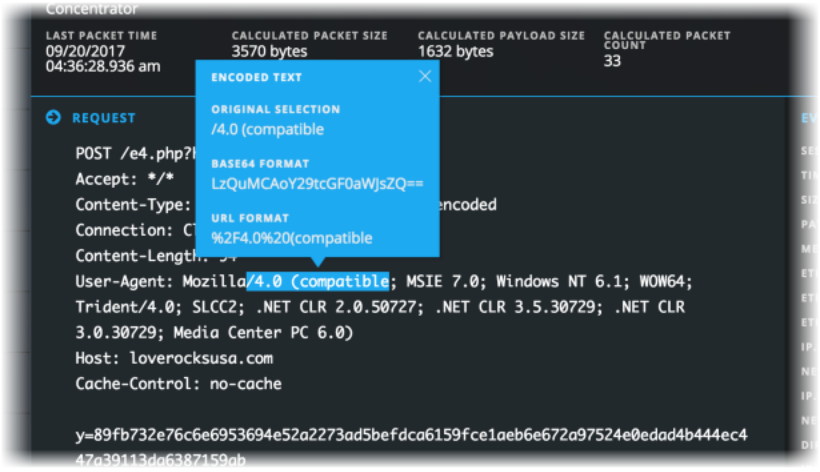
Pour effectuer l'encodage et le décodage dans le panneau Analyse de texte :

1. Dans la **Vue Analyse d'événements**, accédez au panneau Analyse de texte d'une session qui contient du contenu encodé ou décodé.
2. Pour afficher du texte décodé sous forme encodée, faites glisser pour sélectionner le texte contenu dans une seule demande ou réponse.

Un menu propose des options pour encoder et décoder.



3. Cliquez sur **Encoder le texte sélectionné.**
   Le texte encodé s'affiche dans une zone de survol, qui reste en place jusqu'à ce que vous cliquiez sur le ✉, sélectionnez un autre texte dans le panneau Analyse de texte, fermiez le Panneau Événements, sélectionnez un autre événement pour la reconstruction ou passiez à une autre vue de reconstruction.



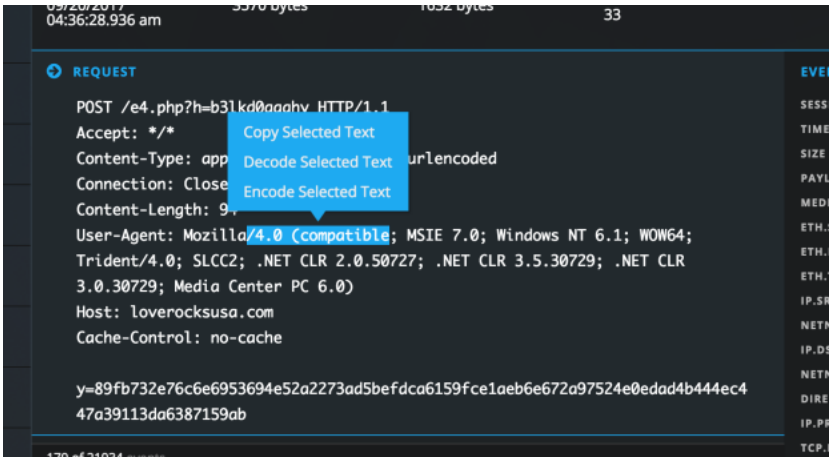
   Lorsqu'un texte plus long est sélectionné, la boîte de survol est déroulante et suffisamment grande pour accueillir l'ensemble du texte, ainsi que le texte décodé.

4. Si la session contient du texte encodé que vous souhaitez afficher sous forme décodée, faites glisser pour sélectionner le texte contenu dans une seule demande ou réponse.
   Un menu propose des options pour encoder et décoder.

5. Cliquez sur **Décoder le texte sélectionné.**
   Le texte décodé s'affiche dans une zone de survol, qui reste en place jusqu'à ce que vous cliquiez sur ✉, sélectionnez un autre texte dans le panneau Analyse de texte, fermiez le Panneau Événements, sélectionnez un autre événement pour la reconstruction ou passiez à une autre vue de reconstruction.

6. Si vous souhaitez copier du texte à partir de la reconstruction de texte, effectuez l'une des opérations suivantes :

   a. Faites glisser pour sélectionner du texte, cliquez avec le bouton droit de la souris et sélectionnez **Copier** Texte sélectionné dans le menu.



b. Faites glisser pour sélectionner du texte, puis sélectionnez **Décoder le texte sélectionné** ou **Coder le texte sélectionné**. Dans la zone de survol, sélectionnez le texte de votre choix et saisissez **CTRL-C**.
Le texte sélectionné est copié dans le Presse-papiers et disponible pour être collé dans une requête.

7. Lorsque vous avez terminé, cliquez sur ■ pour fermer la boîte de survol.

Afficher le texte décompressé pour une session de réseau HTTP dans le panneau Analyse de texte

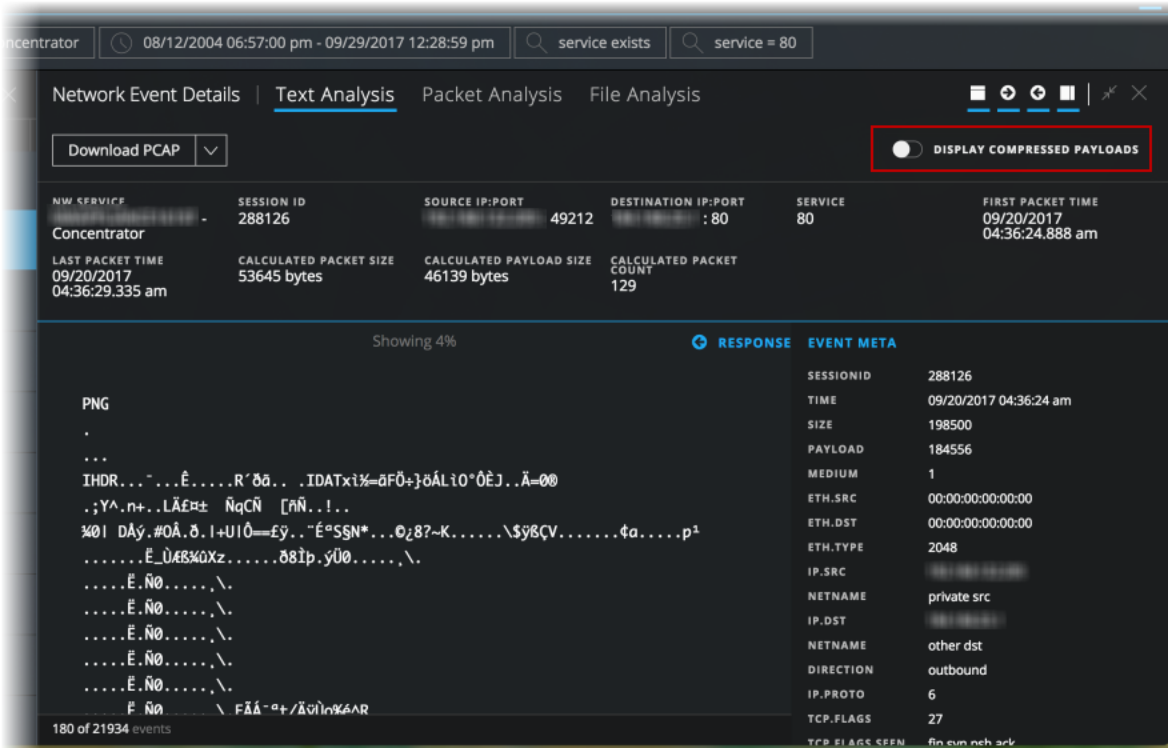
Lorsque le contenu d'une session de réseau HTTP est compressé et que vous affichez le panneau Analyse de texte, NetWitness Platform affiche le contenu décompressé par défaut. Cela vous aide à déceler la présence d'un modèle et à afficher les caractères lisibles par l'utilisateur. Vous pouvez basculer entre une vue compressée et décompressée du texte compressé.

Remarque : Le texte décompressé n'est pas disponible pour le panneau Analyse de paquets, le panneau Analyse de fichiers, les sessions de réseau non-HTTP et les données des fichiers log.

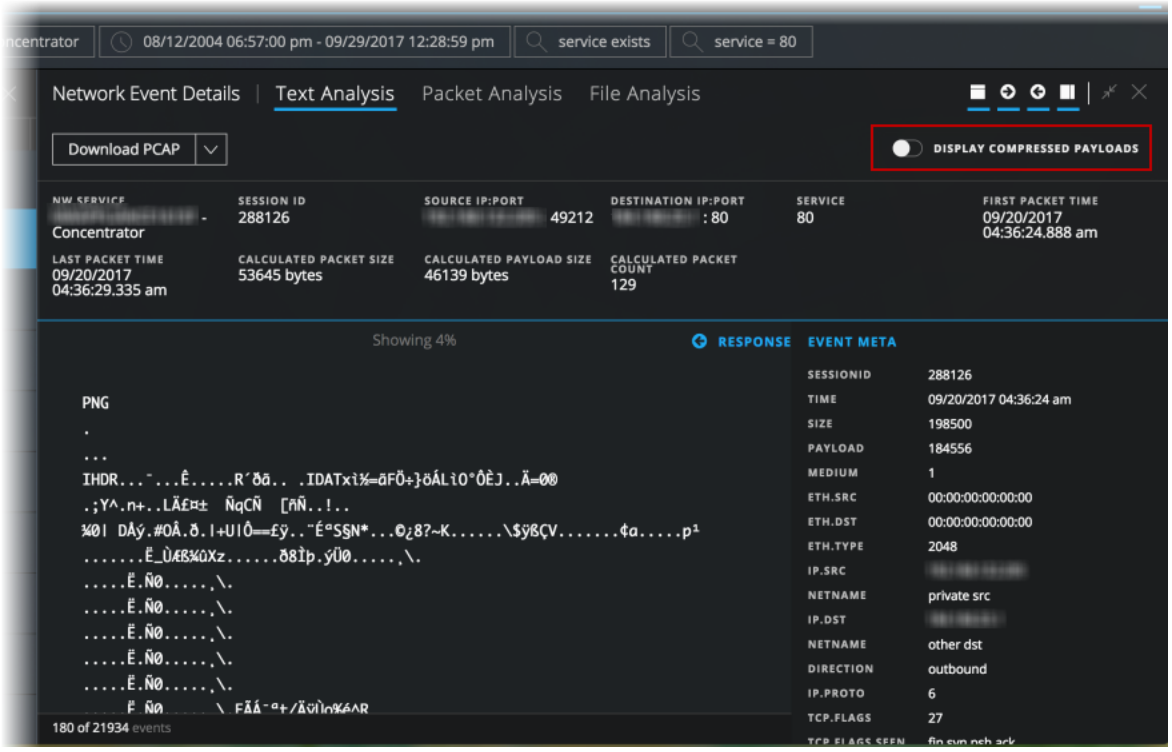
Le bouton de modification entre le texte compressé et décompressé est uniquement présent dans le panneau Analyse de texte et est activé uniquement si du texte compressé est présent.

Pour afficher le texte décompressé :

1. Ouvrez le panneau Analyse de texte d'une session HTTP qui contient le contenu compressé.
Par défaut, la session est reconstruite avec le texte décompressée. Au-dessus de la reconstruction se trouve le commutateur **Afficher les charges utiles compressées**.



2. Pour afficher le même texte sous sa forme compressée, cliquez sur le commutateur.
   La vue change afin que le texte compressé ne soit plus lisible par l'utilisateur. Le commutateur indique que l'option Afficher les paquets compressés est activée.



3. Pour revenir à la vue du texte décompressé, cliquez à nouveau sur le commutateur.

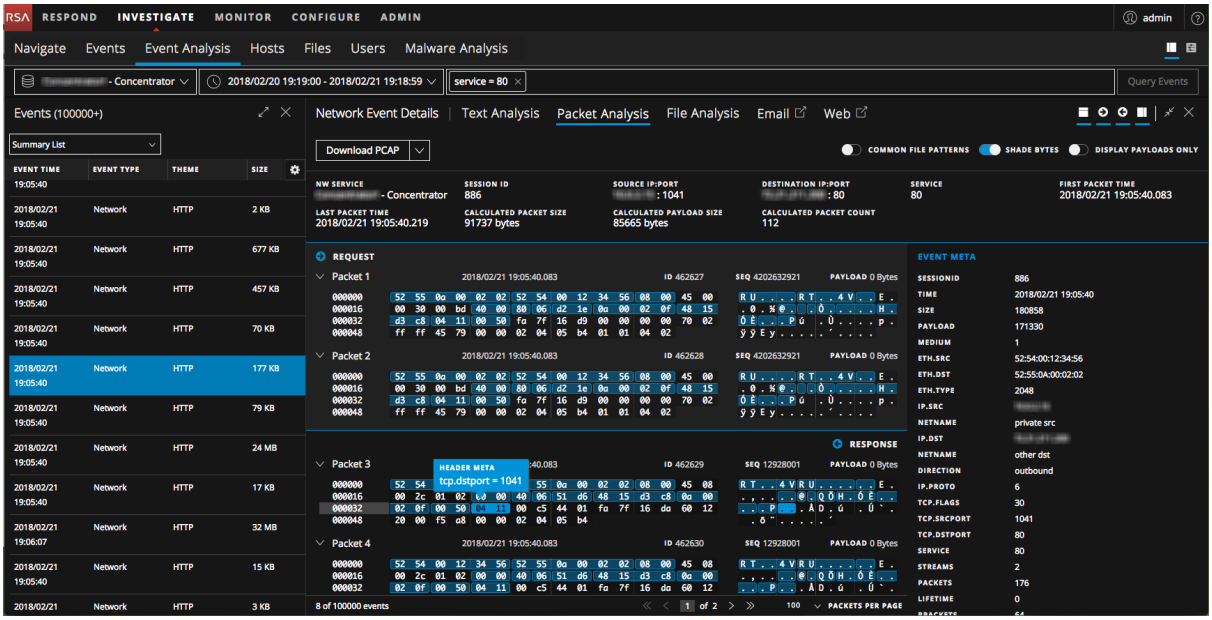
Utiliser l'option Charge utile uniquement dans le panneau d'analyse de paquets d'une session réseau

Lors de l'affichage d'une reconstruction d'une session réseau dans le panneau Analyse de paquets, vous pouvez choisir d'afficher uniquement la charge utile principale de chaque paquet. Par défaut, l'en-tête de paquet et les octets de pied de page s'affichent pour chaque paquet. Vous pouvez les masquer en cliquant sur le bouton Afficher les charges utiles uniquement. Si vous affichez uniquement les octets de charge utile, vous pouvez rétablir la valeur par défaut de chaque paramètre en définissant le commutateur Afficher les charges utiles uniquement sur activé. Ce paramètre persiste jusqu'à ce que vous le modifiiez ou actualisiez le navigateur.

- Si l'option Afficher les charges utiles uniquement est désactivée, le nombre de paquets, d'en-têtes de paquet, de pied de page de paquet et de charge utile s'affichent.
- Si l'option Afficher les charges utiles uniquement est activée, aucun en-tête de paquet et aucun octet de pied de page n'est affiché. Seul le contenu du paquet de 16 octets hexadécimaux par ligne et l'ASCII correspondant par ligne s'affichent.

Pour afficher la charge utile uniquement :

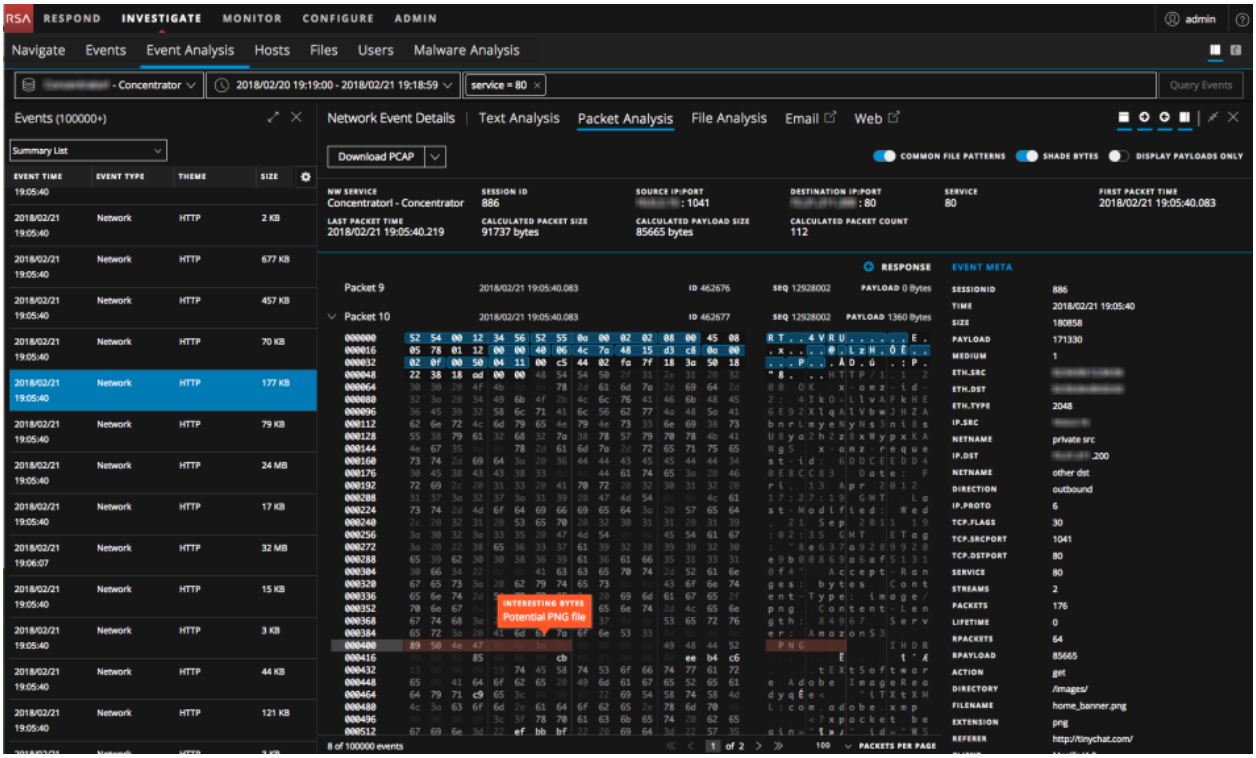
1. Dans la vue **Analyse d'événements**, accédez au panneau Analyse de paquets d'une session de réseau.
   Par défaut, la session est reconstruite avec l'en-tête de paquet, le pied de page et la charge utile est affichée.



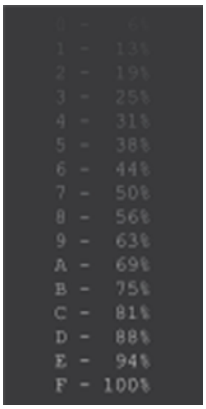
2. Pour modifier la vue afin d'afficher uniquement la charge utile pour chaque paquet, cliquez sur le commutateur **Afficher les charges utiles uniquement**.
   La vue change pour que seule la charge utile soit visible. Les paquets contigus du même côté sont concaténés pour rendre la charge utile plus lisible et compréhensible.

Afficher les octets mis en surbrillance dans le panneau Analyse des paquets

Lorsque vous ouvrez une reconstruction dans le panneau Analyse de paquets pour la première fois, les octets d'en-tête significatifs dans chaque paquet sont mis en surbrillance en bleu et les octets de charge utile se distinguent à l'aide d'une ombre pour vous aider à comprendre le contenu du paquet. La figure suivante affiche la valeur Analyse de paquets par défaut avec une mise en évidence et une ombre sur les octets.



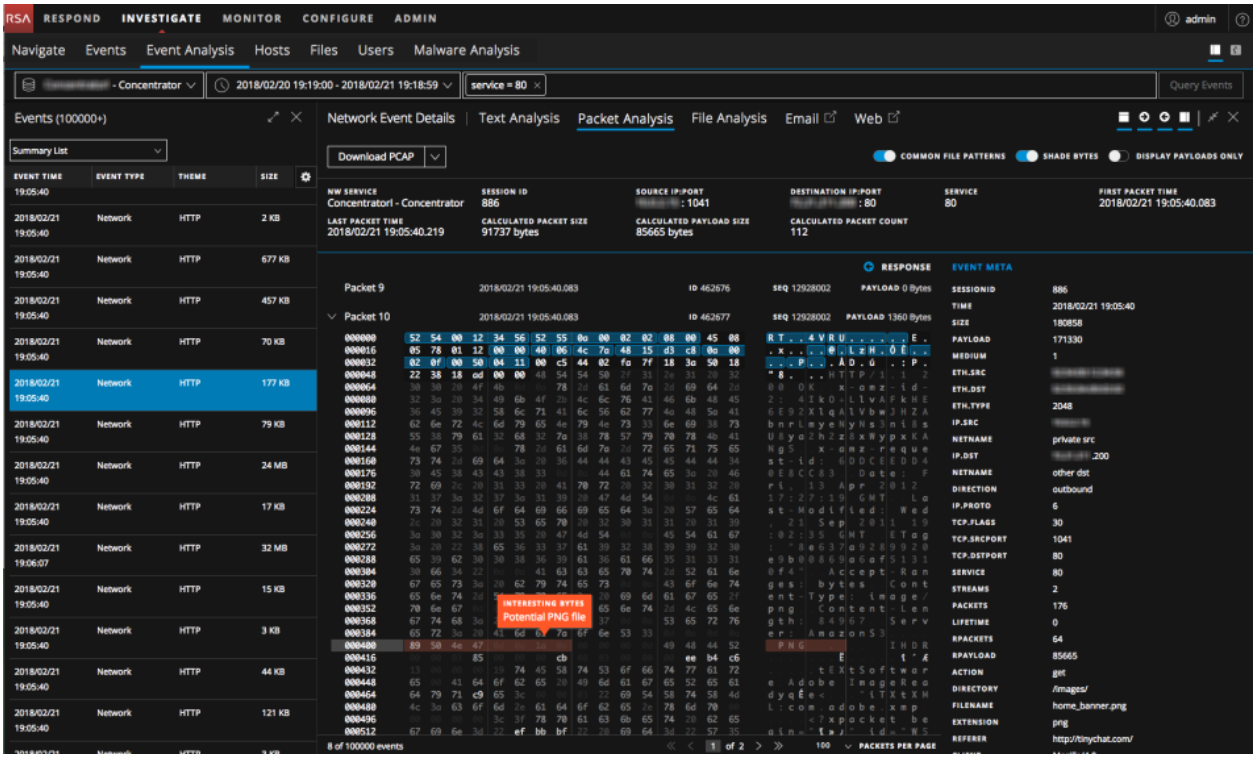
L'option Octets d'ombrage ajoute un ombrage pour identifier les différents octets hexadécimaux (00 à FF) à l'aide des degrés de mise en surbrillance. Les octets près de la plage inférieure sont plus transparents et les octets proches de 255 sont plus opaques. Les octets hexadécimaux et ASCII sont grisés. Voici un exemple d'ombre appliquée à chaque octet hexadécimal.



Le commutateur Octets d'ombrage contrôle l'ombrage d'octets. Lorsque vous activez ou désactiver Octets d'ombrage, votre paramètre persiste jusqu'à ce que vous modifiiez ou actualisiez le navigateur.

Mettre en surbrillance les types de fichiers communs dans le panneau Analyse des paquets

Dans le panneau Analyse des paquets, les analystes peuvent afficher ou masquer la mise en évidence de certains types de fichiers courants en fonction de la signature d'un fichier. Lorsque la fonction Modèles de fichiers communs est activée, les octets de chiffre miracle dans la signature d'un fichier sont mis en surbrillance dans la charge utile et vous pouvez pointer sur la mise en surbrillance pour afficher le type potentiel du fichier. Dans cet exemple, `89 50 4e 47` est mis en surbrillance dans la charge utile hexadécimale et `PNG` est mis en surbrillance dans la charge utile ASCII. Lorsque vous survolez les octets mis en surbrillance, le type de fichier potentiel associé au nombre magique est fourni dans une zone de survol.



Voici les types de fichiers et les nombres magiques correspondants qui sont mis en surbrillance s'ils sont présents dans la charge utile :

Type de fichier	Signature hexadécimale	Codage ASCII
Exécutable DOS / Windows PE	4D 5A	MZ
Portable Network Graphics (PNG)	89 50 4E 47 0D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF

Type de fichier	Signature hexadécimale	Codage ASCII
JPEG/Exif	45 78 69 66	Exif
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
Exécutable non portable	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
Ancien document Office (doc, xls, ppt, msg et autres)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
Formats de fichier ZIP et formats dérivés, tels que JAR, ODF, OOXML	50 4B	PK..
Format de fichier 7-zip (7z)	37 7A BC AF 27 1C	7z¼¯'
Fichier de classe Java, binaire Mach-O Fat	CA FE BA BE	Êþº¾
Postscript	25 21 50 53	%!PS
Script Unix/Linux Shell	23 21	#!
Exécutables Executable and Linkable Format (ELF)	7F 45 4C 46	.ELF

Pour afficher les signatures des fichiers courants dans le panneau Analyse de paquets :

1. Accédez au panneau Analyse de paquets et activez l'option **Modèles de fichier communs**. S'il existe plus d'un élément mis en surbrillance dans la vue, tous sont affichés.
2. Pour afficher la boîte de survol, placez le curseur sur la mise en surbrillance.

Rechercher un contexte supplémentaire dans la vue d'analyse d'événement

Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.2 ou ultérieure. Dans les versions antérieures, vous pouvez également rechercher un contexte supplémentaire dans les vues Naviguer ou Événements, comme décrit dans Rechercher un contexte supplémentaire dans les vues Naviguer et Événements.

À partir de la vue Analyse des événements, vous pouvez consulter les détails et les renseignements sur les éléments associés à un événement dans le service Context Hub. Ces éléments, ou entités, sont des identifiants, par exemple une adresse IP, un nom d'utilisateur, un nom d'hôte, un nom de domaine, un nom de fichier ou hachage de fichier. Les données issues de sources configurées, comme RSA NetWitness Endpoint, peuvent vous aider à comprendre ce qui se passe.

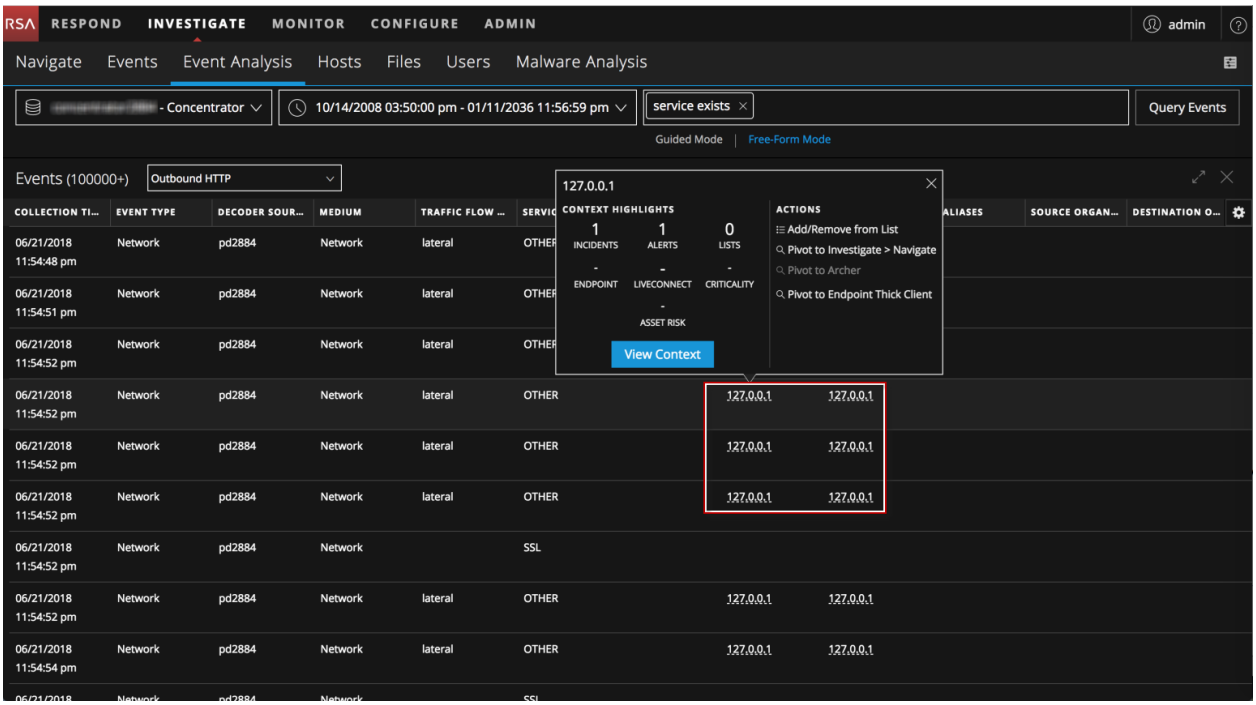
Remarque : Pour activer l'affichage des informations contextuelles, votre administrateur doit ajouter le service Context Hub dans la plate-forme RSA NetWitness et configurer les sources de données pour le service Context Hub comme décrit dans le *Guide de configuration de Context Hub*. Les analystes nécessitent également un rôle disposant de l'autorisation `Context Lookup`, comme décrit dans « Autorisations du rôle » et « Gérer les utilisateurs avec les rôles et autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Le service Context Hub est un service centralisé qui agrège les données sur les entités de plusieurs sources de données configurables. Ces données peuvent étendre votre procédure d'enquête avec un contexte supplémentaire au-delà des résultats immédiats d'une requête spécifique. Par exemple, le service Context Hub peut vous indiquer si une entité donnée a été mentionnée dans des incidents, alertes, flux ou publications de renseignements de la communauté.

Dans le panneau Événements, l'En-tête d'événement ou le panneau Méta de l'événement, vous pouvez voir les entités soulignées. Si une entité est soulignée, NetWitness Platform renseigne les informations relatives à ce type d'entité dans le service Context Hub. Des informations supplémentaires relatives à cette entité peuvent être disponibles dans le service Context Hub.

Remarque : Les entités Active Directory disposant d'informations contextuelles disponibles ne sont pas soulignées, mais vous pouvez survoler ces entités pour voir si des informations contextuelles sont disponibles.

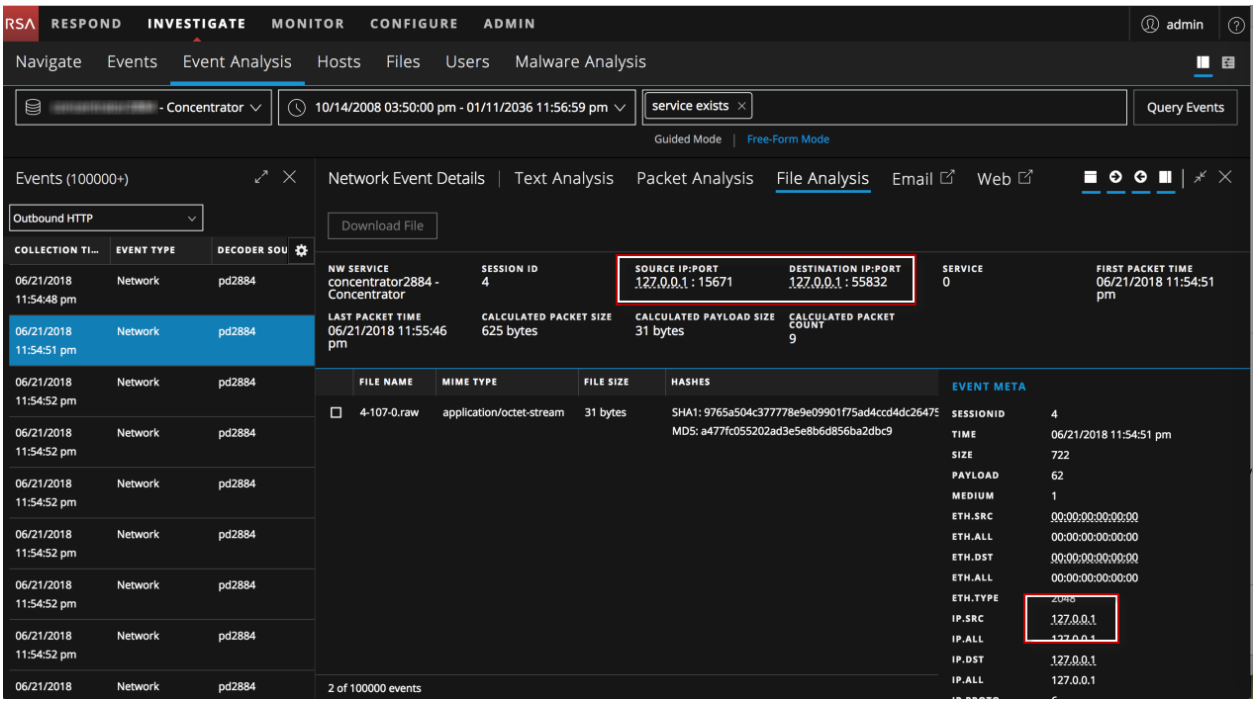
La figure suivante montre les entités soulignées dans le panneau Événements avec l'info-bulle contextuelle ouverte.



L'info-bulle contextuelle comporte deux sections : Points forts du contexte et actions.

- Les informations contenues dans la section Points forts du contexte vous aident à déterminer les actions que vous devez entreprendre. Elles peuvent afficher des données connexes pour les Incidents, les Alertes, les Listes, le Point de terminaison, Live Connect, la Criticité et Risques liés aux ressources. En fonction de vos données, vous pourrez peut-être cliquer sur ces éléments pour plus d'informations.
- La section Actions répertorie les actions disponibles. Dans l'exemple, les options Ajouter à la liste/Supprimer de la liste, Pivoter vers Investigate > Naviguer et Pivoter vers le client Endpoint Thick sont disponibles.

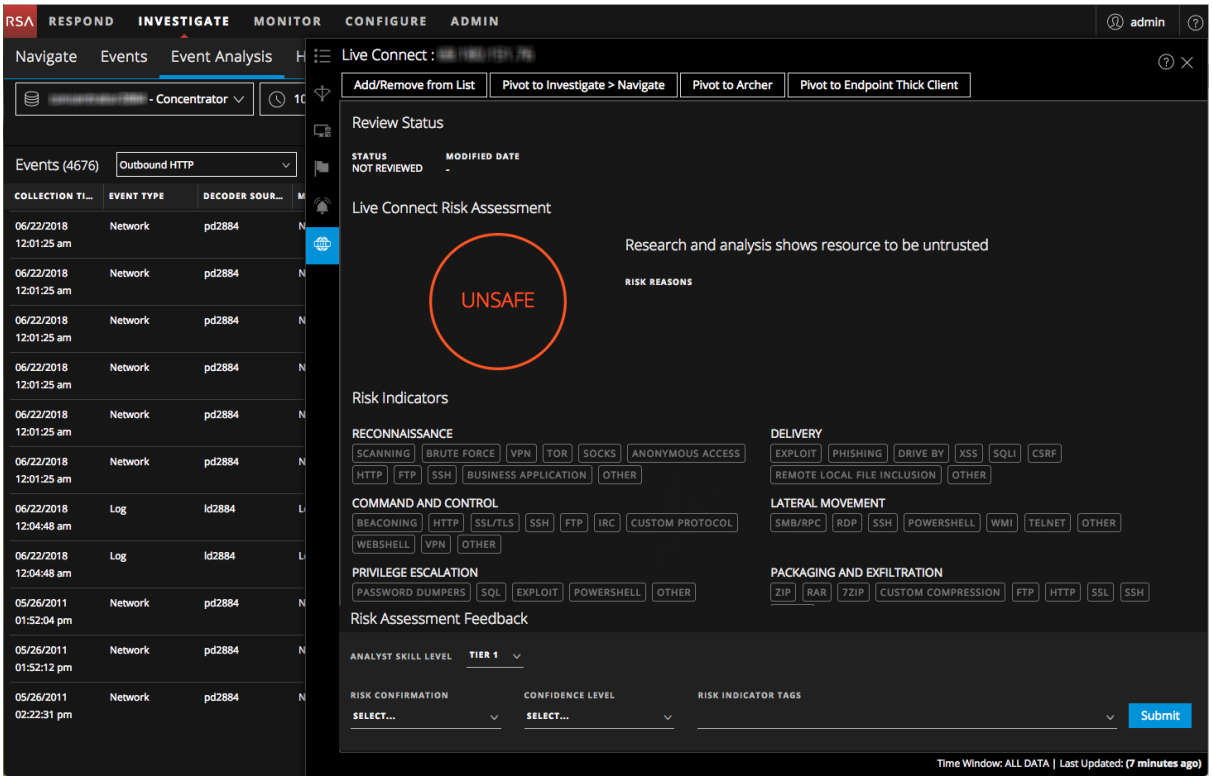
La figure suivante illustre les entités soulignées du panneau En-tête de l'événement et du panneau Méta de l'événement méta.



Lorsque vous cliquez sur Afficher le contexte dans l'info-bulle contextuelle, Context Hub interroge les sources de données configurées pour les informations pertinentes, et le panneau de recherche contextuelle s'ouvre à partir du côté droit de la fenêtre du navigateur. Le panneau Recherche contextuelle est renseigné avec les informations du service Context Hub dès que possible. Dans le panneau Recherche contextuelle, vous pouvez visualiser et explorer des sources de données pour approfondir la procédure d'enquête. Pour une description détaillée des informations affichées dans chaque source de données du panneau Recherche contextuelle, consultez Panneau Recherche contextuelle. Vous pouvez également prendre toute action disponible dans la section Actions.

Pour afficher des informations dans le panneau Recherche contextuelle, dans la vue Analyse d'événement, procédez comme suit :

1. Pointez sur différentes valeurs méta pour voir les sources de données pour lesquelles des données sont disponibles.
   Une info-bulle contextuelle affiche une liste des données de contexte disponibles pour la valeur méta sélectionnée.
2. Cliquez sur **Afficher le contexte** dans l'info-bulle contextuelle pour ouvrir le panneau Recherche contextuelle.
   Le panneau Recherche contextuelle s'ouvre depuis le côté droit de la fenêtre du navigateur. Le panneau Recherche contextuelle est renseigné avec les informations du service Context Hub dès que possible.



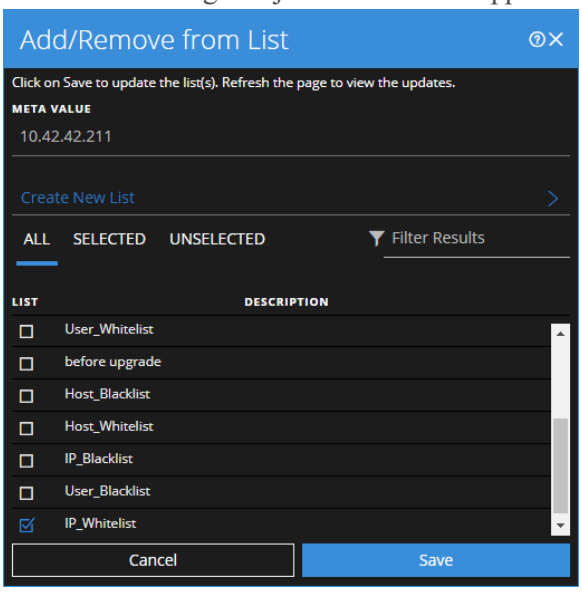
3. Pour effectuer des actions sur une entité, sélectionnez l'une des actions disponibles dans l'info-bulle contextuelle : Ajouter à la liste/Supprimer de la liste, Pivoter vers Investigate > Naviguer, Pivoter vers Archer et Pivoter vers le client Endpoint Thick. Pour en savoir plus, consultez Pivoter vers Investigate > Naviguer, Pivot vers Archer, Pivoter vers NetWitness Endpoint Thick Client et Ajouter une entité à une liste blanche.

> **Remarque :** L'action Pivot vers Archer est désactivé lorsque les données Archer ne sont pas disponibles ou lorsqu'Archer DataSource ne répond pas. Vérifiez que la configuration RSA Archer est activée et configurée correctement. Il va est de même pour Pivot to NetWitness Endpoint Thick Client ; si l'option est désactivée, vérifiez que NetWitness Endpoint Thick Client est installé et configuré correctement.

Ajouter une entité à une liste blanche

Vous pouvez ajouter n'importe quelle entité soulignée à une liste, comme une liste blanche ou noire, à partir d'une info-bulle de contexte. Par exemple, pour réduire les faux positifs, vous pouvez ajouter à la liste blanche un domaine souligné pour l'exclure des entités associées.

1. Dans le panneau Événements, En-tête de l'événement ou Méta de l'événement, survolez l'entité soulignée que vous souhaitez ajouter à une liste Context Hub. (Les entités Active Directory avec des données de contexte peuvent également être ajoutées, mais elles ne sont pas soulignées.)
   Une info-bulle contextuelle montrant les actions disponibles s'affiche.
2. Dans la section **Actions** de l'info-bulle, cliquez sur **Ajouter à la liste/Supprimer de la liste**.
   La boîte de dialogue Ajouter à la liste/Supprimer de la liste affiche les listes disponibles.



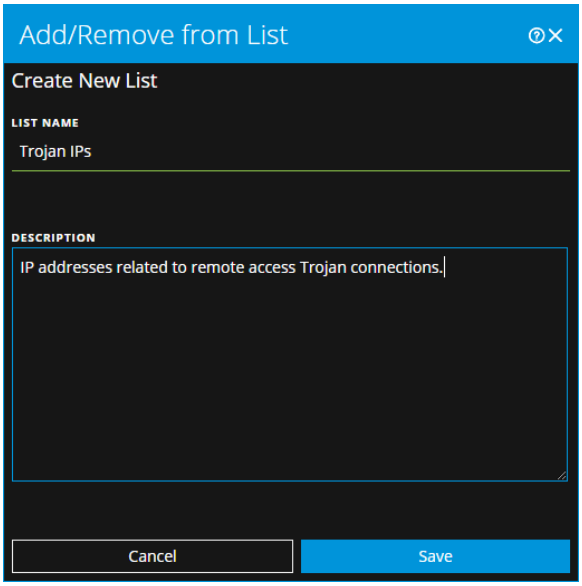
3. Sélectionnez une ou plusieurs listes, puis cliquez sur **Enregistrer**.
   L'entité est ajoutée aux listes sélectionnées. Boîte de dialogue Ajouter à la liste/Supprimer de la liste fournit des informations supplémentaires.

Créer une liste

Vous pouvez créer des listes dans Context Hub à partir de la vue Analyse de l'événement. En plus d'utiliser des listes dans des entités de liste blanche et de liste noire, vous pouvez utiliser des listes pour surveiller des entités présentant un comportement anormal. Par exemple, pour améliorer la visibilité d'une adresse IP suspecte et du domaine faisant l'objet d'une enquête, vous pouvez les inclure dans deux listes distinctes. La première liste peut concerner les domaines suspectés d'être liés aux connexions de commande et contrôle, et une autre liste peut concerner les adresses IP liées aux connexions de chevaux de Troie autorisant un accès à distance. Vous pouvez ensuite identifier les indicateurs de compromis à l'aide de ces listes.

Pour créer une liste dans Context Hub :

1. Dans le panneau Événements, En-tête de l'événement ou Méta de l'événement, survolez l'entité soulignée que vous souhaitez ajouter à une liste Context Hub. (Les entités Active Directory avec des données de contexte peuvent également être ajoutées à une nouvelle liste, mais elles ne sont pas soulignées.)
   Une info-bulle contextuelle indiquant les actions disponibles s'affiche.
2. Dans la section **Actions** de l'info-bulle, cliquez sur **Ajouter à la liste/Supprimer de la liste**.
3. Dans la boîte de dialogue Ajouter à la liste/Supprimer de la liste, cliquez sur **Créer une nouvelle liste**.



4. Saisissez une valeur **Nom de la liste** unique pour obtenir la liste. Le nom de la liste n'est pas sensible à la casse.
5. (Facultatif) Saisissez une **DESCRIPTION** pour la liste.
   Les analystes disposant des autorisations adéquates peuvent également exporter des listes au format CSV à envoyer à d'autres analystes pour un suivi et une analyse approfondis. Le *Guide de configuration de Context Hub* fournit des informations supplémentaires.

Pivoter vers Investigate > Naviguer

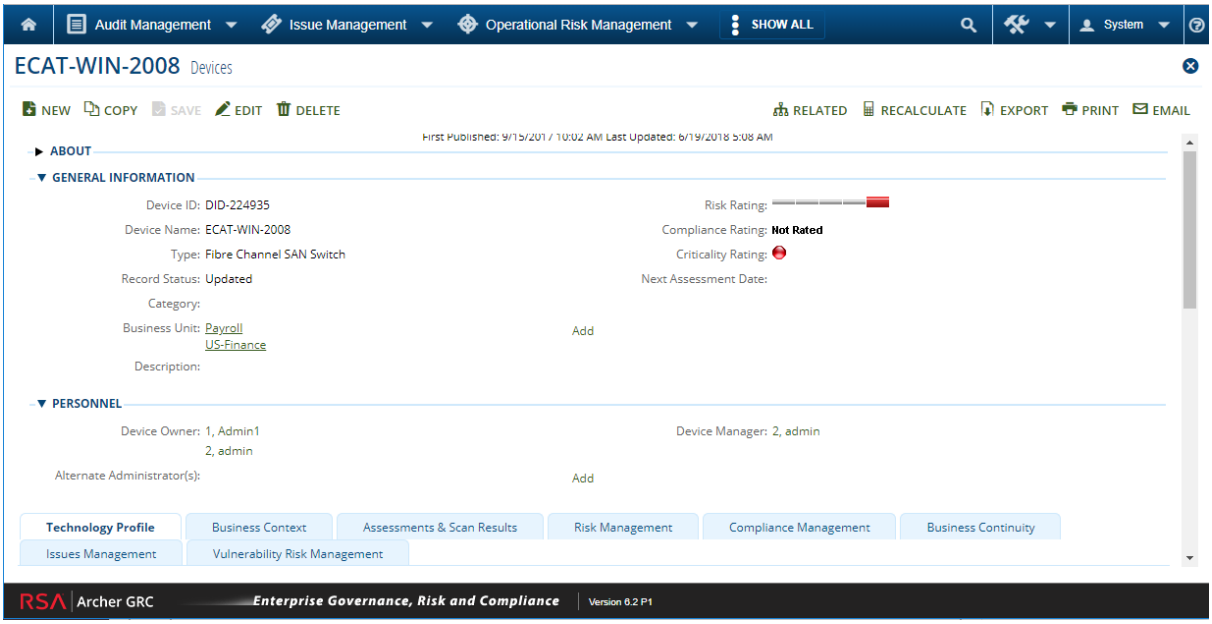
Pour une procédure d'enquête plus approfondie de l'entité, vous pouvez accéder à la vue Naviguer.

1. Dans le panneau Événements, l'En-tête d'événement ou le panneau Méta de l'événement, pointez sur n'importe quelle entité soulignée. (Les entités Active Directory avec des données de contexte peuvent également faire l'objet d'une enquête, mais elles ne sont pas soulignées.)
2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers Investigate> Naviguer**.
   La vue Naviguer s'ouvre, ce qui vous permet d'effectuer une procédure d'enquête plus approfondie. Pour plus d'informations, consultez Procédure d'enquête relative aux métadonnées dans la vue Naviguer.

Pivot vers Archer

Pour afficher plus de détails sur le périphérique RSA Archer® Cyber Incident & Breach Response, vous pouvez pivoter vers la page de détails de l'appareil. Ces informations s'affichent uniquement pour l'adresse IP, l'hôte et l'adresse Mac.

1. Dans le panneau Événements, l'En-tête d'événement ou le panneau Méta de l'événement, pointez sur n'importe quelle entité soulignée (adresse IP, hôte et adresse Mac).
2. Dans la section **ACTIONS** de l'info-bulle contextuelle, sélectionnez **Pivoter vers Archer**.
3. La page de détails **RSA Archer Cyber Incident & Breach Response** de l'appareil s'ouvre si vous êtes connecté à l'application. Sinon, l'écran de connexion s'affiche.



Remarque : Le lien Pivot vers Archer est désactivé lorsque les données Archer ne sont pas disponibles ou lorsqu'Archer DataSource ne répond pas. Vérifiez que la configuration RSA Archer est activée et configurée correctement.

Pour plus d'informations, consultez le *guide d'intégration Archer*.

Pivoter vers NetWitness Endpoint Thick Client

Si l'application de client Thick NetWitness Endpoint est installée, vous pouvez la démarrer via l'info-bulle de contexte. À partir de là, vous pouvez mener davantage l'enquête sur une adresse IP suspecte, un hôte ou une adresse MAC.

1. Dans le panneau Événements, l'En-tête d'événement ou le panneau Méta de l'événement, pointez sur n'importe quelle entité soulignée.
2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers le client Endpoint Thick**. L'application de client Thick NetWitness Endpoint s'ouvre en dehors de votre navigateur Web.

Remarque : La version 4.4 du client Thick NetWitness Endpoint (NWE) doit être installée sur le même serveur, les clés méta NWE doivent exister dans le fichier `table-map.xml` sur le Log Decoder et les clés méta NWE doivent exister dans le fichier `index-concentrator-custom.xml`. Le client Thick NWE est une application Windows uniquement. Les instruments de configuration complets sont fournis dans le *Guide d'utilisation du point de terminaison NetWitness* pour la Version 4.4.

Télécharger des données dans la vue Analyse d'événements

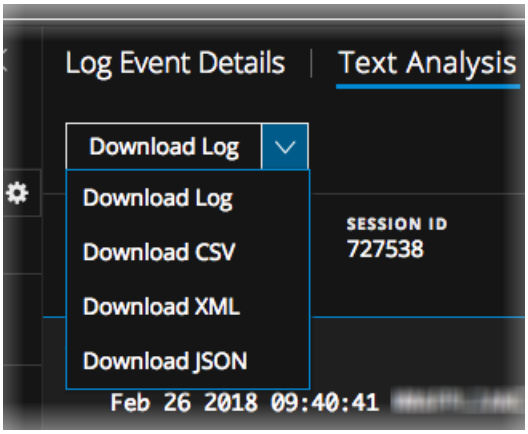
Dans la vue Analyse d'événements, vous pouvez télécharger des événements, logs et fichiers.

Télécharger un log dans le panneau Analyse de texte

Lors de l'affichage d'une reconstruction de log dans le panneau Analyse de texte, vous pouvez télécharger un fichier log dans les formats suivants à l'aide des options dans le menu déroulant Journal de téléchargements :

- Log brut (log) avec l'option **Journal de téléchargements**
- Valeurs séparées par des virgules (CSV) avec l'option **Télécharger le fichier CSV**
- Extensible Markup Language (XML) avec l'option **Télécharger le fichier XML**
- JavaScript Object Notation (JSON) avec l'option **Télécharger JSON**

Il s'agit d'un exemple de reconstruction de log avec les options de menu déroulant Journal de téléchargements.



Remarque : L'option journal de téléchargement est applicable uniquement pour les événements de point de terminaison qui ont au moins une valeur méta supérieure à 256 caractères. Pour un événement de point de terminaison, le journal brut est renseigné uniquement lorsque la valeur Meta dépasse 256 caractères. Les fichiers exécutée depuis longtemps ou téléchargés historiquement ne sont pas téléchargeables.
Par exemple, les valeurs méta telles que les arguments de lancement peuvent dépasser 256 caractères. Dans ce cas, 256 caractères sont disponibles en tant que valeur méta alors que la valeur complète est disponible dans le journal brut à afficher.

Le fichier log téléchargé contient le log et est nommé pour aider à identifier le service sur lequel le log a été collecté, l'ID de session, et le type de fichier. Voici un exemple de nom de fichier pour un log brut : **Concentrator_SID2.log**. Le fichier log exporté est nommé à l'aide de la convention suivante :

```
<service-ID or host name>_SID<n>.<filetype>
```

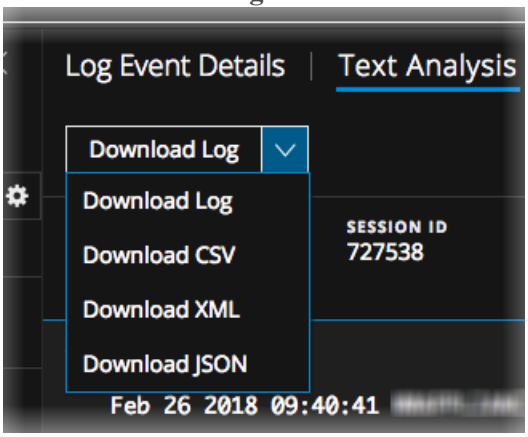
où :

- `<service-ID or host name>` est le nom du service (par exemple, Concentrator ou Broker) où la session a été enregistrée.
- `SID<n>` est le numéro d'ID de la session.
- `<filetype>` identifie le format du log téléchargé. Voici les types de log possibles : log brut, CSV, XML et JSON. Par défaut, le format est un log brut.

Remarque : Quelques formats n'ont pas d'horodatage ou l'adresse IP de l'appareil sur lequel l'événement a été généré. Un log téléchargé au format CSV, XML ou JSON possède donc une valeur supplémentaire appelée `timestamp` ainsi que le contenu de log brut. Les informations supplémentaires dans le log sont dans ce formulaire : `Log timestamp="1490824512" source="10.12.35.65"`.

Pour télécharger le log d'une session :

Dans le panneau Analyse de texte d'un événement de log, sélectionnez l'un des formats de fichier pour le log téléchargé.
-Pour télécharger le log en tant que log brut (le format par défaut), cliquez sur **Télécharger le log**.
-Pour télécharger le log dans l'un des autres formats, cliquez sur la flèche vers le bas sur le bouton **Journal de téléchargements** et sélectionnez l'un des formats de fichier pour le log téléchargé.



Le fichier log est téléchargé sur votre système de fichiers local dans le format spécifié. Si vous initiez un téléchargement et quittez la vue pendant que le log est en cours d'extraction et avant le démarrage du téléchargement du log, le log n'est pas téléchargé dans votre navigateur. Un message vous avertit que vous trouverez le log téléchargé dans la file d'attente de travail.

Télécharger des Données d'événements réseau dans le panneau Analyse de texte ou le panneau Analyse de paquets

Lors de l'affichage d'un événement de réseau reconstruit dans le panneau Analyse de paquets ou le panneau Analyse de texte, vous pouvez exporter des fichiers de données de réseau pour approfondir l'analyse. Le téléchargement inclut des événements pour la période en cours et un point de recherche verticale. Vous pouvez télécharger les données de ces formulaires :

- L'événement entier en tant que fichier de capture de paquets (`*.pcap`) avec l'option **Télécharger PCAP**.

- La charge utile en tant que fichier `*.payload` à l'aide de l'option **Télécharger toutes les charges utiles**.
- La charge utile de requête en tant que fichier `*.payload1` à l'aide de l'option **Télécharger la charge utile de la demande**.
- La charge utile de réponse en tant que fichier `*.payload2` à l'aide de l'option **Télécharger la charge utile de la réponse**.

Voici un exemple de nom de fichier pour un fichier PCAP : `C01 - Concentrator_SID1697309.pcap`. Le fichier de données de réseau exporté est nommé à l'aide de la convention suivante :

`<service-ID or host name>_SID<n>.<filetype>`

où :

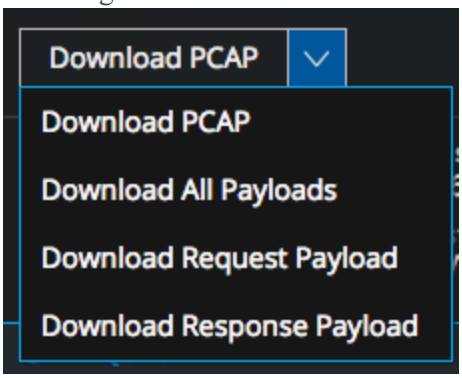
- `<service-ID or host name>` est le nom du service (par exemple, Concentrator ou Broker) où la session a été enregistrée.
- `SID<n>` est le numéro d'ID de la session.
- `<filetype>` est pcap, payload, payload1 ou payload2.

Si le téléchargement est rapide, les données du réseau sont téléchargées directement dans votre navigateur. Si le téléchargement prend plus de temps en raison de facteurs de réseau ou de la taille de fichier, le fichier est téléchargé en arrière-plan et la tâche est suivie dans la file d'attente Jobs. Dans ce cas, vous pouvez vérifier vos tâches dans la file d'attente et obtenir le fichier lorsque le téléchargement est terminé.

Remarque : Si vous initiez un téléchargement et quittez la vue pendant que le fichier est en cours d'extraction et avant le démarrage du téléchargement du fichier, le fichier n'est pas téléchargé dans votre navigateur. Un message vous avertit que vous trouverez le document téléchargé dans la file d'attente de travail.

Pour exporter un événement en tant que fichier de données réseau :

Accédez au panneau Analyse de paquets d'un événement de réseau et l'un des formats de fichier pour le fichier téléchargé.
-Pour télécharger l'événement en tant que fichier PCAP (le format par défaut), cliquez sur **Télécharger le PCAP**.
-Pour télécharger l'événement dans l'un des autres formats, cliquez sur la flèche vers le bas sur le bouton **Télécharger le PCAP** et sélectionnez l'un des formats de fichier pour les données d'événement téléchargées.



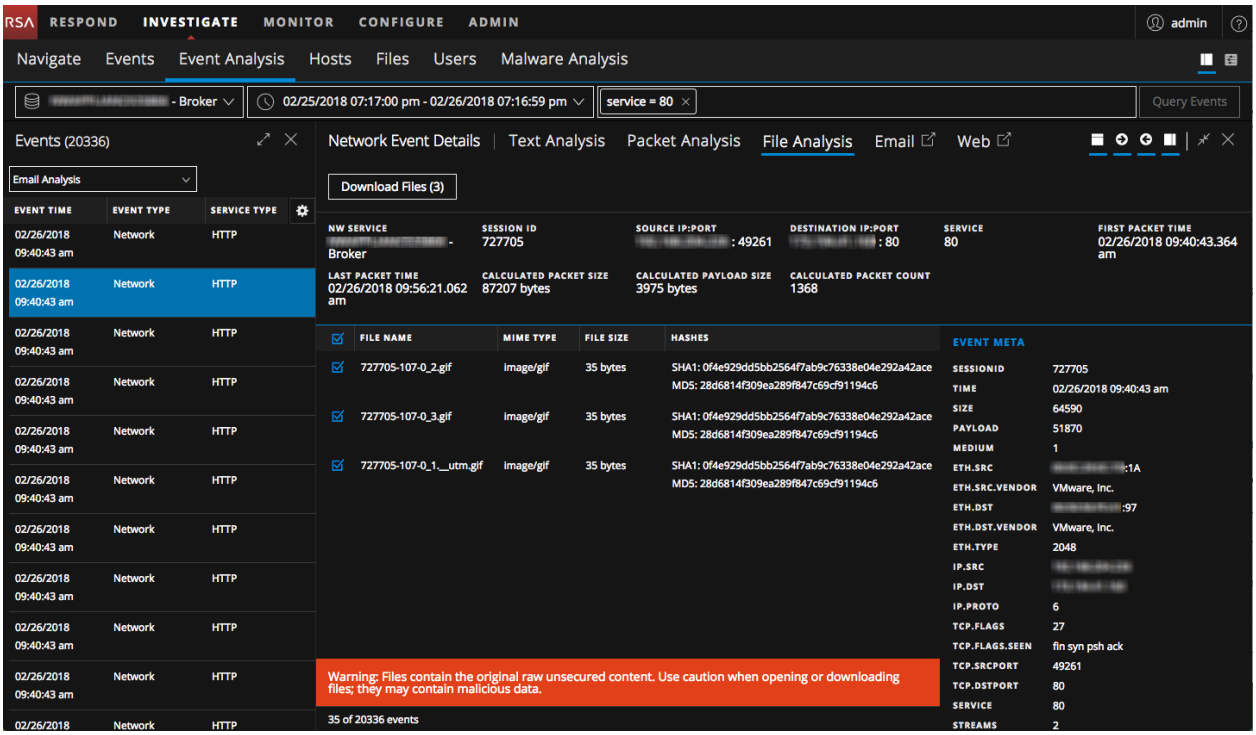
Le fichier de données réseau est téléchargé sur votre système de fichiers local dans le format spécifié.

Télécharger des fichiers à partir d'un événement de réseau dans le panneau Analyse de fichiers

Lors de l'affichage d'événements de réseau reconstitués qui contiennent des fichiers dans le panneau Analyse de fichiers, vous pouvez sélectionner un fichier, un ou plusieurs fichiers ou tous les fichiers à télécharger sur votre système de fichiers local.

Remarque : Si vous initiez un téléchargement et quittez la vue pendant que le fichier est en cours d'extraction et avant le démarrage du téléchargement du fichier, le fichier n'est pas téléchargé dans votre navigateur. Un message vous avertit que vous trouverez le fichier téléchargé dans la file d'attente de travail.

Lorsque des fichiers sont sélectionnés, le bouton Télécharger les fichiers devient actif et reflète le nombre de fichiers sélectionnés.



Le fait de cliquer sur le bouton exporte les fichiers sélectionnés en tant qu'archive zip protégée par un mot de passe. Le mot de passe pour ouvrir l'archive exportée est `netwitness`. L'exportation des fichiers dans ce formulaire garantit que :

- L'archive n'est pas mise en quarantaine par les logiciels antivirus.
- Les fichiers potentiellement malveillants ne sont pas automatiquement ouverts par l'application par défaut et exécutés.

Voici un exemple de nom de fichier pour une archive : `C01 - Concentrator_SID1697309_FC1.zip`. L'archive exportée est nommée à l'aide de la convention suivante :

`<service-ID or host name>_SID<n>_FC<n>.zip`

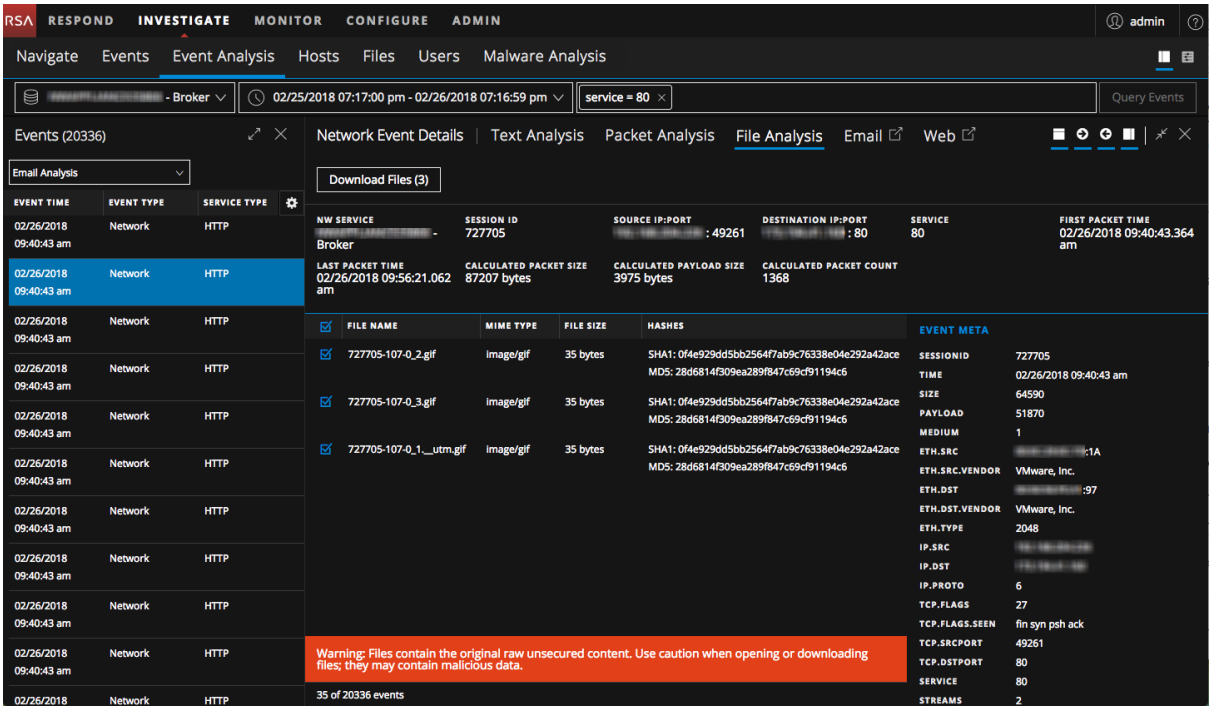
où :

- `<service-ID or host name>` est le nom du service (par exemple, Concentrator ou Broker) où la session a été enregistrée.
- `SID<n>` est le numéro d'ID de la session.
- `FC<n>` est le nombre de fichiers contenus dans l'archive.

Attention : Procédez avec prudence lors de la décompression et de l'ouverture de fichiers qui sont associés à une application par défaut ; par exemple, une feuille de calcul Excel peut automatiquement s'ouvrir dans Excel avant de vous permettre d'avoir le temps de vérifier qu'elle ne présente aucun risque.

Pour exporter des fichiers dans un événement reconstruit :

1. Dans la vue **Analyse d'événements** , accédez au panneau Analyse de fichiers d'un événement qui contient les fichiers.



2. Cliquez sur un ou plusieurs fichiers que vous souhaitez extraire, puis cliquez sur **Télécharger les fichiers**.
   La tâche est planifiée et une fois l'opération terminée, le fichier sélectionné est téléchargé, sous la forme d'une archive zip protégée par mot de passe, sur le système de fichiers local.
3. Pour ouvrir l'archive sur votre système de fichiers local, saisissez le mot de passe suivant lorsque vous y êtes invité : `netwitness`.

Agir sur les données dans la vue Analyse d'événements

Lorsque vous avez trouvé des données intéressantes dans la vue Analyse d'événements, vous pouvez effectuer des recherches internes dans NetWitness Endpoint et RSA Live, ainsi que des recherches externes de valeurs méta dans des ressources communautaires comme Historique SANS IP et la Recherche ThreatExpert.

Ouvrir un événement Endpoint dans le Client Thick NetWitness Endpoint

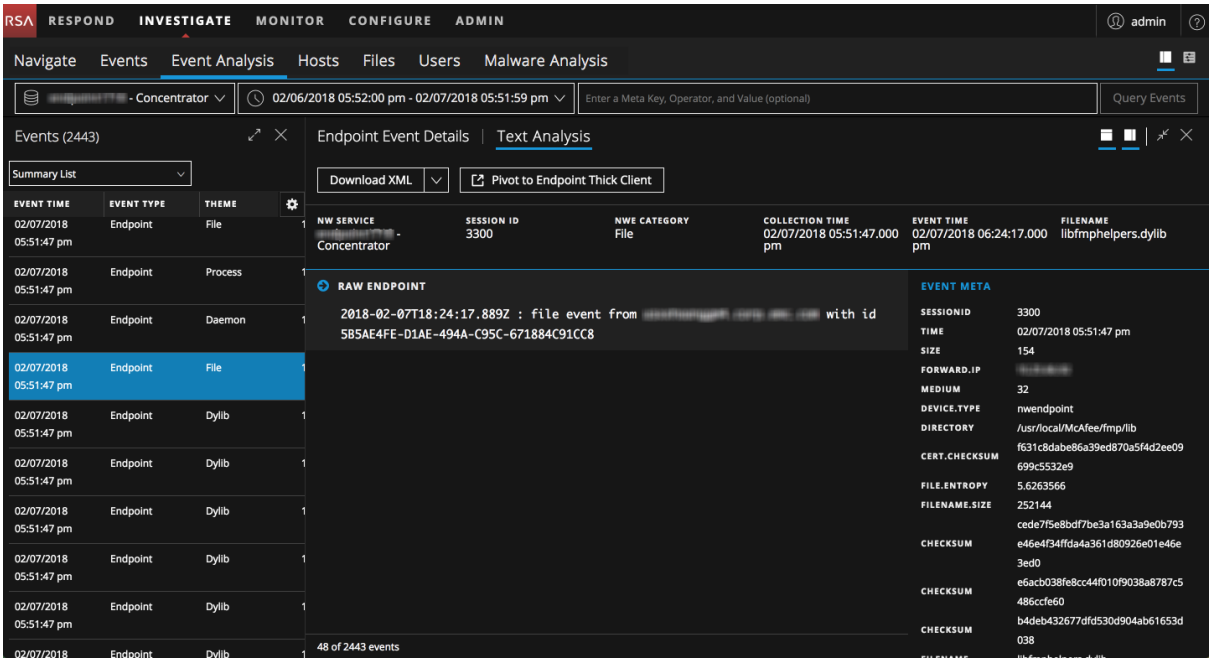
Lors de l'affichage d'un événement de point de terminaison dans le panneau Analyse de texte, vous pouvez faire pivoter pour analyser le même événement dans NetWitness Endpoint. Le Client Thick NWE offre des fonctionnalités supplémentaires au-delà de fonctionnalités intégrées dans NetWitness Endpoint Insights.

Remarque : La version 4.4 du client Thick NetWitness Endpoint (NWE) doit être installée sur le même serveur, les clés méta NWE doivent exister dans le fichier `table-map.xml` sur le Log Decoder et les clés méta NWE doivent exister dans le fichier `index-concentrator-custom.xml`. Le client Thick NWE est une application Windows uniquement. Les instruments de configuration complets sont fournis dans le *Guide d'utilisation du point de terminaison NetWitness* pour la Version 4.4.

Pour ouvrir un événement dans NetWitness Endpoint :

1. (Version 11.0 et ultérieures) Accédez à **ENQUÊTER** > **Naviguer** et procédez comme suit :
   a. Dans le menu déroulant **Requête**, sélectionnez **Avancé** et saisissez l'une des requêtes suivantes : `nwe.callback_id exists` ou `device.type='nwendpoint'`
   Les données Endpoint s'affichent dans le panneau Valeurs.
   b. Cliquez sur un événement avec le bouton droit de la souris, puis sélectionnez **Analyse d'événements** dans le menu.
2. (Version 11.1 ou supérieure) Accédez à la **ENQUÊTER** > **Analyse d'événements**. Dans le menu déroulant **Requête**, sélectionnez **Avancé** et saisissez l'une des requêtes suivantes : `nwe.callback_id exists` ou `device.type='nwendpoint'`
   Les données Endpoint s'affichent dans le panneau Événements.

3. Sélectionnez un événement.
   La vue Analyse d'événements s'ouvre avec l'événement sélectionné affiché dans l'Analyse de texte.

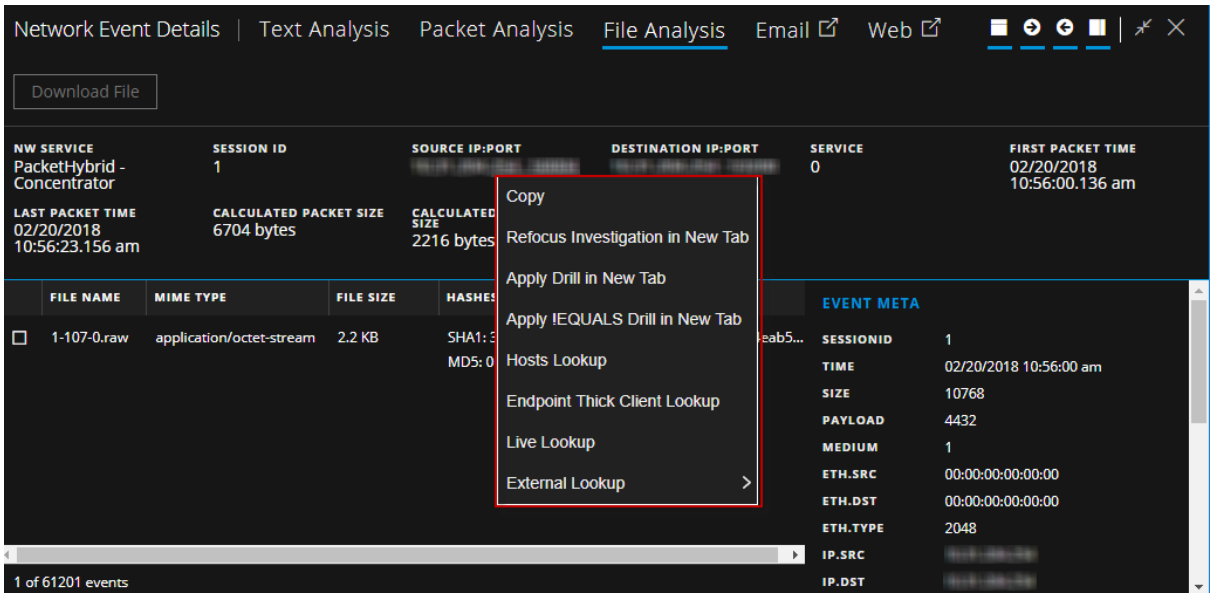


4. Dans l'en-tête d'événement, cliquez sur **Pivoter vers Endpoint.** Un nouvel onglet de navigateur avec l'URL `ecatui://<id>` s'ouvre et le client Thick NWE se lance. Si le Client Thick NetWitness Endpoint n'est pas installé, aucune donnée ne s'affiche et le message suivant apparaît : `Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

Effectuer des recherches de valeurs méta dans l'Analyse d'événements

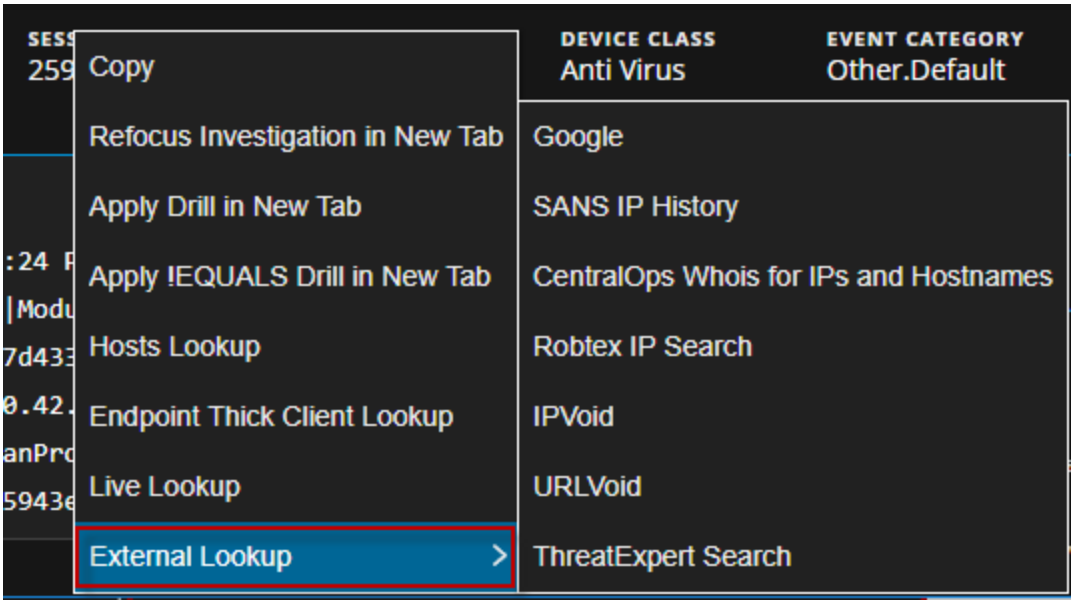
Dans la vue Analyse d'événements, vous pouvez poursuivre la procédure d'enquête des valeurs méta d'un événement en cliquant avec le bouton droit sur certaines valeurs méta et en utilisant les options du menu déroulant. Tous les champs ne proposent pas des actions quand on clique avec le bouton droit. Pour effectuer des recherches internes et externes :

1. Dans la vue Analyse d'événements, cliquez avec le bouton droit sur une valeur méta dans la Liste d'événements, dans le panneau Méta de l'événement ou dans l'En-tête d'événement. Certaines valeurs méta disposent d'un menu déroulant.



2. Sélectionnez l'une des actions internes suivantes :
   - **Copier** : Copie la valeur méta dans la zone de stockage temporaire.
   - **Recentrer la Procédure d'enquête dans un nouvel onglet** : Démarre une autre procédure d'enquête dans un nouvel onglet en se concentrant sur la valeur méta sélectionnée.
   - **Appliquer l'extraction dans un nouvel onglet** : Applique la recherche verticale et la lance dans un nouvel onglet pour effectuer une recherche verticale des données dans la vue Naviguer.
   - **Appliquer l'extraction !ÉGAL dans un nouvel onglet** : Applique (!ÉGAL) à la valeur méta et lance un nouvel onglet, ce qui exclut la valeur méta des résultats.
   - **Recherche d'hôtes** : Recherche la valeur dans Procédure d'enquête > vue Hôtes.
   - **Recherche dans le client Endpoint Thick** : Analyse la valeur méta dans le client Endpoint Thick (pour les clients dotés de l'agent Endpoint).
   - **Recherche dans Live** : Recherche une valeur méta sur RSA Live pour approfondir l'analyse.

3. Pour une recherche externe, survolez une valeur méta, faites un clic droit et sélectionnez **Recherche externe**.



4. Dans le sous-menu, sélectionnez l'une des recherches externes disponibles :
   - **Google** : Recherche une valeur méta sur Google.com.
   - **Historique SANS IP** : Recherche une valeur méta sur l'historique SANS IP, domaine = `http://isc.sans.org/ipinfo.html?ip=ipaddress`
   - **CentralOps Whois pour adresses IP et noms d'hôte** : Recherche une valeur méta sur CentralOps Whois pour adresses IP et noms d'hôte, domaine `=http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true`
   - **Recherche d'adresses IP Robtex** : Recherche une valeur méta sur Robtext IP Search, domaine = `https://www.robtex.com/cidr/domain.ipaddress`
   - **IPVoid** : Recherche une valeur méta sur IPVoid, domaine `=http://www.ipvoid.com/scan/domain/`
   - **URLVoid** : Recherche une méta-valeur sur URLVoid, domaine `=http://www.urlvoid.com/scan/ipaddress/`
   - **Recherche ThreatExpert** : Recherche une valeur de méta IP sur Recherche ThreatExpert, domaine `=http://www.threatexpert.com/reports.aspx?find=IP address`

Enquête sur les hôtes et les fichiers

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Les analystes peuvent utiliser les vues Hôtes et Fichiers de RSA NetWitness Platform pour rechercher des hôtes ou des fichiers.

Les analystes qui mènent une analyse avec Investigation doivent disposer des rôles et autorisations du système appropriés pour leur compte utilisateur. Un administrateur doit configurer des rôles et des autorisations conformément à la description de la rubrique Rôles et autorisations pour les analystes Endpoint. Pour plus d'informations sur les rôles et les autorisations, reportez-vous à la rubrique *Guide de la sécurité du système et de la gestion des utilisateurs*.

Les analystes peuvent :

- Examiner les hôtes
- Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure
- Examiner les fichiers

Examiner les hôtes

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Pour mener une procédure d'enquête sur les hôtes :

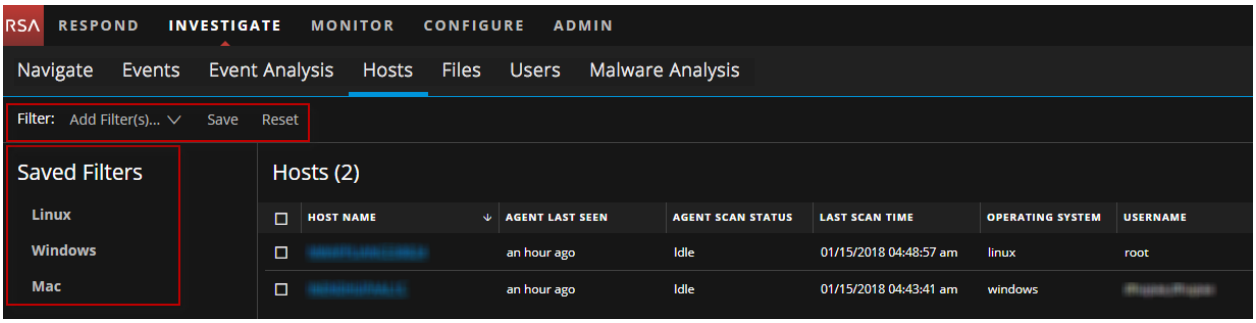
1. Accédez à **ENQUÊTER** > **Hôtes**.
   Une liste des hôtes avec un agent Endpoint installé s'affiche.
2. Sélectionnez les hôtes que vous souhaitez analyser, puis cliquez sur **Démarrer l'analyse**. Pour plus d'informations, voir Analyse des hôtes.
3. À la fin du processus d'analyse des hôtes, cliquez sur le nom d'hôte pour examiner les résultats de l'analyse. Pour plus d'informations, voir le Examiner les détails de l'hôte.

Remarque : Pour examiner les hôtes de NetWitness Endpoint 4.4, reportez-vous à la section Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure.

Filtrer les hôtes

Vous pouvez filtrer les hôtes sur le système d'exploitation ou sélectionner les champs dans le menu déroulant Ajouter un filtre.

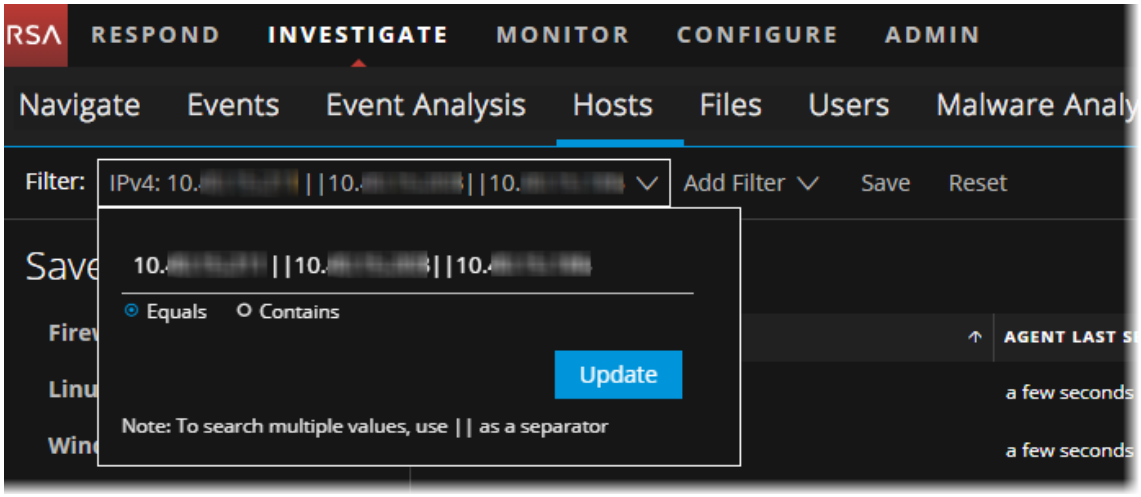
Remarque : Lors du filtrage sur une grande quantité de données, utilisez au moins un champ indexé avec l'opérateur `Equals` pour de meilleures performances. Les champs suivants sont indexés dans la base de données - `Hostname`, `IPV4`, `Operating System` et `Last Scan Time`.



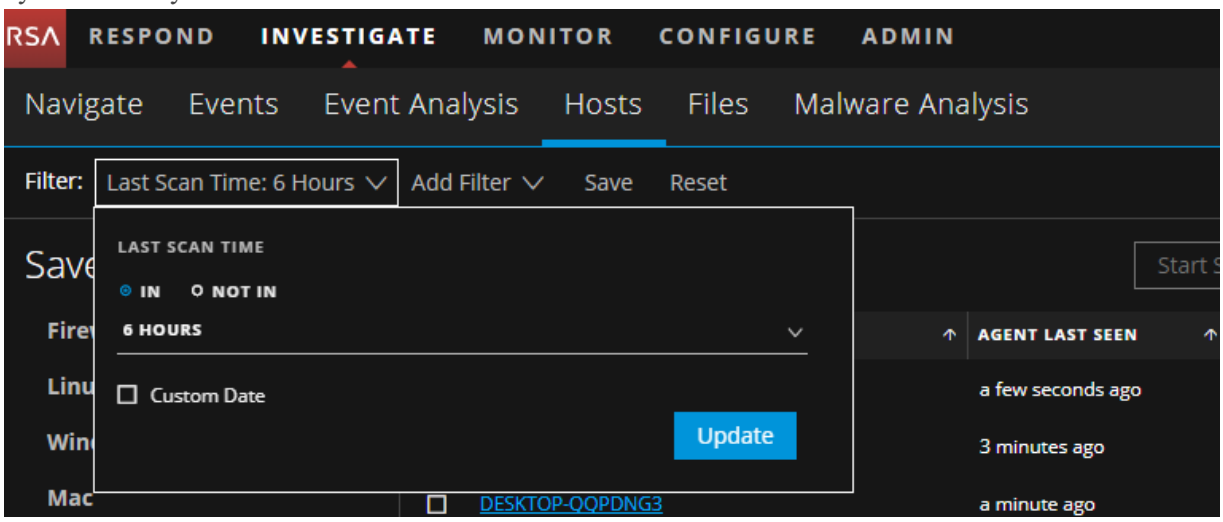
Pour rechercher plusieurs valeurs au sein d'un champ, définissez l'option de filtre sur `Equals`, et utilisez `||` comme séparateur.

Voici quelques exemples :

- En utilisant l'opérateur `Equals` pour plusieurs valeurs IPV4 avec un séparateur `||`.



- En utilisant l'opérateur `IN` avec le paramètre Heure de la dernière analyse afin de filtrer les agents ayant été analysés au cours des 6 dernières heures.



Cliquez sur **Enregistrer** pour enregistrer la recherche et fournir un nom (jusqu'à 250 caractères alphanumériques). Le filtre est ajouté au panneau Filtres enregistrés, sur la gauche. Pour supprimer un filtre, placez le pointeur sur le nom puis cliquez sur  .

Remarque : Les caractères spéciaux ne sont pas autorisés, à l'exception du caractère de soulignement (_) et du trait d'union (-) lors de l'enregistrement du filtre.

Analyse des hôtes

Vous pouvez effectuer une analyse à la demande ou planifier une analyse pour une exécution quotidienne ou hebdomadaire. Pour plus d'informations sur la planification d'une analyse, reportez-vous à la section *Guide de configuration Endpoint Insights*.

Remarque : Vous ne pouvez pas effectuer une analyse pour les agents NetWitness Endpoint 4.4 à partir de l'interface utilisateur de NetWitness Platform.

Analyse à la demande

Vous pouvez souhaiter effectuer une analyse à la demande si :

- Un fichier de la section Fichiers globaux s'avère être malveillant.
- Un fichier malveillant est présent sur différents hôtes du réseau.
- Vous souhaitez examiner un hôte qui est infecté.
- Obtenir le dernier snapshot de l'hôte.

Lors de l'analyse des hôtes, l'Agent Endpoint récupère les données suivantes utiles à la procédure d'enquête :

- Les pilotes, processus, DLL, fichiers (exécutables), services et exécutions automatiques en cours d'exécution sur l'hôte.
- Les entrées de fichier d'hôte et les tâches planifiées.
- Les informations du système telles que le partage réseau, les correctifs Windows installés, les tâches Windows, les utilisateurs connectés, l'historique bash et les produits de sécurité installés.

Pour démarrer une analyse :

1. Accédez à **ENQUÊTER** > **Hôtes**.
2. Sélectionnez un ou plusieurs hôtes (jusqu'à 100) à la fois pour l'analyse à la demande, puis cliquez sur **Démarrer l'analyse**.
3. Cliquez sur **Démarrer l'analyse** dans la boîte de dialogue.
   Cette opération permet d'effectuer une analyse rapide de tous les modules exécutables chargés en mémoire. Elle dure environ 10 minutes.

Les états d'analyse sont les suivants :

État	Description
Inactif	Aucune analyse en cours.
Analyse	Analyse en cours.
Démarrage de l'analyse	Une demande d'analyse est envoyée au serveur, mais l'agent recevra la demande la prochaine fois qu'il communiquera avec le serveur.
Arrêt de l'analyse	Une demande d'arrêt de l'analyse est envoyée au serveur, mais l'agent recevra la demande la prochaine fois qu'il communiquera avec le serveur.

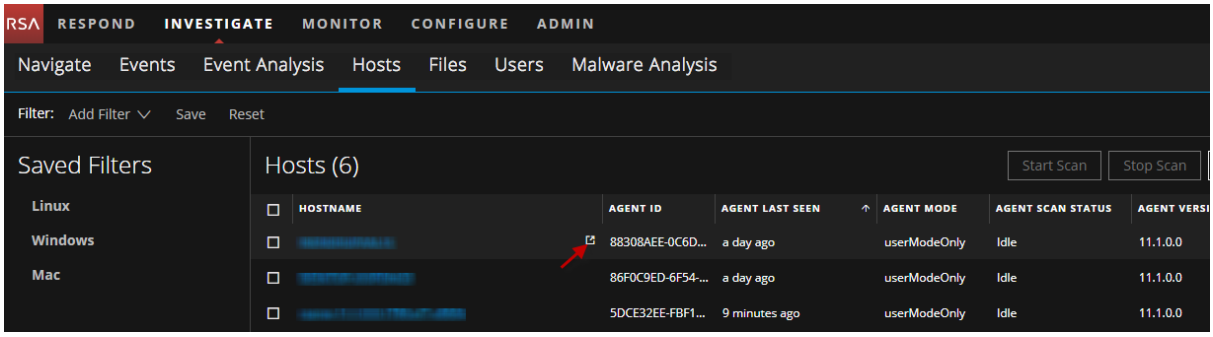
Pivoter vers les vues Naviguer et Analyse d'événements.

Si vous devez rechercher un hôte particulier, une adresse IP (IPV4) ou un nom d'utilisateur pour rechercher une activité associée sur une période donnée, vous pouvez faire pivoter les vues Naviguer et Analyse d'événements pour obtenir le contexte complet de l'activité. Par défaut, la période est définie sur 1 jour. Il est possible de modifier la plage horaire.

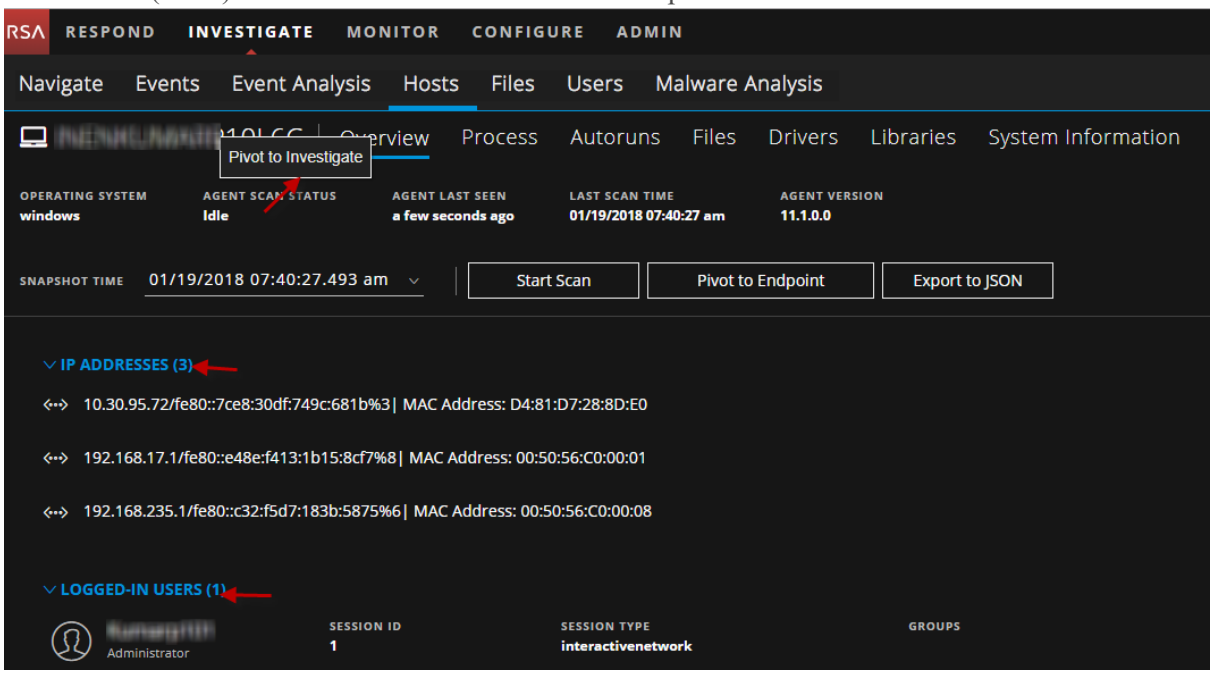
Remarque : Le pivotement vers la vue Naviguer ou Analyse d'événements n'est pas pris en charge pour IPV6.

Pour pivoter vers la vue Naviguer ou Analyse d'événements :

1. Go to **ENQUÊTER** > **Hôtes** ou **ENQUÊTER** > **Fichiers**.
2. Cliquez sur  en regard du nom d'hôte.



Autre possibilité, dans l'onglet Présentation, vous pouvez effectuer un clic droit sur le nom d'hôte, l'adresse IP (IPV4) ou les utilisateurs connectés à faire pivoter.

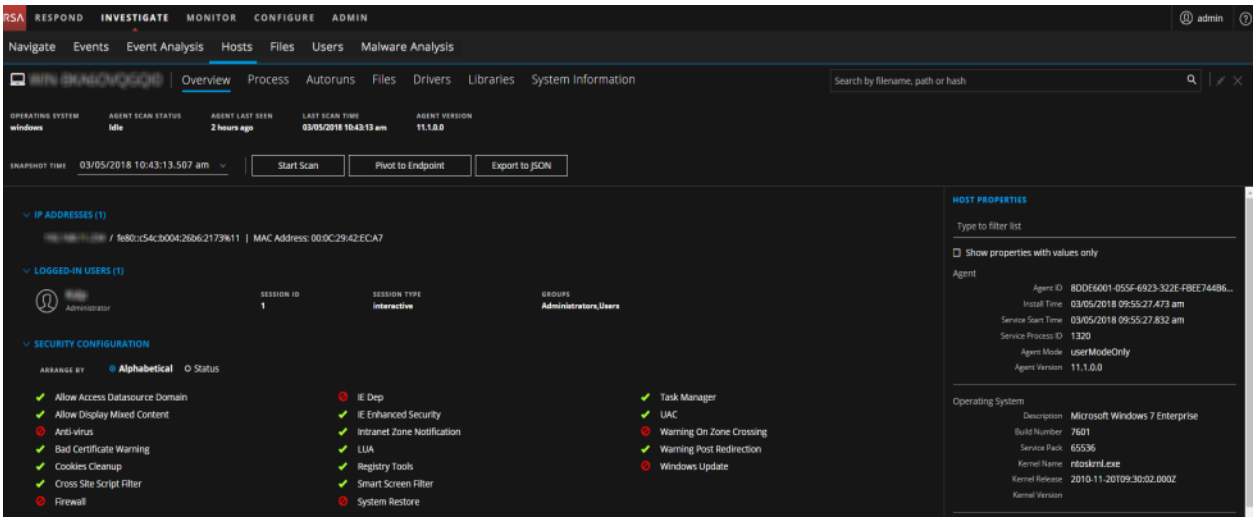


3. Dans la boîte de dialogue Sélectionner un service, sélectionnez l'un des services requis pour la procédure d'enquête.

4. Cliquez sur **Naviguer** ou **Analyse d'événements** pour analyser les données.

Examiner les détails de l'hôte

Pour rechercher des fichiers suspects sur un hôte, cliquez sur le nom d'hôte et affichez les détails de l'hôte ou lancez une analyse à la demande pour obtenir les informations les plus récentes.



Recherche dans les snapshots

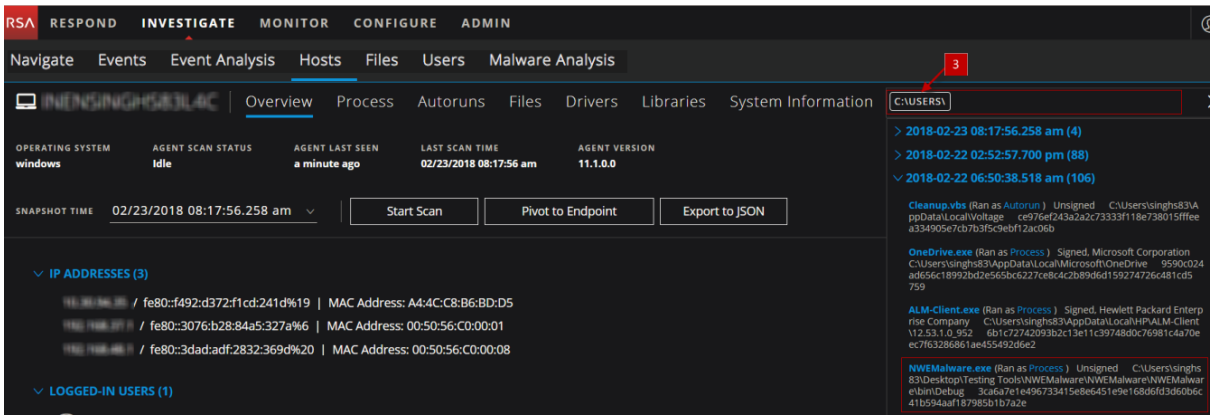
Pour rechercher un hôte ou vérifier s'il est infecté par un programme malveillant connu, vous pouvez rechercher les occurrences du nom de fichier, du chemin du fichier ou de la somme de contrôle SHA-256.

Remarque : Pour rechercher une somme de contrôle SHA-256, fournissez la chaîne de hachage entière dans la zone de recherche.

Le résultat affiche des détails, tels que le nom du fichier, les informations de signature, ainsi que son interaction avec le système (exécuté en tant que processus, bibliothèque, exécution automatique, service, tâche ou pilote). Pour afficher plus de détails sur ces résultats, cliquez sur la catégorie.

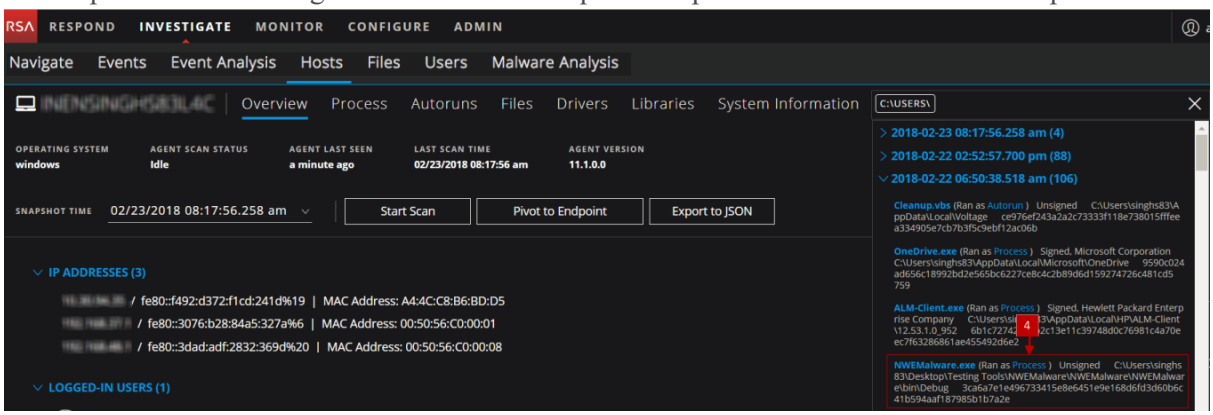
Par exemple, un utilisateur a cliqué et exécuté une pièce jointe malveillante via un e-mail d'hameçonnage et l'a téléchargé sur `C:\Users`. Pour examiner ce fichier :

1. Accédez à **ENQUÊTER** > **Hôtes**.
2. Sélectionnez l'hôte que vous souhaitez examiner.
3. Dans l'onglet **Présentation**, entrez le chemin du fichier `C:\Users` dans la zone de recherche. La recherche affiche tous les fichiers exécutables de ce dossier. Dans cet exemple, le fichier `NWEMalware.exe`, est un fichier non signé susceptible d'être malveillant.



Ce fichier est exécuté en tant que processus.

4. Pour afficher les détails de ce fichier, cliquez sur **Traiter** dans les résultats.
   Cette opération ouvre l'onglet Processus dans lequel vous pouvez afficher les détails du processus.



Analyser les processus

Dans la vue Hôtes, sélectionnez l'onglet **Processus**. Vous pouvez afficher les processus qui s'exécutaient au moment de l'analyse de l'hôte sélectionné. Les colonnes Nom de processus et ID de processus (PID) s'affichent sous la forme :

- Arborescence - vous pouvez accéder à chaque processus et afficher le processus enfant ou parent associé.
- Vue Liste - Vous pouvez trier le nom du processus et les colonnes PID.

Cliquez sur pour changer de vue.

Voici un exemple de l'arborescence :

En examinant les processus, il est important afficher les arguments de lancement. Même les fichiers légitimes peuvent être utilisés à des fins malveillantes, il est donc important de les voir tous pour déterminer s'il y a une activité malveillante.

Par exemple,

- `rundll32.exe` est un fichier exécutable Windows légitime classé comme étant un fichier fiable. Toutefois, une personne malveillante peut utiliser ce fichier exécutable pour charger une DLL de programme malveillant. Par conséquent, lors de l'affichage des processus, vous devez afficher les arguments du fichier `rundll32.exe`.
- `LSASS.EXE` est un enfant `WININIT.EXE`. Il ne doit comporter que les processus enfants. Souvent, un programme malveillant utilise cet exécutable pour vider les mots de passe ou l'imiter pour masquer un système (`lass.exe`, `lssass.exe`, `lsasss.exe`, etc.).
- La plupart des applications utilisateur légitimes comme Adobe, les navigateurs Web, etc. ne génèrent pas de processus enfants comme `cmd.exe`. Si c'est le cas, examiner les processus.

Analyser les exécutions automatiques

Dans la vue Hôtes, sélectionnez l'onglet **Exécutions automatiques**. Vous pouvez afficher les exécutions automatiques, services et tâches cron qui sont en cours d'exécution pour l'hôte sélectionné.

Par exemple, dans l'onglet Services, vous pouvez rechercher l'heure de création du fichier. L'heure de compilation est trouvée dans chaque fichier PE (Portable Executable) de l'en-tête PE. L'horodatage est rarement falsifié, même si une personne malveillante peut facilement le modifier avant de le déployer sur le point final de la victime. Cet horodatage peut indiquer si un nouveau fichier est introduit. Vous pouvez comparer l'horodatage du fichier sur le système pour connaître le décalage par rapport à l'heure de création. Si un fichier a été compilé il y a quelques jours, mais que l'horodatage de ce fichier sur le système indique qu'il a été créé il y a quelques années, il indique que le fichier est altéré.

Analyser les fichiers

Dans la vue Hôtes, sélectionnez l'onglet **Fichiers**. Vous pouvez afficher la liste des fichiers analysés sur l'hôte au moment de l'analyse. Par défaut, le tableau affiche 100 fichiers. Pour afficher plus de fichiers, cliquez sur **Charger davantage** au bas de la page.

Par exemple, de nombreux chevaux de Troie écrivent des noms de fichiers aléatoires lors de la suppression de leurs charges utiles pour empêcher une recherche facile sur les points de terminaison dans le réseau en fonction du nom de fichier. Si un fichier est nommé `svch0st.exe`, `scvhost.exe` ou `svchosts.exe`, cela indique que le fichier Windows légitime nommé `svchost.exe` est en cours de reproduction.

Analyse des bibliothèques

Dans la vue Hôtes, sélectionnez l'onglet **Bibliothèques**. Vous pouvez afficher la liste des bibliothèques chargées au moment de l'analyse.

Par exemple, un fichier avec une entropie élevée est marqué comme doté de fonctionnalités. Un fichier compressé signifie qu'il est compressé pour réduire sa taille (ou pour masquer les chaînes malveillantes et les informations de configuration).

Analyser les pilotes

Dans la vue Hôtes, sélectionnez l'onglet **Pilotes**. Vous pouvez afficher la liste des pilotes s'exécutant sur l'hôte au moment de l'analyse.

Par exemple, à l'aide de ce panneau, vous pouvez vérifier si le fichier est signé ou non signé. Un fichier signé par un fournisseur de confiance tel que Microsoft et Apple, avec le terme, `valid`, indique qu'il s'agit d'un fichier fiable.

Analyser les informations du système

Dans la vue Hôtes, sélectionnez l'onglet **Informations du système**. Ce panneau répertorie les informations du système. Pour le système d'exploitation Windows, le panneau affiche les entrées du fichier hôte et les partages réseau de cet hôte.

Par exemple, les programmes malveillants peuvent utiliser des entrées de fichier hôte pour bloquer les mises à jour antivirus.

Supprimer un hôte

Pour supprimer manuellement des hôtes à partir de l'interface utilisateur :

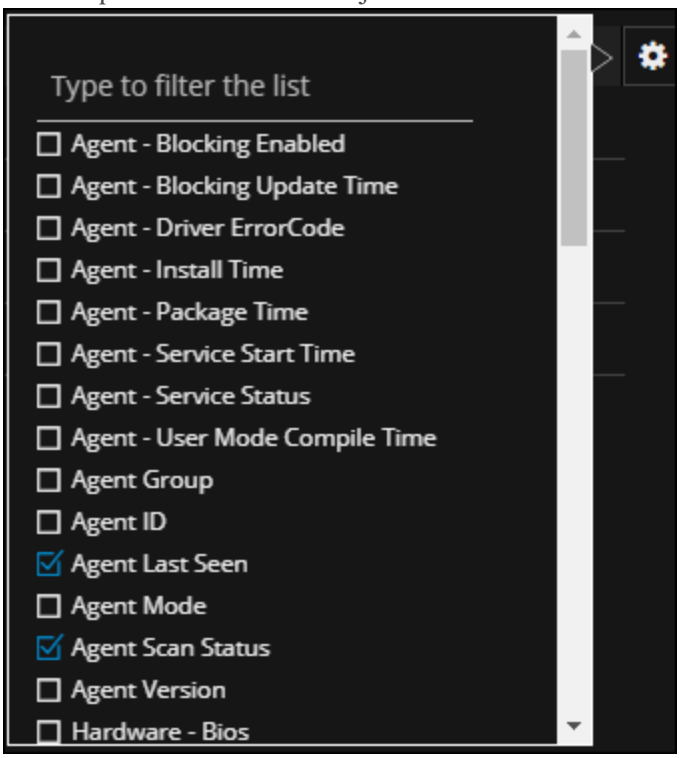
1. Accédez à **ENQUÊTER > Hôtes**.
2. Sélectionnez les hôtes à supprimer dans la vue Hôtes, puis cliquez sur **Supprimer**.
   Cela supprime toutes les données de point de terminaison collectées pour les hôtes sélectionnés.

Remarque : Si vous supprimez accidentellement un hôte dans la vue Hôtes, le serveur Endpoint interdit toutes les demandes en provenance de cet agent. L'agent doit être désinstallé manuellement de l'hôte et réinstallé pour qu'il apparaisse dans la vue Hôtes.

Définir les Préférences d'hôtes

Par défaut, la vue Hôtes affiche plusieurs colonnes et les hôtes sont triés en fonction de l'heure de la première analyse. Si vous souhaitez afficher des colonnes spécifiques et trier les données sur un champ spécifique :

1. Accédez à **ENQUÊTER > vue Hôtes**.
2. Sélectionnez les colonnes en cliquant sur dans le coin inférieur droit. L'exemple suivant montre l'écran qui s'affiche lors de l'ajout de colonnes :



3. Trier les données de la colonne requise.

Remarque : Il s'agit de votre vue par défaut chaque fois que vous vous connectez à la vue Hôtes.

Exporter les attributs de l'hôte

Vous pouvez exporter jusqu'à 100 000 attributs d'hôte à la fois. Pour extraire les attributs d'hôte dans un fichier de valeurs séparées par des virgules (CSV).

1. Accédez à **ENQUÊTER > Hôtes**.
2. Filtrez les hôtes en sélectionnant l'option de filtre requise.

3. Ajoutez des colonnes en cliquant sur  dans le coin inférieur droit.
4. Cliquez sur **Exporter dans un fichier CSV.**

Vous pouvez enregistrer ou ouvrir le fichier CSV.

Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Si vous disposez de NetWitness Endpoint 4.4.0.2 ou version ultérieure dans votre déploiement, vous pouvez afficher les données Endpoint de ces hôtes dans les vues **ENQUÊTER > Hôtes** et **ENQUÊTER > Fichiers**

Si les hôtes NetWitness Endpoint 4.4.0.2 ne s'affichent pas, reportez-vous à la section « Intégration de NetWitness Endpoint 4.4.0.2 ou une version ultérieure à NetWitness Endpoint 11.1 » dans le *Guide de configuration Endpoint Insights*.

Les hôtes NetWitness Endpoint 4.4.0.2 peuvent être identifiés dans la vue Hôtes à l'aide de la version de l'agent. Vous ne pouvez pas effectuer d'analyse à la demande sur ces hôtes. Pour examiner ces hôtes, vous devez utiliser l'interface utilisateur NetWitness Endpoint 4.4.0.2 ou ultérieure.

Remarque : Pour basculer vers le client Thick à partir de l'interface utilisateur de NetWitness Suite, NetWitness Endpoint 4.4.0.2 ou version ultérieure doit être installé.

Pour examiner un hôte dans l'interface utilisateur NetWitness Endpoint :

1. Accédez à **ENQUÊTER** > **Hôtes**.
2. Sélectionnez l'hôte 4.4 à partir du tableau.
3. Cliquez sur **Pivoter vers Endpoint**.

Remarque : L'option **Pivoter vers Endpoint** n'est pas applicable aux hôtes NetWitness Endpoint Insights 11.1.

Examiner les fichiers

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Les analystes peuvent utiliser la vue Fichiers (**ENQUÊTER > Fichiers**) pour identifier des fichiers suspects en examinant le nom de fichier, la taille de fichier, l'entropie, le format, le nom de l'entreprise, la signature et le checksum.

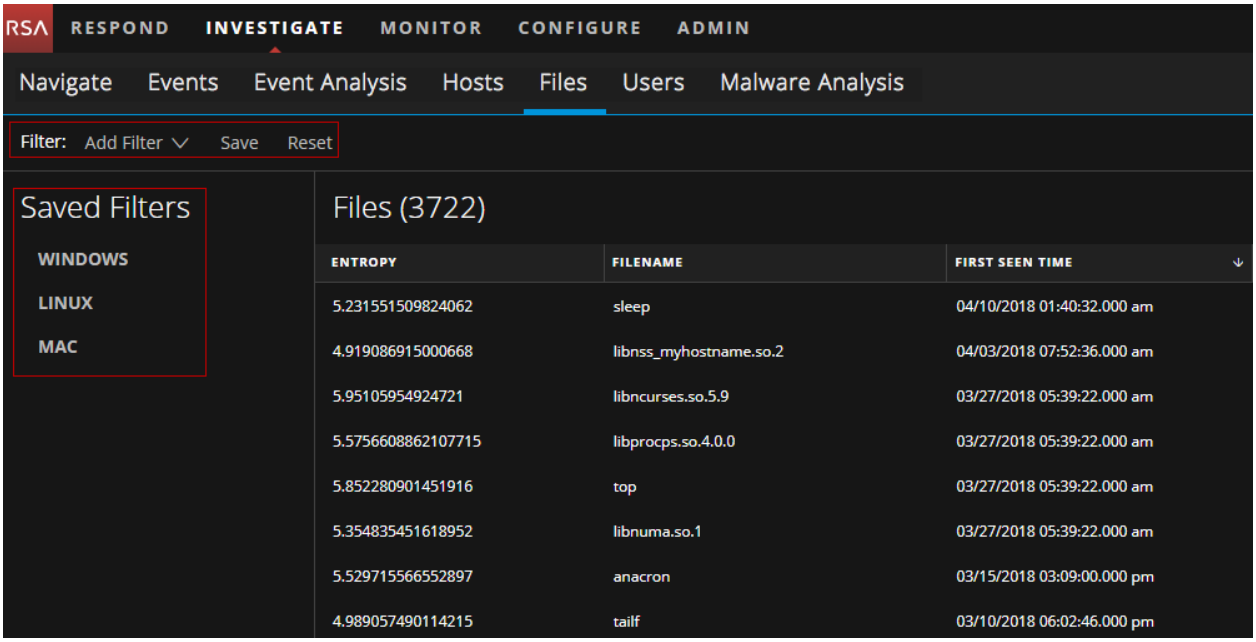
Par exemple, lorsque vous recherchez un nom de fichier, si un environnement est infecté par le ransomware WannaCry, l'analyste peut filtrer la liste à l'aide de ce nom de fichier. Vous pouvez également rechercher ce ransomware à l'aide du checksum.

La taille du fichier peut être un indicateur lors de l'évaluation d'un fichier. Les chevaux de Troie sont généralement inférieurs à 1 Mo et la majorité d'entre eux sont même inférieurs à 500 Ko.

Filtrer les fichiers

Vous pouvez filtrer les fichiers sur le système d'exploitation ou sélectionner les champs dans le menu déroulant Ajouter un filtre.

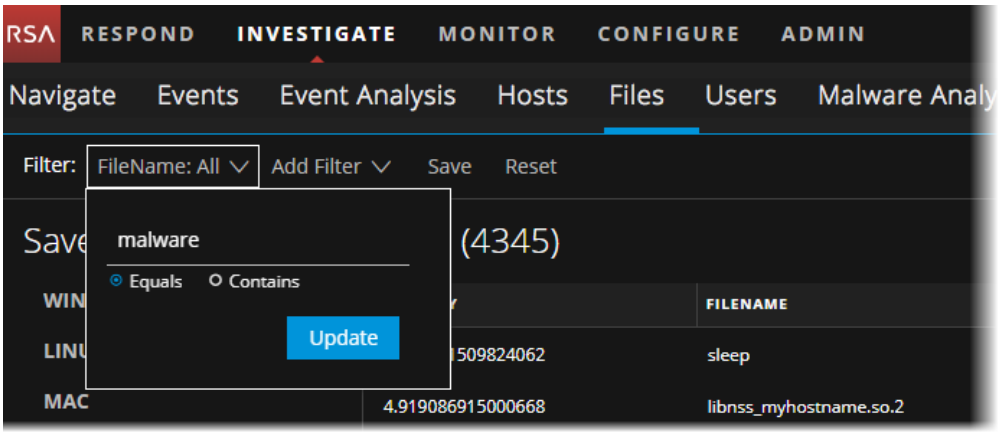
Remarque : Lors du filtrage sur un jeu de données volumineux, utilisez au moins un champ indexé avec l'opérateur `Equals` pour de meilleures performances. Les champs suivants sont indexés dans la base de données : Nom de fichier, MD5, Système d'exploitation, Heure de la première visualisation et Format.



Cliquez sur **Enregistrer** pour enregistrer la recherche et fournir un nom (jusqu'à 250 caractères alphanumériques). Le filtre est ajouté au panneau Filtres enregistrés, sur la gauche. Pour supprimer un filtre, placez le pointeur sur le nom puis cliquez sur  .

Remarque : Les caractères spéciaux ne sont pas autorisés, à l'exception du caractère de soulignement (_) et du trait d'union (-) lors de l'enregistrement du filtre.

Par exemple, des fichiers de filtrage avec le nom de fichier `malware` utilisant l'opérateur `Equals`.



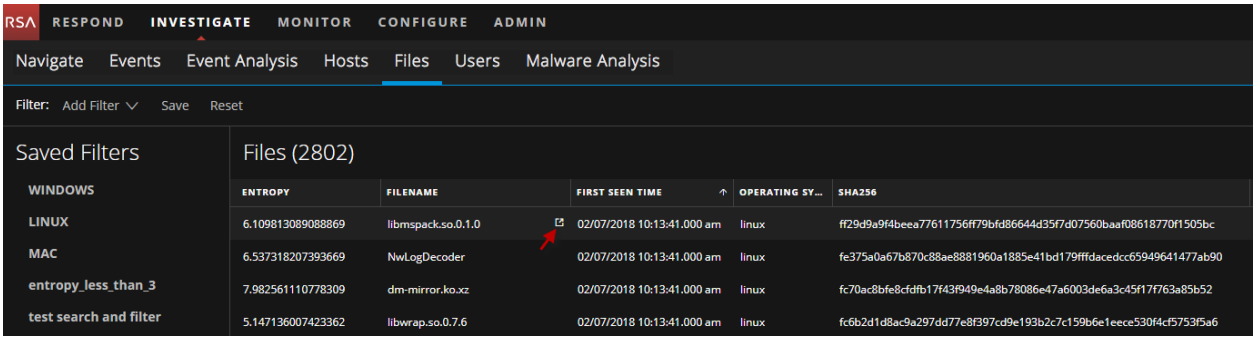
Remarque : Pour la taille du fichier, 1 Ko est calculé comme 1 024 octets. Par exemple, si la taille réelle du fichier est 8 421 octets, l'interface utilisateur affiche 8,2 Ko au lieu de 8,22 Ko. Il est recommandé d'effectuer une recherche au format octets avec l'opérateur `Equals`.

Pivoter vers les vues Naviguer et Analyse d'événements.

Si vous avez besoin de réaliser une procédure d'enquête sur un nom de fichier ou de hachage particulier (SHA256 et MD5) dans les fichiers globaux pour rechercher une activité associée sur une période, vous pouvez pivoter vers les vues Naviguer et Analyse d'événements pour obtenir tout le contexte du fichier. Par défaut, la période est définie sur 1 jour. Vous pouvez modifier l'intervalle de temps en conséquence.

Pour pivoter vers la vue Naviguer ou Analyse d'événements :

1. Accédez à **ENQUÊTER > Hôtes**.
2. Cliquez sur  en regard du nom de fichier ou de hachage.



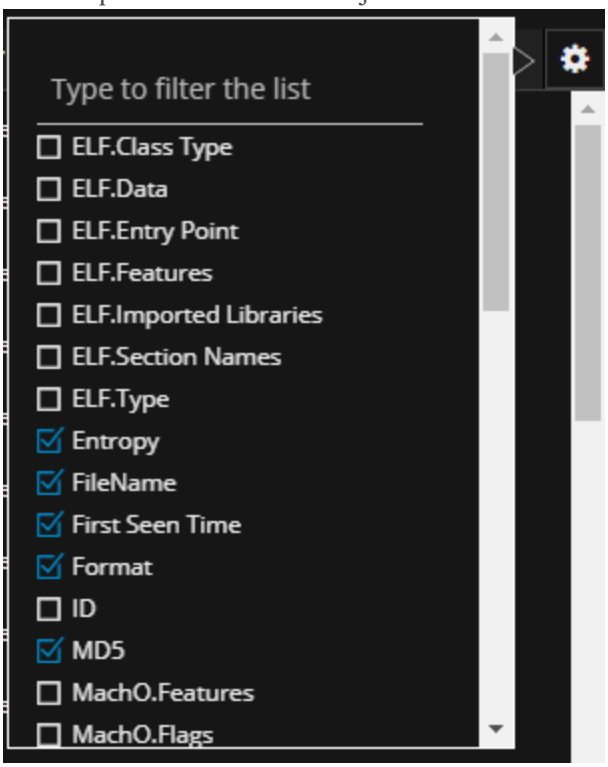
3. Dans la boîte de dialogue Sélectionner un service, sélectionnez l'un des services requis pour la procédure d'enquête.
4. Cliquez sur **Naviguer** ou **Analyse d'événements** pour analyser les données.

Remarque : Lorsque vous pivotez vers la vue Naviguer ou Analyse d'événements, les résultats mettent du temps à charger si les valeurs ne sont pas indexées. Pour plus d'informations, reportez-vous à la section Résolution des problèmes liés à NetWitness Investigate.

Définir les préférences de fichiers

Par défaut, la vue Fichiers affiche plusieurs colonnes et les fichiers sont triés en fonction de l'Heure de la première visualisation. Si vous souhaitez afficher des colonnes spécifiques et trier les données sur un champ spécifique :

1. Accédez à **ENQUÊTER > Fichiers**.
2. Sélectionnez les colonnes en cliquant sur dans le coin inférieur droit. L'exemple suivant montre l'écran qui s'affiche lors de l'ajout de colonnes :



3. Trier les données de la colonne requise.

Remarque : Il s'agit de votre vue par défaut chaque fois que vous vous connectez à la vue Fichiers.

Exporter des fichiers globaux

Pour extraire la liste de fichiers globaux dans un fichier CSV.

Remarque : Lors du filtrage sur un jeu de données volumineux, utilisez au moins un champ indexé avec l'opérateur `Equals` pour de meilleures performances. Vous pouvez exporter jusqu'à 100 000 à la fois.

1. Accédez à **ENQUÊTER > Fichiers**.
2. Filtrez les fichiers en sélectionnant l'option de filtre requise.
3. Ajoutez des colonnes en cliquant sur  dans le coin inférieur droit.
4. Cliquez sur **Exporter dans un fichier CSV.**

Vous pouvez enregistrer ou ouvrir le fichier CSV.

Mener une analyse de malware

Les analystes peuvent utiliser le service RSA NetWitness Platform Malware Analysis pour détecter les malware dans certains fichiers et données.

Les analystes qui mènent une analyse avec NetWitness Platform Malware Analysis doivent disposer des rôles et autorisations du système appropriés pour leur compte utilisateur.

Les procédures suivantes fournissent des instructions sur l'utilisation de Malware Analysis :

- Lancer une procédure d'enquête Malware Analysis.
- Télécharger des fichiers pour l'analyse Malware Analysis.
- Implémenter du contenu YARA personnalisé.
- Filtrer les données de dashlet dans la vue Récapitulatif des événements.
- Examiner les fichiers et événements d'analyse dans le formulaire de liste
- Afficher l'analyse Malware Analysis détaillée d'un événement.

Fonctions Malware Analysis

NetWitness Platform Malware Analysis est un processeur automatisé d'analyse de malware, conçu pour analyser certains types d'objets fichiers (par exemple, Windows portable executable (PE), PDF et MS Office) afin d'évaluer la probabilité de leur malveillance.

Malware Analysis détecte des indicateurs de compromission en utilisant quatre méthodologies distinctes d'analyse :

- Analyse de session de réseau (réseau)
- Analyse de fichier statique (statique)
- Analyse de fichier dynamique (sandbox)
- Analyse de communauté de sécurité (communauté)

Chacune des quatre méthodologies distinctes d'analyse est conçue pour compenser toutes faiblesses inhérentes aux autres. Par exemple, Analyse de fichier dynamique peut compenser des attaques de type Zero-Day qui ne sont pas détectées pendant la phase Analyse de communauté de sécurité. En évitant l'analyse de programme malveillant qui se concentre strictement sur une méthodologie, l'analyste a plus de chances d'être protégé contre des résultats faux négatifs.

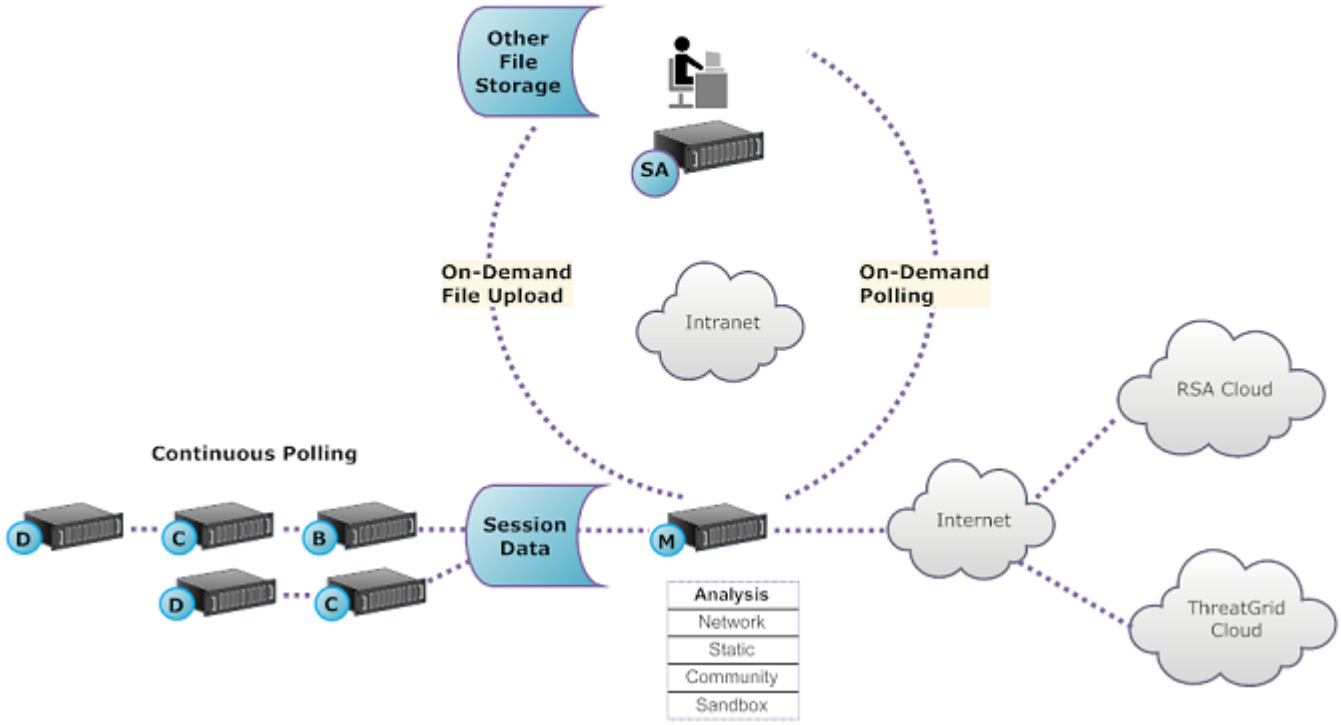
En plus des indicateurs de compromission intégrés, Malware Analysis prend également en charge les indicateurs de compromission écrits en langage YARA. YARA est un langage de règles qui permet aux chercheurs spécialisés d'identifier et de classer les échantillons de programmes malveillants. Cela permet aux auteurs d'IOC d'ajouter des fonctionnalités de détection à RSA Malware Analysis en créant des règles YARA et en les publiant dans RSA Live. Ces IOC basés sur YARA dans RSA Live seront automatiquement téléchargés et activés sur l'hôte abonné afin de compléter l'analyse existante qui est réalisé dans chaque fichier analysé.

Malware Analysis possède également des caractéristiques qui prennent en charge les alertes pour Incident Management.

Présentation fonctionnelle

La figure suivante illustre la relation fonctionnelle entre les services de base (Decoder, Concentrator et Broker), le service Malware Analysis et le NetWitness Server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



Le service Malware Analysis analyse des objets de fichier en utilisant une combinaison des méthodes suivantes :

- **Rappel automatique continu d'un Concentrator ou d'un Broker** pour extraire les sessions identifiées par un parser qui présentent un contenu potentiellement malveillant.
- **Rappel à la demande d'un Concentrator ou d'un Broker** pour extraire les sessions identifiées par un analyste de malware qui présentent un contenu potentiellement malveillant.
- **Téléchargement de fichiers à la demande** à partir d'un dossier spécifique à l'utilisateur.

Lorsque l'interrogation automatique d'un Concentrator ou d'un Broker est activée, le service Malware Analysis extrait et classe par priorité en permanence le contenu exécutable, les documents PDF et les documents Microsoft Office sur votre réseau, directement à partir de données capturées et analysées par votre service de base. Étant donné que le service Malware Analysis se connecte à un Concentrator ou un Broker pour extraire uniquement les fichiers exécutables qui sont marqués comme étant des programmes malveillants potentiels, le processus est à la fois rapide et efficace. Ce processus est continu et ne nécessite aucune surveillance.

Lorsque l'interrogation automatique d'un Concentrator ou d'un Broker est choisie, l'analyste de malware utilise Investigation pour explorer les données capturées et choisir des sessions à analyser. Le service Malware Analysis utilise ces informations pour interroger automatiquement le Concentrator ou le Broker et télécharger les sessions spécifiées en vue de leur analyse.

Le téléchargement à la demande de fichiers fournit une méthode permettant à l'analyste d'examiner des fichiers capturés externes à l'infrastructure de base. Le malware choisit un emplacement de dossier et identifie un ou plusieurs fichiers à télécharger et à faire analyser par Malware Analysis. Ces fichiers sont analysés en utilisant la même méthodologie que les fichiers extraits automatiquement de sessions de réseau.

Méthode d'analyse

Pour l'analyse réseau, le service Malware Analysis recherche des caractéristiques qui semblent s'écarter de la norme, tout comme le fait un analyste. En consultant des centaines à des milliers de caractéristiques et en associant les résultats dans un système de notation pondéré, des sessions légitimes qui ont par coïncidence quelques caractéristiques anormales sont ignorées, alors que celles qui sont réellement incorrectes sont mises en surbrillance. Les utilisateurs peuvent apprendre des modèles qui indiquent une activité anormale dans les sessions et qui servent d'indicateurs justifiant un examen plus poussé, appelés indicateurs de compromission.

Le service Malware Analysis peut effectuer une analyse statique concernant des objets suspects qu'il trouve sur le réseau et déterminer si ces objets contiennent du code malveillant. Pour l'analyse Communauté, un nouveau programme malveillant détecté sur le réseau est poussé vers le RSA Cloud pour vérifier au regard des flux et données d'analyse de programme malveillant propres à RSA du SANS Internet Storm Center, du SRI International, du Département du Trésor et de VeriSign. Pour l'analyse Sandbox, les services peuvent également pousser des données dans des hôtes principaux de gestion des événements et des informations de sécurité (SIEM) (le ThreatGrid Cloud).

Malware Analysis comporte une méthode d'analyse spécifique en partenariat avec des experts et des leaders du secteur dont les technologies peuvent enrichir le système de notation Malware Analysis.

NetWitness ServerAccédez au service Malware Analysis

Le NetWitness Server est configuré pour se connecter au service Malware Analysis et importer les données marquées pour être soumises à une analyse plus approfondie dans Investigation. L'accès se base sur trois niveaux d'inscription.

- Inscription gratuite : Tous les clients NetWitness Platform bénéficient d'une inscription gratuite, avec une clé d'évaluation gratuite pour l'analyse ThreatGrid. Le service Malware Analysis est limité à 100 exemples de fichiers par jour. Le nombre d'exemples (dans le jeu de fichiers ci-dessus) soumis au ThreatGrid Cloud pour l'analyse sandbox est limité à 5 par jour. Si une session de réseau comporte 100 fichiers, les clients atteindront la limite du taux après traitement de la session de réseau unique. Si 100 fichiers ont été téléchargés manuellement, alors la limite du taux est atteinte.
- Niveau d'inscription standard : Le nombre d'envois au service Malware Analysis est illimité. Le nombre d'exemples soumis au ThreatGrid Cloud pour une analyse sandbox est de 1 000 par jour.
- Niveau d'inscription entreprise : Le nombre d'envois au service Malware Analysis est illimité. Le nombre d'exemples soumis au ThreatGrid Cloud pour analyse sandbox est de 5 000 par jour.

Méthode de notation

Par défaut, les Indicateurs de compromission (IOC) sont réglés pour refléter les bonnes pratiques du secteur. Pendant l'analyse, les IOC qui se déclenchent entraîne un déplacement vers le haut ou vers le bas de la note pour indiquer la probabilité que l'exemple soit malveillant. Le réglage des IOC est exposé dans NetWitness Platform afin que l'analyste du programme malveillant puisse choisir de remplacer la note attribuée ou de désactiver l'évaluation d'un IOC. L'analyste a la possibilité d'utiliser le réglage par défaut ou de personnaliser complètement le réglage selon des besoins spécifiques.

Les IOC basés sur YARA sont imbriqués dans les IOC intégrés au sein de chaque catégorie intégrée et ne sont pas distincts des IOC natifs. Lors de la visualisation des IOC dans la vue Configuration de service, les administrateurs peuvent sélectionner YARA dans la liste de sélection Module pour consulter une liste de règles YARA.

Après qu'une session est importée dans NetWitness Platform, toutes les fonctionnalités d'affichage et d'analyse dans Investigation sont disponibles pour poursuivre l'analyse des Indicateurs de compromission. Lorsqu'ils sont consultés dans Investigation, les IOC YARA sont différenciés des IOC intégrés natifs par la balise `Yara rule`.

Déploiement

Le service Malware Analysis est déployé en tant qu'hôte RSA Malware Analysis distinct. L'hôte Malware Analysis dédié comporte un Broker intégré qui se connecte à l'infrastructure de base (un autre Broker ou Concentrator). Avant l'établissement de cette connexion, une collection de parsers et de feeds doit être ajoutée aux Decoders connectés aux Concentrators et aux Brokers desquels le service Malware Analysis extrait les données. Les fichiers de données suspects peuvent ainsi être marqués en vue de leur extraction. Ces fichiers sont du contenu marqué `malware analysis` qui sont disponibles via le système de gestion de contenu RSA Live.

Modules de note de malware

RSA NetWitness Platform Malware Analysis analyse et donne des scores aux sessions et fichiers intégrés à ces sessions selon quatre catégories d'évaluation : Réseau, Analyse statique, Communauté et Sandbox. Chaque catégorie comprend de nombreuses règles et vérifications individuelles qui sont utilisées pour calculer un score entre 1 et 100. Plus le score est élevé, plus la session est susceptible d'être malveillante et devrait faire l'objet d'une investigation de suivi plus approfondie.

Malware Analysis peut faciliter l'investigation sur l'historique des événements qui ont abouti à une alarme ou un incident réseau. Si vous savez qu'un certain type d'activité se produit sur votre réseau, vous pouvez sélectionner uniquement les rapports présentant un intérêt afin de passer en revue le contenu des collections de données. Vous pouvez également modifier le comportement de chaque catégorie d'évaluation en fonction de la catégorie ou du type de fichiers (Windows PE, PDF et Microsoft Office).

Une fois familiarisé avec les méthodes de navigation au sein des données, vous pouvez explorer les données de manière plus exhaustive via :

- La recherche de types spécifiques d'informations
- L'examen détaillé de contenu spécifique

Les scores des catégories Réseau, Analyse statique, Communauté et Sandbox font l'objet d'une maintenance et d'un reporting de manière indépendante. Lorsque les événements sont affichés en fonction des scores indépendants et qu'une catégorie détecte des malware, cela apparaît dans la section Analyse.

Réseau

La première catégorie examine chaque session de réseau principal afin de déterminer si la livraison des candidats malveillants était suspecte. Par exemple, le téléchargement d'un logiciel bénin depuis un site sécurisé et connu, à l'aide des ports et protocoles adéquats, est considéré comme moins suspect que le téléchargement d'un logiciel connu pour être malveillant, à partir d'un site de téléchargement douteux. Les facteurs d'échantillon utilisés pour l'évaluation de cet ensemble de critères peuvent comprendre des sessions qui :

- contiennent des informations sur la source de menace ;
- se connectent à des sites malveillants connus ;
- se connectent à des domaines/pays à haut risque (par exemple, un domaine .cc) ;
- utilisent des protocoles connus sur des ports non standard ;
- contiennent du JavaScript obscurci.

Analyse statique

La seconde catégorie analyse chaque fichier de la session à la recherche de signes s'obscurcissement afin de prédire la probabilité qu'un fichier se comporte de manière malveillante s'il est exécuté. Par exemple, un logiciel lié à des bibliothèques réseau est plus susceptible de présenter une activité réseau suspecte. Les facteurs d'échantillon utilisés pour l'évaluation de cet ensemble de critères peuvent comprendre :

- des fichiers qui s'avèrent chiffrés XOR ;
- des fichiers qui s'avèrent intégrés dans des formats autres que EXE (par exemple, un fichier PE intégré dans un format GIF) ;
- des fichiers liés à des bibliothèques d'importation à plus hauts risques ;
- des fichiers s'inspirant fortement du format PE.

Communauté

La troisième catégorie évalue la session et les fichiers basés sur les connaissances collectives de la communauté de la sécurité. Par exemple, l'évaluation peut se baser sur la réputation de fichiers dont l'empreinte et le hachage sont déjà connus par des fournisseurs respectés d'antivirus. L'évaluation des fichiers se base aussi sur la connaissance de la communauté de la sécurité sur le site d'origine du fichier.

L'évaluation de la communauté indique aussi si l'antivirus de votre réseau a signalé les fichiers comme malveillants. Elle n'indique pas si le produit antivirus local a pris des mesures pour protéger votre système.

Sandbox

La quatrième catégorie s'attache au comportement du logiciel en l'exécutant dans un environnement sandbox. Lors de l'exécution du logiciel pour analyser son comportement, le score est calculé en identifiant une activité malveillante connue. Par exemple, un logiciel qui se configure pour se lancer automatiquement à chaque redémarrage et établir des connexions IRC présentera un score plus élevé qu'un fichier sans comportement malveillant.

Lancer une procédure d'enquête Malware Analysis

Vous pouvez enquêter sur les données analysées, balisées et évaluées par Malware Analysis en tant que données présentant des indicateurs de compromission. Cela inclut tous les types d'analyses Malware Analysis : rappel continu, rappel à la demande et fichiers téléchargés à la demande. Le rappel continu doit être activé lorsque l'administrateur configure les paramètres de base du service Malware Analysis.

NetWitness Platform offre plusieurs méthodes pour lancer une procédure d'enquête Malware Analysis.

Le plus rapide : Lancement instantané à partir des dashlets Malware Analysis

La façon la plus rapide de commencer une procédure d'enquête Malware Analysis est d'effectuer un lancement instantané à partir du tableau de bord NetWitness Platform via l'un des dashlets Malware Analysis qui répertorient les événements ou les fichiers susceptibles de contenir des malware. Les dashlets sont décrits dans le cadre du contenu RSA NetWitness dans Dashlets. À partir de l'un de ces dashlets, vous pouvez accéder directement aux résultats d'analyse d'un événement spécifique répertorié en tant qu'événement devant faire l'objet d'une procédure d'enquête :

- Liste des principaux malwares fortement suspects
- Liste des principaux malwares de type Zero Day
- Dashlet Malware à forte probabilité d'indicateur de compromission et scores élevés

Rappel à la demande à partir d'une valeur méta dans la vue Naviguer

Pour lancer un rappel à la demande à partir d'une procédure d'enquête, cliquez avec le bouton droit de la souris sur une valeur méta dans la vue Naviguer, puis choisissez une option dans le menu contextuel. Une fois le rappel terminé, les données analysées sont disponibles pour Malware Analysis (reportez-vous à Lancer une analyse Malware Analysis à partir de la vue Naviguer).

Enquêter sur un service RSA spécifique

Vous pouvez également commencer une procédure d'enquête Malware Analysis basée sur un service dans Enquêter > vue Malware Analysis. Pour toute procédure d'enquête Malware Analysis basée sur un service, ce dernier doit être spécifié dans Enquêter > vue Malware Analysis:Inve

1. Investigate ouvre la vue Malware Analysis avec le service par défaut spécifié par l'utilisateur sélectionné.
2. Si aucun service par défaut n'est spécifié, une boîte de dialogue vous permet de sélectionner le service Malware Analysis devant faire l'objet d'une procédure d'enquête.
3. Lorsqu'un service est sélectionné dans la vue Malware Analysis, la vue Récapitulatif des événements correspondante, et analyse en continu les données du service s'ouvre.

Cette rubrique fournit des instructions sur toutes les méthodes de lancement d'une procédure d'enquête Malware Analysis.

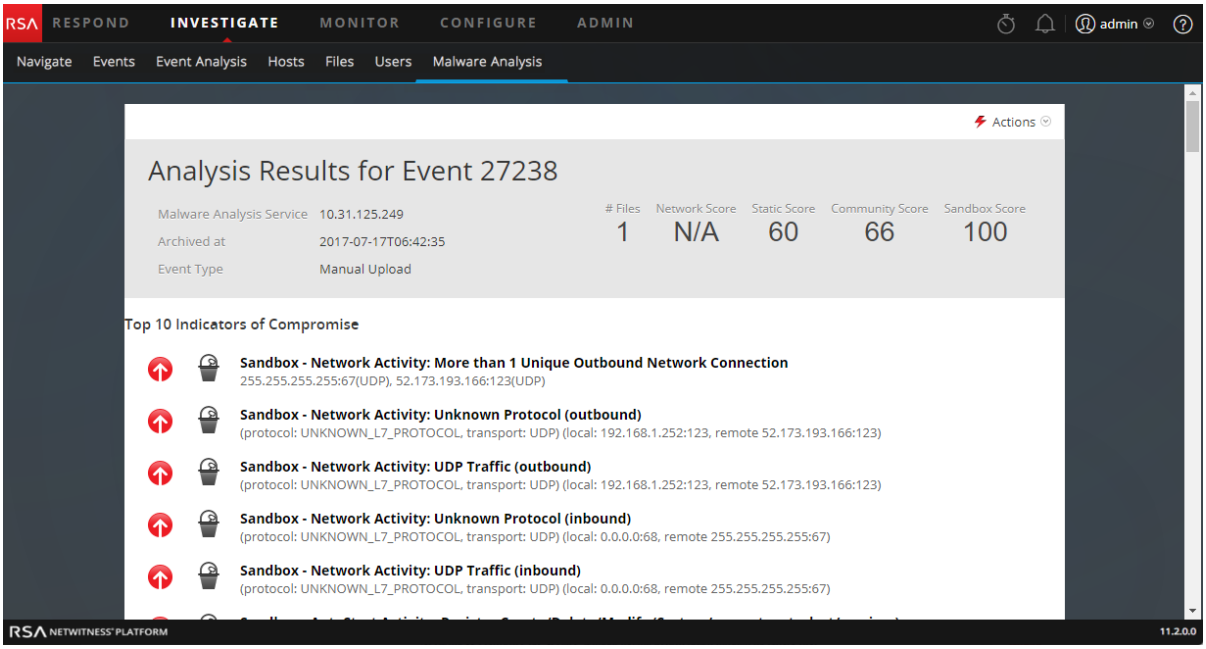
Lancer une procédure d'enquête sur les malware à partir d'un dashlet Malware Analysis

Il existe une condition préalable à respecter pour cette procédure : l'un des dashlets suivants doit être visible dans le tableau de bord NetWitness Platform ou dans la vue Malware Analysis. De plus, il doit comporter des événements ou des fichiers répertoriés. Si vous ne voyez pas de dashlets, ajoutez-les et configurez-les.

- Liste des principaux malwares fortement suspects
- Liste des principaux malwares de type Zero Day
- Dashlet Malware à forte probabilité d'indicateur de compromission et scores élevés

Pour lancer une procédure d'enquête sur les malware à partir d'un dashlet Malware Analysis :

1. Connectez-vous à NetWitness Platform et recherchez l'un des dashlets ci-dessus dans la vue Surveiller ou dans la vue Malware Analysis
2. Dans le dashlet, double-cliquez sur un événement ou un fichier pour obtenir une analyse plus approfondie. Une analyse détaillée de l'événement dans la liste d'événements, ou l'événement auquel est associé le fichier dans la liste de fichiers, s'affiche dans la vue Malware Analysis.



Pour en savoir plus sur la configuration des dashlets Malware Analysis dans le tableau de bord Surveiller, reportez-vous à « Dashlets » dans le *Guide de mise en route de NetWitness Platform*.

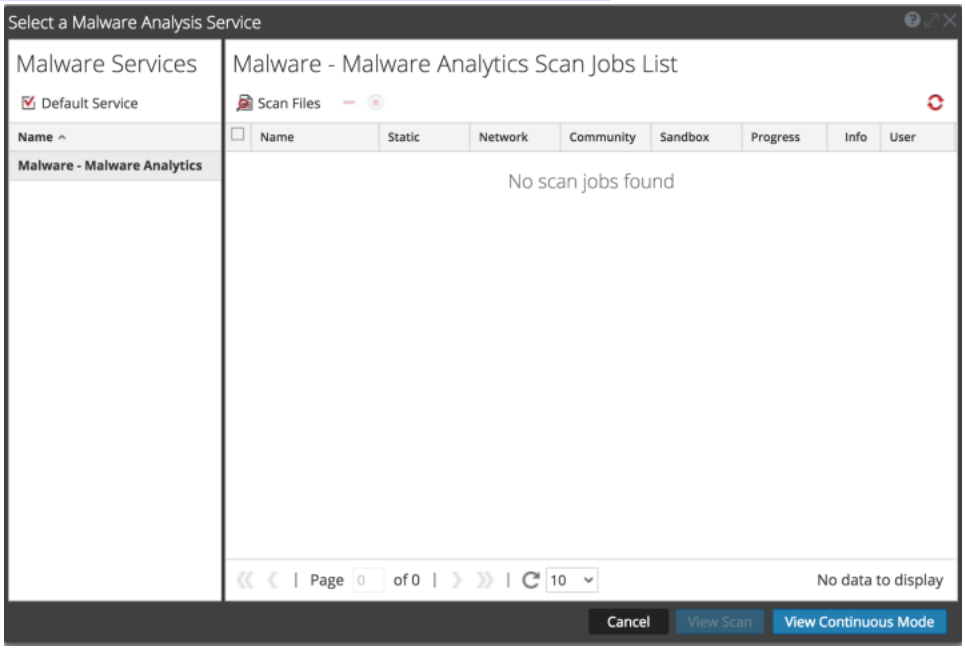
Pour en savoir plus sur les façons dont vous pouvez configurer et filtrer les informations dans les dashlets de la vue Malware Analysis, reportez-vous à la section Filtrer les données de dashlet dans la vue Récapitulatif des événements.

Pour en savoir plus sur les actions que vous pouvez effectuer dans les résultats d'analyse, reportez-vous à la section Afficher l'analyse Malware Analysis détaillée d'un événement.

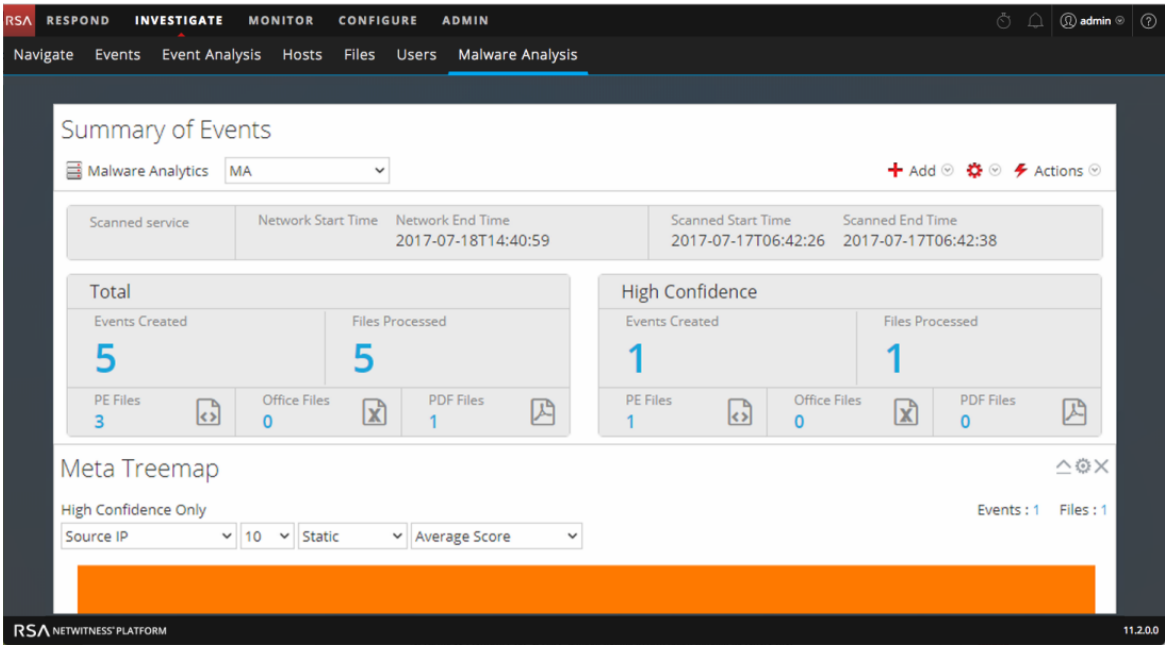
Lancer une procédure d'enquête Malware Analysis (aucun service par défaut)

Pour commencer une procédure d'enquête sans service par défaut :

1. Accédez à **ENQUÊTER** > **Malware Analysis**.
   La boîte de dialogue Sélectionner un service Malware Analysis s'affiche en présentant les hôtes et services Malware Analysis disponibles pour l'utilisateur actuel dans le volet de gauche, et les tâches d'analyse disponibles dans le volet de droite. Ce volet des tâches d'analyse contient les mêmes colonnes que le dashlet Liste de tâches d'analyse des malware dans le tableau de bord Unified. En outre, il comporte une barre d'outils et des options d'affichage, qui sont décrites dans la Boîte de dialogue Sélectionner un service Malware Analysis.



2. Dans la liste des hôtes Malware Analysis, sélectionnez un hôte pour afficher la liste des tâches d'analyse correspondantes dans le volet de droite. Ces tâches sont créées lors de l'analyse d'un événement ou d'un fichier (reportez-vous aux sections Télécharger des fichiers pour l'analyse Malware Analysis et Lancer une analyse Malware Analysis à partir de la vue Naviguer).
3. Pour débuter une analyse, procédez de l'une des façons suivantes :
   a. Sélectionnez une analyse, puis cliquez sur **Afficher l'analyse**.
   b. Cliquez sur **Afficher le mode continu**.
      La vue Récapitulatif des événements correspondant à l'analyse sélectionnée s'affiche avec les dashlets par défaut ouverts. Chaque utilisateur peut ajouter, modifier et supprimer des dashlets par défaut, qui persistent à travers différentes procédures d'enquête. Les utilisateurs peuvent également restaurer les dashlets par défaut, comme indiqué dans la section Filtrer les données de dashlet dans la vue Récapitulatif des événements.

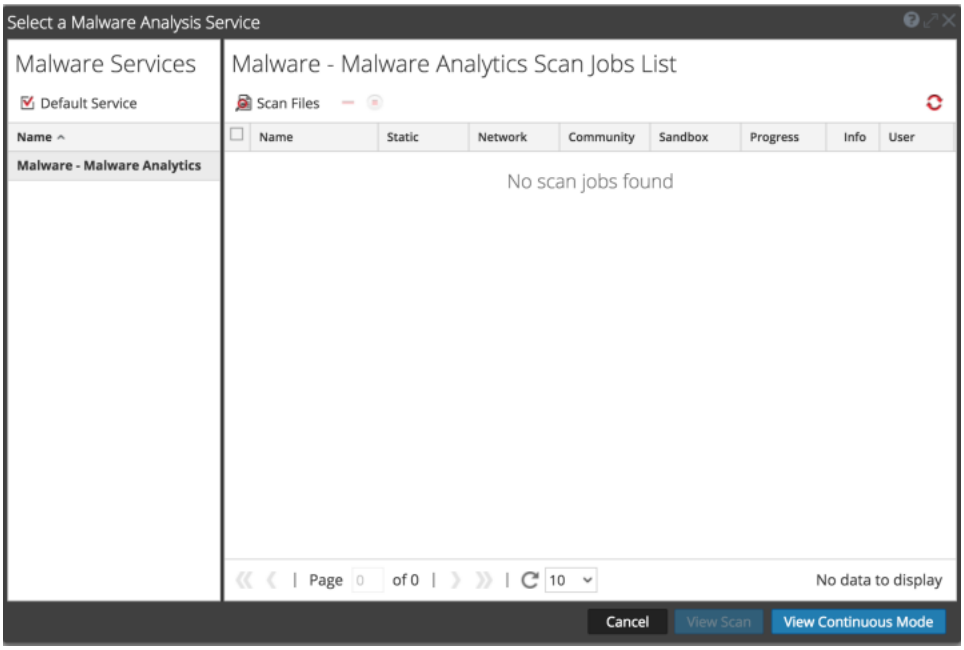


Définir ou effacer le service par défaut

Vous pouvez définir ou effacer le service par défaut dans la boîte de dialogue Sélectionner un service Malware Analysis.

Pour définir un service par défaut :

1. Cliquez sur le nom du service dans la barre d'outils de la vue Récapitulatif des événements.
   La boîte de dialogue Sélectionner un service Malware Analysis s'affiche.



2. Sélectionnez un service dans la liste des services Malware disponibles, puis cliquez sur Default Service.

   Le service devient la valeur par défaut (indiquée par ☑ devant le nom d'hôte).

3. Pour effacer le service par défaut, sélectionnez-le dans la grille, puis cliquez sur Default Service.
   Aucun service par défaut n'est défini.

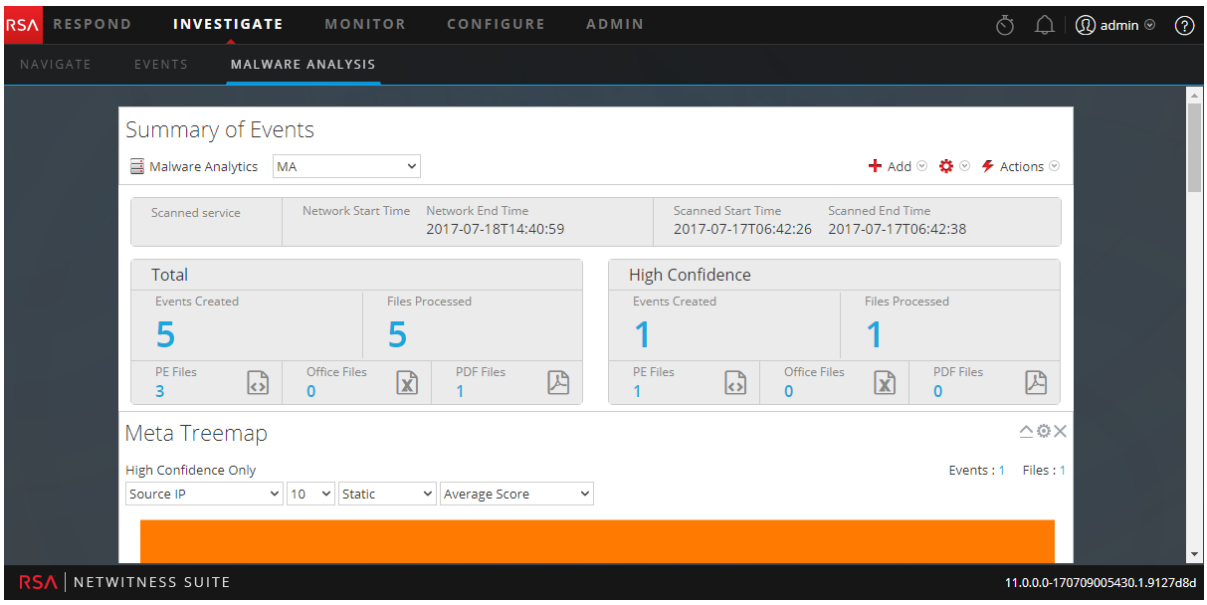
Télécharger et analyser des fichiers

Un analyste de malware possédant l'autorisation `Initiate Malware Analysis Scan` peut charger des fichiers à analyser à l'aide de l'option Analyser des fichiers dans la boîte de dialogue Sélectionner un service Malware Analysis (voir Télécharger des fichiers pour l'analyse Malware Analysis. Un administrateur peut télécharger des fichiers de capture de paquets pour Malware Analysis dans la vue Système de services comme décrit dans « Télécharger le fichier de capture de paquets » dans le *Guide de configuration de Decoder et Log Decoder*.

Commencer une procédure d'enquête (service par défaut spécifié)

Pour commencer une procédure d'enquête avec un service par défaut :

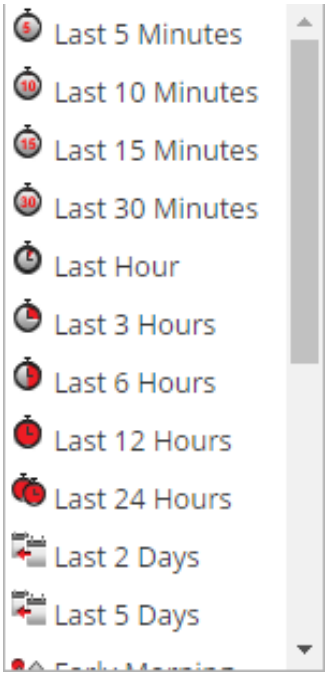
1. Accédez à **ENQUÊTER** > **Malware Analysis**.
   La vue Récapitulatif des événements correspondant à l'analyse continue du service sélectionné s'affiche avec les dashlets par défaut ouverts. Chaque utilisateur peut ajouter, modifier et supprimer des dashlets par défaut, qui persistent à travers différentes procédures d'enquête. Les utilisateurs peuvent également restaurer les dashlets par défaut, comme indiqué dans la section Filtrer les données de dashlet dans la vue Récapitulatif des événements.



Appliquer un filtre basé sur des paramètres de durée aux résultats

Vous pouvez appliquer un filtre de seuil pour actualiser les résultats des dashlets choisis.

1. Pour sélectionner une autre période, sélectionnez **Mode continu** ou une autre analyse dans la barre d'outils.
   Le Récapitulatif des événements de malware pour l'analyse sélectionnée s'affiche.
2. Pour sélectionner une nouvelle période d'analyse, cliquez sur la liste de sélection de période, dans la barre d'outils. Les périodes disponibles sont les suivantes : 5 dernières minutes, 10 dernières minutes, 15 dernières minutes, 30 dernières minutes, Dernière heure, 3 dernières heures, 6 dernières heures, 12 dernières heures, 24 dernières heures, 2 derniers jours, 5 derniers jours, Début de matinée, Matin, Après-midi, Soir, Toute la journée, Hier, Cette semaine, La semaine dernière ou Personnalisé.



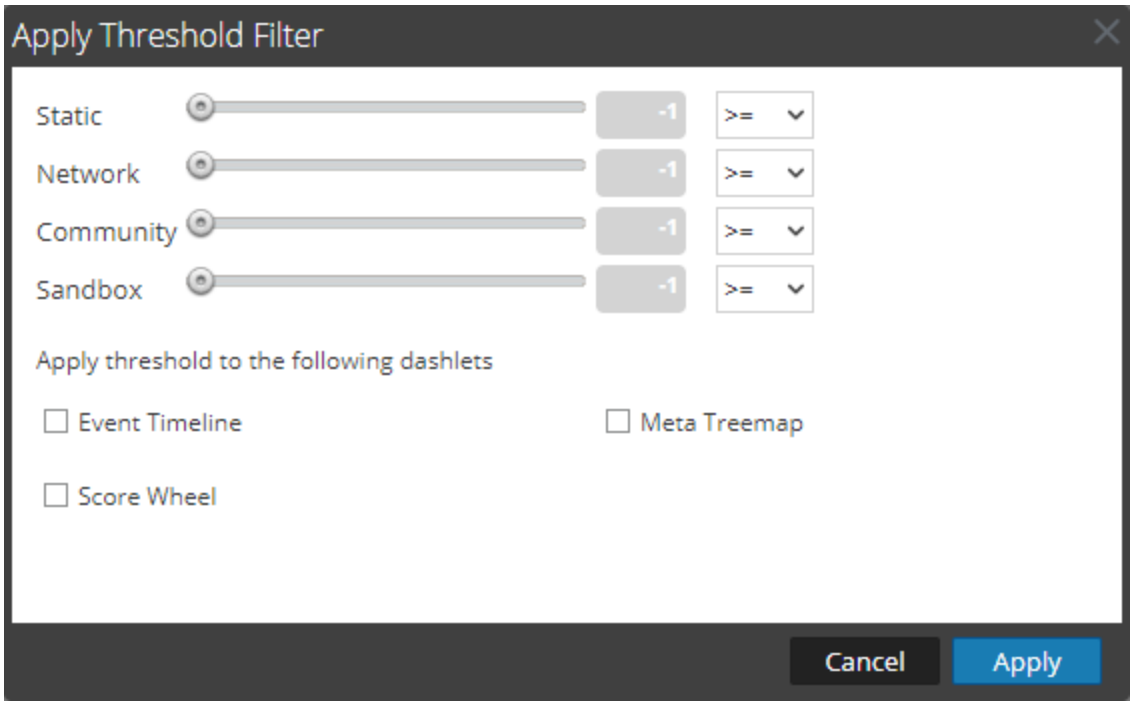
   Les résultats sont mis à jour immédiatement.
3. Pour actualiser une analyse en mode continu avec de nouvelles données, cliquez sur .

Appliquer un filtre de seuil aux résultats d'analyse en mode continu

Vous pouvez appliquer un nouveau filtre de seuil à une instance des dashlets Malware à forte probabilité d'indicateur de compromission et scores élevés, Compartimentage des méta, Roue des scores et Chronologie d'événements.

Pour personnaliser les scores appliqués à l'analyse, dans la barre d'outils, procédez comme suit :

1. Sélectionnez > **Appliquer le filtre de seuil.**
   La boîte de dialogue Appliquer le filtre de seuil s'affiche.



2. Pour limiter les événements affichés à ceux dont le score est supérieur à une certaine valeur, procédez comme suit :
   a. Faites glisser le curseur sur les barres de défilement des modules Static, Network, Community et Sandbox.
   b. Pour sélectionner les dashlets où les seuils s'appliquent, activez les cases à cocher appropriées.
   c. Cliquez sur **Appliquer**.

Supprimer ou resoumettre une analyse à la demande avec de nouveaux paramètres de contournement

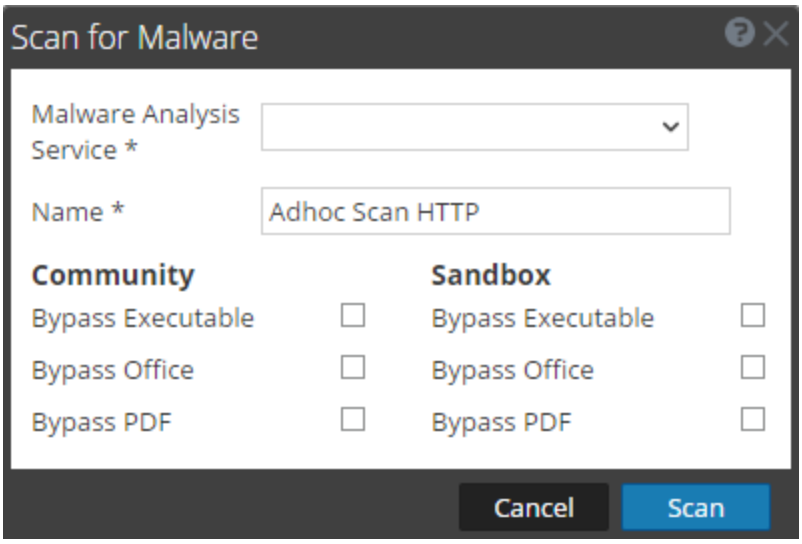
Vous pouvez supprimer ou resoumettre une analyse à la demande avec d'autres paramètres de contournement que ceux spécifiés dans la vue Configuration des services pour un service Malware Analysis.

Pour supprimer une analyse lorsque vous visualisez une analyse à la demande, procédez comme suit :

1. Sélectionnez **Actions** > **Supprimer l'analyse**.
   Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'analyse.
2. Cliquez sur **Yes**.
   L'analyse sélectionnée est supprimée.

Pour appliquer d'autres paramètres de contournement à l'analyse actuelle :

1. Sélectionnez **Actions > Renvoyer l'analyse**.
   La boîte de dialogue Analyser les malwares s'affiche.



2. Sélectionnez les paramètres de contournement à utiliser pour la nouvelle analyse, puis cliquez sur **Analyser**.
   Malware Analysis réinitialise le cache et resoumet le fichier pour une nouvelle analyse. Les tâches d'analyse sont ajoutées à la file d'attente des tâches.
3. Une fois la tâche terminée, faites défiler l'affichage vers la gauche et sélectionnez **Afficher**.
   Le Récapitulatif des événements de malware pour l'analyse sélectionnée s'affiche.

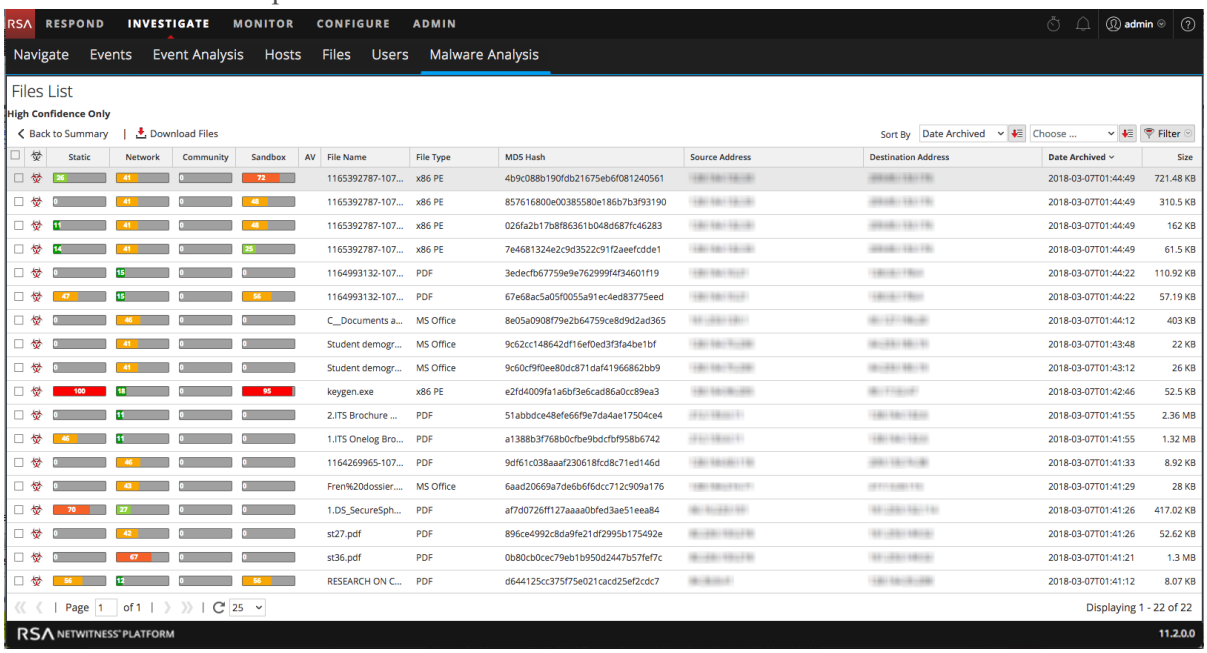
Afficher la liste des fichiers

Vous pouvez afficher la liste des fichiers d'un événement à partir de la vue Malware Analysis Récapitulatif des événements et à partir de chacun des graphiques de visualisation : Chronologie d'événements, Répartition des méta, Compartimentage des méta et Roue des scores.

Pour afficher la liste des fichiers, procédez de l'une des façons suivantes :

- Dans la vue Récapitulatif des événements, cliquez sur le nombre de fichiers dans la ligne **Total** ou la ligne **Forte probabilité** sous **Fichiers traités**, **Fichiers PE**, **Fichiers Office** ou **Fichiers PDF**. La liste de fichiers s'affiche.
- Dans un dashlet de visualisation, cliquez sur le numéro situé en regard du champ **Fichiers**, dans le coin supérieur droit du dashlet.

La liste de fichiers du point d'extraction sélectionné s'affiche.



Dans la liste de fichiers, vous pouvez rechercher un fichier par son nom ou son hachage de fichier MD5. Vous pouvez également trier la liste à l'aide de deux critères, dans l'ordre croissant ou décroissant, et vous pouvez télécharger les fichiers comme indiqué dans la section Examiner les fichiers et événements d'analyse dans le formulaire de liste.

Pour revenir à la vue Récapitulatif des événements, cliquez sur **Retour au récapitulatif**.

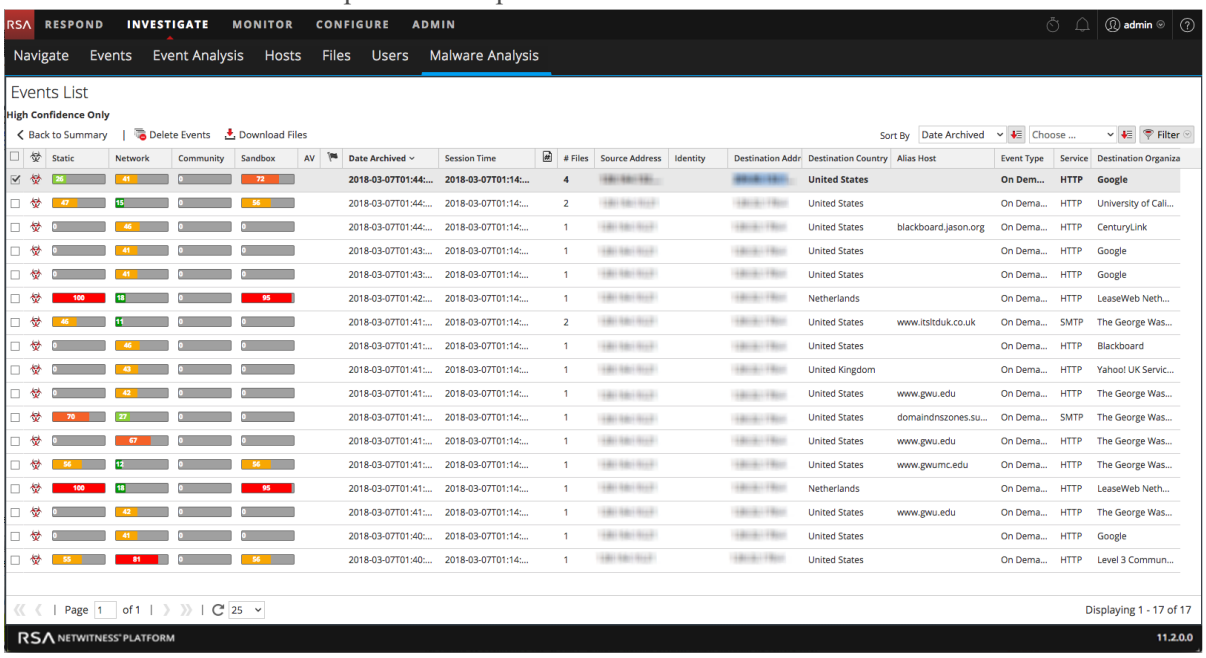
Afficher la liste d'événements

Dans la vue Malware Analysis Récapitulatif des événements et à partir de chacun des graphiques de visualisation (Chronologie d'événements, Répartition des méta, Compartimentage des méta et Roue des scores), vous pouvez sélectionner des événements à afficher dans la grille des événements.

Pour afficher la liste d'événements, procédez de l'une des façons suivantes :

- Dans la vue Récapitulatif des événements, cliquez sur le nombre d'événements créés dans la ligne **Total** ou la ligne **Forte probabilité**. La liste Événements s'affiche.
- Dans un dashlet de visualisation, cliquez sur le numéro situé en regard du champ Événements, dans le coin supérieur droit du dashlet.

La liste d'événements correspondant à la période sélectionnée s'affiche.



Implémenter du contenu YARA personnalisé

En plus des indicateurs de compromission intégrés, Malware Analysis prend également en charge les indicateurs de compromission écrits en langage YARA. YARA est un langage de règles qui permet aux chercheurs spécialisés d'identifier et de classer les échantillons de malware. RSA rend disponible les indicateurs de compromission intégrés YARA dans RSA Live ; ceux-ci sont automatiquement téléchargés et activés sur les hôtes souscrits.

Les clients ayant des compétences et des connaissances avancées peuvent ajouter des capacités de détection à RSA Malware Analysis en créant des règles YARA et en les publiant dans RSA Live ou en les plaçant dans un dossier surveillé pour que l'hôte les utilise.

Comme l'environnement des programmes malveillants et des menaces évolue, il est important de passer en revue et d'examiner les règles personnalisées existantes. Des mises à jour sont souvent nécessaires pour intégrer de nouvelles méthodes de détection. RSA met également à jour les règles YARA dans Live de temps à autre. Pour recevoir des mises à jour, vous pouvez vous abonner à RSA Blog et RSA Live à l'adresse http://blogs.rsa.com/feed.

Ce document fournit des informations pour aider les clients à implémenter des règles YARA personnalisées dans Malware Analysis.

Conditions préalables

L'hôte sur lequel vous ajoutez des règles personnalisées doit être configuré pour prendre en charge la création de règles YARA comme décrit dans la rubrique « Activer le contenu YARA personnalisé » du *Guide de configuration de Malware Analysis*.

Version et ressources YARA

RSA Malware Analysis est fourni avec YARA version 3.7 (rév :167). Pour connaître la version exacte, vous pouvez exécuter `yara -v` sur l'hôte Malware Analysis comme indiqué dans cet exemple :

```
[root@TESTHOST yara] # yara -v
 yara 3.7 (rev:167)
```

Clés métas dans les règles YARA

Malware Analysis est conforme à d'autres sources de règles YARA. Il consomme également des clés métas supplémentaires qui sont spécifiques à Malware Analysis. Chaque règle YARA est équivalente à un indicateur de compromission dans Malware Analysis. L'exemple ci-dessous illustre les définitions méta dans une règle :

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Clé méta	Description
iocName	(Obligatoire) Il s'agit du nom que MA utilise comme nom de règle. Il est spécifique à Malware Analysis et est nécessaire pour ajouter la règle à la liste d'indicateurs de compromission.
fileType	Définit le type de fichiers. Les valeurs possibles sont les suivantes : WINDOWS_PE, MS_OFFICE et PDF. Si aucune valeur n'est spécifiée, celle par défaut est WINDOWS_PE.
score	Si la règle YARA est déclenchée, cette valeur est ajoutée au score statique. S'il n'est pas spécifié, la valeur par défaut est 10.
ceiling	Il s'agit du montant maximal qui est ajouté aux scores statiques quand une règle est déclenchée plusieurs fois en une seule session. Par exemple, chaque fois qu'une règle est déclenchée, 20 points sont ajoutés au score statique, et si vous ne voulez pas ajouter plus de 40 points lorsque la règle est déclenchée plus de deux fois, vous pouvez spécifier un plafond de 40. S'il n'est pas spécifié, la valeur par défaut est 100.
highConfidence	Cette valeur définit la balise de Forte probabilité, qui est configurée sur les indicateurs intégrés de compromission quand des indicateurs signalent avec forte probabilité la présence de programmes malveillants. Si cette valeur n'est pas spécifiée, la valeur de fichier par défaut est false.

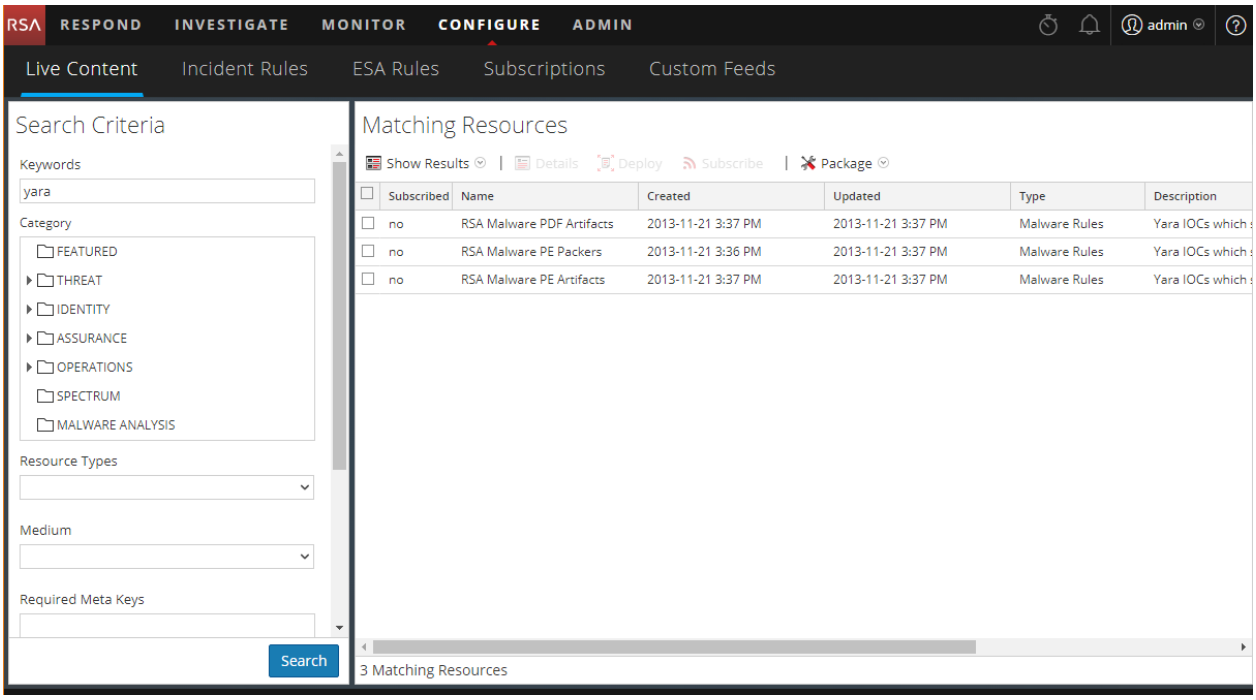
Remarque : Reportez-vous à l'URL suivante pour les ressources YARA : https://code.google.com/p/yara-project/downloads/list. NetWitness Platform utilise YARA 3.7 et non pas YARA 2.0.

Contenu YARA

RSA Live contient 3 ensembles de règles Yara :

- Packers PE
- Artefacts PDF
- Artefacts PE

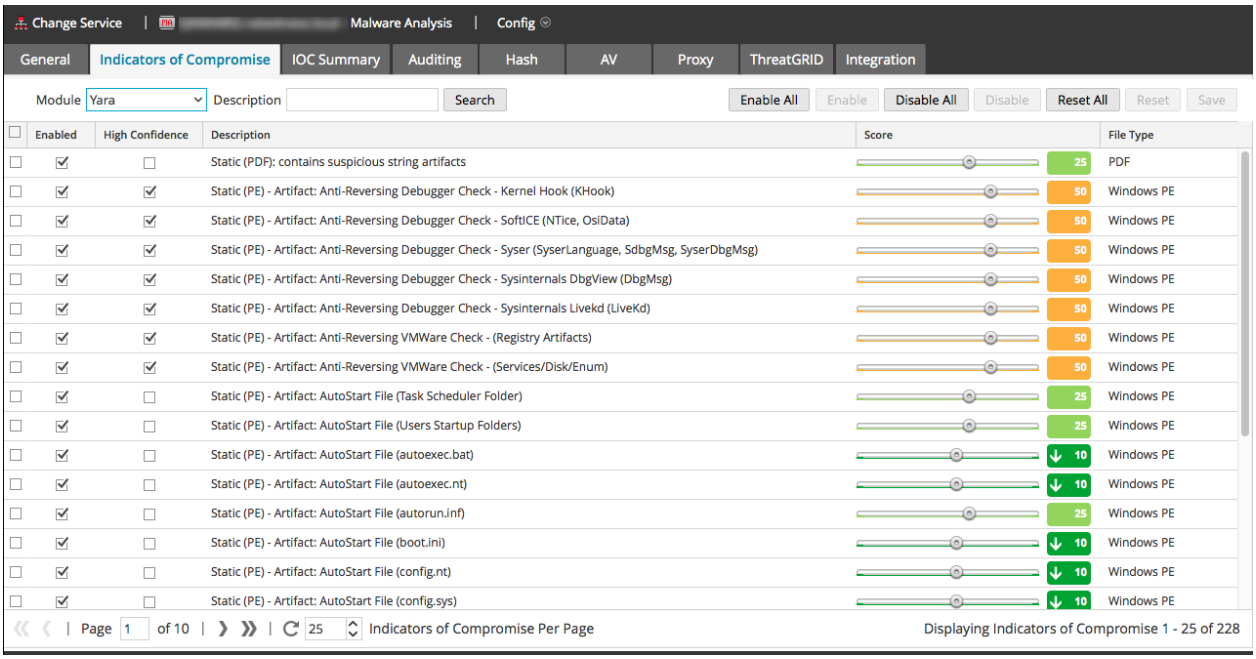
La figure suivante illustre le contenu YARA disponible en tant que règles YARA dans NetWitness Platform Live.



Sur l'hôte Malware Analysis, les règles YARA résident dans `/var/lib/netwitness/malware-analytics-server/spectrum/yara`, comme illustré dans l'exemple ci-dessous.

```
[root@TESTHOST yara]# pwd
 /var/lib/netwitness/malware-analytics-server/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_packers.yara
```

Les règles individuelles sont répertoriées comme indicateurs de compromission dans la vue Configuration du service Malware Analysis > onglet Indicateurs de compromission. Pour les visualiser, utilisez le module Yara comme filtre. Vous pouvez ajuster la configuration d'une règle individuelle de la même manière que vous configurez d'autres indicateurs de compromission.



Ajouter des règles YARA personnalisées

Pour introduire des règles YARA personnalisées à partir d'autres sources :

1. Afin de garantir que les règles YARA suivent le format et la syntaxe corrects, utilisez la commande YARA pour compiler la règle YARA comme le montre l'exemple suivant. Si la règle YARA compile sans erreur, sa syntaxe est correcte.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
   [root@TESTHOST yara]#
   ```

2. Assurez-vous que les règles personnalisées ne reproduisent pas de règles YARA existantes issues de RSA ou d'autres sources. Toutes les règles YARA sont dans `/var/lib/netwitness/malware-analytics-server/spectrum/yara`

3. Assurez-vous que les clés métas prises en charge par RSA sont incluses afin d'organiser les règles YARA en tant que partie des indicateurs de compromission configurables, puis nommez le fichier avec l'extension yara (<filename>.yara). Pour une meilleure organisation, assurez-vous que la méta `iocName` est incluse dans la section méta comme illustré dans l'exemple suivant.

   Exemple :

   ```
   rule HEX_EXAMPLE
   {
       meta:
           author = "RSA"
           info = "HEX Detection"
          iocName = "Hex Example"
        strings:
           $hex1 = { E2 34 A1 C8 23 FB }
           $wide_string = "Ausov" wide ascii
   ```

```
        condition:
           $hex1 or $wide_string
}
```

4. Lorsque vous êtes prêt, placez le fichier YARA personnalisé dans le dossier que le service Malware Analysis surveille :
   `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
   Le fichier est utilisé en une minute.
   Ensuite, NetWitness Platform déplace le fichier vers le dossier `processed`, et la nouvelle règle est ajoutée à la vue Configuration du service Malware Analysis > onglet Indicateurs de compromission.

Examiner les fichiers et événements d'analyse dans le formulaire de liste

Lors de l'affichage du récapitulatif des événements dans une analyse Malware Analysis, vous pouvez cliquer sur un nombre de fichiers ou un nombre d'événements pour afficher la liste des fichiers ou la liste des événements pour analyse (voir Lancer une procédure d'enquête Malware Analysis). Dans la liste des fichiers et la liste des événements, vous pouvez rechercher un fichier par nom de fichier ou hachage de fichier MD5, trier la liste en utilisant deux critères avec l'ordre croissant/décroissant, et télécharger des fichiers. Lorsque vous trouvez un événement ou un fichier intéressant dans la liste des événements ou la liste des fichiers, vous pouvez consulter de nombreux détails sur l'événement dans la vue Détails de l'événement.

Pour chaque événement de la liste des événements, NetWitness Platform fournit les informations suivantes :

- Indiqué en tant qu'événement Forte probabilité, qui est considéré comme contenant probablement des Indicateurs de compromission.
- Le score numérique de chaque module de note : Statique, Réseau, Communauté et Sandbox
- Notes de fournisseur antivirus.
- Balise Influencé par une règle personnalisée.
- Date d'archivage de l'événement.
- Durée de la session.
- Filtre de hachage MD5.
- Nombre de fichiers dans l'événement.
- Adresse IP source de l'événement.
- Identité.
- Adresse IP de destination.
- Pays de destination.
- Nom de l'hôte de l'alias.
- Type d'événement, par exemple, Réseau.
- Service utilisé par l'événement.
- Organisation de destination

Pour chaque fichier de la liste des fichiers, NetWitness Platform fournit les informations suivantes :

- Indiqué en tant qu'événement Forte probabilité, qui est considéré comme contenant probablement des Indicateurs de compromission.
- Le score numérique de chaque module de note : Statique, Réseau, Communauté et Sandbox
- Notes de fournisseur antivirus.

- Nom du fichier.
- Type de fichier.
- Filtre de hachage MD5.
- Adresse IP source de l'événement contenant le fichier.
- Adresse IP de destination.
- Date de l'événement contenant le fichier archivé.
- Taille du fichier.

Trier la liste des fichiers ou la liste des événements

Vous pouvez trier la liste des fichiers ou la liste des événements en fonction du nom de la colonne par ordre croissant ou décroissant. Vous pouvez choisir une ou deux colonnes.

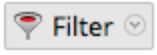
Pour trier la liste :

1. Dans la première liste déroulante **Trier par**, choisissez un nom de colonne et le sens du tri :  par ordre décroissant ou  par ordre croissant.
2. (Facultatif) Dans la deuxième liste déroulante **Trier par**, choisissez un nom de colonne, le sens du tri,  par ordre décroissant ou  par ordre croissant.
   Les titres des colonnes reflètent l'ordre de tri sélectionné.

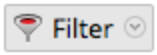
Filtrer la liste en fonction du nom de fichier ou du hachage de fichier MD5

Vous pouvez filtrer la liste des fichiers et la liste des événements par nom de fichier ou hachage de fichier. Avec cette fonctionnalité, vous pouvez spécifier un sous-ensemble limité des données d'origine sur la base des critères de recherche.

Remarque : Lorsque vous effectuez une recherche, la recherche porte sur l'analyse en cours d'affichage et non sur toutes les analyses.

1. Cliquez sur 

   .
   La boîte de dialogue Filtrer s'affiche.
2. Saisissez une valeur dans les champs **Nom de fichier** ou **Hachage MD5**, puis cliquez sur **Filtrer**. Les champs Nom de fichier et Hachage ne tiennent pas compte de la casse. Les caractères génériques ou expressions régulières ne sont pas pris en charge. Le filtre est basé sur des correspondances exactes. Vous pouvez sélectionner un nom de fichier ou de hachage dans la liste des fichiers ou la liste des événements, puis le copier-coller dans la boîte de dialogue.
3. Cliquez sur **Filtrer**.
   Malware Analysis filtre la liste pour n'afficher que les fichiers ou événements avec le hachage sélectionné

4. Pour revenir à la liste non filtrée, cliquez sur 

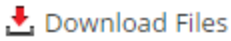
. Lorsque la boîte de dialogue Filtrer s'affiche, cliquez sur **Réinitialiser**.

Télécharger les fichiers à partir de la liste des fichiers

NetWitness Platform vous permet de sélectionner et de télécharger des fichiers à partir de la liste des fichiers ou de la liste des événements.

Attention : Soyez prudent(e) lors du téléchargement des fichiers à partir de Malware Analysis car certains fichiers peuvent contenir un code malveillant. Le téléchargement de fichier est une autorisation spécifique qui peut être configurée, reportez-vous à la section « Définir les rôles et autorisations pour les analystes » dans le *Guide de configuration de Malware Analysis* pour plus de détails.

Pour télécharger les fichiers à partir de la liste des fichiers ou la liste des événements :

1. Dans **Liste de fichiers** ou **Liste d'événements**, activez la case à cocher en regard d'une ou de plusieurs lignes.
2. Dans la barre d'outils, sélectionnez 

.
   La boîte de dialogue Téléchargement de fichier de malware s'affiche.
3. Exécutez l'une des opérations suivantes :
   a. Si vous décidez de ne pas télécharger le fichier, cliquez sur **Annuler**.
   b. Si vous souhaitez télécharger le fichier, cliquez sur le bouton **Télécharger**.
      Le ou les fichiers sélectionnés sont téléchargés dans une archive zip avec le nom `Malware_Files.zip`

Supprimer des événements de l'analyse

Dans la liste des événements, sélectionnez un ou plusieurs événements et supprimez-les de l'analyse. Cela est utile pour la suppression des événements qui ne sont pas intéressants.

Pour supprimer un événement de l'analyse en cours de consultation :

1. Dans **Liste d'événements**, sélectionnez un ou plusieurs événements.
2. Dans la barre d'outils, cliquez sur 

.
   NetWitness Platform vous demande de confirmer que vous souhaitez supprimer les événements.
3. Dans la fenêtre de confirmation, cliquez sur **Oui**.
   Les événements sélectionnés sont supprimés.

Revenir à la vue Récapitulatif des événements

Pour quitter la liste des fichiers ou la liste des événements pour revenir à la vue Récapitulatif des événements, cliquez sur **Retour au récapitulatif**.

Ouvrir l'analyse détaillée d'un événement

Lorsque vous examinez les événements ou les fichiers dans la liste des fichiers ou des événements, vous pouvez double-cliquer sur un événement ou un fichier pour ouvrir une analyse détaillée de l'événement de la liste d'événements ou de l'événement auquel le fichier de la liste des fichiers est associé (voir Afficher l'analyse Malware Analysis détaillée d'un événement).

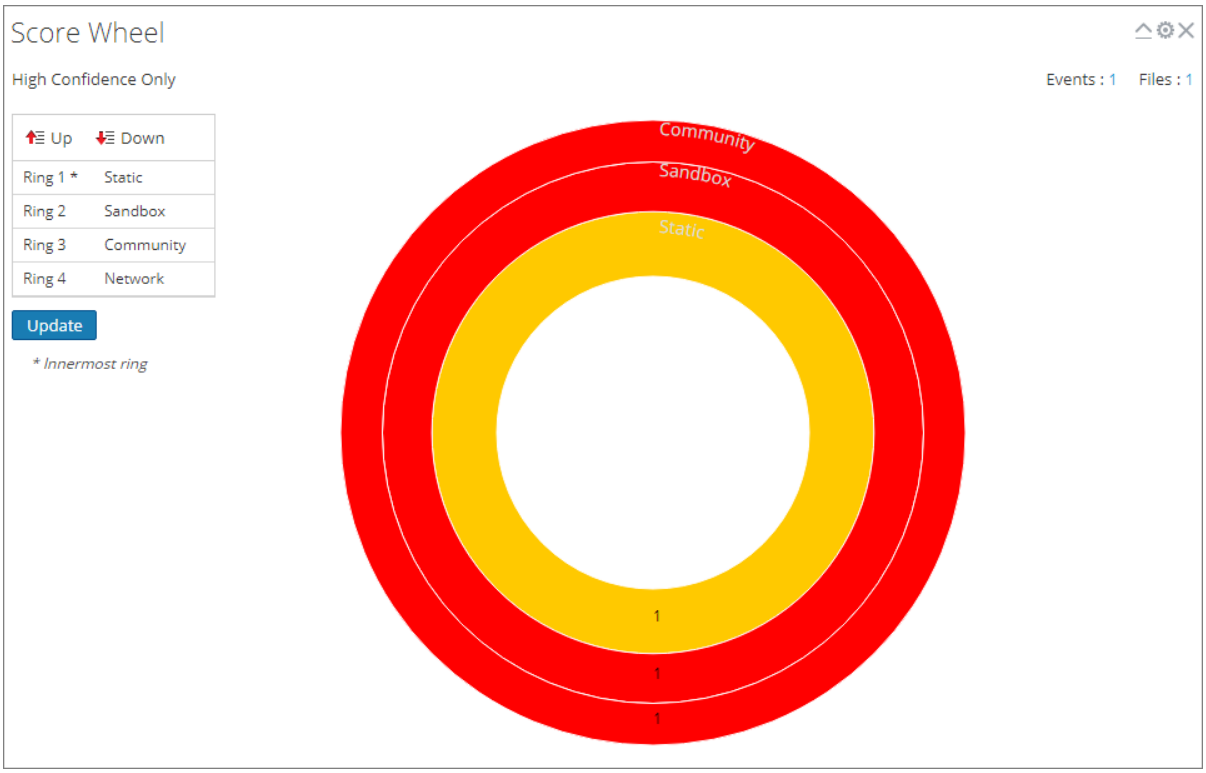
Filtrer les données de dashlet dans la vue Récapitulatif des événements

Le récapitulatif des événements fournit un résumé de l'analyse à l'étude avec des dashlets sélectionnables. Le récapitulatif des événements est fixe, mais les analystes peuvent configurer chaque dashlet pour filtrer les informations et effectuer une recherche verticale dans les données.

Le reste de cette rubrique fournit des instructions sur la gestion et la configuration de dashlets.

Configurer le dashlet Roue des scores

La roue des scores est une visualisation de haut niveau des sessions analysées qui ont obtenu des scores haut, moyen ou faible dans chacune des catégories de notation : Statique, Réseau, Communauté et Sandbox La roue des scores est un moyen rapide d'effectuer une recherche verticale dans des sessions pour les passer en revue. Chaque anneau représente une catégorie de notation différente pour que vous puissiez comparer visuellement les résultats par catégorie.

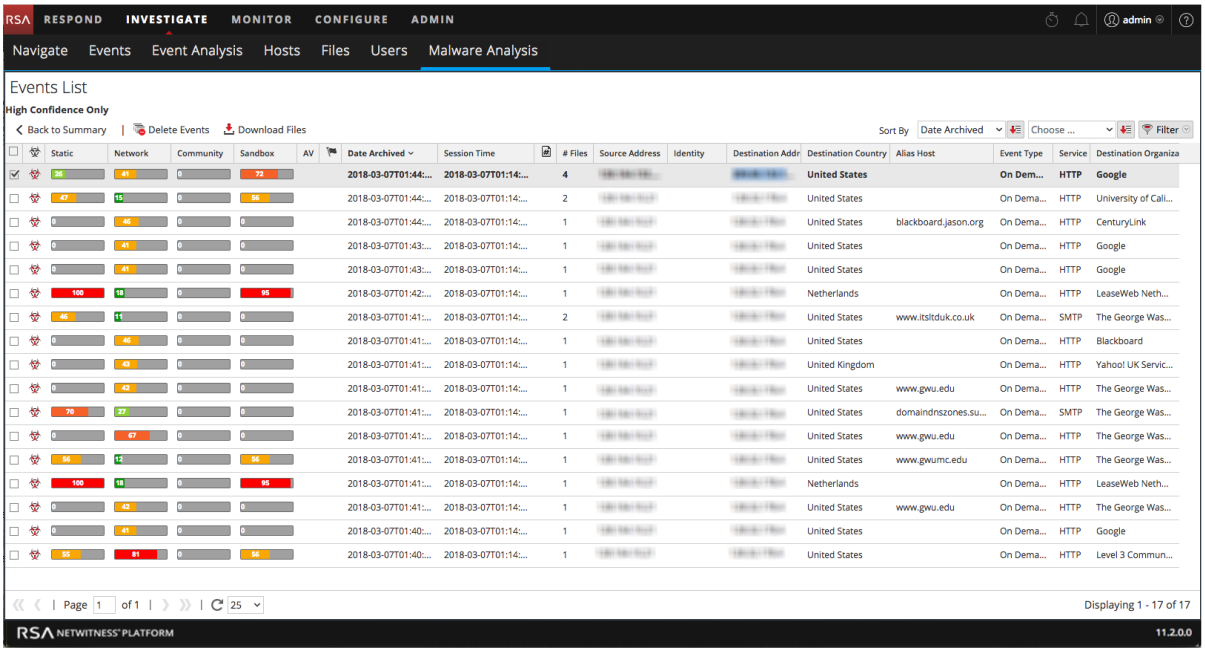


Vous pouvez modifier l'ordre des anneaux pour mettre en évidence des indicateurs de compromission qui ont été marqués dans une catégorie, mais pas dans une autre. La comparaison des mêmes résultats dans un ordre d'anneaux différent offre une visibilité sur les vulnérabilités supplémentaires dans une session. Vous pouvez effectuer une recherche verticale dans des sessions d'intérêt. Les exemples suivants montrent deux exemples d'utilisation possibles.

Exemple de candidat de type Zero Day.

Cet exemple indique comment réaliser une recherche verticale dans des sessions que la Communauté n'a pas signalé comme malveillantes, mais qui ont été repérées par toutes les autres catégories de notation. La liste des sessions met en évidence les candidats Zero Day.

1. Configurez les bagues Roue des scores dans l'ordre suivant :
   Communauté (le plus à l'intérieur) > **Statique** > **Réseau** > **Sandbox** (le plus à l'extérieur)
2. Cliquez sur la tranche rouge dans l'anneau situé le plus à l'extérieur (Sandbox) qui s'aligne avec une tranche verte sur l'anneau le plus à l'intérieur (Communauté) : vert (le plus à l'intérieur) -> **Statique** : rouge -> **Réseau** : rouge -> **Sandbox** : rouge (le plus à l'extérieur).



Exemple de sessions malveillantes

Cet exemple montre comment réaliser une recherche verticale dans des sessions dans lesquelles toutes les catégories de notation identifient la liste des sessions comme malveillantes, en indiquant que Malware Analysis a confiance qu'il s'agisse de programmes malveillants.

1. Configurez les bagues Roue des scores dans l'ordre suivant :
   Communauté (le plus à l'intérieur) > **Statique** > **Réseau** > **Sandbox** (le plus à l'extérieur)
2. Cliquez sur la tranche rouge dans l'anneau situé le plus à l'extérieur (Sandbox) qui s'aligne avec une tranche rouge sur l'anneau le plus à l'intérieur (Communauté) : rouge (le plus à l'intérieur) -> Statique : rouge -> Réseau : rouge -> Sandbox : rouge (le plus à l'extérieur).

Réorganiser la séquence d'anneaux par module de notation

Dans la roue des scores, vous pouvez réorganiser la séquence d'anneaux par module de notation. Dans un premier temps, la séquence d'anneaux de l'intérieur vers l'extérieur est statique, réseau, communauté et Sandbox.

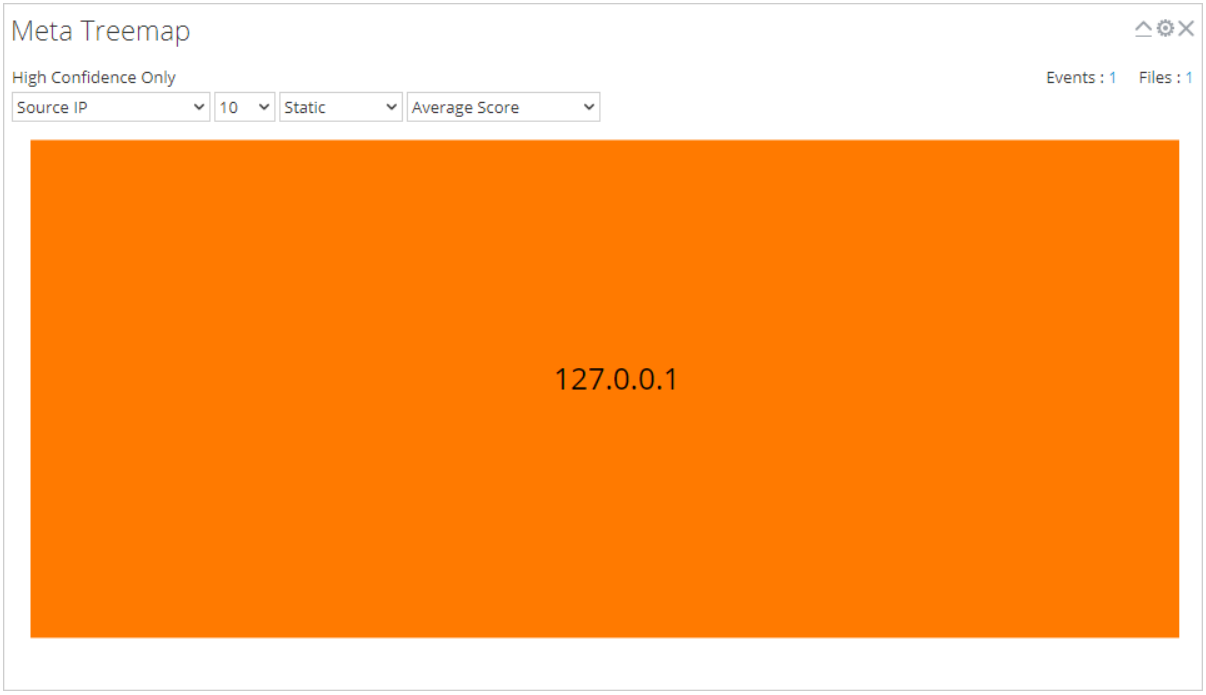
Pour modifier la séquence des anneaux :

1. Exécutez l'une des opérations suivantes :
   a. Cliquez et faites glisser chaque module de notation vers le haut ou vers le bas.
   b. Sélectionnez chaque module de notation et utilisez les boutons Haut et Bas pour les déplacer.

2. Lorsque la séquence d'anneaux correspond à ce que vous souhaitez, cliquez sur le bouton **Mettre à jour**.
   La roue des scores est actualisée avec la nouvelle séquence.

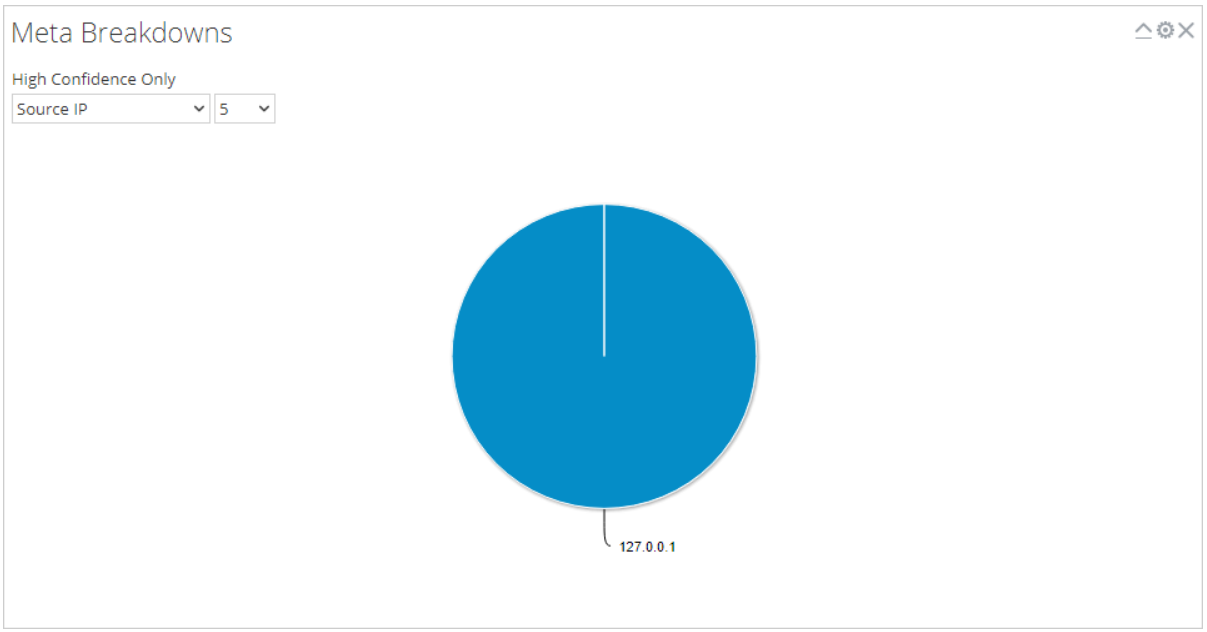
Configurer le dashlet de Compartimentage des méta

Dans le graphique de compartimentage des méta, vous pouvez visualiser et filtrer les répartitions des méta, par type, nombre et analyse. Utilisez les trois listes de sélection pour définir le filtre et le graphique de compartimentage des méta se met à jour immédiatement.



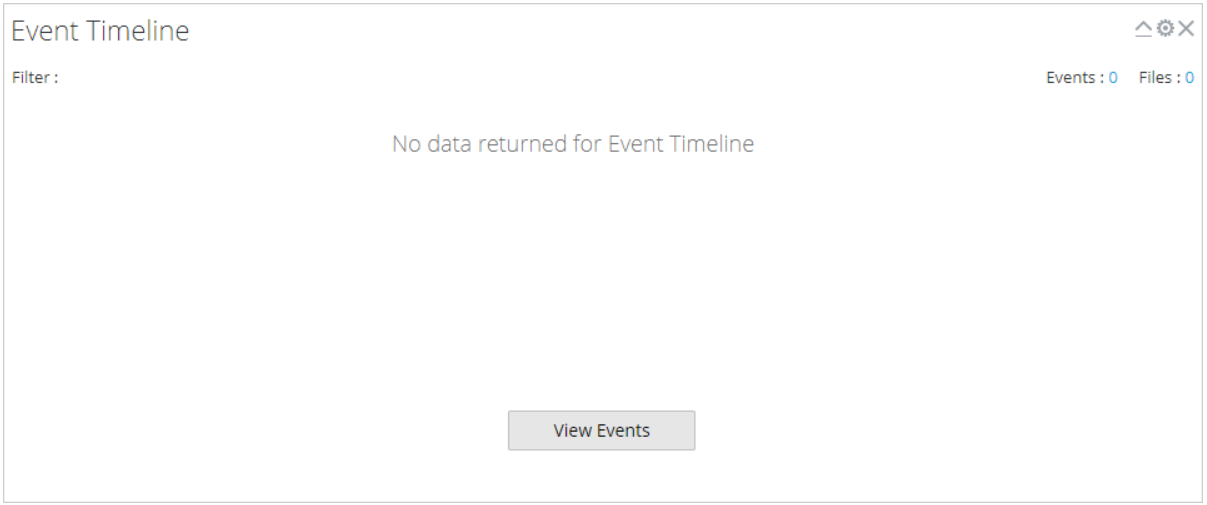
Configurer le dashlet de Répartition des méta

Le dashlet de répartition des méta est une visualisation des valeurs d'une clé méta spécifique dans un graphique circulaire. Dans le graphique de répartition des méta, vous pouvez filtrer les répartitions des méta par type et nombre. Utilisez les deux listes de sélection pour définir le filtre et le graphique de répartition des méta se met à jour immédiatement.



Configurer le dashlet Chronologie d'événements

Le dashlet de la Chronologie d'événements est une visualisation des événements le long d'une chronologie. Aucun filtre supplémentaire n'est disponible pour la chronologie des événements.

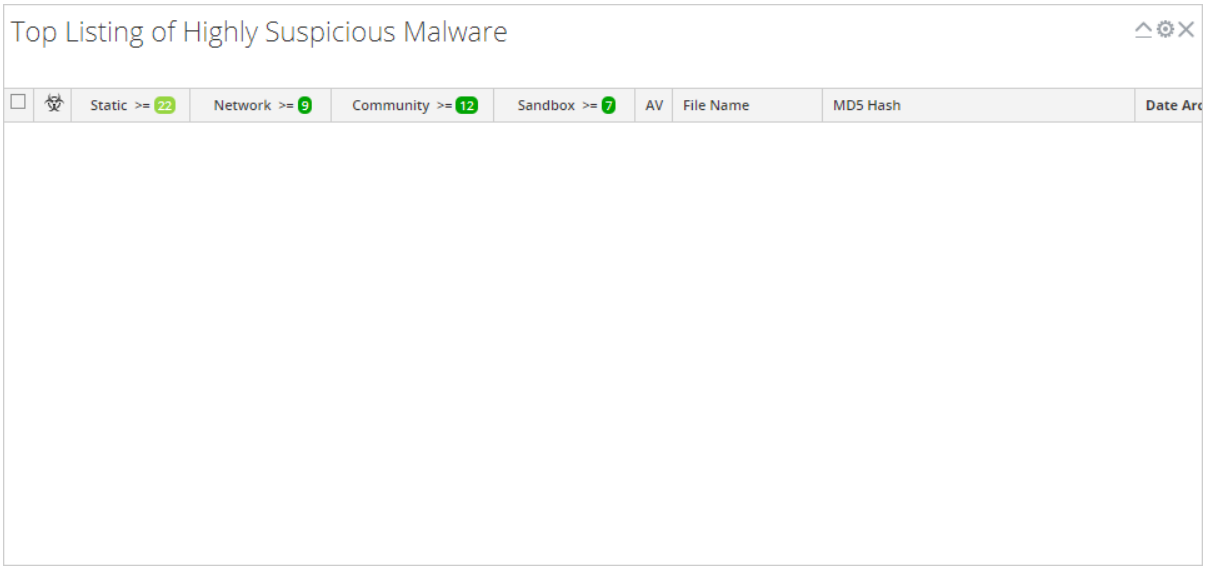


Ouvrir Tous les événements dans la liste des événements

À partir de la chronologie des événements, vous pouvez ouvrir la liste complète des événements dans la liste des événements. Pour ce faire, cliquez sur **Visualiser les événements**. Cette option n'est pas identique au fait de cliquer sur le nombre à côté des événements, ce qui est similaire pour tous les graphiques de visualisation. Elle ouvre le point de recherche verticale en cours dans la liste des événements.

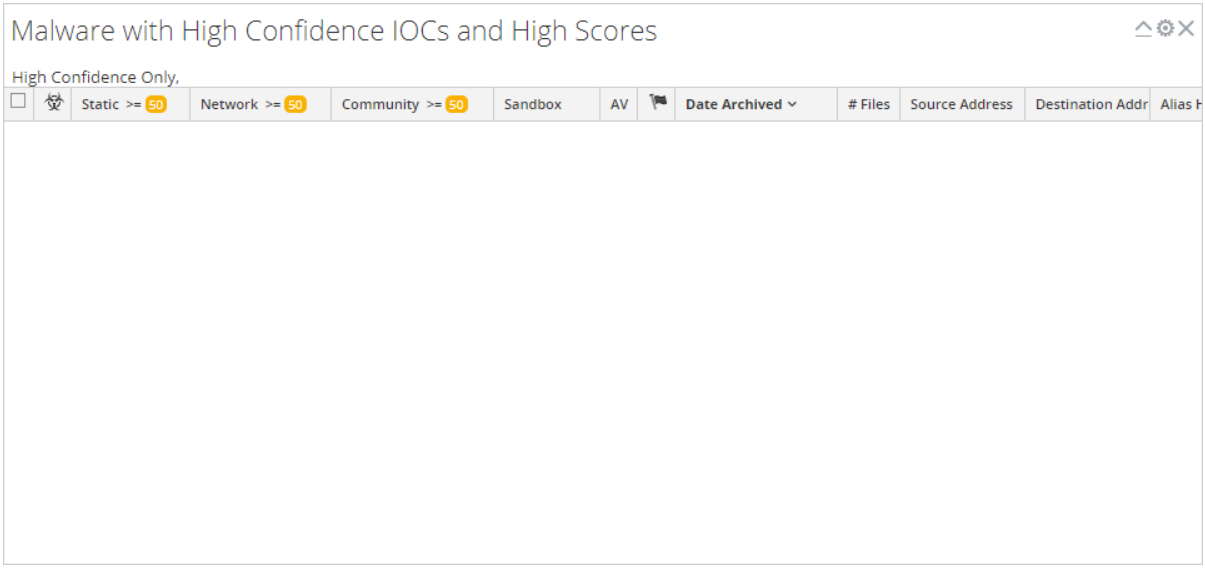
Configurer le dashlet Liste des principaux malwares fortement suspects

Le dashlet Liste des principaux malwares fortement suspects présente les 10 événements les plus suspects dans la liste des événements ou dans la liste des fichiers. Ce dashlet est également disponible dans le tableau de bord Surveiller, et les options de configuration sont décrites dans le cadre du contenu RSA NetWitness dans Dashlets.



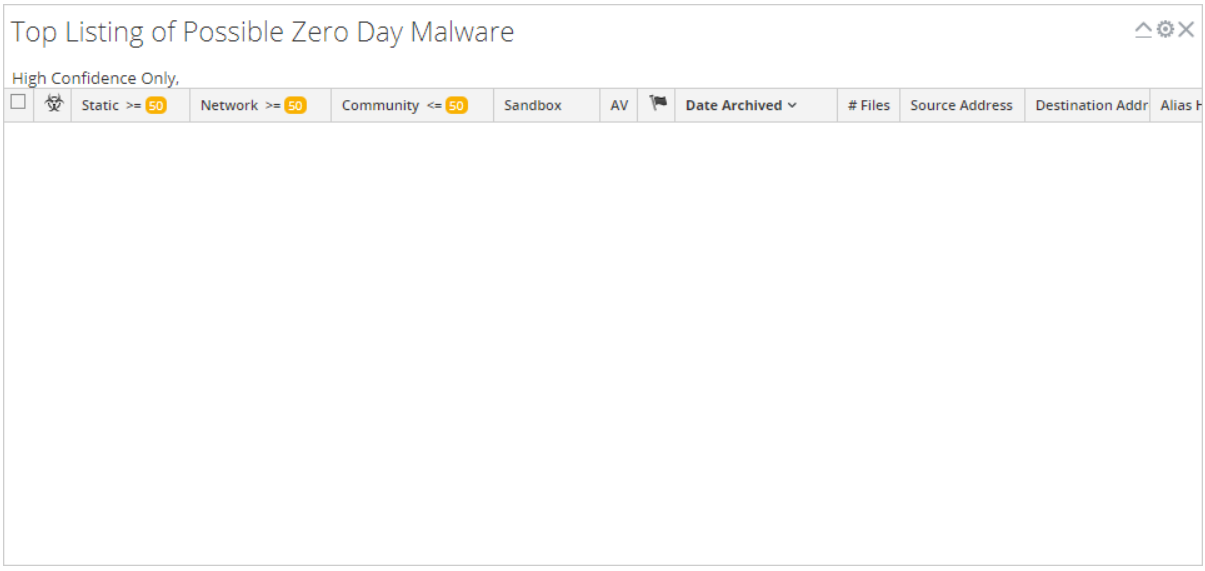
Configure le Dashlet Malware à forte probabilité d'indicateur de compromission et scores élevés

Le dashlet Malware à forte probabilité d'indicateur de compromission et scores élevés présente des indicateurs de compromission qui ont à la fois des scores élevés et une forte probabilité que les événements sont susceptibles de contenir des programmes malveillants. Le dashlet est également disponible dans le tableau de bord Unified, et les options de configuration sont décrites dans le cadre du contenu RSA NetWitness dans Dashlets.



Configurer le Dashlet Liste des principaux malwares de type Zero Day

Le dashlet Liste des principaux malwares de type Zero Day présente les événements de type Zero Day potentiels dans la liste des événements ou la liste des fichiers. Le dashlet est également disponible dans le tableau de bord Unified, et les options de configuration sont décrites dans le cadre du contenu RSA NetWitness dans Dashlets.



Télécharger des fichiers pour l'analyse Malware Analysis

Il existe deux méthodes permettant aux analystes de télécharger des fichiers pour l'analyse Malware Analysis.

Un analyste de malware possédant l'autorisation de Lancer une analyse Malware Analysis peut télécharger des fichiers à analyser à l'aide de l'option Analyser des fichiers dans la boîte de dialogue Sélectionner un service Malware Analysis.

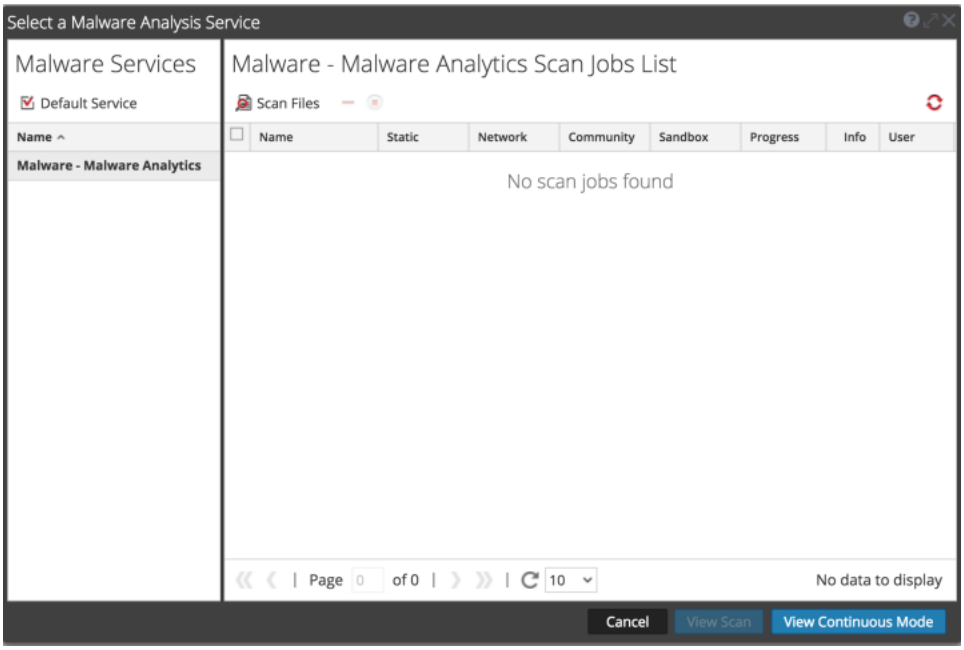
Il est également possible de télécharger un fichier à analyser à l'aide d'un partage de fichiers observé.

Télécharger des fichiers manuellement

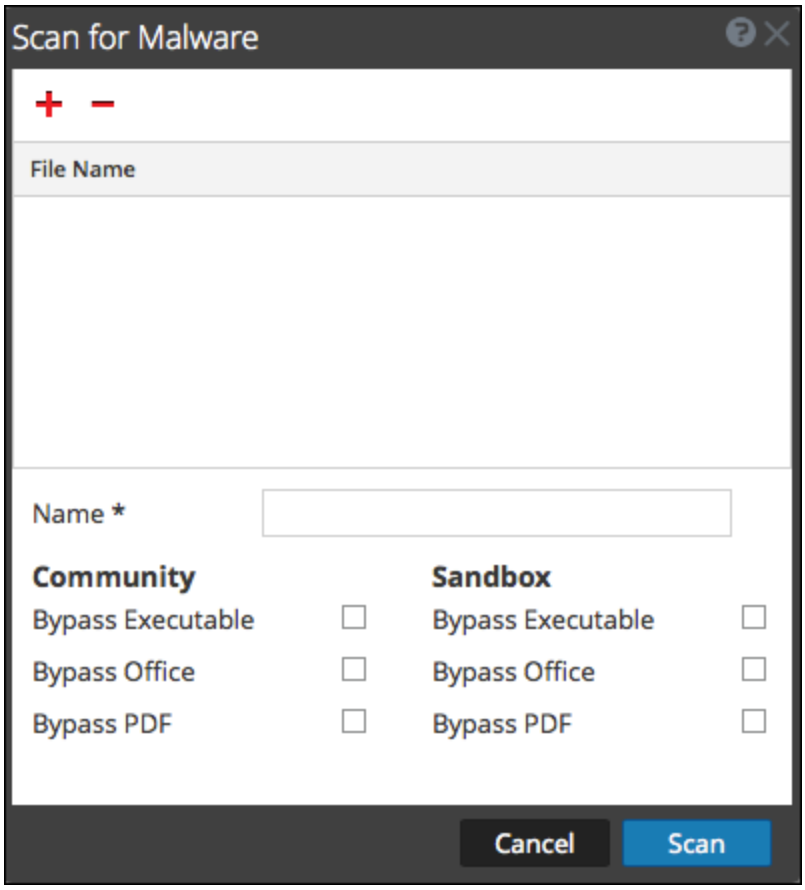
Cette rubrique fournit les instructions permettant de lancer l'analyse à la demande d'un fichier téléchargé. Lorsque vous téléchargez un fichier en vue d'une analyse, NetWitness Platform lance la tâche de téléchargement, puis l'ajoute à la file d'attente. Une fois la tâche terminée, vous pouvez consulter l'analyse dans Malware Analysis.

Pour télécharger un fichier à analyser :

1. Accédez à **ENQUÊTER > Malware Analysis**.
   La boîte de dialogue Sélectionner un service Malware Analysis s'affiche. Les hôtes et services Malware Analysis disponibles pour l'utilisateur actif y sont indiqués dans le panneau de gauche.



2. Cliquez sur **Afficher l'analyse**.
   La boîte de dialogue Analyser les malwares s'affiche.



3. Cliquez sur + pour afficher le système de fichiers et sélectionner les fichiers à télécharger.
4. Sélectionnez un ou plusieurs fichiers dans la liste, puis cliquez sur **Ouvrir**.
   Les noms de ces fichiers sont ajoutés. Avant de traiter un fichier, Malware Analysis utilise des caractères d'échappement dans le nom de ce fichier. Le nombre maximal de caractères du nom de fichier après la séquence d'échappement est 200. Si le nom de fichier contient plus de 200 caractères, Malware Analysis tronque les caractères du nom de fichier et affiche le nom de fichier tronqué dans l'interface utilisateur NetWitness Platform.
5. Continuez à ajouter et à supprimer des fichiers jusqu'à ce que vous ayez établi la liste des fichiers à télécharger.
6. Attribuez un nom à l'analyse, puis sélectionnez les types de fichiers à ignorer. Cette possibilité est particulièrement utile pour les archives zip qui contiennent différents types de fichier et écrase les paramètres de contournement par défaut.
7. Cliquez sur **Analyser**.
   La tâche d'analyse est envoyée et NetWitness Platform affiche un message de confirmation indiquant que l'envoi a été effectué correctement. La demande d'analyse est ajoutée au dashlet Liste des tâches d'analyse. Les paramètres de contournement de cette boîte de dialogue remplacent les paramètres par défaut dans les paramètres de configuration Malware Analysis de base.

8. La tâche est ajoutée à la liste des tâches d'analyse dans la boîte de dialogue Sélectionner un service Malware Analysis et dans le dashlet Liste des tâches d'analyse du tableau de bord unifié.
9. Lorsque l'analyse est terminée, double-cliquez dessus pour la consulter.
   Le Récapitulatif des événements de malware pour l'analyse sélectionnée s'affiche.

Télécharger des fichiers à partir d'un dossier de suivi

Pour télécharger des fichiers à partir d'un dossier surveillé, vous pouvez déposer des fichiers dans un partage de fichiers surveillé pour Malware Analysis. Les analystes peuvent partager les règles YARA, les fichiers de hachage et les archives au format zip infectées avec Malware Analysis.

Malware Analysis surveille un partage de fichiers et utilise automatiquement les fichiers placés dans des dossiers spécifiques dans le partage de fichiers. Cette fonctionnalité est utile pour :

- Importer en bloc des fichiers de hachage à partir de `/var/lib/rsamalware/spectrum/hashWatch`.
- Ajouter des règles personnalisées YARA à la liste des indicateurs de compromission (IOC) sur l'hôte à partir de `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`.
- Créer des tâches d'analyse à la demande à partir d'une archive zip de fichiers zip infectés, à partir de `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Les analystes doivent préparer les fichiers pour l'utilisation en fonction des exigences ; l'extension du fichier doit être correcte et le fichier doit être copié dans le dossier surveillé approprié dans le partage de fichiers.

Importer une liste de hachage

Pour importer une liste de hachage à partir d'un répertoire surveillé, la liste de hachage doit être au format spécifié et doit être triée selon md5. Vous pouvez faire glisser un fichier au format spécifié dans un dossier (`/var/lib/rsamalware/spectrum/hashWatch`) stocké sur l'hôte Malware Analysis pour qu'il soit importé automatiquement dans la base de données de hachage locale. La procédure à utiliser est décrite dans « Configurer le filtre de hachage » dans le *Guide de Configuration de Malware Analysis*.

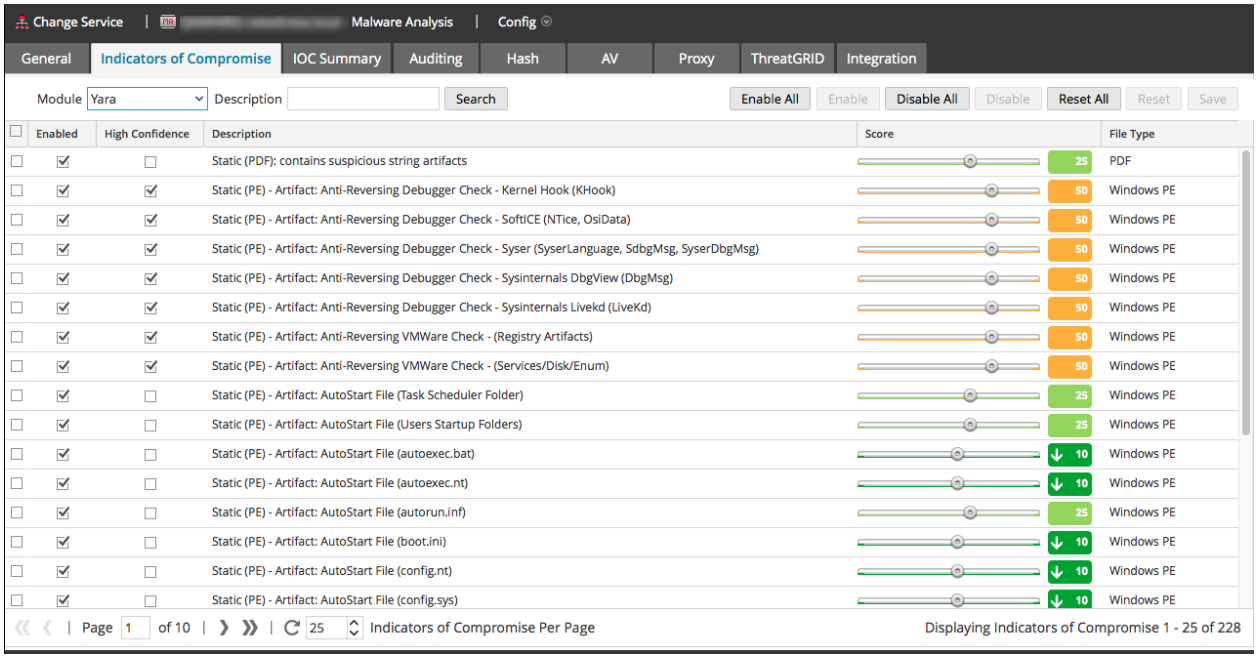
Pour importer une liste de hachage à l'aide de la méthode du dossier surveillé :

1. Dans le répertoire **`/var/lib/rsamalware/spectrum/hashWatch`** , copiez les listes de hachage que vous souhaitez importer.
   NetWitness Platform Malware Analysis surveille automatiquement ce dossier et traite les fichiers qui y sont placés.
   a. Malware Analysis ajoute chaque hachage trouvé dans les listes de hachage au filtre de hachage.
   b. En cas d'erreurs de traitement, la consignation s'effectue dans :
      `/var/lib/rsamalware/spectrum/hashWatch/error`
   c. Les fichiers traités sont catalogués
      ici : `/var/lib/rsamalware/spectrum/hashWatch/processed`
   d. Les fichiers traités ne sont pas supprimés du répertoire hashWatch.
2. Après l'importation du hachage en bloc, l'administrateur système peut utiliser cronjob pour nettoyer les fichiers traités précédemment.

Importer les règles YARA vers la liste IOC

Les clients ayant des compétences et des connaissances avancées peuvent ajouter des capacités de détection à RSA Malware Analysis en créant des règles YARA et en les publiant dans RSA Live ou en les plaçant dans un dossier surveillé pour que l'hôte les utilise. La rubrique Implémenter du contenu YARA personnaliséfournit des informations détaillées sur les conditions requises pour utiliser un contenu YARA personnalisé et créer des règles.

Lorsque les règles sont prêtes, placez les fichiers YARA personnalisés dans le dossier que le service Malware Analysis surveille :
`/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
Le fichier est utilisé en une minute.
Ensuite, NetWitness Platform déplace le fichier vers le dossier `processed`, et la nouvelle règle est ajoutée à la vue Configuration du service Malware Analysis > onglet Indicateurs de compromission.



Importer des fichiers dans la liste des tâches d'analyse

Lorsque vous obtenez des exemples issus des solutions de sécurité du périmètre et que vous souhaitez effectuer une analyse approfondie des fichiers, vous pouvez compresser les fichiers et protéger l'archive avec `infected`, avant de l'ajouter au dossier surveillé pour que Malware Analysis la traite. Cette archive compressée est prête à être placée dans le dossier surveillé:
`/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Remarque : La taille maximale de l'archive est de 100 Mo.

Pour analyser les fichiers zip infectés protégés par mot de passe, Malware Analysis utilise les archives dans un dossier surveillé et crée une tâche à la demande qui est ajoutée à la liste des tâches d'analyse.

1. En étant connecté en tant qu'administrateur, compressez les fichiers à traiter avec le mot de passe `infected` et placez le fichier zip dans
   `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   En une ou deux minutes, Malware Analysis utilise l'archive et crée une tâche à la demande dans la

liste des tâches d'analyse. Le nom de la tâche d'analyse correspond au nom du fichier, l'utilisateur correspond à **partage de fichiers** et le type d'événement correspond à 1. L'archive est déplacée dans `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`

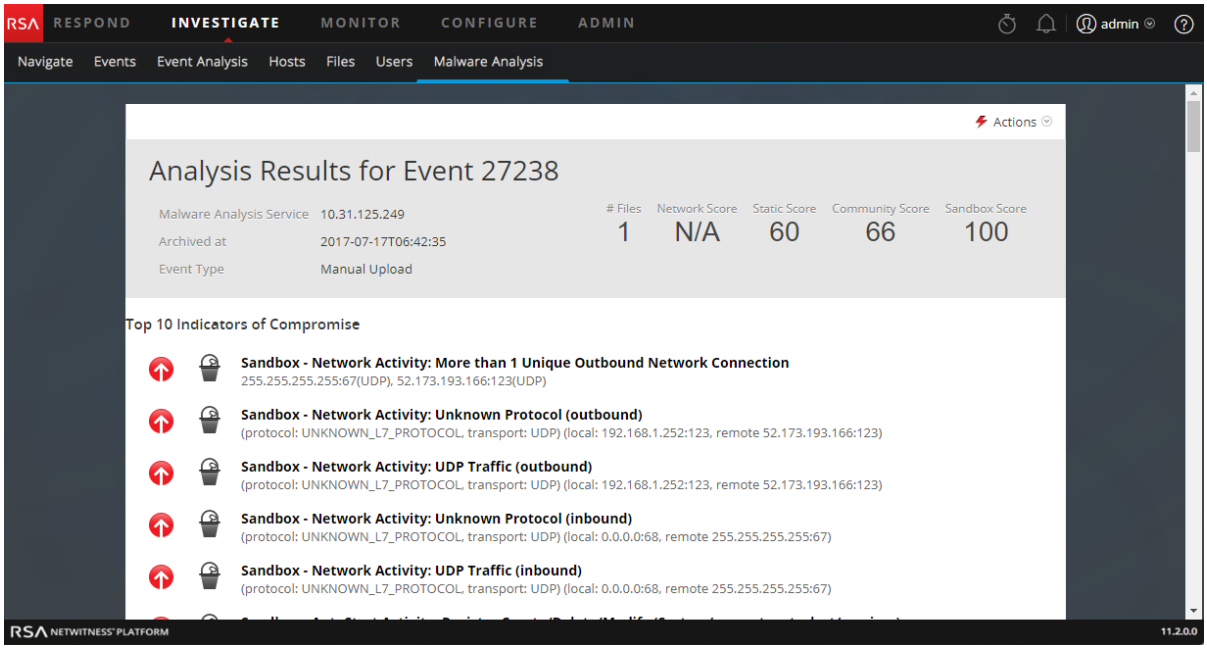
2. Lorsque la tâche est ajoutée à la liste des tâches d'analyse, exécutez un script ou cronjob pour nettoyer le fichier zip dans `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

Afficher l'analyse Malware Analysis détaillée d'un événement

Lors de l'affichage de la liste des événements individuels dans une analyse Malware Analysis au sein de la grille Malware Analysis Événements, vous pouvez double-cliquer sur un événement pour afficher les résultats d'analyse détaillée de l'événement.

Voir les détails de l'analyse Malware Analysis pour un événement

1. Démarrez une procédure d'enquête sous l'onglet **Malware Analysis**.
   Le Récapitulatif des événements de Malware s'affiche et contient quatre graphiques, y compris le graphique Chronologie d'événements.
2. Exécutez l'une des opérations suivantes :
   a. Pour afficher tous les événements dans la Chronologie d' événements, cliquez sur le bouton **Afficher les événements**.
   b. Double-cliquez sur les données dans **Répartition des méta**, **Compartimentage des méta** ou **Roue des scores**.
      La liste Événements s'affiche.
3. Double-cliquez sur un événement.
   Les résultats d'analyse de l'événement s'affichent.

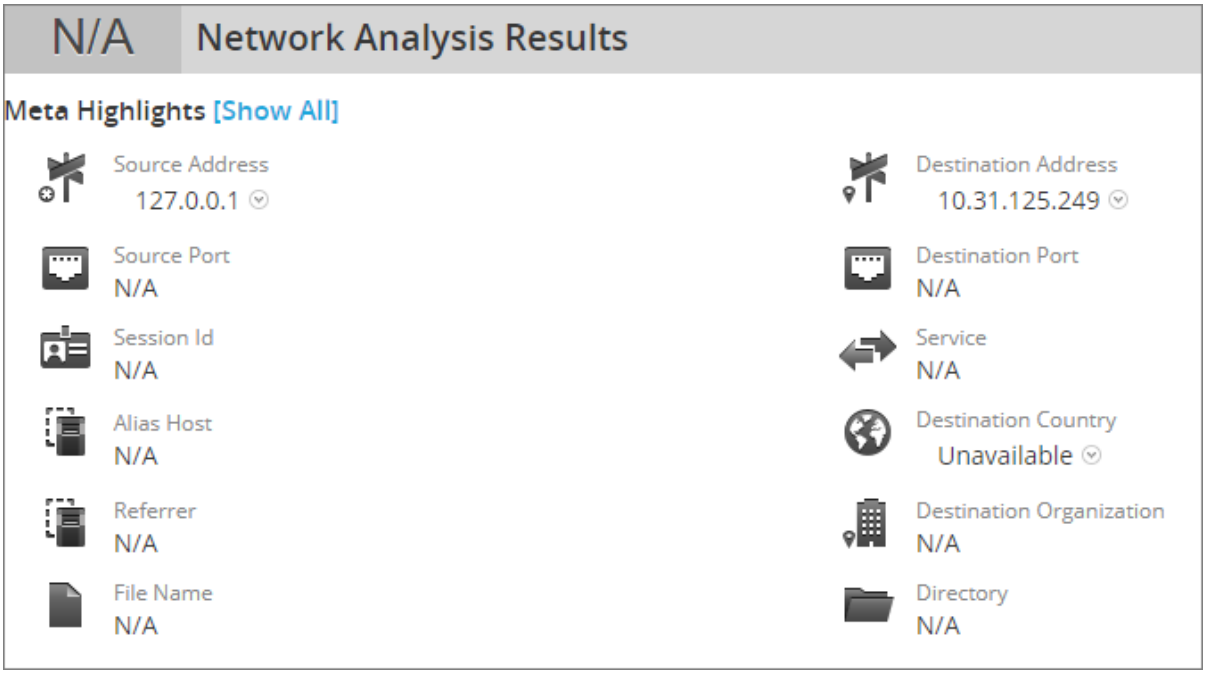


4. (Facultatif) Si vous souhaitez supprimer un événement, sélectionnez **Actions > Supprimer un événement**.
5. Pour afficher une reconstruction de la session réseau, sélectionnez **Actions > Afficher la session réseau**.
   La session s'ouvre dans la vue Naviguer > Reconstruction d'événement.

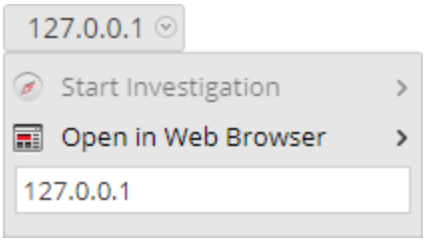
Pivotage des résultats de l'analyse réseau

Vous pouvez faire pivoter les résultats de l'analyse réseau de différentes manières :

1. Faites défiler l'écran vers les résultats de l'analyse réseau.



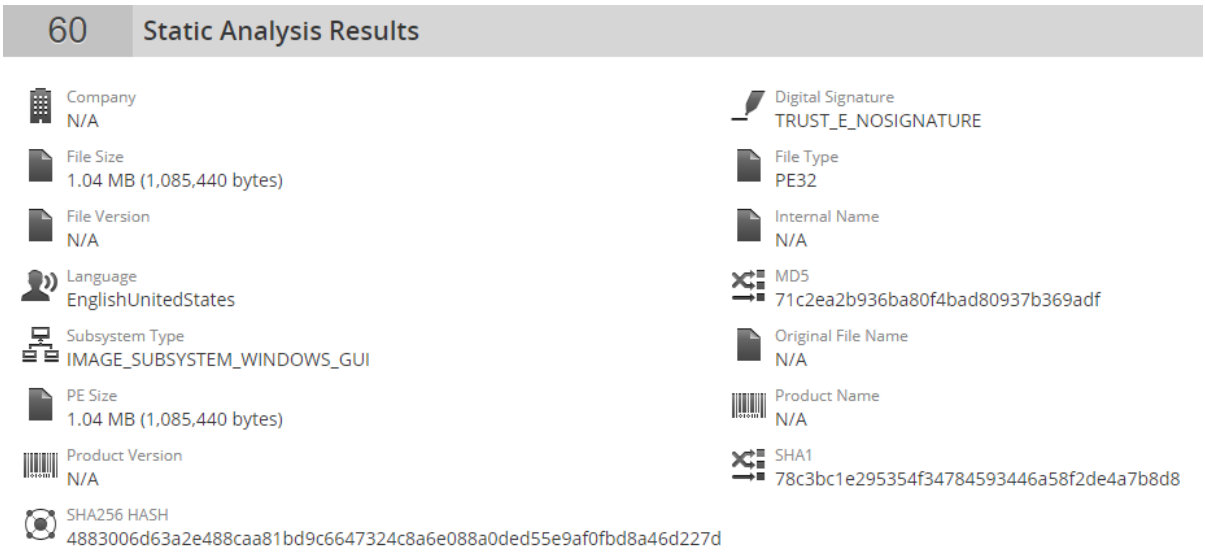
2. Placez le pointeur sur une valeur méta, puis cliquez dessus avec le bouton gauche de la souris. Le menu contextuel s'affiche.



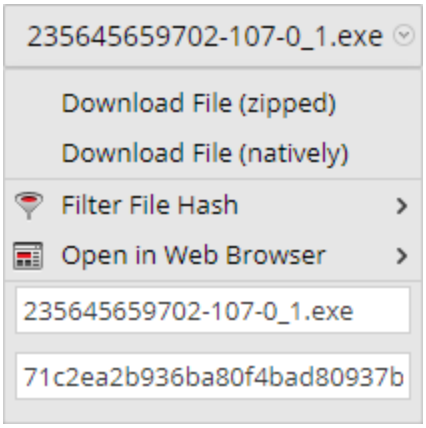
3. Pour afficher la valeur méta sélectionnée dans la vue **Naviguer**, sélectionnez **Démarrer Investigation** et une option d'heure.
4. Pour afficher la métavaleur sélectionnée dans un navigateur, sélectionnez **Ouvrir dans un navigateur Web > Ouvrir dans Google**.

Utiliser les actions de fichier dans les résultats de l'analyse statique

1. Faites défiler l'écran vers les résultats de l'analyse statique.



2. Pour télécharger un fichier, sélectionnez le nom du fichier et soit **Télécharger le fichier (compressé)**, soit **Télécharger le fichier (mode natif)** dans le menu déroulant. Il est plus sûr de télécharger un fichier en format compressé.



3. Si vous souhaitez marquer le fichier comme sûr ou non dans la liste de hachage, sélectionnez **Hachage de fichier de filtre** et **Marquer le hachage comme correct** ou **Marquer le hachage comme incorrect**.

Voir les détails des résultats de l'analyse de la communauté

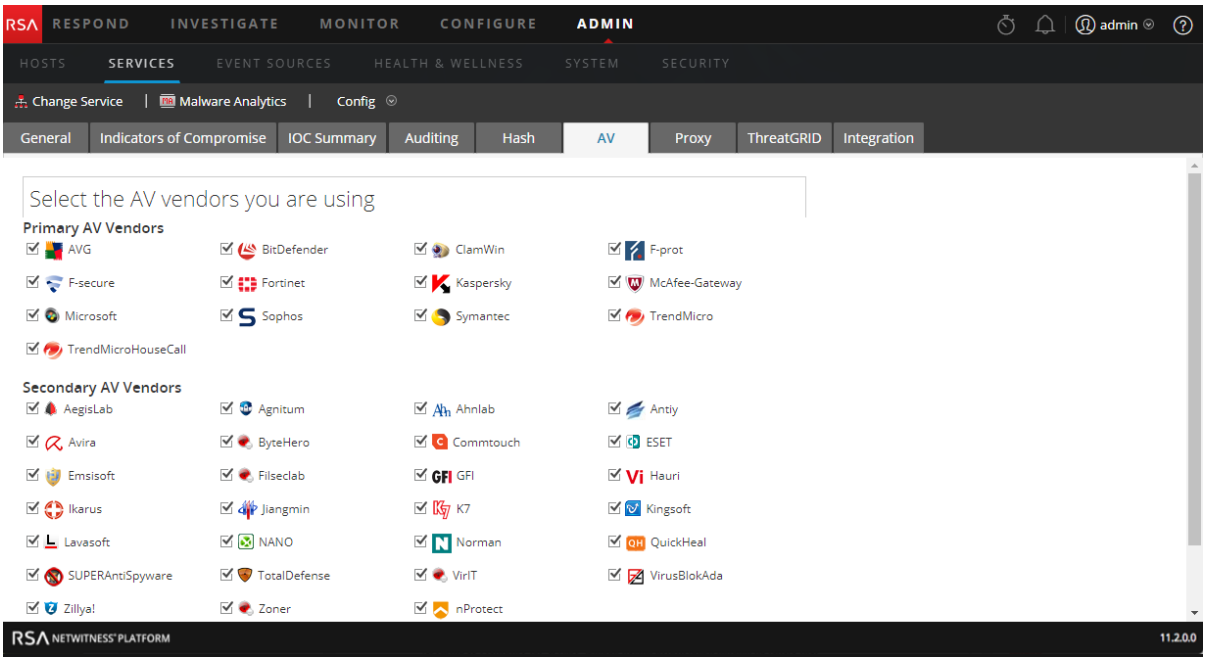
Résultats de l'analyse de la communauté résume les résultats de la communauté, identifiant les indicateurs de compromission qui ont été marqués comme risqués ou identifiés comme corrects.

En outre, cette vue répertorie les résultats des fournisseurs AV installés et des fournisseurs d'antivirus non installés. Vous pouvez comparer les résultats des fournisseurs AV installés qui ont été configurés pour le service Malware Analysis actuel par rapport aux résultats de la Communauté. Vous pouvez également visualiser les résultats de la liste des fournisseurs AV qui ne sont pas configurés comme installés pour le service Malware Analysis actuel.

Chaque ligne de résultats des fournisseurs AV inclut une icône de bouclier pour indiquer si le IOC a été découvert par un fournisseur principal ( ) ou un fournisseur secondaire ( ) de la communauté. Elle indique également le nom du fournisseur installé ou non installé, ainsi que le nom du logiciel malveillant ou le risque détecté par la communauté et le fournisseur AV. Si le fournisseur AV n'a pas détecté de risque, **-- Non détecté --** s'affiche à la place du nom du risque.

La section Fournisseurs d'antivirus non installés est extensible pour afficher toutes les entrées, mais est réduite par défaut pour minimiser le besoin de faire défiler l'écran. Cliquer sur le signe + permet de développer la liste.

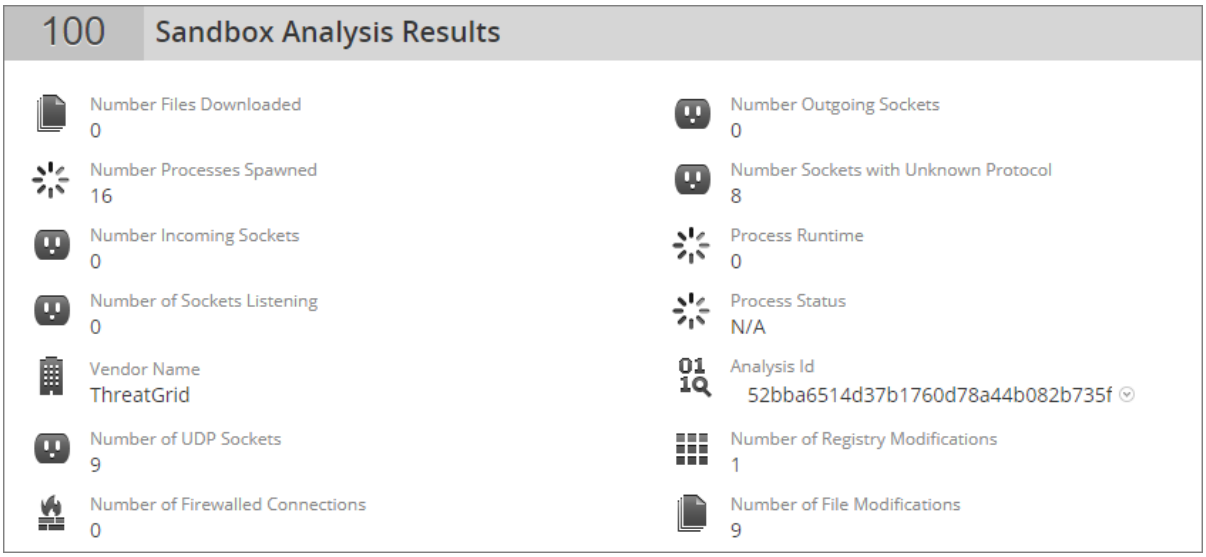
Si aucun fournisseur AV installé n'a été configuré pour le service Malware Analysis actuel, le message suivant s'affiche : Aucun fournisseur d'antivirus n'est signalé comme étant installé. Accédez à la page de configuration du service Malware Analysis pour identifier les fournisseurs AV installés.



Afficher les résultats de l'analyse sandbox dans l'interface utilisateur ThreatGrid

Si vous vous êtes inscrit(e) à ThreatGrid, vous pouvez consulter les résultats sandbox directement dans ThreatGrid.

1. Faites défiler l'écran vers les résultats de l'analyse sandbox.



2. Cliquez sur **ID de l'analyse** et sélectionnez **Ouvrir dans ThreatGrid**.
   Le rapport d'analyse ThreatGrid s'affiche.

Résolution des problèmes liés à NetWitness Investigate

Cette section fournit des informations sur les problèmes rencontrés lors de l'utilisation de NetWitness Investigate.

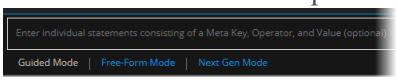
Problèmes liés à la vue Naviguer et la vue Événements

Message	`Not indexed; will experience longer than usual load times.` dans la boîte de dialogue Gérer les groupes méta
Problème	Les clés méta de la boîte de dialogue Gérer les groupes méta sont marquées d'un point d'exclamation rouge et le message d'erreur s'affiche. Cela peut se produire lors de l'enquête sur un Broker ou un Decoder et de l'ajout d'un groupe méta avec des clés méta qui ne sont pas indexées dans le fichier d'index ou le fichier d'index personnalisé pour le service. Pour un Broker, cela pourrait signifier que le Broker n'a pas commencé à agréger des données à partir d'un Concentrator. Dans ce cas, le Broker n'obtiendra pas le contenu du fichier d'index personnalisé à partir des services globaux et les clés ne seront pas indexées. Pour un Décoder, cela signifie que les clés méta ne sont pas indexées dans l'index Decoder ou le fichier d'index personnalisé.
Explication	Pour résoudre le problème sur un Broker, déconnectez-vous, connectez-vous et redémarrez le service Broker afin qu'il puisse agréger les informations de clé méta des Concentrators connectés. Pour résoudre le problème sur un Décoder, modifiez le fichier d'index personnalisé pour indexer les clés méta, déconnectez-vous, connectez-vous et redémarrez le service Decoder.

Comportement	Lorsqu'ils sont téléchargés à partir de la vue Reconstruction d'événement, les logs et les métadonnées sont toujours au format texte, quel que soit le format sélectionné dans la vue Événements.
Problème	Lorsque vous téléchargez des métadonnées ou un log dans la vue Reconstruction d'événement, le format que vous avez sélectionné dans la vue Événements n'est pas utilisé. Les données exportées sont toujours au format texte.
Explication	Téléchargez les métadonnées et les logs dans la vue Événements si vous souhaitez utiliser un autre format que le format texte.

Problèmes liés à la vue Analyse d'événements

Comportement	Le générateur de requêtes dans la version 11.2 inclut le mode Next Gen, une

Problème	fonctionnalité bêta non documentée.
	La version 11.2 comprenait une fonctionnalité bêta non documentée, appelée mode Next Gen, dans le générateur de requêtes de la vue Analyse d'événements qui était encore en cours de développement et de test. Le mode Next Gen a été désactivé dans le correctif 11.2.0.1.
Explication	Si vous voyez le mode Next Gen ne l'utilisez pas ; vous devez utiliser uniquement le mode Guidé et le mode Formulaire libre dans le générateur de requêtes pour garantir des résultats cohérents et prévisibles. 

Message	`Investigation Profiles/OOTB column groups are not present in Event Analysis`
Problème	Après une mise à niveau vers RSA NetWitness v11.1, les groupes de colonnes par défaut - Endpoint Analysis, Outbound SSL et Outbound Http ne sont pas ajoutés sous les groupes de colonnes. En outre, peu de profils de procédure d'enquête sont manquants après la mise à niveau.
Explication	Ce problème se produit uniquement après avoir créé un groupe de colonnes personnalisé portant le même nom que le nouveau groupe de colonnes personnalisé OOTB de la version 11.1. Par exemple, si vous créez un groupe de colonnes personnalisé dans la version 11.0 nommé **RSA Endpoint Analysis** après la mise à niveau vers la version 11.1. Parce que ce nom existe déjà dans la version 11.1, les groupes de colonnes OOTB et les profils OOTB ne seront pas disponibles dans l'interface utilisateur. Pour résoudre ce problème, remplacez le nom du groupe de colonnes personnalisé par un autre et redémarrez le serveur Jetty à l'aide de la commande suivante sur le serveur NetWitness : `systemctl restart jetty`

Message	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
Problème	Lorsque vous cliquez sur **Pivoter vers Endpoint** dans la vue Analyse d'événements, aucune donnée ne s'affiche et le message s'affiche.
Explication	La Version 4.4 du client Thick NetWitness Endpoint doit être installée sur le même serveur, les clés méta NWE doivent exister dans le fichier `table-map.xml` sur le Log Decoder et les clés méta NWE doivent exister dans le fichier `index-concentrator-custom.xml`. Le client Thick NWE est une application Windows uniquement. Les instruments de configuration complets sont fournis dans le *Guide d'utilisation du point de terminaison NetWitness* pour la Version 4.4.

Message	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the Physical Host Upgrade Guide).`

Problème	Lorsque vous tentez de rechercher un service qui n'a pas été mis à jour vers la version 11.1 dans la vue Analyse d'événements, le message d'information s'affiche.
Explication	Lorsqu'un analyste ouvre la vue Analyse d'événements en mode mixte (c'est-à-dire que certains services sont mis à niveau vers la version 11.1 et d'autres vers les versions 11.0.0.x ou 10.6.x), l'accès basé sur les rôles (RBAC) n'est pas appliqué uniformément. Cela affecte l'affichage et le téléchargement du contenu, ainsi que la validation des filtres dans le fil d'Ariane interactif. Ce message d'information apparaît à l'ouverture de la vue Analyse d'événements. Lorsque vous sélectionnez un service, les services qui ne sont pas à jour sont affichés dans une zone rouge, avec le message que le service n'est pas à jour. Lorsque votre administrateur a mis à niveau tous les services connectés vers la version 11.1, ces fonctionnalités fonctionnent comme prévu.

Message	`Forbidden. You cannot access the requested page.`
Problème	Lorsque vous tentez d'accéder à la vue Analyse d'événements, la vue s'ouvre avec le message.
Explication	Votre administrateur a empêché l'accès à la vue Analyse d'événements à l'aide du rôle et des autorisations.

Message	`Insufficient permissions for the requested data.`
Problème	Lorsque vous tentez d'accéder à un événement dans Analyse d'événements par n'importe quel moyen, la reconstruction n'apparaît pas, mais le message s'affiche.
Explication	Vous avez saisi un ID d'événement pour un événement que vous n'êtes pas autorisé à afficher. L'administrateur peut avoir mis quelques restrictions pour limiter l'accès en fonction des rôles et des autorisations.

Message	`Invalid session ID: <<eventId>>`
Problème	Aucun paramètre `sessionId` ne correspond au paramètre `sessionId` que vous recherchez.
Explication	Le motif de l'ID de session non valide peut varier. Vous avez peut-être modifié l'ID de session manuellement, alors qu'aucune session de ce type n'existe. Il se peut aussi qu'un Broker ait été interrogé et que les données agrégées n'aient pas été actualisées, et dans ce cas, ce message d'erreur peut s'afficher pour une session qui n'existe plus.

Message	`No text data was generated during content reconstruction. This could mean that the event data was corrupt/invalid, or that an administrator has disabled the transmission of raw endpoint events in the Endpoint server configuration. Check the other reconstruction views.`
Problème	Lorsque vous reconstruisez un événement en tant que texte dans la vue Analyse d'événements, aucune donnée n'apparaît mais le message s'affiche.

Explication	Si le texte brut n'apparaît pas dans d'autres vues Analyse d'événements ou dans les reconstructions de vues d'événements, et si vous pensez que les données ne sont pas corrompues ni incorrectes, votre administrateur a probablement désactivé la transmission des événements de points de terminaison bruts sur le serveur NetWitness Endpoint. Contactez votre administrateur pour plus d'informations.

Message	`Session is unavailable for viewing.`
Problème	Lors de l'interrogation d'un ID d'événement, la reconstruction ne s'affiche pas, mais le message s'affiche.
Explication	La requête que vous avez saisie tente d'examiner les données restreintes ; par exemple, si vous êtes autorisé(e) à voir uniquement les données des fichiers log, mais que vous utilisez un lien vers les données réseau que vous étiez autorisé(e) à voir hier.

Message	`The session id is too large to be handled:<<eventId>`
Problème	Le nombre entier sessionId que vous avez saisi, modifié ou obtenu à partir de la vue Evénements ou de la vue Naviguer est trop volumineux.
Explication	Si vous avez saisi ou modifié le paramètre sessionId dans la vue Analyse d'événements manuellement, vous avez peut-être créé un nombre entier qui est trop volumineux pour être traité par Event Analysis.

Comportement	Lors de la création d'un filtre dans la vue Analyse d'événements, vous ne pouvez pas saisir une expression complexe à l'aide de l'opérateur `AND` ou `OR` dans le Générateur de requête.
Problème	Le Générateur de requête dans la vue Analyse d'événements prend uniquement en charge les expressions simples sous la forme `<meta key><operator><meta value>`.
Explication	Si vous souhaitez entrer un filtre utilisant l'opérateur `AND` ou `OR`, vous devez l'entrer dans la vue Naviguer ou Événements, puis l'ouvrir dans la vue Analyse d'événements. Vous pouvez entrer des expressions complexes sous la forme de deux filtres distincts dans la vue Analyse d'événements. Les filtres sont associés lorsque vous exécutez la requête.

Problèmes liés à la vue Hôtes

Message	`An error has occurred. The Endpoint Server may be offline or inaccessible.`
Problème	Lorsque vous tentez d'accéder à la vue Hôtes ou Fichiers, la vue s'ouvre avec un message d'erreur.
Explication	Le serveur Endpoint ou le serveur Nginx ne fonctionne pas. Vérifiez l'état du serveur

	Endpoint sous **Admin** > **Service** ou vérifiez si l'adresse IP de l'hôte du serveur Endpoint est enregistrée avec le serveur d'administration. Pour plus d'informations, reportez-vous au *Guide d'installation des hôtes physiques* ou au *Guide d'installation des hôtes virtuels*. Si le service n'est pas exécuté, démarrez le serveur Endpoint.

Problème	Les vues Hôtes et Fichiers ne se chargent pas dans le navigateur Safari.
Explication	Lorsque vous ouvrez les pages Ember dans le navigateur Safari avec un certificat SSL non approuvé, les vues Hôtes et Fichiers ne se chargent pas. Pour charger les vues. 1. Cliquez sur le menu contextuel **Afficher le certificat**. 2. Activez la case à cocher **Toujours faire confiance à NetWitness lors de la connexion à <adresse IP>**. 3. Cliquez sur **Continuer**. 4. Saisissez votre nom d'utilisateur et votre mot de passe. 5. Cliquez sur **Valider les paramètres**.

Message	`No process information was found.`
Problème	Lorsque vous tentez d'accéder à l'onglet Processus ou Bibliothèques dans la vue Détails de l'hôte, les informations détaillées de l'hôte ne sont pas disponibles, et la vue s'ouvre avec ce message d'erreur.
Explication	Les données d'analyse ne sont pas disponibles pour l'une des raisons suivantes : • La première analyse n'est pas terminée • La politique de rétention des données a supprimé tous les snapshots

Problèmes liés à la vue Fichiers

Comportement	Les valeurs méta mettront du temps à se charger.
Problème	Les valeurs méta ne sont pas indexées par valeurs.
Explication	Au cours de la procédure d'enquête, en pivotant vers la vue Naviguer ou la vue Analyse d'événements depuis la vue Fichiers, si le nom de fichier ou le hachage (SHA256 et MD5) ne sont pas indexés par valeurs, les résultats correspondants mettront du temps à se charger car le service Concentrator doit générer l'index en accédant à la base de données méta et en récupérant la valeur méta pour chaque événement. Vous devez indexer manuellement les valeurs avant de pivoter.

Problème	Le filtrage des fichiers prend plus de temps pour charger les résultats dans l'interface utilisateur.
Explication	Dans la vue Fichiers, lors du filtrage des fichiers avec l'opérateur `Contains`, les

	résultats mettent quelques secondes pour se charger dans l'interface utilisateur. Vous devez utiliser au moins un champ indexé avec l'opérateur `Equals`lors du filtrage des fichiers.

Matériaux de référence Enquêter

Cette section a pour but de vous aider à comprendre l'objectif et l'applications des vues Enquêter NetWitness. Chaque vue fait l'objet d'une brève introduction et comporte un tableau Que voulez-vous faire, contenant des liens vers les procédures associées. En outre, certains documents de référence comprennent des workflows et des recherches rapides pour mettre en évidence des fonctions importantes de l'interface utilisateur.

Voici les vues principales :

- Vue Enquêter
- Vue Naviguer
- Vue Événements
- Vue Analyse d'événements
- Vue Fichiers
- Vue Hôtes
- Vue Analyse de malware

Il s'agit d'une liste alphabétique des autres vues, panneaux et boîtes de dialogue.

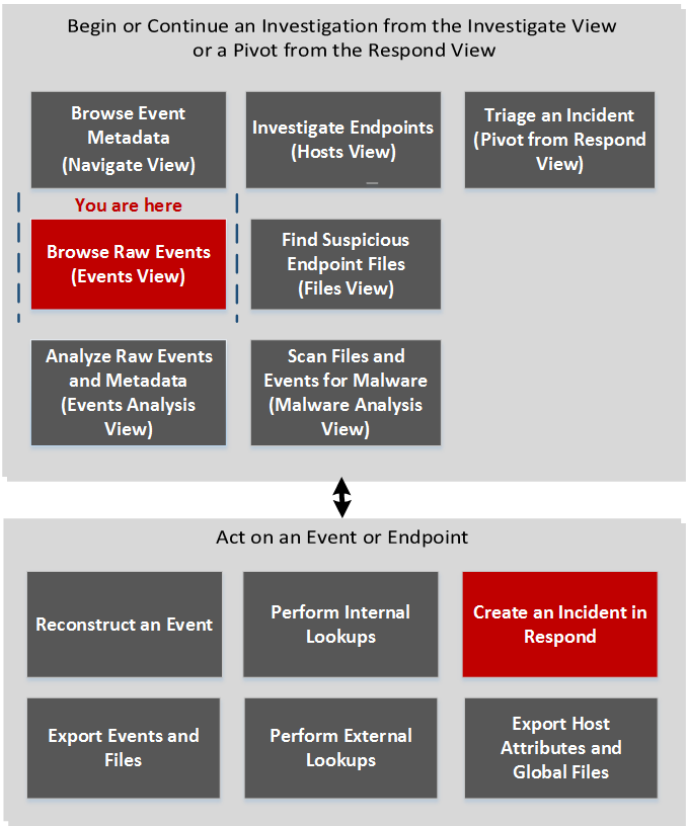
- Boîte de dialogue Ajouter à la liste/Supprimer de la liste
- Panneau Recherche contextuelle
- Boîte de dialogue Créer un incident
- Vue Analyse d'événements
- Vue Analyse d'événements - Panneau Analyse de texte
- Vue Analyse d'événements - Panneau Analyse de paquets
- Vue Analyse d'événements - Panneau Analyse de fichiers
- Vue Reconstruction d'événement
- Vue Hôtes - Onglet Exécutions automatiques
- Vue Hôtes - Onglet Pilotes
- Vue Hôtes - Onglet Fichiers
- Vue Hôtes - Onglet Bibliothèques
- Vue Hôtes - Onglet Présentation
- Vue Hôtes - Onglet processus
- Vue Hôtes - Onglet Informations du système
- Boîte de dialogue Enquêter
- Onglet Procédure d'enquête - Panneau Préférences utilisateur

- Liste d'événements d'analyse de malware et liste Fichiers
- Boîte de dialogue Gérer les groupes de colonnes
- Boîte de dialogue Gérer les clés méta par défaut
- Boîte de dialogue Gérer les groupes méta
- Boîte de dialogue Gérer les profils
- Vue Naviguer
- Boîte de dialogue Requête
- Boîte de dialogue Analyser les malwares
- Boîte de dialogue Sélectionner un service Malware Analysis
- Boîte de dialogue Paramètres pour les vues Enquêter

Boîte de dialogue Ajouter des événements à un incident

Dans la boîte de dialogue Ajouter des événements à un incident, les analystes peuvent ajouter des alertes à un incident existant de façon à ce que les responsables de la réponse aux incidents puissent consulter les événements associés dans le cadre de leur réponse aux incidents. Pour accéder à cette boîte de dialogue lors de la procédure d'enquête sur un service dans la vue Événements, sélectionnez **Incidents** > **Ajouter à un incident existant** dans la barre d'outils.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces ou Responsable de la réponse aux incidents	ajouter un ou plusieurs événements à un incident existant ou à un nouvel incident*	Ajouter des événements à un incident pour obtenir une réponse

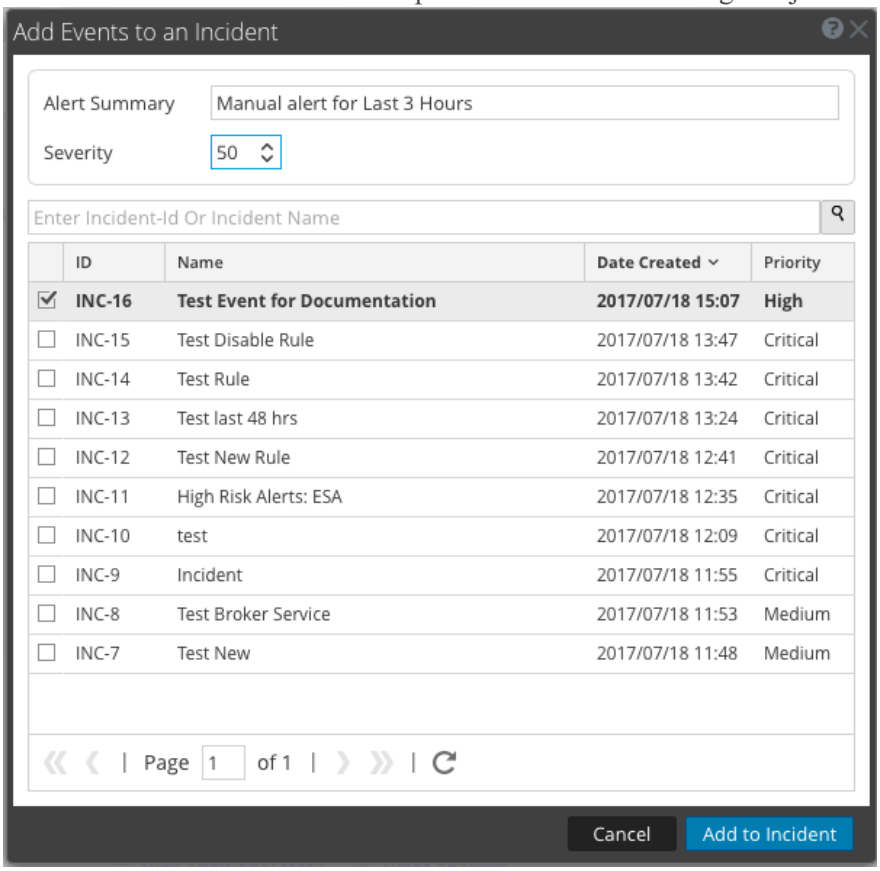
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Événements

Aperçu rapide

La figure suivante est un exemple de la boîte de dialogue Ajouter des événements à un incident. Le tableau décrit les informations et options de la boîte de dialogue Ajouter des alertes à un incident.



Fonctionnalité	Description
Récapitulatif de l'alerte	Le champ Récapitulatif de l'alerte est rempli par la requête qui a produit les alertes que vous avez sélectionnées pour créer cet incident. Le champ Gravité reflète la gravité de l'alerte sélectionnée, soit un nombre entier compris entre 1 et 100.
Rechercher	Permet de rechercher un événement existant.
ID	ID de l'incident. Vous pouvez trier les ID par ordre croissant ou décroissant.
Nom	Nom de l'incident. Vous pouvez trier les noms par ordre croissant ou décroissant.
Date de création	Affiche la date et l'heure de création de l'incident. Vous pouvez trier les dates par ordre croissant ou décroissant.
Priorité	Affiche la priorité de l'incident, qu'elle soit faible ou critique.
Annuler	Ferme la boîte de dialogue sans enregistrer les modifications.

Fonctionnalité	Description
Ajouter à l'incident	Ajoute les alertes à l'incident. Une boîte de dialogue confirme que les alertes ont été ajoutées avec succès.

Boîte de dialogue Ajouter à la liste/Supprimer de la liste

La boîte de dialogue Ajouter à la liste/Supprimer de la liste permet d'ajouter une valeur d'entité ou une métadonnée à une liste existante Context Hub, ou de l'en supprimer, ou encore de créer une nouvelle liste. Lorsque vous recherchez une adresse IP ou une autre entité et que vous la trouvez suspecte ou intéressante, vous pouvez l'ajouter à une liste qui a été ajoutée à une source de données. Par exemple, les listes blanches ou les listes noires sont des exemples de listes fréquemment utilisées. Cela améliore la visibilité des adresses IP suspectes et réduit les faux positifs qui n'ont pas besoin d'une investigation plus approfondie.

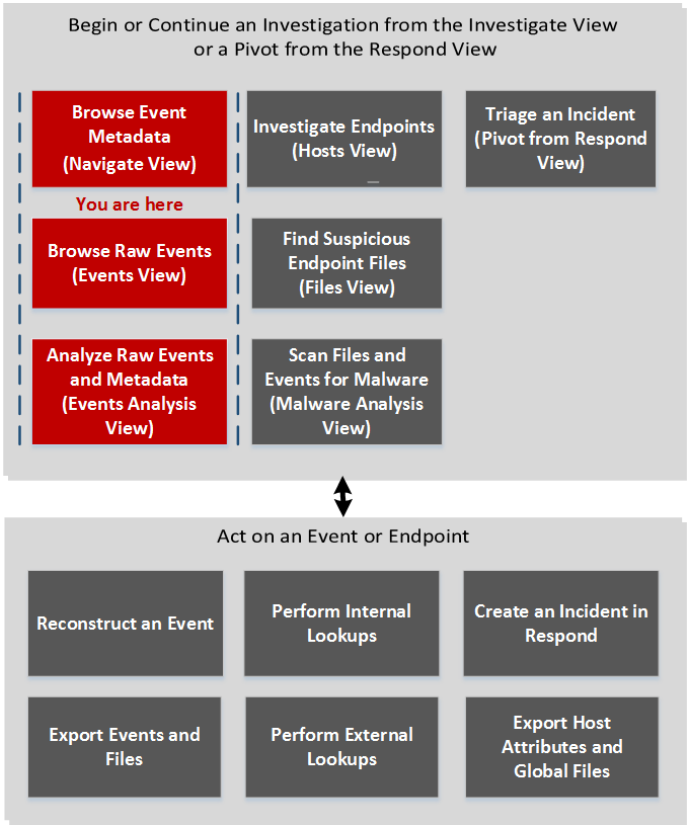
Vous pouvez ajouter des entités ou des valeurs méta à plusieurs listes. Par exemple, vous pouvez les ajouter à une liste de domaines suspects liés à des connexions de commande et de contrôle, et à une autre liste concernant les adresses IP liées aux connexions de chevaux de Troie autorisant un accès à distance. Si aucune liste n'est disponible, vous pouvez en créer une.

La boîte de dialogue est disponible dans NetWitness Investigate et dans NetWitness Respond. Lorsque vous travaillez dans Investigate, dans la vue Naviguer, Événements ou Analyse d'événements (version 11.2), vous pouvez ajouter des valeurs méta pour les clés méta `Source IP`, `Destination IP` ou `Username` à une liste Context Hub existante ou vous pouvez créer une nouvelle liste contenant les valeurs méta. Lorsque vous ajoutez des métavaleurs à une liste, vous pouvez rechercher un contexte supplémentaire sur ces métavaleurs.

- Pour afficher la boîte de dialogue dans la vue Naviguer ou Événements, cliquez avec le bouton droit de la souris sur une métavaleur sous `Source IP`, `Destination IP` ou `Username`), puis sélectionnez **Ajouter à la liste/Supprimer de la liste** dans le menu contextuel.
- Pour afficher la boîte de dialogue dans la vue Analyse d'événement, pointez sur une valeur et sélectionnez **Ajouter à la liste/Supprimer de la liste** dans la section Actions de l'info-bulle contextuelle.

Workflow

Le diagramme de workflow suivant montre une vue générale du workflow dans la vue Enquêter avec l'emplacement de la tâche Ajouter à la liste mis en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers

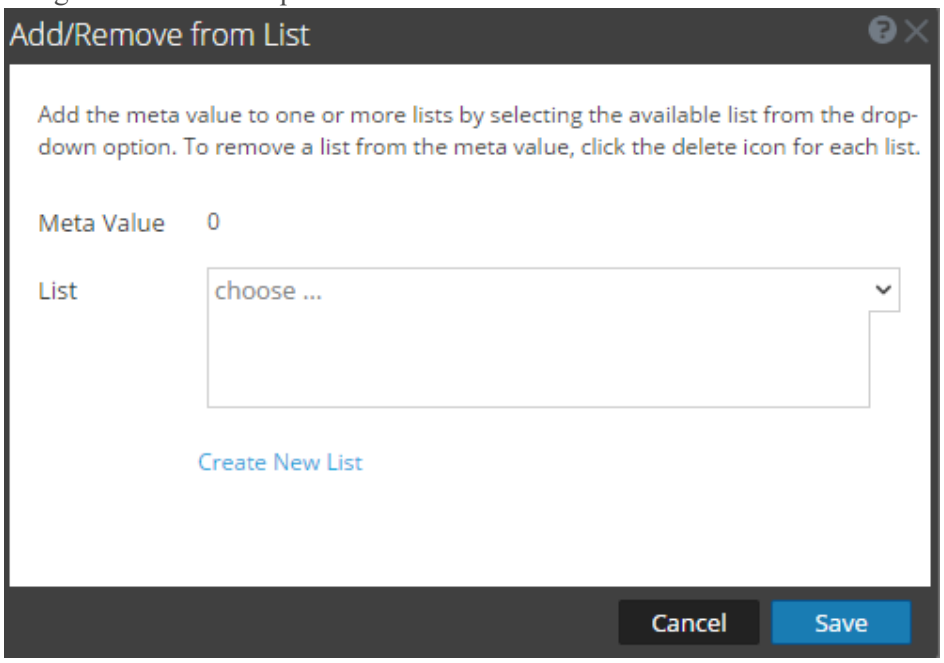
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	créer ou ajouter des métavaleurs à une liste Context Hub*	Gérer Listes Context Hub et Valeurs de la liste dans les vues Naviguer et Événements ou Rechercher un contexte supplémentaire dans la vue d'analyse d'événement

Rubriques connexes

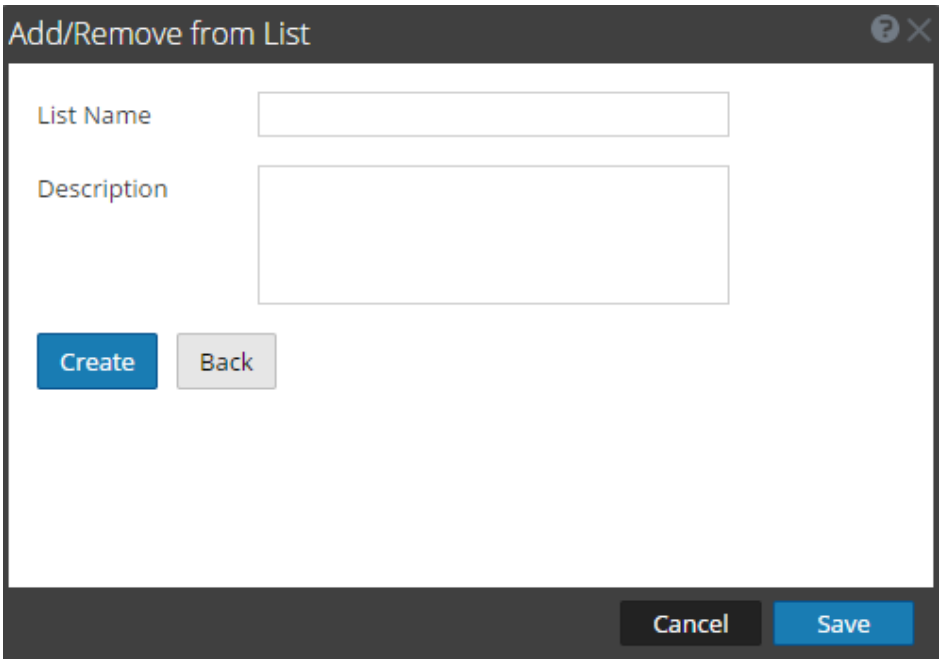
- Rechercher un contexte supplémentaire dans les vues Naviguer et Événements
- Vue Naviguer
- Vue Événements
- Vue Analyse d'événements

Recherche rapide dans les vues Naviguer et Événements

La figure suivante donne un exemple de l'option Ajouter à la liste/Supprimer de la liste de la boîte de dialogue de la liste lorsqu'elle est ouverte initialement.



La figure suivante affiche la boîte de dialogue lorsque vous sélectionnez la boîte de dialogue Créer une nouvelle liste.

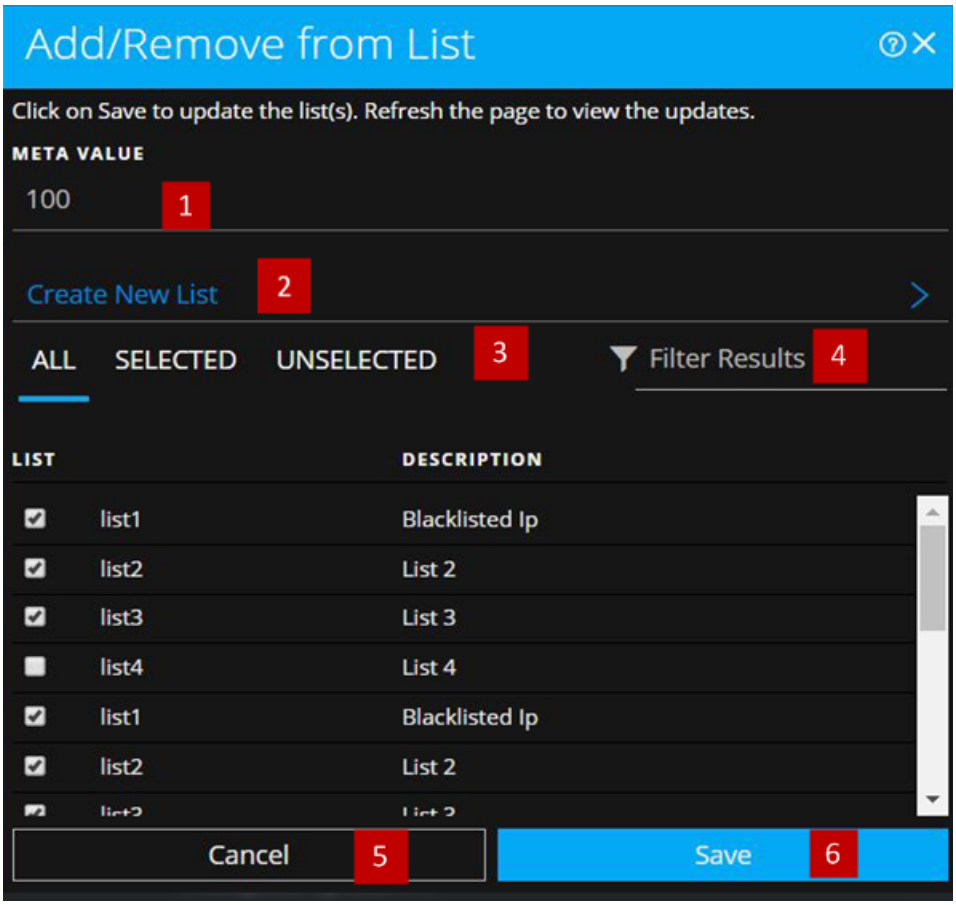


Le tableau suivant décrit les fonctionnalités des boîtes de dialogue Ajouter à la liste/Supprimer de la liste et Créer une nouvelle liste.

Fonctionnalité	Description
Valeur méta	Valeur méta à ajouter à la liste existante ou à la nouvelle liste.
Répertorier	Liste à laquelle la métavaleur sélectionnée doit être ajoutée. Un menu déroulant contient les listes disponibles auxquelles vous pouvez ajouter la métavaleur.
Créer une nouvelle liste	Ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez créer une nouvelle liste pour la métavaleur sélectionnée.
Nom de la liste	Nom de la nouvelle liste.
Description	Description de la nouvelle liste.
Créer	Crée une nouvelle liste après avoir renseigné les champs obligatoires.
Précédent	En mode de création d'une nouvelle liste, annule l'opération de création et revient à la boîte de dialogue d'origine.
Annuler	Annule l'ajout de la métavaleur à une liste et ferme la boîte de dialogue.
Enregistrer	Enregistre toutes les modifications apportées aux listes et ferme la boîte de dialogue.

Aperçu rapide de la vue Analyse d'événements (version 11.2 et supérieure)

Voici un exemple de la boîte de dialogue **Ajouter à la liste/Supprimer de la liste** de la vue Analyse d'événements.



1 Entités ou métadonnées à ajouter ou supprimer.
2 Créer une nouvelle liste à l'aide des métadonnées sélectionnées.
3 Sélectionnez l'un des onglets : Tous, Sélectionné ou Désélectionné.
4 Effectuer une recherche à l'aide du nom de la liste ou de sa description.
5 Annuler l'action.
6 Enregistrer pour mettre à jour les listes ou créer une nouvelle liste.

Le tableau suivant présente les options de la boîte de dialogue Ajouter à la liste/Supprimer de la liste.

Option	Description
VALEUR MÉTA	Affiche l'entité ou la métadonnée sélectionnée qui doit être ajoutée ou supprimée à partir d'une ou plusieurs listes. Vous pouvez également créer une nouvelle liste à l'aide de la valeur sélectionnée.
Créer une nouvelle liste	Une boîte de dialogue vous permet de créer une nouvelle liste à l'aide de la métadonnée sélectionnée.
ALL	Affiche toutes les listes de Context Hub disponibles. Les listes qui contiennent l'entité ou la métadonnée sélectionnée sont sélectionnées. Cochez une case pour ajouter une entité ou une métadonnée à une liste. Désactivez une case à cocher pour la supprimer de la liste.

Option	Description
SÉLECTIONNÉ	Affiche les listes qui contiennent l'entité ou la métadonnée sélectionnée. (Toutes les listes sont sélectionnées.)
DÉSÉLECTIONNÉ	Affiche uniquement les listes qui contiennent l'entité ou la métadonnée sélectionnée. (Toutes les listes sont désélectionnées.)
Filtrer les résultats	Saisissez le nom ou la description d'une liste spécifique pour effectuer la recherche dans plusieurs listes.
LISTE	Affiche le nom de toutes les listes.
Description	Affiche des informations relatives à la liste sélectionnée. La description que vous fournissez lors de la création d'une liste s'affiche dans cette boîte de dialogue. Par exemple : Cette liste contient toutes les adresses IP répertoriées dans la liste noire.
Annuler	Annule l'opération.
Enregistrer	Enregistre les modifications.

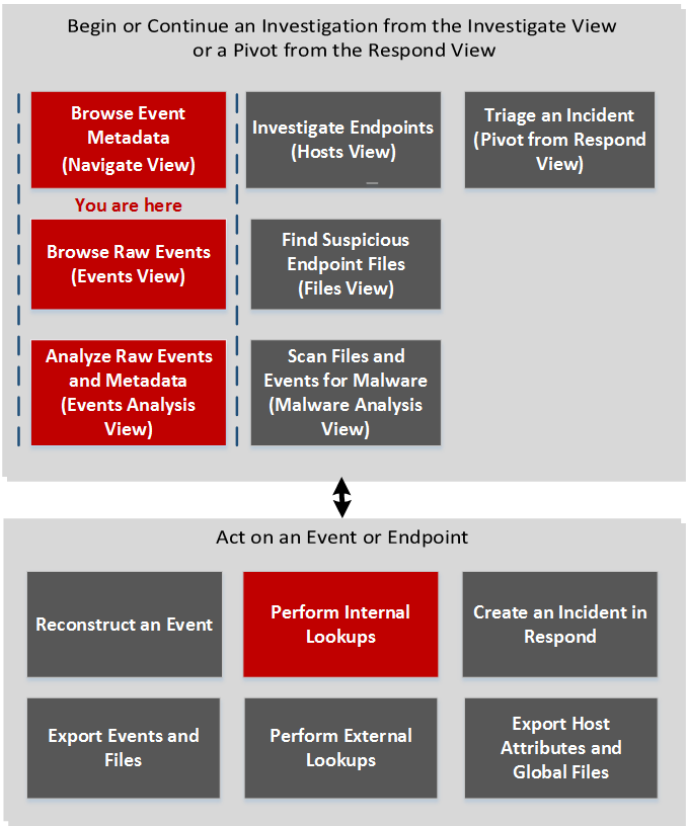
Panneau Recherche contextuelle

Une fois qu'un administrateur a configuré le service Context Hub, vous pouvez afficher les informations contextuelles des métavaleurs dans la vue Naviguer, la vue Événements et la vue Analyse d'événements (Version 11.2). Le service Context Hub est pré-configuré avec un adressage du type de méta et de la clé méta par défaut. Pour plus d'informations sur l'adressage de la métavaleur du service Context Hub avec une clé méta de procédure d'enquête, consultez la rubrique « Gérer l'adressage du type de métadonnées et de la clé méta » du *Guide de configuration de Context Hub*

Le panneau Recherche contextuelle s'affiche sur le côté droit de la vue Naviguer et vue Événements. Les métavaleurs qui ont été ajoutées à une liste Context Hub sont mises en surbrillance en gris dans les résultats de la vue Naviguer ou de la vue Événements. Dans la vue Analyse d'événement, ils sont marqués d'un trait de soulignement. Lorsque vous cliquez avec le bouton droit de la souris sur une valeur en surbrillance et sélectionnez **Recherche contextuelle** dans le menu contextuel qui en résulte, les résultats de recherche sont affichés dans le panneau Recherche contextuelle pour les sources configurées pour la métavaleur sélectionnée. Vous pouvez sélectionner une source dans la barre d'icônes du Panneau Recherche contextuelle pour afficher les informations contextuelles.

La présentation et le contenu du panneau Recherche contextuelle diffèrent selon que celui-ci est ouvert dans la vue Naviguer ou Événements ou dans la vue Analyse d'événements.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	rechercher le contexte supplémentaire d'une métavaleur*	Rechercher un contexte supplémentaire dans les vues Naviguer et Événements et Rechercher un contexte supplémentaire dans la vue d'analyse d'événement

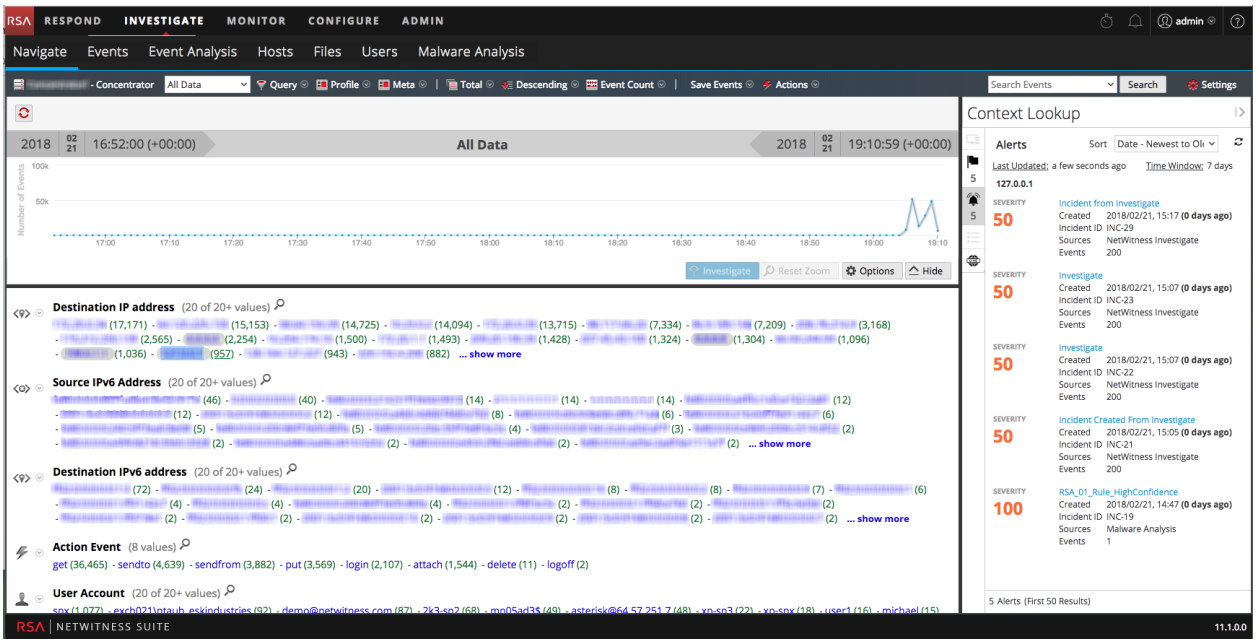
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Événements
- Vue Naviguer
- Vue Analyse d'événements
- « Commentaires et partage de données NetWitness » dans le *Guide de gestion des services Live*

Aperçu rapide (dans les vues Naviguer et Événements)

La figure suivante est un exemple du panneau Recherche contextuelle tel qu'il apparaît dans la vue Naviguer et Événements. Les contrôles et les fonctionnalités sont décrits dans le tableau.



Fonctionnalité	Description
Barre Options de la source	Affiche les icônes des sources disponibles : Point de terminaison, Incidents, Alertes et Listes.
Nom de la source	Affiche le nom de la source en fonction de l'icône sélectionnée : • Point de terminaison • Incidents • Alertes • Listes • Live Connect
Trier	Propose une liste déroulante d'options pour trier les informations de contexte répertoriées. Les options de tri possibles sont Gravité - Élevée à faible, Gravité - Faible à élevée, Date - La plus ancienne à la plus récente, et Date - La plus récente à la plus ancienne. Les options de tri varient par type de source.
	Actualise les résultats de la recherche.
<n items> (Premiers résultats <n>)	Le pied de page indique le nombre total de résultats et le nombre de résultats actuellement affichés. Par exemple, 5 alertes (50 premiers résultats).

Incidents

Les incidents s'affichent d'abord selon un critère de temps (du plus récent au plus ancien), puis sur un critère de priorité. Les informations suivantes s'affichent pour les recherches d'incidents :

- Nom et ID de l'incident
- Priorité des incidents
- Valeur de risque
- Date de création de l'incident
- État de l'incident
- Personne affectée à l'incident
- Dernière mise à jour: indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Période : Elle se base sur la valeur définie dans le champ « Durée de la requête (jours) » de la fenêtre Configurer Répondre. Pour plus d'informations, consultez la rubrique « Configurer Respond en tant que source de données » du *Guide de configuration de Context Hub*.
- Trier : Ce champ déroulant permet de modifier l'ordre de tri en fonction de la période ou de la priorité.

Alertes

Les alertes s'affichent en fonction de la Gravité. Les informations suivantes s'affichent pour les recherches d'alertes :

- Nom de l'alerte
- Gravité de l'alerte
- Date de création de l'alerte
- ID d'incident : ID de l'incident associé à l'alerte (le cas échéant).
- Sources : Nom de la source d'événement
- Nombre d'événements associés à l'alerte.
- Dernière mise à jour : indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Période : Elle se base sur la valeur définie dans le champ « Durée de la requête (jours) » de la fenêtre Configurer Répondre. Pour plus d'informations, consultez la rubrique « Configurer Respond en tant que source de données » du *Guide de configuration de Context Hub*
- Trier : Ce champ déroulant permet de modifier l'ordre de tri en fonction de la période et de la priorité.

Listes

Les informations suivantes s'affichent pour les recherches de listes :

- Nom de la liste
- Propriétaire ayant créé la liste
- Date de création

- Date de dernière mise à jour
- Description de la liste

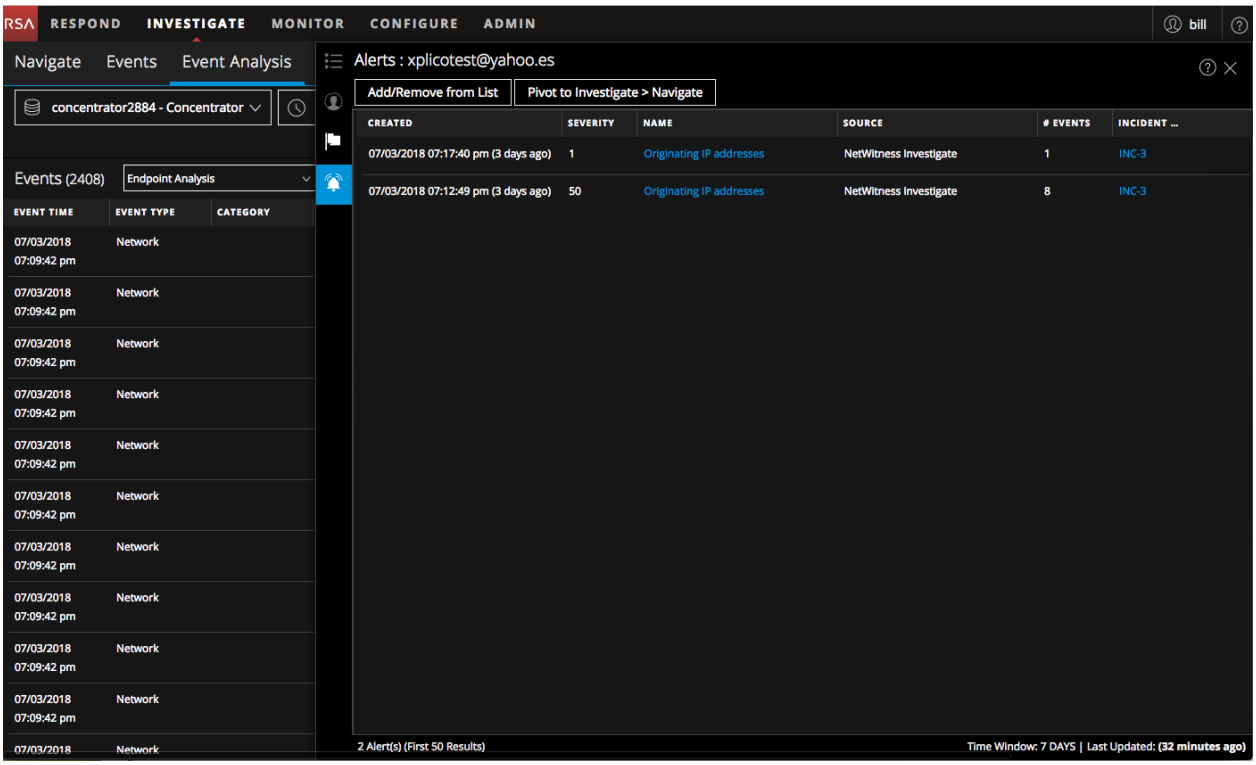
Endpoint

Les informations suivantes s'affichent pour les recherches de points de terminaison.

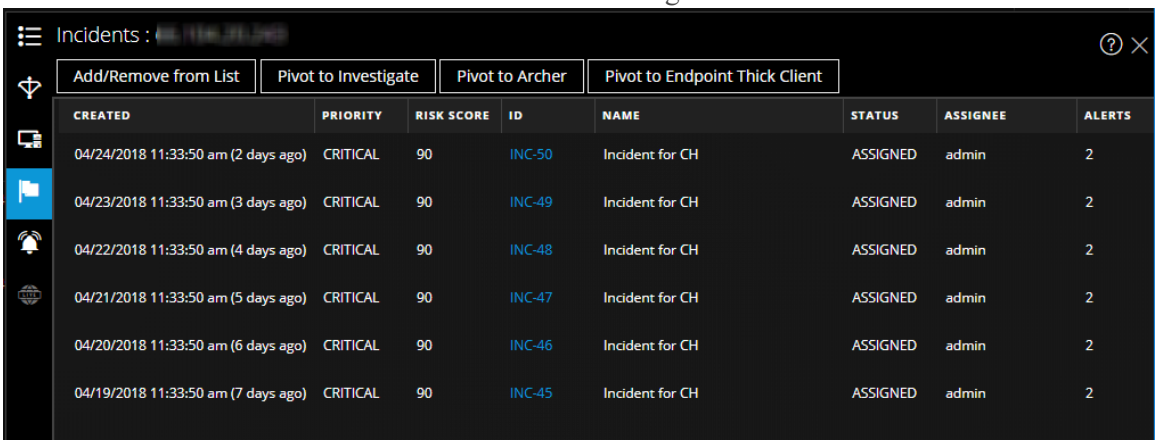
- Nom et adresse IP de la machine.
  En cliquant sur le nom ou l'adresse IP de la machine, vous serez dirigé vers l'interface utilisateur du point de terminaison pour approfondir la procédure d'enquête.
- Dernière mise à jour : indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Note de l'ordinateur : le score IIOC de la machine est agrégé en fonction des scores des modules.
- Nombre de modules : nombre de fichiers actifs pour la machine sélectionnée.
- Dernière mise à jour: indique quand les résultats de l'analyse ont été mis à jour pour la dernière fois dans le point de terminaison.
- Dernière connexion utilisateur
- Adresse MAC de la machine
- Version du système d'exploitation
- Notes Admin (le cas échéant)
- État Admin (le cas échéant)
- Modules les plus suspects (modules dont le score IIOC est supérieur à 500). Cet élément se base sur la valeur définie dans le champ « Valeur IIOC minimale » de la fenêtre Configurer le point de terminaison. La valeur par défaut pour la « Valeur IIOC minimale » est de 500.
- Niveaux IIOC de la machine

Aperçu rapide de la vue Analyse d'événements (version 11.2 et supérieure)

La figure suivante est un exemple du panneau Recherche contextuelle tel qu'il apparaît dans la vue d'Analyse d'événement.



Les informations contextuelles ou les résultats de la requête affichés dans le panneau Recherche contextuelle dépendent de l'entité sélectionnée et des sources de données associées. Le panneau Recherche contextuelle comporte des onglets distincts pour chacune des sources de données. Les onglets sont: répertorier la source de données, Archer, Active Directory, point de terminaison, incidents, alertes et Live Connect. La figure suivante affiche le panneau Recherche contextuelle pour une entité sélectionnée dans la vue Détails sur l'incident avec l'onglet Incidents dans Vue.

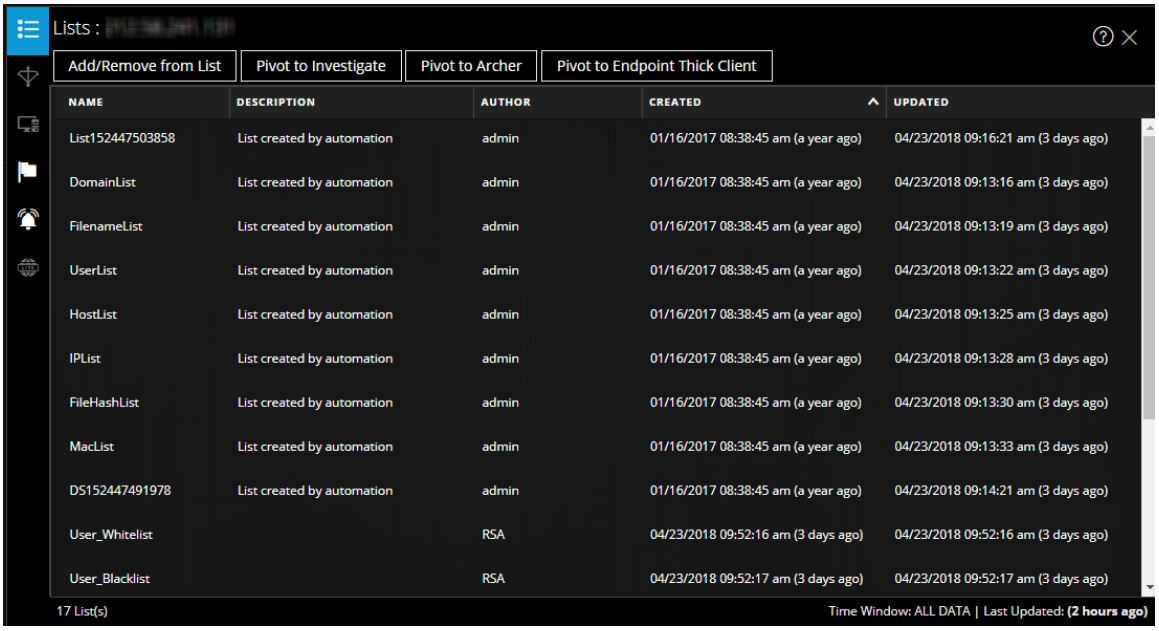


Le tableau suivant décrit les données disponibles sur chaque onglet et les entités prises en charge.

Onglet	Description	Entités prises en charge
 (Listes)	Affiche toutes les données de liste associées à l'entité ou aux métadonnées sélectionnées. Le résultat est trié selon la dernière liste mise à jour.	Toutes les entités
 (Archer)	Affiche des informations relatives aux ressources, ainsi que la criticité, à l'aide de la source de données Archer.	IP, hôte et Mac
 (Active Directory)	Affiche toutes les informations utilisateur pour l'utilisateur sélectionné.	Utilisateur
 (NetWitness Endpoint)	Affiche les informations de source de données NetWitness Endpoint pour l'entité ou les métadonnées sélectionnées, notamment les machines, les modules et les niveaux IIOC. Les modules sont triés de la valeur IOC la plus élevée à la valeur IIOC la plus faible et les niveaux IIOC sont triés du niveau IOC le plus élevé au niveau IOC le plus faible.	IP, adresse MAC et hôte
 (Incidents)	Affiche la liste des incidents associés à l'entité ou aux métadonnées sélectionnées. Le résultat est trié des incidents les plus récents aux incidents les plus anciens.	Toutes les entités
 (Alertes)	Affiche la liste des alertes associées à l'entité ou aux métadonnées sélectionnées. Le résultat est trié des alertes les plus récentes aux alertes les plus anciennes.	Toutes les entités
 (Live Connect)	Affiche les informations relatives à Live Connect.	IP, domaine et hachage de fichier

Onglet Listes

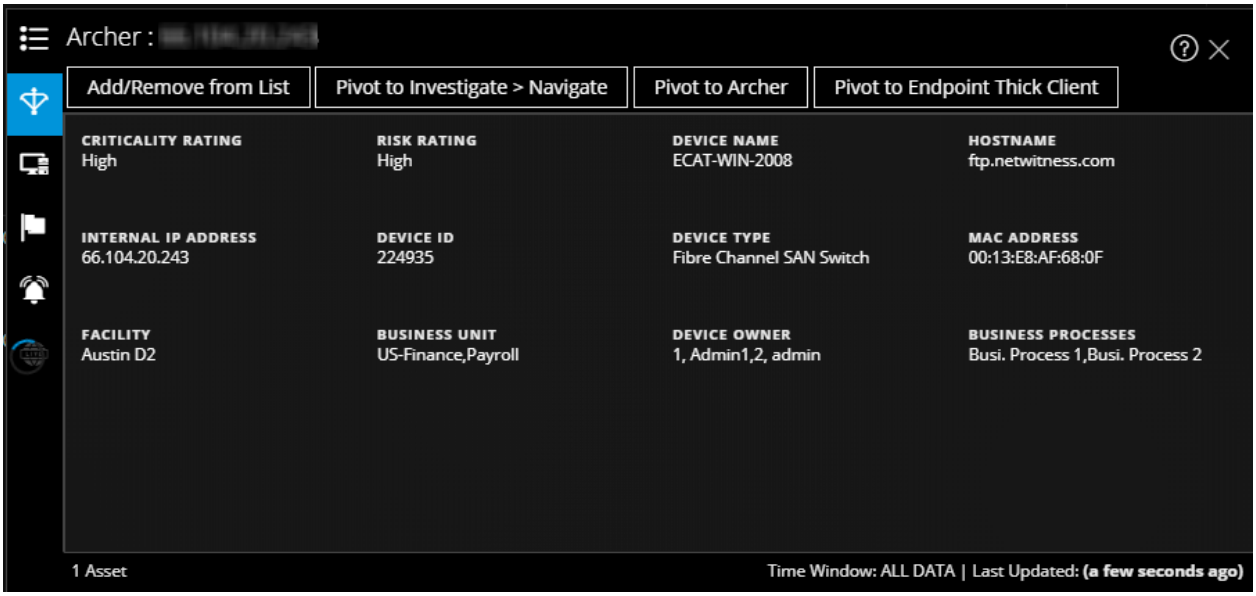
Le panneau Recherche contextuelle des listes présente une ou plusieurs listes associées à l'entité sélectionnée ou la métadonnée sélectionnée. La figure suivante offre un exemple du panneau Recherche contextuelle pour les listes et le tableau décrit les champs.



Champ	Description
Nom	Nom de la liste (défini lors de la création de la liste).
Description	Description de la liste (définie lors de la création de la liste).
Auteur	Propriétaire ayant créé la liste.
Créé	Date de création de la liste.
Mise à jour	Date de mise à jour ou de modification de la liste.
Nombre	Nombre de listes dans lesquelles l'entité ou la métadonnée sélectionnée est disponible.
Période	La fenêtre Période se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses. Par défaut, toutes les données de listes sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

Onglet Archer

Le panneau Recherche contextuelle d'Archer affiche des informations relatives aux ressources, ainsi que la criticité à l'aide de la source de données Archer pour les entités IP, Hôte et Mac. La figure suivante donne un exemple du panneau Recherche contextuelle pour Archer, et chaque champ est décrit dans le tableau.



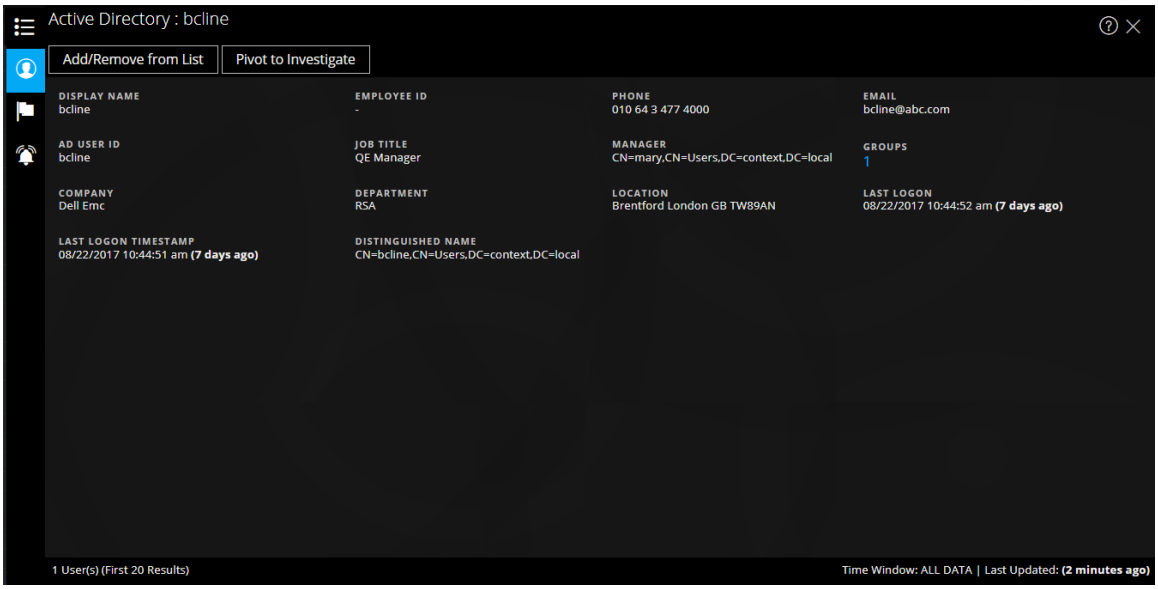
Champ	Description
Degré de criticité	Degré de criticité opérationnel du périphérique en fonction des applications que ce dernier prend en charge. La criticité peut avoir les valeurs Non évaluée, Faible, Relativement faible, Moyenne, Relativement élevée, ou Élevée.
Évaluation des risques	Ce champ identifie le risque estimé pour le périphérique sur la base de la dernière évaluation, ainsi que le risque moyen pour les sites utilisant ce dernier. L'évaluation du risque peut être définie comme étant Grave, Élevée, Moyenne, Faible, ou Minimale.
Nom du périphérique	Le nom unique du périphérique.
Nom d'hôte	Le nom d'hôte du périphérique.
Adresse IP	L'adresse IP interne principale du périphérique.
ID du périphérique	La valeur indiquée automatiquement, qui identifie de manière unique l'enregistrement parmi toutes les applications du système.
Type	Le type de périphérique, par exemple, serveur, ordinateur portable, bureau, etc.
Sites	Ce champ fournit des liens vers les enregistrements relatifs à ce périphérique dans l'application Sites.

Champ	Description
Entité	Fournit des liens vers les enregistrements associés à ce périphérique dans l'application Entité. Pour plus de trois valeurs d'unité d'entreprise, vous pouvez passer le curseur sur le champ pour afficher les valeurs.
Propriétaire du périphérique	Le propriétaire responsable du périphérique qui bénéficie des droits en lecture et mise à jour sur l'enregistrement.
Décompte	Le nombre de ressources disponibles.
Période	La fenêtre Période se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses. Par défaut, toutes les données Archer sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

Remarque : Dans les versions localisées, seuls ces douze champs sont affichés : Degré de criticité, évaluation des risques, propriétaire du périphérique, unité commerciale, nom d'hôte, adresse MAC, installations, adresse IP, type, ID de périphérique, nom de périphérique et processus d'entreprise.

Onglet Active Directory

La figure suivante offre un exemple du panneau de recherche contextuelle d'Active Directory.



Le panneau Recherche contextuelle d'Active Directory affiche l'ensemble des informations, incidents et alertes connexes pour un utilisateur. Vous pouvez effectuer la recherche à l'aide des formats suivants :

- userPrincipalName
- Domain\UserName
- sAMAccountName

Si l'utilisateur existe dans plusieurs domaines ou plusieurs forêts, toutes les informations de contexte associées sont affichées pour l'utilisateur spécifique.

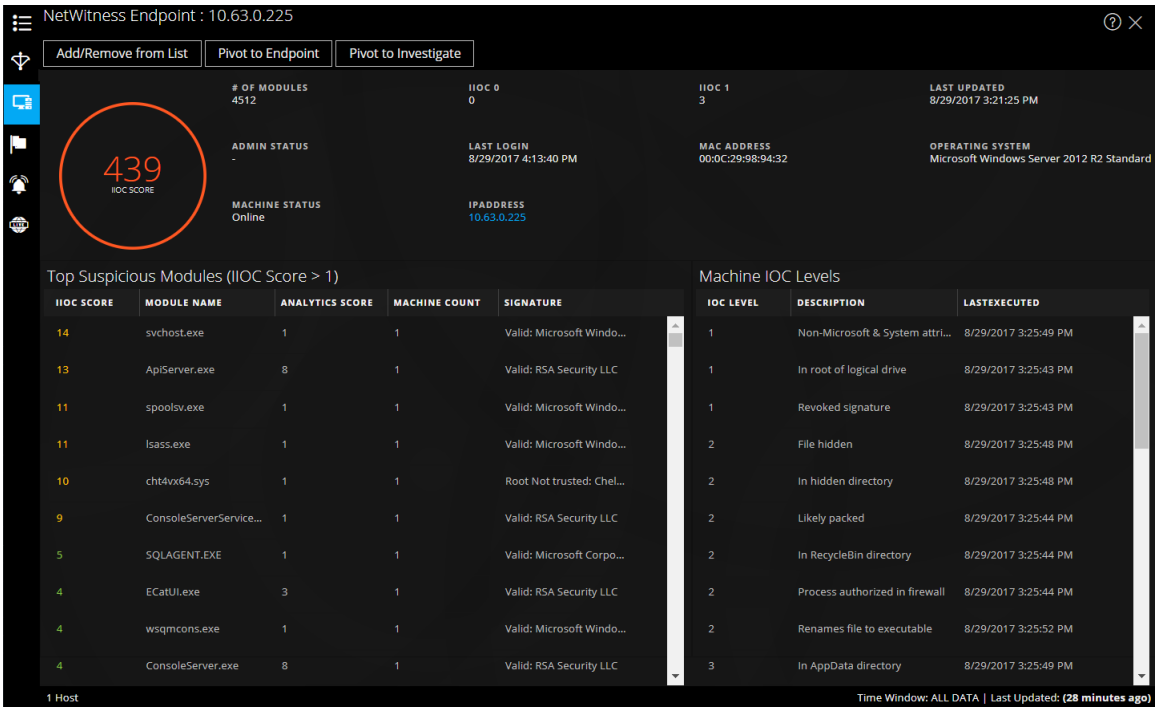
Les informations suivantes s'affichent pour Active Directory.

Champ	Description
Nom d'affichage	Nom de l'utilisateur.
ID de l'employé	ID d'employé de l'utilisateur.
Tél.	Le numéro de téléphone mobile de l'utilisateur.
E-mail	L'identifiant e-mail de l'utilisateur
ID utilisateur AD	L'identification unique de l'utilisateur spécifique au sein d'une organisation.
Poste	La désignation de l'utilisateur.
Gestionnaire	Nom du responsable de l'utilisateur.
Groupes	La liste des groupes dont l'utilisateur est membre.
Entreprise	Nom de l'entreprise de l'utilisateur.

Champ	Description
Département	Le nom du département de l'organisation auquel appartient l'utilisateur.
Lieu	L'emplacement physique de l'utilisateur.
Dernière connexion	L'heure à laquelle l'utilisateur s'est connecté au système, uniquement si le Catalogue global est défini.
Horodatage de la dernière connexion	L'heure à laquelle l'utilisateur s'est connecté au système.
Nom unique	Le nom unique attribué à l'utilisateur.
Décompte	Nombre d'utilisateurs
Période	La fenêtre Période se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, toutes les données Active Directory sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

Onglet NetWitness Endpoint

La figure suivante offre un exemple du panneau Recherche contextuelle pour NetWitness Endpoint.



Les informations suivantes s'affichent pour IIOC.

Champ	Description
Nbre de modules	Le nombre de modules sur lesquels porte la recherche.
État admin	L'état Admin (le cas échéant)
Dernière mise à jour	L'heure de la dernière actualisation des données.
Dernière connexion	L'heure à laquelle l'utilisateur s'est connecté pour la dernière fois.
Adresse MAC	L'adresse MAC de la machine.
Système d'exploitation	La version du système d'exploitation utilisé par la machine NetWitness Endpoint.
État de l'ordinateur	L'état du module actuellement visionné : En ligne, hors ligne, actif ou inactif.
Adresse IP	L'adresse IP du module spécifique.

Les informations suivantes s'affichent pour les modules.

Champ	Description
Score IIOC	Le score IIOC de la machine est un score agrégé basé sur les scores des modules. Cet élément se base sur la valeur définie dans le champ « Valeur IIOC minimale » de la boîte de dialogue Paramètres de source de données pour Context Hub. La valeur par défaut pour la « Valeur IIOC minimale » est de 500. Consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.
Nom du module	Le nom du module qui est consulté.
Score d'analyse	Le nombre de fichiers actifs pour la machine sélectionnée.
Nombre de machines	Le nombre de machines sur lesquelles cet IOC particulier a été déclenché.
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires. Par exemple, Google, Apple, etc.

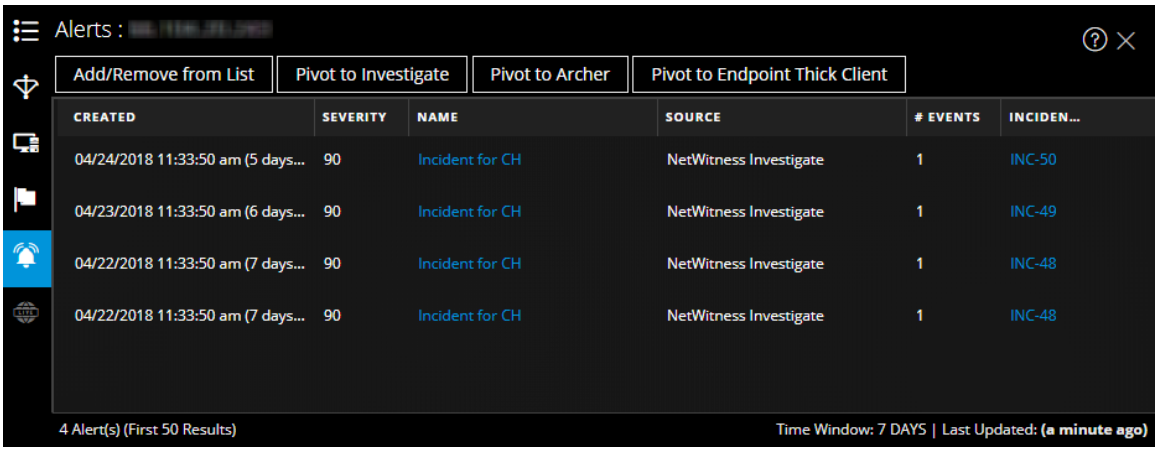
Les informations suivantes s'affichent pour les machines.

Champ	Description
Niveaux IOC	Les niveaux IOC.
Description	La description des niveaux IOC, le cas échéant.
Dernière exécution	L'heure à laquelle la tâche a été exécutée.
Décompte	Le nombre d'hôtes sur lesquels porte la recherche.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, toutes les données NetWitness Endpointsont extraites.

Champ	Description
Dernière mise à jour	Le moment de la dernière mise à jour des résultats de l'analyse dans la base de données NetWitness Endpoint.

Onglet Alertes

La figure suivante est un exemple du panneau contextuel pour Alerts qui s'affiche en fonction de l'heure (du plus récent au plus ancien), puis de l'état de gravité.

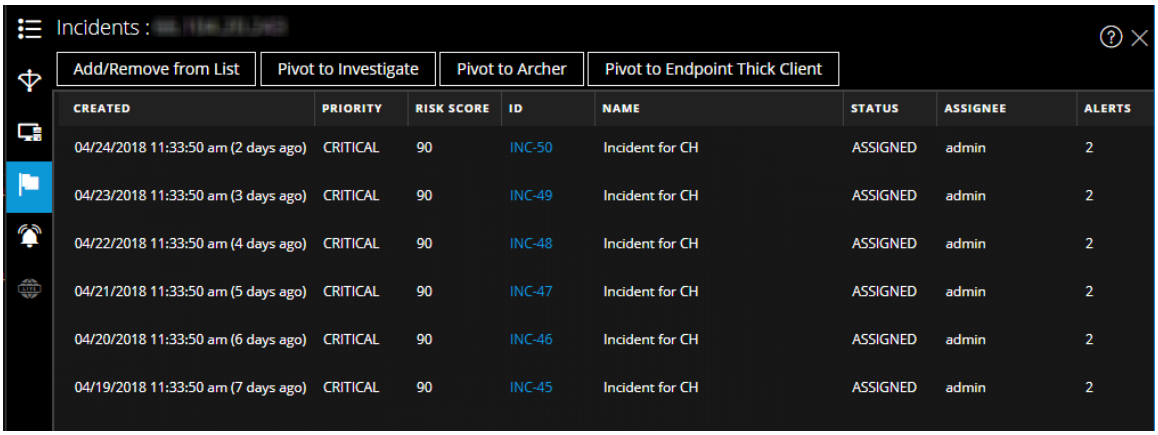


Le panneau Recherche contextuelle des alertes affiche les informations suivantes.

Champ	Description
Créé	La date et l'heure de création de l'alerte.
Gravité	La valeur de gravité des alertes.
Nom	Nom de l'alerte. Vous pouvez cliquer sur le nom pour afficher les détails d'une alerte spécifique.
Source	Le nom de la source de l'alerte à partir du déclenchement de l'alerte.
Événements	Le nombre d'événements associés à l'alerte.
ID d'incident	L'ID de l'incident associé à l'alerte (le cas échéant). Vous pouvez cliquer sur l'ID pour afficher les détails d'une alerte spécifique.
Décompte	Le nombre d'alertes Par défaut, seules les 100 premières alertes sont affichées. Pour plus d'informations sur la façon de configurer les paramètres, consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, les données d'alerte pour les 7 derniers jours sont extraites.
Dernière mise à jour	Indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois.

Onglet Incidents

La figure suivante est un exemple du panneau contextuel des incidents qui s'affiche en fonction de l'heure (du plus récent au plus ancien), puis de l'état de priorité.

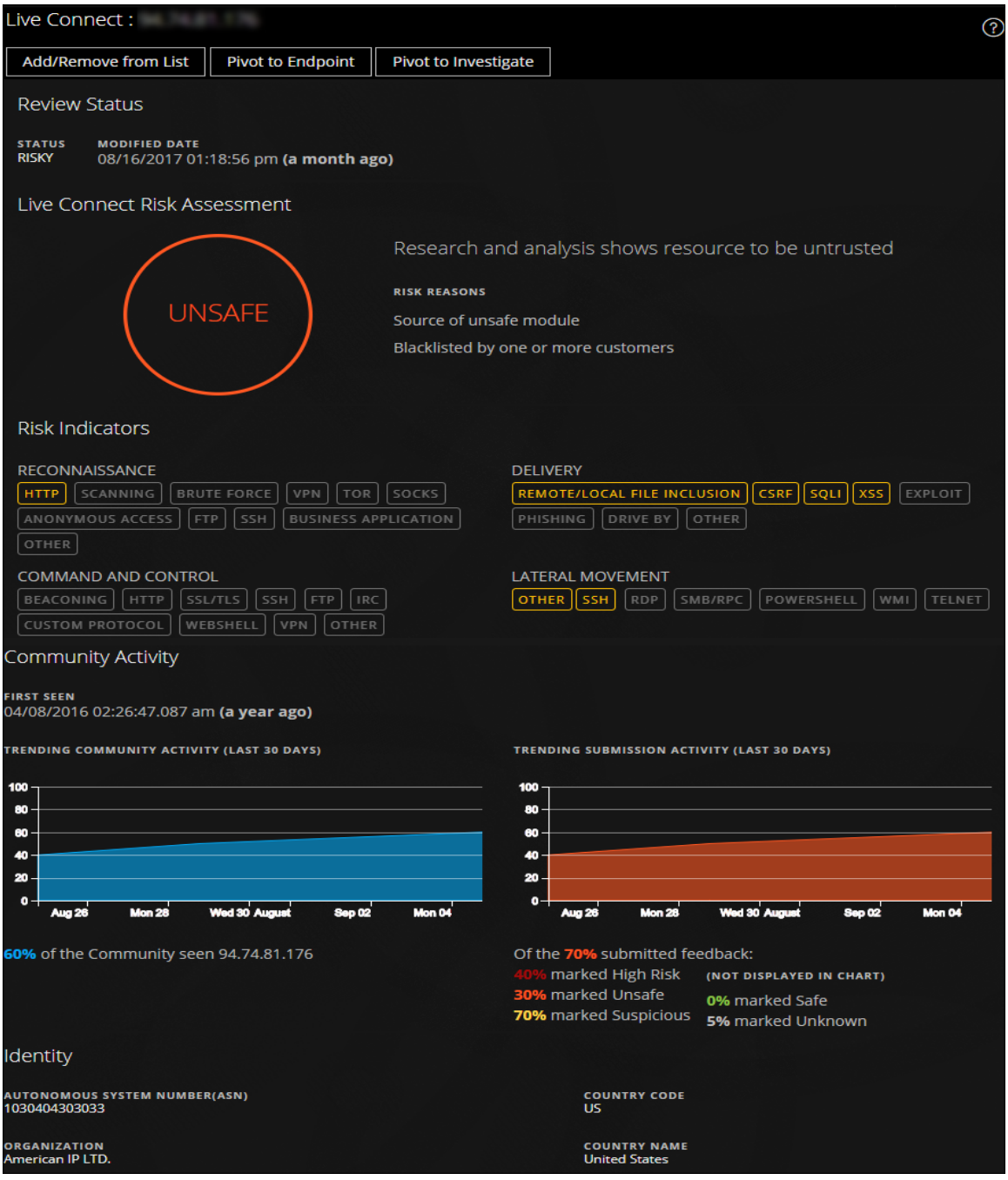


Le panneau Recherche contextuelle des incidents affiche les informations suivantes.

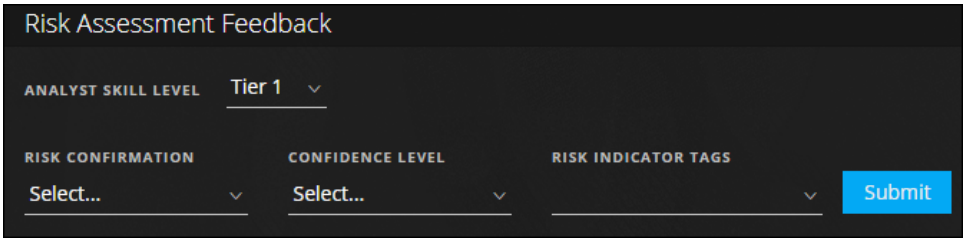
Champ	Description
Créé	La date de création de l'incident
Priorité	L'état de priorité des incidents
Valeur de risque	La valeur de risque des incidents
ID	L'ID de l'incident. Vous pouvez cliquer sur cet ID pour afficher les détails de l'incident.
Nom	Nom de l'incident.
État	L'état de l'incident.
Personne affectée	Le propriétaire actuel de l'incident
Alertes	Le nombre d'alertes associées à l'incident
Décompte	Le nombre d'incidents Par défaut, seuls les 100 premiers incidents sont affichés. Pour plus d'informations sur la façon de configurer les paramètres, consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, les données d'alerte pour les 7 derniers jours sont extraites.
Dernière mise à jour	Indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois.

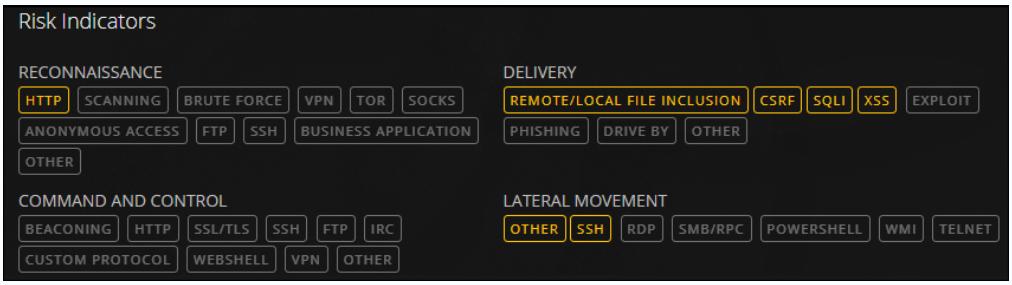
Onglet Live Connect

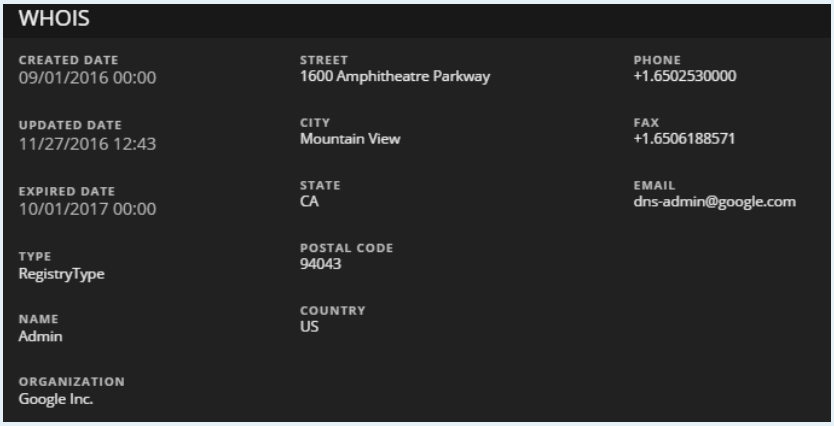
La figure suivante est un exemple de panneau Contexte pour Live Connect, et le tableau décrit les informations affichées.

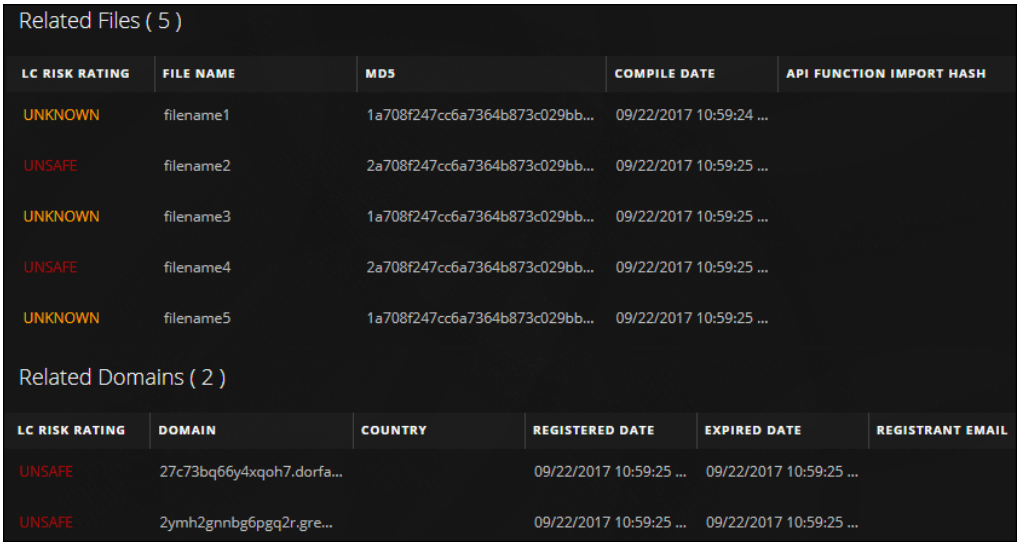


Champ	Description
État de révision	L'état de révision de l'entité Live Connect sélectionnée (IP, fichier ou domaine) en fonction de l'activité des analystes. Cela permet d'avoir une visibilité sur l'activité des analystes au sein d'une organisation. **État** Voici les types d'état : • **Nouveau :** Les résultats d'une recherche pour une adresse IP sont affichés pour la première fois au sein de l'organisation. • **Affiché :** Un analyste de l'organisation a déjà affiché les résultats d'une recherche pour une adresse IP. • **Marqué comme étant Sûr :** Un analyste de l'organisation a déjà affiché les résultats d'une recherche et marqué l'adresse IP comme étant sûre. • **Marqué comme étant Risqué :** Un analyste de l'organisation a déjà affiché les résultats d'une recherche et marqué l'adresse IP comme étant risquée.
Évaluation des risques	L'évaluation des risques concernant l'entité Live Connect sélectionnée (IP, fichier ou domaine) en fonction des commentaires des analystes et de l'analyse Live Connect. Les catégories d'évaluation des risques sont les suivantes : • **Sûr :** L'entité Live Connect est considérée comme sûre. • **Inconnu :** Live Connect ne dispose pas de suffisamment d'informations relatives à cette entité pour calculer le risque. • **Risque élevé** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. Les entités marquées comme étant à « Risque élevé » requièrent votre attention immédiate. • **Suspect** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'analyse indique une activité potentiellement menaçante qui nécessite une action. • **Dangereux :** Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'entité est classée comme étant à risque élevé, suspecte ou dangereuse et affiche les motifs de risque associés en conséquence.

Champ	Description
Commentaires sur l'évaluation des risques	 Commentaires sur l'évaluation des risques permettant à l'analyste d'envoyer des commentaires de renseignements sur les menaces concernant une entité au serveur Live Connect. • **Niveau de compétence de l'analyste** Vous trouverez ci-dessous des options relatives au niveau de compétence de l'analyste : ◦ **Niveau 1** - Les analystes de ce niveau définissent les procédures de correction et décident si un incident doit être transféré à d'autres zones d'un SOC (Centre des opérations de sécurité). Il s'agit de la valeur par défaut. ◦ **Niveau 2** - Les analystes examinent les incidents et capturent les renseignements à partir d'une procédure d'enquête pour générer des commentaires dans différents flux de travail d'un SOC. ◦ **Niveau 3** - Les analystes partagent les résultats d'une procédure d'enquête avec l'organisation du SOC. En général, ils gèrent les incidents et disposent d'un large éventail de compétences et d'outils nécessaires pour répondre aux incidents. **Remarque :** Lors de la création d'un nouvel utilisateur pour NetWitness Platform (analyste), un administrateur doit être en mesure d'identifier l'utilisateur comme étant de niveau 1, de niveau 2 ou de niveau 3. • **Confirmation du risque** - Confirmation du risque pour l'entité Live Connect sélectionnée (IP, fichier ou domaine). Les catégories de confirmation du risque sont les suivantes : ◦ **Sûr** : L'entité Live Connect est considérée comme sûre. ◦ **Inconnu** : L'analyste n'a pas suffisamment d'informations pour fournir une confirmation de risque ◦ **Risque élevé** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. Les entités marquées comme étant à « Risque élevé » requièrent votre attention immédiate. ◦ **Suspect** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'analyse indique une activité potentiellement menaçante qui nécessite une action.

Champ	Description
	◦ **Dangereux** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. • **Niveau de confiance** - Le niveau de confiance d'un analyste fournissant des commentaires sur l'entité Live Connect. Les catégories de niveau de confiance sont les suivantes : Élevé, Moyen ou Faible • **Balises d'indication des risques** - Permet de sélectionner une catégorie de balise en fonction de l'analyse.
Activité de la communauté	Activités de la communauté, telles que : • Date du premier affichage dans la communauté. • Heure du premier affichage de l'adresse IP/du fichier/du domaine (heure actuelle - heure du premier affichage). **Tendance de l'activité de la communauté :** Si l'adresse IP est connue au sein de la communauté RSA, une représentation graphique de la tendance de l'activité de la communauté s'affiche pour les éléments suivants : • Utilisateurs (en %) ayant déjà consulté l'adresse IP dans la communauté Live Connect. • Utilisateurs (en %) ayant envoyé des commentaires pour l'adresse IP. • Utilisateurs (en %) ayant marqué l'adresse IP comme dangereuse.
Indicateurs de risque	 Les indicateurs de risque sont mis en surbrillance en fonction des balises qui sont affectées par la communauté aux entités (adresses IP, fichiers ou domaines). Les balises sont classées comme suit : Reconnaissance, Livraison, Commande et Contrôle, Mouvement latéral, Utilisation de niveaux de privilège excessifs, et Emballage et exfiltration. Ces balises sont des exemples et varient selon les entrées reçues de la communauté sur le serveur Live Connect. L'analyste peut choisir les balises d'indication des risques appropriées tout en fournissant les commentaires de révision. Les balises mises en surbrillance indiquent que l'entité sélectionnée est associée à cette catégorie et à cette balise en particulier. Le fait de cliquer sur les balises mises en surbrillance affiche la description de la balise.

Champ	Description
Identité	Fournit les informations d'identité suivantes pour l'entité ou la métadonnée sélectionnée : Pour l'adresse IP : Numéro de système autonome (ASN), préfixe, code du pays et nom du pays, inscrit (Organisation) et date. Pour le hachage de fichier : Nom de fichier, taille du fichier, MD5, SH1, SH256, temps de compilation et type MIME. Pour le domaine : Nom de domaine et adresse IP associée.
Informations sur le certificat	Fournit les informations suivantes sur le certificat pour le hachage de fichier sélectionné : Émetteur de certificat, validité du certificat, algorithme de signature et numéro de série du certificat.
Informations WHO IS	 Les informations **WHO IS** fournissent les détails de la propriété d'un domaine donné. Les informations suivantes concernant le propriétaire du domaine s'affichent : Date de création, date de mise à jour, date d'expiration, type (type d'enregistrement), nom, organisation, adresse avec code postal, pays, téléphone, télécopie et courriel.
Fichiers associés	Les fichiers associés sont affichés pour les types d'entités IP et domaine. Une liste de fichiers associés connus est affichée, avec les informations suivantes : Évaluation du risque Live Connect (sûr, risqué ou inconnu), nom de fichier, MD5, heure et date de compilation, fonction API, hachage d'importation et type MIME.
Domaines connexes	Les domaines connexes sont affichés pour les types d'entités IP et domaine. Une liste de domaines connexes connus est affichée, avec les informations suivantes : Évaluation du risque Live Connect (sûr, risqué ou inconnu), nom de domaine, nom du pays, date d'enregistrement, date d'expiration et adresse E-mail de l'inscrit.

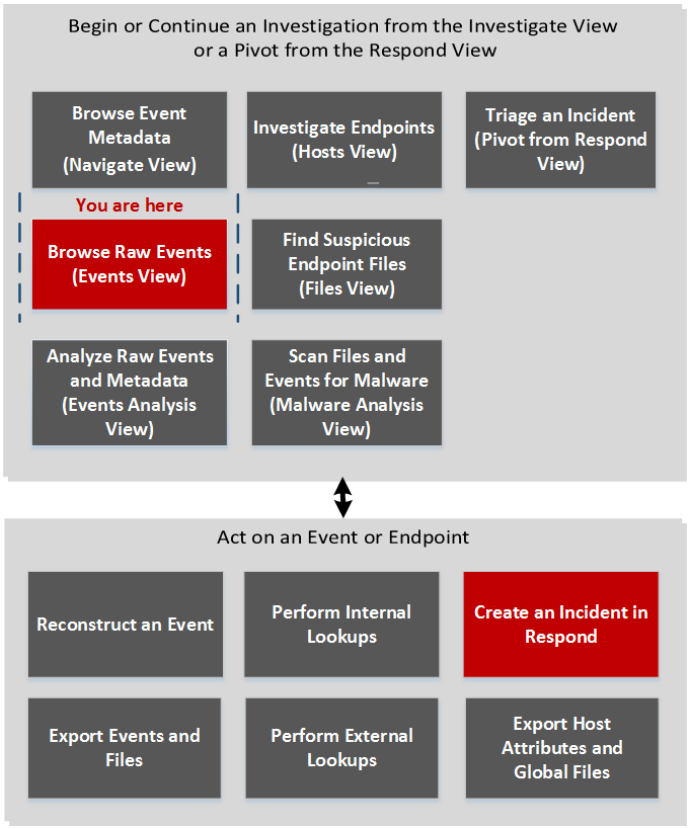
Champ	Description
Adresses IP connexes	 Les adresses IP associées sont affichées pour les types d'entités Domaine et Fichiers. Une liste d'adresses IP associées connues est affichée, avec les informations suivantes : Évaluation du risque Live Connect (sûr, risqué ou inconnu), adresse IP, nom de domaine, code et nom du pays, nom du pays, date d'enregistrement, date d'expiration et adresse E-mail de l’inscrit.

Boîte de dialogue Créer un incident

Dans la boîte de dialogue Créer un incident, les analystes peuvent créer un incident à partir des événements sélectionnés dans la vue Événements. L'incident est alors disponible pour les responsables de la réponse aux incidents qui utilisent Respond.

Pour accéder à cette boîte de dialogue, lors de la recherche d'un service sous Investigation > vue Événements, sélectionnez **Incidents > Créer un nouvel incident** dans la barre d'outils.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

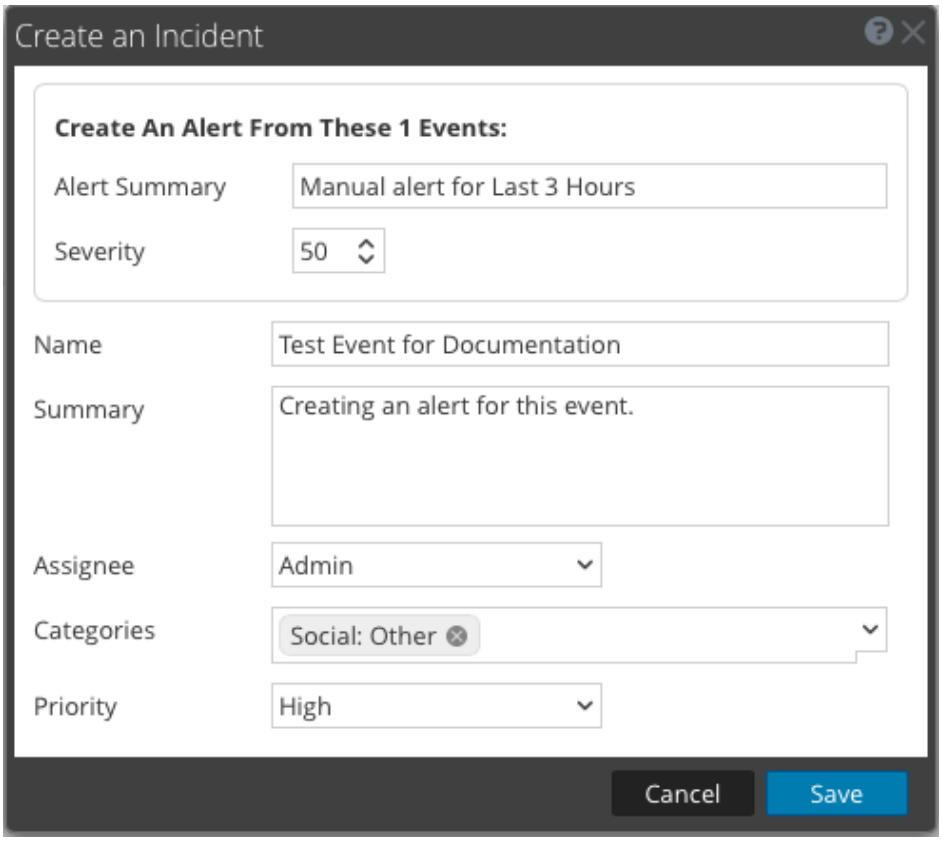
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces ou Responsable de la réponse aux incidents	ajouter un ou plusieurs événements à un incident existant ou à un nouvel incident*	Ajouter des événements à un incident pour obtenir une réponse

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Naviguer
- Vue Événements

Aperçu rapide

La figure suivante est un exemple de la boîte de dialogue Créer un incident. Les fonctions sont décrites dans le tableau.



Fonctionnalité	Description
Créer un résumé à partir de ces événements	Le champ Récapitulatif de l'alerte est rempli par la requête qui a produit les alertes que vous avez sélectionnées pour créer cet incident. Le champ Gravité reflète la gravité de l'alerte sélectionnée, soit un nombre entier compris entre 1 et 100.
Nom	(Obligatoire) Nom désignant l'incident. Dans cet exemple, le nom est Exemple d'incident. Vous pouvez fournir un nom qui identifie clairement la nature des événements qui seront ajoutés à cet incident.
Résumé	(Facultatif) Description de l'incident. Un bon résumé identifie clairement l'incident pour les analystes et les répondants.
Personne affectée	(Facultatif) Affecte l'incident à un utilisateur dans le SOC. Permet d'ouvrir la liste déroulante affichant les noms d'utilisateur du personnel SOC qui répond aux incidents.
Catégories	(Facultatif) Identifie les catégories d'incidents. Permet d'ouvrir la liste déroulante des catégories et sous-catégories d'incidents. Vous pouvez sélectionner une ou plusieurs catégories auxquelles l'incident appartient. Les catégories sont réparties entre ces principaux groupes : Environnement, Erreur, Piratage, Malware, Utilisation incorrecte et Social.
Priorité	Identifie la priorité de l'incident. Permet d'ouvrir la liste déroulante des priorités : Critique, Élevé, Moyen ou Faible.

Fonctionnalité	Description
Annuler	Ferme la boîte de dialogue sans enregistrer les modifications.
Enregistrer	Enregistre l'incident et ferme la boîte de dialogue. Un message confirme que l'incident a été correctement créé.

Vue Analyse d'événements

Dans la vue Analyse d'événements, les analystes peuvent visualiser les métadonnées et les événements bruts grâce aux fonctions interactives qui améliorent la capacité à déceler des schémas significatifs dans les données. Il s'agit d'une solution alternative à la vue statique Reconstruction d'événement. Vous pouvez examiner les événements liés au réseau, aux logs et aux points de terminaison dans la vue Analyse d'événements. La vue Analyse d'événements propose la reconstruction des paquets, des textes et des logs, mais ne prend pas directement en charge la reconstruction par courrier électronique et Web. Toutefois, dans la version 11.1 ou supérieure, vous pouvez ouvrir une reconstruction des résultats actuels par courrier électronique et Web dans la vue Événements.

Remarque : L'administrateur attribue aux analystes les autorisations d'accès à cette vue. Si votre administrateur ne vous a pas octroyé d'accès et que vous accédez à la vue Analyse d'événements d'une manière ou d'une autre, le message suivant s'affichera : `Forbidden. You cannot access the requested page.` Par exemple, si vous visualisez une reconstruction de la vue Événements et que vous tentez d'afficher la même reconstruction dans la vue Analyse d'événements, le message `Forbidden` s'affichera.

Les événements affichés dans la vue Analyse d'événements concernent le point d'extraction actuel dans la vue Vue Naviguer ou Événements. À partir de la version 11.1, les événements peuvent correspondre aux résultats d'une requête saisie dans le fil d'Ariane de la vue Analyse d'événements. Quelle que soit la source de la requête, la vue Analyse d'événements affiche les événements dans l'ordre chronologique. Vous pouvez réorganiser et redimensionner les colonnes. Dans la version 11.1 ou supérieure, vous pouvez également choisir les colonnes que vous souhaitez afficher, et sélectionner l'un des groupes de colonnes intégrés ou un groupe de colonnes personnalisé.

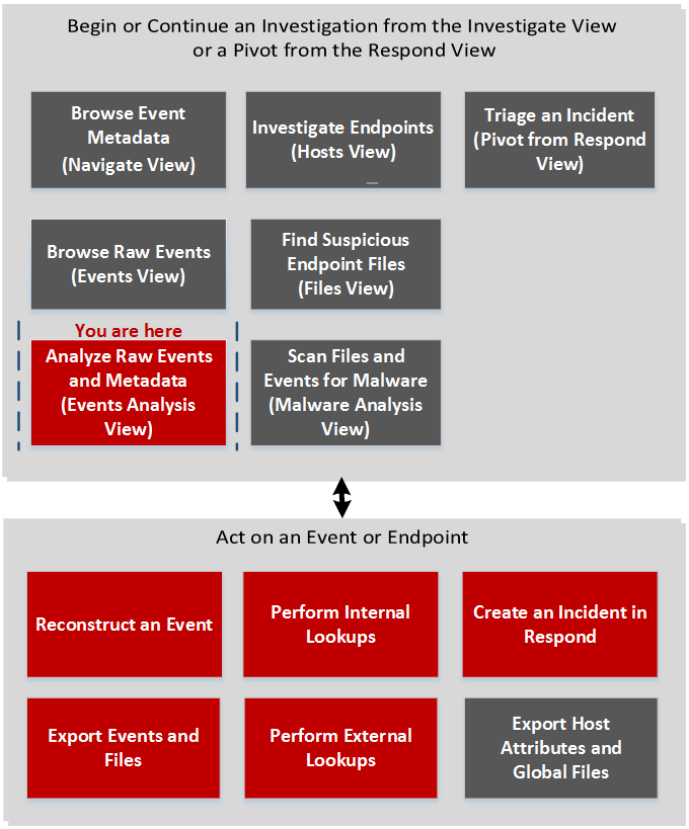
Lorsque vous cliquez sur un événement, le panneau Détails des événements réseau, Détails des événements de consignation ou Détails des événements liés aux points de terminaison s'ouvre dans la même fenêtre de navigateur. Chaque type d'événement comprend un ou plusieurs types d'analyse : Analyse de texte, Analyse de paquets et Analyse de fichiers.

Plusieurs points d'accès à cette vue sont décrits dans la section Commencer une procédure d'enquête dans la vue Analyse d'événements.

Remarque : Si vous accédez à Analyse des événements à partir de la vue Répondre, vous pouvez voir l'analyse d'événement pour un événement sélectionné dans un incident ; les options sont un sous-ensemble des options disponibles lorsque vous ouvrez un événement à partir de la vue Enquêter. Pour obtenir des fonctionnalités complètes et examiner d'autres événements, vous pouvez accéder directement à la vue Analyse des événements (ENQUÊTER > Analyse d'événements).

Workflow

La figure suivante procure une vue générale du workflow illustrant les tâches que vous pouvez effectuer dans NetWitness Investigate, avec les tâches de la vue Analyse d'événements mises en surbrillance en rouge.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts*	Commencer une procédure d'enquête dans la vue Analyse d'événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	rechercher des événements dans la vue Analyse d'événements (Version 11.1)*	Filtrer les résultats dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter les événements et fichiers dans la vue Analyse d'événements*	Télécharger des données dans la vue Analyse d'événements
Responsable de la recherche des menaces	reconstruire des événements dans la vue Analyse d'événements*	Examiner les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	effectuer des recherches externes à partir de la vue Analyse d'événements (Version 11.1)*	Agir sur les données dans la vue Analyse d'événements
Responsable de la recherche des menaces	rechercher des événements dans la vue Naviguer	Procédure d'enquête relative aux métadonnées dans la vue Naviguer
Responsable de la recherche des menaces	rechercher des événements dans la vue Événements	Examiner les événements bruts dans la vue Événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements - Panneau Analyse de paquets
- Vue Analyse d'événements - Panneau Analyse de texte
- Vue Analyse d'événements - Panneau Analyse de fichiers

Aperçu rapide

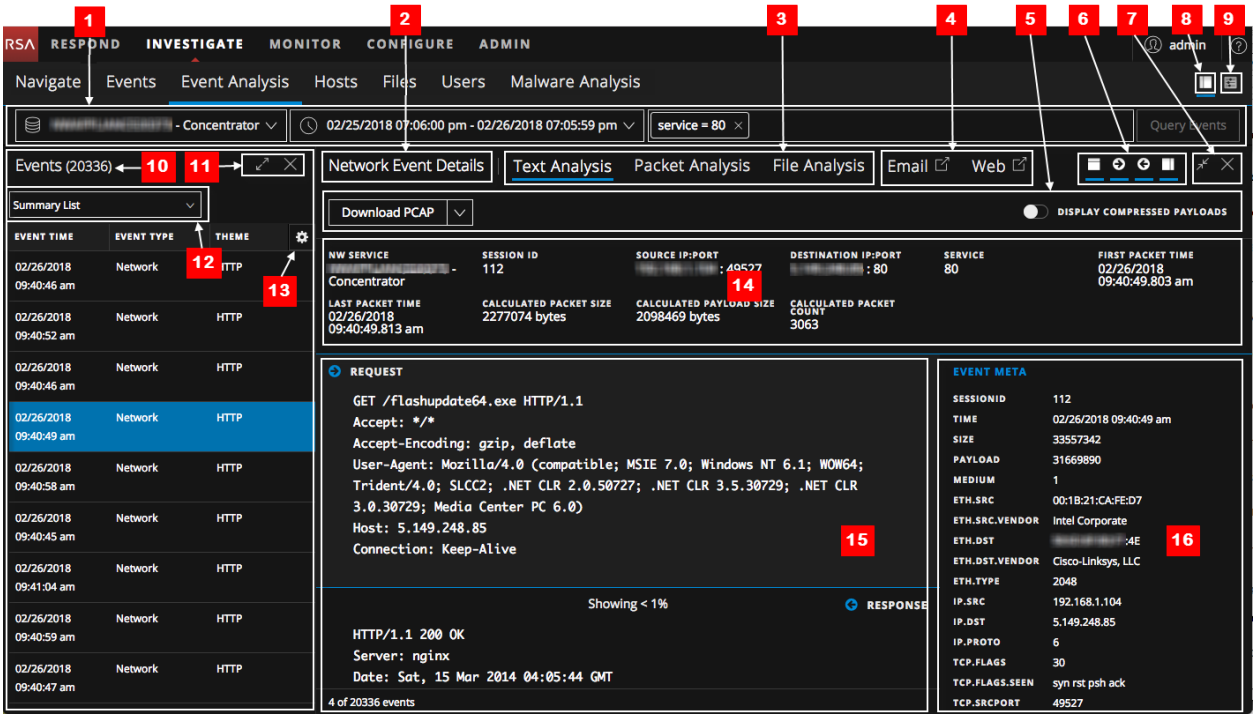
Lorsque vous ouvrez Investigate pour la première fois, les champs de saisie d'une requête s'affichent afin que vous puissiez sélectionner un service avec une période, et saisir une requête facultative.

- La version 11.0 propose des champs de saisie dans les vues Naviguer et Événements.
- La version 11.1 propose des champs de saisie dans les vues Naviguer, Événements et Analyse d'événements.

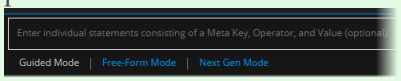
Lorsque vous ouvrez un point d'extraction dans la vue Analyse d'événements, le service en cours d'investigation compte les résultats de la requête initiale dans une limite de 100 000 événements et les 100 premiers événements (paquets, logs et points de terminaison) sont chargés dans le panneau Événements. Les colonnes du panneau Événements sont les suivantes : Heure de l'événement, Type d'événement (Réseau, Log ou Point de terminaison), Taille des événements et Récapitulatif. Vous pouvez :

- Faire défiler la liste, puis cliquer sur **Charger davantage** pour consulter les 100 événements suivants.
- Sélectionner un groupe de colonnes (Version 11.1 ou supérieure).
- Sélectionner les colonnes que vous souhaitez inclure (Version 11.1 ou supérieure).
- Faire glisser les colonnes pour les réorganiser.
- Rendre les colonnes plus larges ou plus étroites.
- Afficher l'analyse d'un événement.

La figure suivante met en évidence les principales caractéristiques de la vue Analyse d'événements pour la version 11.1 ou supérieure.



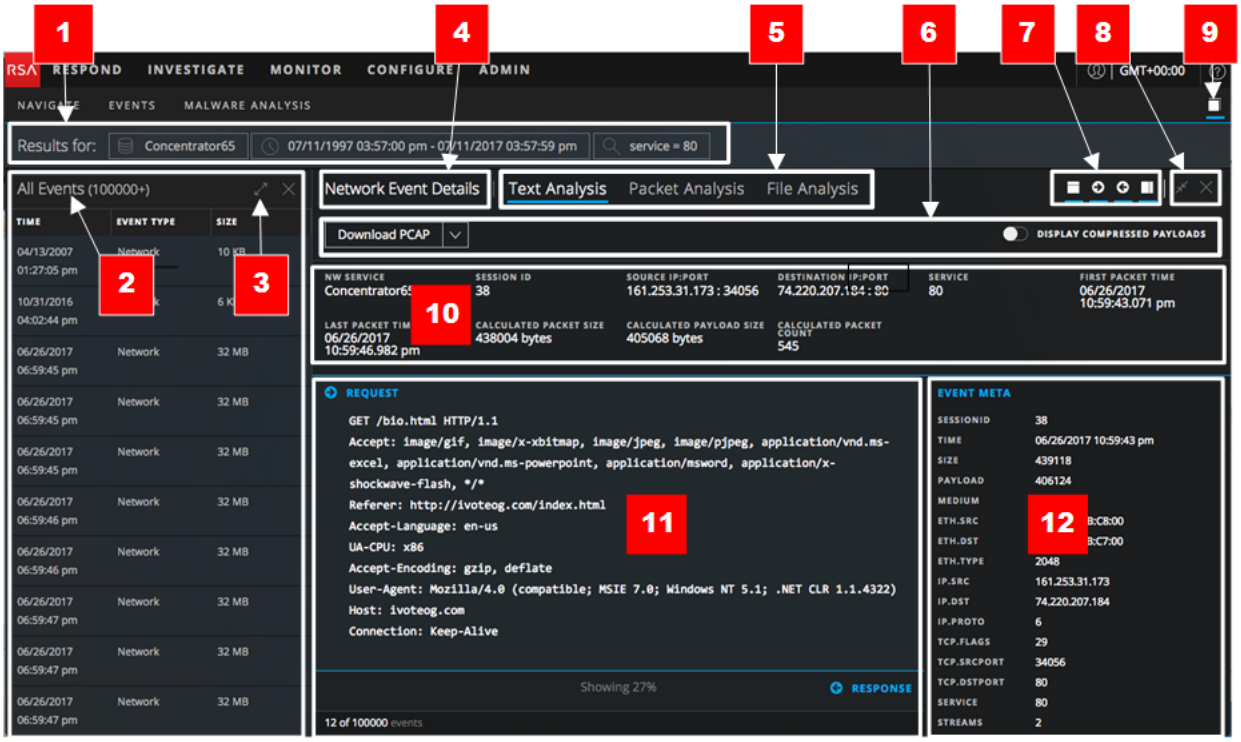
Remarque : La version 11.2 comprenait une fonctionnalité bêta non documentée, appelée mode Next Gen, dans le générateur de requêtes de la vue Analyse d'événements qui était encore en cours de développement et de test ; Le mode Next Gen suivant a été désactivé dans le correctif 11.2.0.1. Si vous voyez le mode Next Gen ne l'utilisez pas ; vous devez utiliser uniquement le mode Guidé et le mode Formulaire libre dans le générateur de requêtes pour garantir des résultats cohérents et prévisibles.



1	**Fil d'Ariane interactif** : Lorsqu'un service est sélectionné, le sélecteur de service, le sélecteur de période et les requêtes que vous avez saisies s'affichent. Dans la version 11.1 ou supérieure, vous pouvez sélectionner un service, comme décrit dans la section Commencer une procédure d'enquête dans la vue Analyse d'événements et affiner la requête, comme décrit dans Filtrer les résultats dans la vue Analyse d'événements. En cliquant sur le bouton **Envoyer une requête**, une demande est envoyée au service sélectionné afin que les données soient chargées.
2	Le type d'événement en cours d'analyse est reflété dans l'en-tête : **Détails des événements réseau**, **Détails des événements de consignation** ou **Détails des événements liés aux points de terminaison**. Chaque vue est décrite en détail dans Examiner les événements dans la vue Analyse d'événements.
3	Les types d'analyse disponibles pour le type d'événement. Les événements réseau peuvent utiliser tous les types d'analyse : texte, paquet et fichier. Les événements de log et de point de terminaison utilisent l'analyse de texte uniquement.
4	Les types d'analyse E-mail et Web ouvrent l'événement en cours sous la forme d'une reconstruction par e-mail ou par Web dans la vue Evénements.
5	Ces options varient en fonction de différents types d'analyse. Elles sont décrites en détail dans Examiner les événements dans la vue Analyse d'événements.

6	Commandes permettant d'afficher ou de masquer l'en-tête d'événement, d'afficher ou masquer des demandes et réponses et d'ouvrir le panneau Méta de l'événement (16). Ces commandes sont décrites dans Examiner les événements dans la vue Analyse d'événements.
7, 11	Commandes permettant de modifier la taille du panneau et de fermer le panneau.
8	Ouvrez à nouveau le panneau Événements ou Panneau Méta de l'événement si vous l'avez fermé.
9	Définit les préférences de la vue Analyse d'événements (voir Configurer la vue Analyse d'événements.
10	Le panneau Événements de la version 11.1 est interactif et affiche les résultats de requête lorsque vous envoyez des requêtes mises à jour. Le panneau Événements indique le nombre d'événements. Vous pouvez réorganiser et redimensionner les colonnes. Vous pouvez faire défiler la liste jusqu'en bas et charger plus d'événements (reportez-vous à la section Examiner les événements dans la vue Analyse d'événements).
12	La liste déroulante Groupe de colonnes affiche les groupes de colonnes intégrés et personnalisés que vous pouvez appliquer au panneau Evénements. Les groupes de colonnes intégrés sont les suivants : Analyse des e-mails, Analyse des points de terminaison, Analyse des programmes malveillants, HTTP sortant, SSL/TLS sortant et Liste récapitulative. Liste récapitulative est le groupe de colonnes par défaut.
13	Paramètres de sélection des colonnes incluses dans le panneau Événements.
14	En-tête d'événement fournissant des informations récapitulatives sur l'événement. Ces informations varient en fonction des différents types d'événement (paquet, log et point de terminaison).
15	Les données d'événement (parfois appelées une charge utile pour les paquets). Les données d'événement pour un événement de log ou de point de terminaison sont généralement une ligne de texte du log brut plutôt qu'une demande et une réponse affichées pour un paquet.
16	Le Panneau Méta de l'événement répertorie les clés méta et les métavaleurs contenues dans les données. Certaines métadonnées sont disponibles pour la recherche ; elles ont une icône de jumelles sur laquelle vous pouvez cliquer pour afficher les données associées en surbrillance dans les données d'événements (reportez-vous à la section Examiner les événements dans la vue Analyse d'événements.

La figure suivante met en évidence les principales caractéristiques de la vue Analyse d'événements pour la version 11.0.0.x.



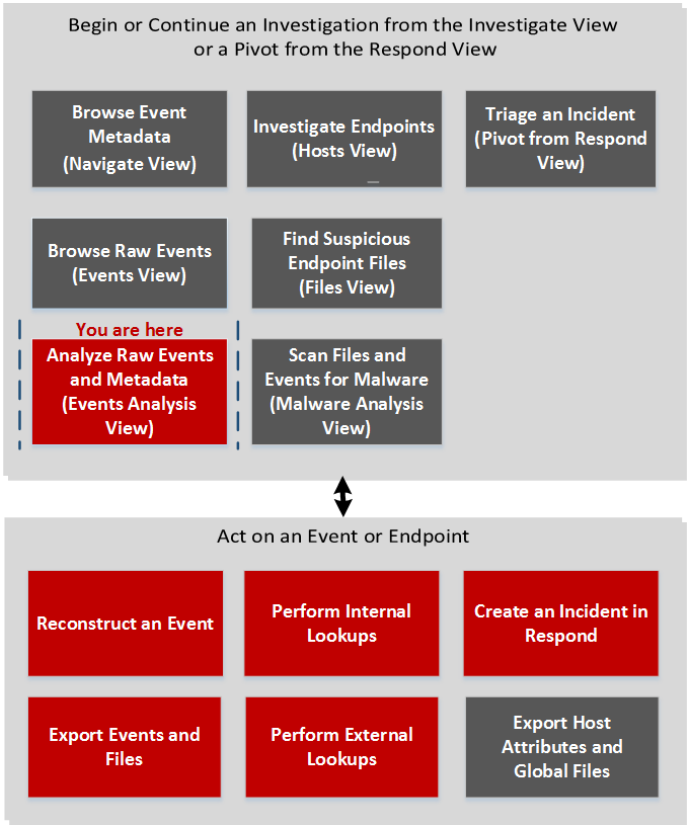
1	Le fil d'Ariane en lecture seule affiche le service et la période sélectionnés, ainsi que la requête saisie dans la vue Naviguer ou la vue Événements.
2	Il s'agit d'une liste en lecture seule des événements en fonction de la requête effectuée dans la vue Naviguer ou la vue Événements. Le panneau Événements indique le nombre d'événements. Vous pouvez réorganiser et redimensionner les colonnes. Vous pouvez faire défiler la liste jusqu'en bas et charger plus d'événements (reportez-vous à la section Examiner les événements dans la vue Analyse d'événements).
3, 8	Commandes permettant de modifier la taille du panneau et de fermer le panneau.
4	Le type d'événement en cours d'analyse est reflété dans l'en-tête : Détails des événements réseau, Détails des événements de consignation ou Détails des événements liés aux points de terminaison. Chaque vue est décrite en détail dans Examiner les événements dans la vue Analyse d'événements.
5	Les types d'analyse disponibles pour le type d'événement. Les événements réseau peuvent utiliser les trois types d'analyse : de texte, de paquets et de fichiers. Les événements de log et de point de terminaison utilisent l'analyse de texte uniquement.
6	Ces options varient en fonction de différents types d'analyse. Elles sont décrites en détail dans Examiner les événements dans la vue Analyse d'événements.
7	Commandes permettant d'afficher ou de masquer l'en-tête d'événement, d'afficher ou masquer des demandes et réponses et d'ouvrir le panneau Méta de l'événement (12). Ces commandes sont décrites dans Examiner les événements dans la vue Analyse d'événements.
9	Ouvrez à nouveau le panneau Événements ou Panneau Méta de l'événement si vous l'avez fermé.
10	En-tête d'événement fournissant des informations récapitulatives sur l'événement. Ces informations varient en fonction des différents types d'événement (paquet, log et point de terminaison).

11	Les données d'événement (parfois appelées une charge utile pour les paquets). Les données d'événement pour un événement de log ou de point de terminaison sont généralement une ligne de texte du log brut plutôt qu'une demande et une réponse affichées pour un paquet.
12	Le Panneau Méta de l'événement répertorie les clés méta et les métavaleurs contenues dans les données. Certaines métadonnées sont disponibles pour la recherche ; elles ont une icône de jumelles sur laquelle vous pouvez cliquer pour afficher les données associées en surbrillance dans les données d'événements (reportez-vous à la section Examiner les événements dans la vue Analyse d'événements.

Vue Analyse d'événements - Panneau Analyse de fichiers

Dans le Analyse de fichiers panneau (**Analyse d'événements** > **Analyse de fichiers),** , vous pouvez en toute sécurité afficher une liste de fichiers et télécharger un ou plusieurs fichiers dans un événement.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	interroger des événements dans la vue Analyse d'événements (Version 11.1)	Filtrer les résultats dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter les événements et fichiers dans la vue Analyse d'événements*	Télécharger des données dans la vue Analyse d'événements
Responsable de la recherche des menaces	reconstruire des événements dans la vue Analyse d'événements	Examiner les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	effectuer des recherches externes à partir de la vue Analyse d'événements (Version 11.1)	Agir sur les données dans la vue Analyse d'événements
Responsable de la recherche des menaces	interroger des événements dans la vue Naviguer	Procédure d'enquête relative aux métadonnées dans la vue Naviguer
Responsable de la recherche des menaces	rechercher des événements dans la vue Événements	Examiner les événements bruts dans la vue Événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle

Rubriques connexes

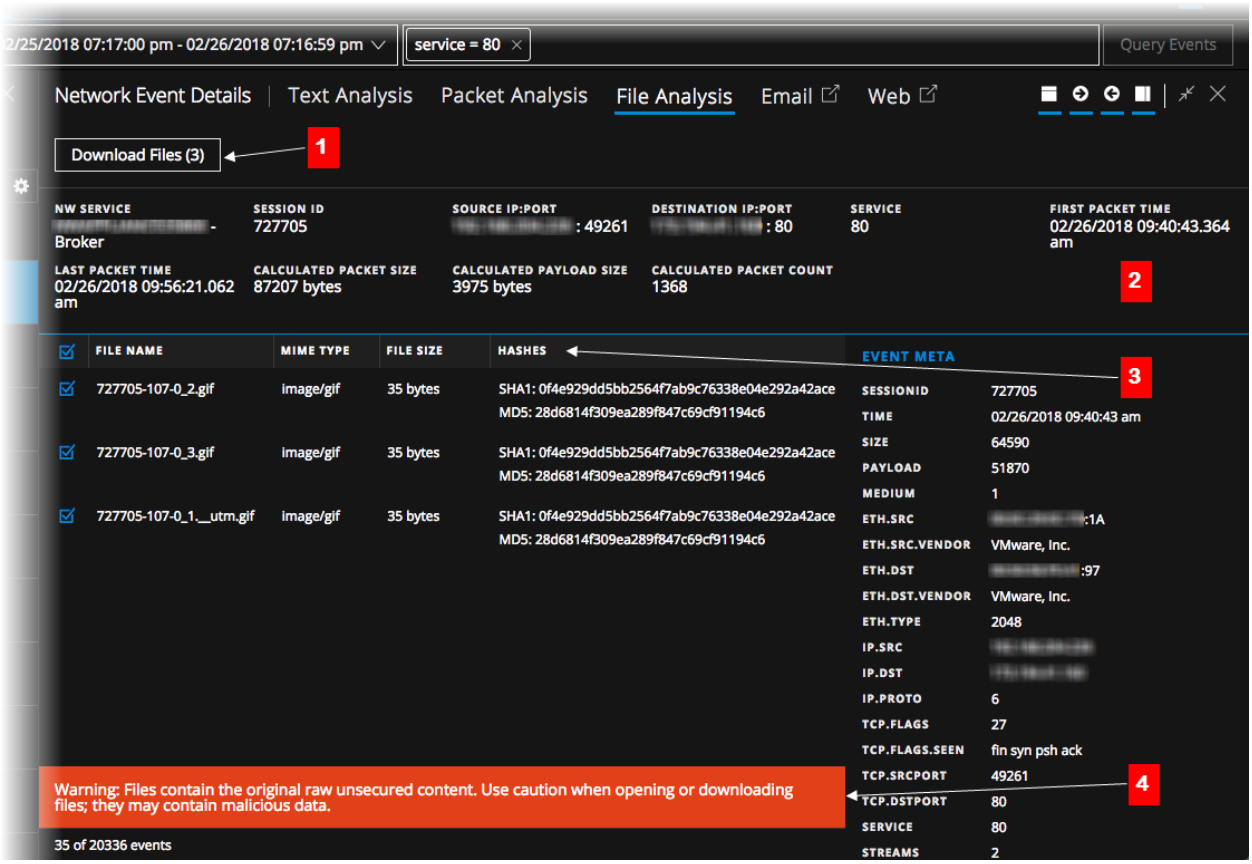
- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements
- Vue Analyse d'événements - Panneau Analyse de texte
- Vue Analyse d'événements - Panneau Analyse de paquets

Aperçu rapide

Le panneau Analyse de fichiers affiche une liste de fichiers associés à un événement réseau. Vous pouvez télécharger les fichiers dans cette vue.

Voici un exemple du Panneau Analyse de fichiers avec les fonctionnalités étiquetées.

Remarque : Les types de reconstruction par E-mail et Web en haut de la figure sont disponibles dans la version 11.1 ou supérieure.

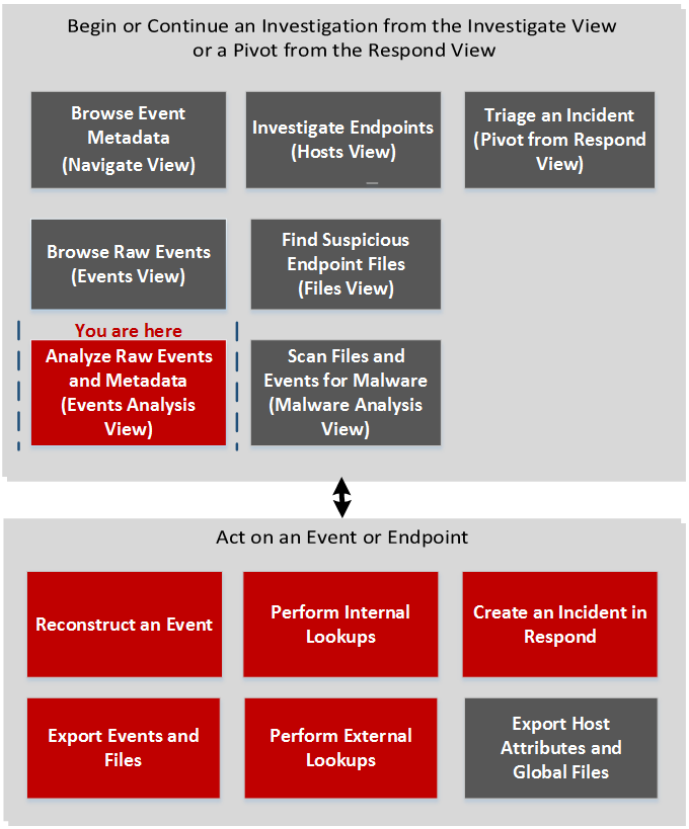


1	Cliquez pour télécharger un ou plusieurs fichiers sélectionnés.
2	L'en-tête d'événement affiche les informations récapitulatives de l'événement réseau qui contient les fichiers.
3	Liste déroulante des fichiers associés que vous pouvez sélectionner et télécharger.
4	Rappel qu'il est nécessaire de faire attention lorsque vous téléchargez des fichiers potentiellement malveillants.

Vue Analyse d'événements - Panneau Analyse de paquets

Dans le panneau Analyse de paquets (**Analyse d'événements > Analyse de paquets),** vous pouvez afficher et analyser de manière interactive et en toute sécurité les paquets et la charge utile d'un événement.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	interroger des événements dans la vue Analyse d'événements (Version 11.1)	Filtrer les résultats dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter les événements et fichiers dans la vue Analyse d'événements*	Télécharger des données dans la vue Analyse d'événements
Responsable de la recherche des menaces	reconstruire des événements dans la vue Analyse d'événements*	Examiner les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	effectuer des recherches externes à partir de la vue Analyse d'événements (Version 11.1)*	Agir sur les données dans la vue Analyse d'événements
Responsable de la recherche des menaces	interroger des événements dans la vue Naviguer	Procédure d'enquête relative aux métadonnées dans la vue Naviguer
Responsable de la recherche des menaces	rechercher des événements dans la vue Événements	Examiner les événements bruts dans la vue Événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements

- Vue Analyse d'événements - Panneau Analyse de texte
- Vue Analyse d'événements - Panneau Analyse de fichiers

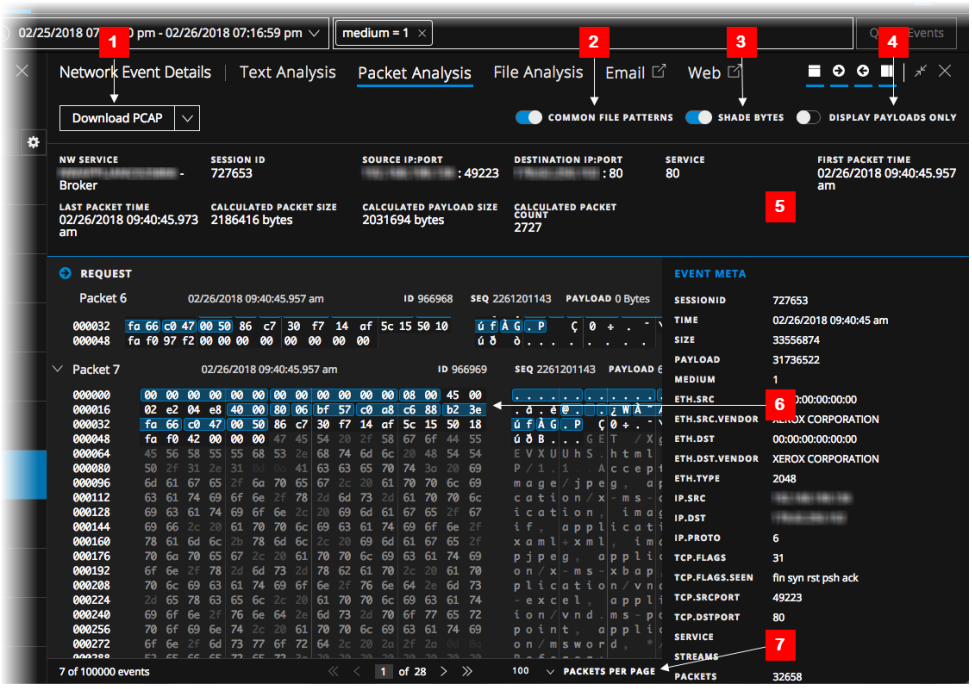
Aperçu rapide

Seuls les événements réseau peuvent être analysés dans le panneau Analyse de paquets. Le panneau Analyse de paquets répertorie chaque paquet de l'événement. La liste des paquets est déroulante. Lorsque vous faites défiler la liste, les informations relatives au paquet ou au texte ainsi que les libellés de requête et de réponse restent visibles, au lieu de quitter l'affichage.

Dans la version 11.1 ou supérieure, vous pouvez utiliser les commandes de pagination pour parcourir les pages, revenir à une page spécifique et sélectionner le nombre de paquets à afficher par page (100, 300 ou 500).

Chaque paquet s'affiche avec l'ombrage et la mise en surbrillance pour aider à identifier les modèles de fichiers communs : octets d'en-tête et de la charge utile significatifs, octets au format hexadécimal et ascii et des signatures de fichiers courants. En outre, vous pouvez ajuster l'affichage de la demande/réponse et afficher ou masquer le récapitulatif du paquet.

Voici un exemple du Panneau Analyse de paquets avec des étiquettes pour identifier les fonctionnalités. Pour plus d'informations et des exemples de chacune de ces fonctionnalités, reportez-vous à la section Examiner les événements dans la vue Analyse d'événements.



1	Options permettant d'exporter un événement réseau. Vous pouvez exporter un PCAP, toutes les charges utiles, charges utiles de demande ou charges utiles de réponse pour une analyse plus approfondie et partager avec d'autres utilisateurs.
2	L'option permettant d'identifier les signatures de fichiers courants est activée par défaut. Les signatures des fichiers courants sont mises en surbrillance en orange ; placer le curseur sur la mise en surbrillance révèle le type de fichier.
3	L'option Octets d'ombrage ajoute un ombrage pour identifier les différents octets hexadécimaux (00 à FF) à l'aide des degrés de mise en surbrillance.
4	L'option permettant d'afficher les charges utiles masque uniquement les en-têtes des paquets, ce qui laisse plus d'espace pour la charge utile.
5	L'en-tête d'événement.

6 Les octets significatifs sont surlignés sur un arrière-plan bleu ; lorsque vous déplacez le curseur sur la mise en surbrillance, les métadonnées s'affichent dans une zone de survol.

7 (Version 11.1 ou supérieure) Les commandes de pagination des paquets permettent une plus grande flexibilité pour parcourir la liste de paquets. Lorsqu'une commande n'est pas disponible, l'image est grisée. Par exemple, lorsque vous affichez la page 1, les commandes et sont grisées.

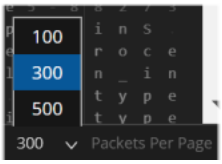
- Aller à la première page

- Aller à la page précédente

1 of 206 - Aller à une page spécifique

- Aller à la page suivante

- Aller à la dernière page

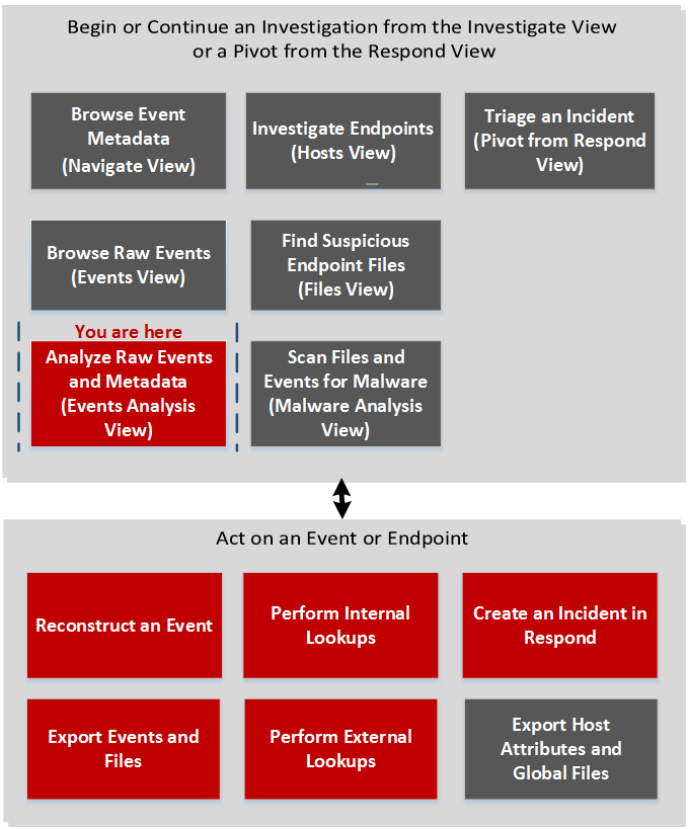


- Sélectionner le nombre de paquets par page

Vue Analyse d'événements - Panneau Analyse de texte

Dans le panneau Analyse de texte (**Analyse d'événements > Analyse de texte),** vous pouvez afficher et analyser en toute sécurité la charge utile de texte brut d'un événement. Le panneau Analyse de texte comprend des fonctions qui peuvent afficher du texte décompressé ou compressé, développer les entrées tronquées, effectuer l'encodage et le décodage aux formats URLet Base64, et télécharger des événements réseau, des logs, et des événements de point de terminaison. Le panneau Analyse de texte est disponible pour tous les types d'événements : réseau, log et point de terminaison.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	interroger des événements dans la vue Analyse d'événements (Version 11.1)	Filtrer les résultats dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter les événements et fichiers dans la vue Analyse d'événements*	Télécharger des données dans la vue Analyse d'événements
Responsable de la recherche des menaces	reconstruire des événements dans la vue Analyse d'événements*	Examiner les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	effectuer des recherches externes à partir de la vue Analyse d'événements (Version 11.1)*	Agir sur les données dans la vue Analyse d'événements
Responsable de la recherche des menaces	interroger des événements dans la vue Naviguer	Procédure d'enquête relative aux métadonnées dans la vue Naviguer
Responsable de la recherche des menaces	rechercher des événements dans la vue Événements	Examiner les événements bruts dans la vue Événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

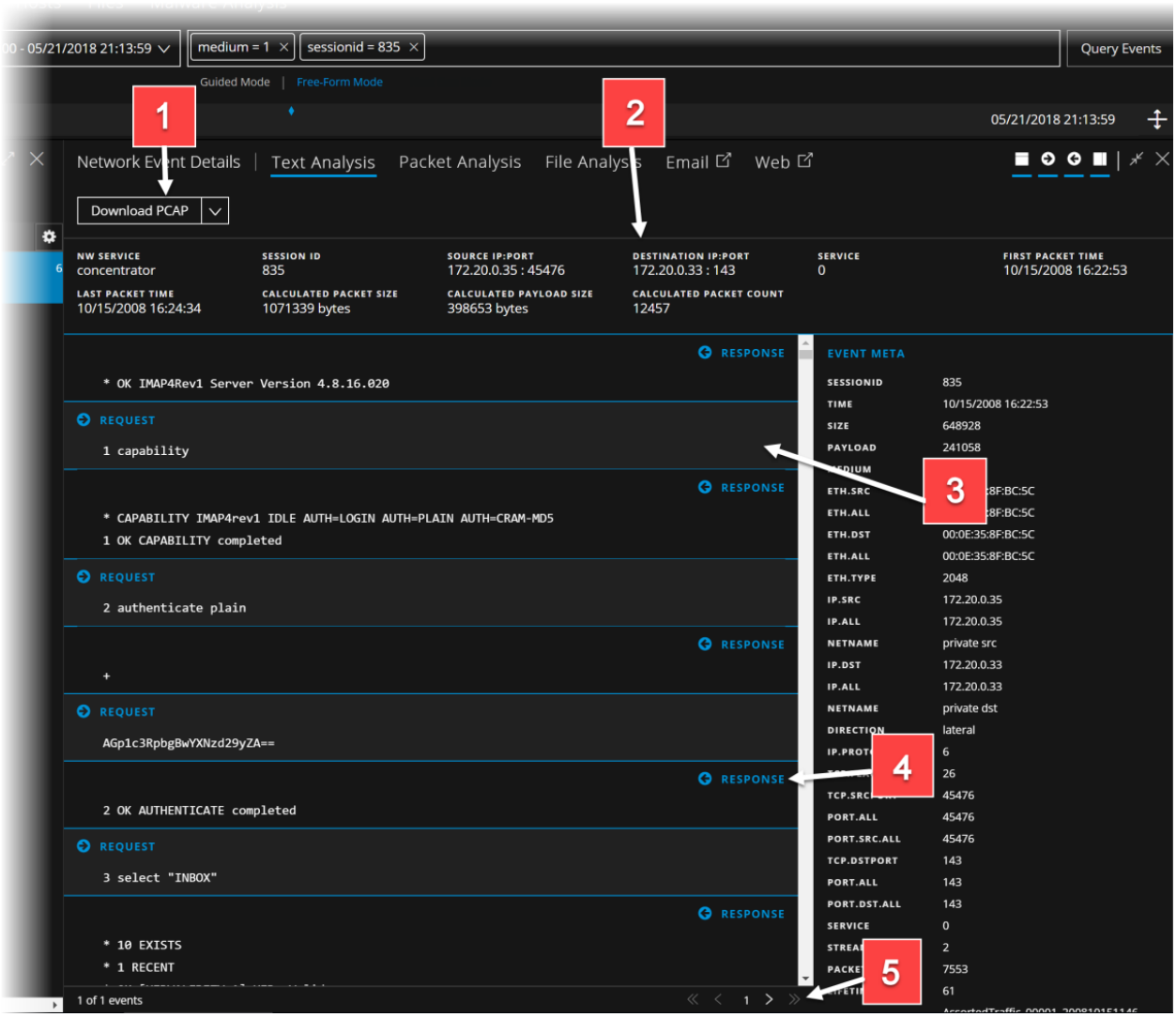
Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements

- Vue Analyse d'événements - Panneau Analyse de paquets
- Vue Analyse d'événements - Panneau Analyse de fichiers

Aperçu rapide

La vue Analyse d'événements affiche le texte d'un seul événement dans le panneau Analyse de texte. Lorsque vous cliquez sur un événement dans le panneau Liste d'événements, le panneau adjacent présente l'analyse de texte. Seul le log brut pour les événements de log et de point de terminaison sont représentés dans le panneau Analyse de texte. Pour les événements réseau, l'orientation du paquet (demande ou réponse) et le contenu de chaque paquet sont fournis au format texte. Pour plus d'exemples de la Analyse de texte, reportez-vous à la section Analyse des événements bruts et des métadonnées dans la vue Analyse d'événements. Pour les procédures détaillées, reportez-vous à la section Examiner les événements dans la vue Analyse d'événements.



1 Options permettant d'exporter un log, un fichier PCAP ou des fichiers pour une analyse plus approfondie et un partage avec d'autres utilisateurs. Ce menu de téléchargement est pour les données réseau.

2	Les informations d'en-tête d'événement.
3	La charge utile d'un événement réseau inclut les demandes et les réponses. Il s'agit de la partie de la demande du paquet.
4	Il s'agit de la partie de la réponse du paquet.
5	(Version 11.2 ou supérieure) Les commandes de pagination des événements permettent une plus grande flexibilité pour parcourir la liste de événements. Lorsqu'une commande n'est pas disponible, l'image est grisée. Par exemple, lorsque vous affichez la page 1, les commandes et sont grisées. - Aller à la première page - Aller à la page précédente - Aller à la page suivante - Accéder à la dernière page (uniquement disponible une fois que vous avez accédé à la dernière page)

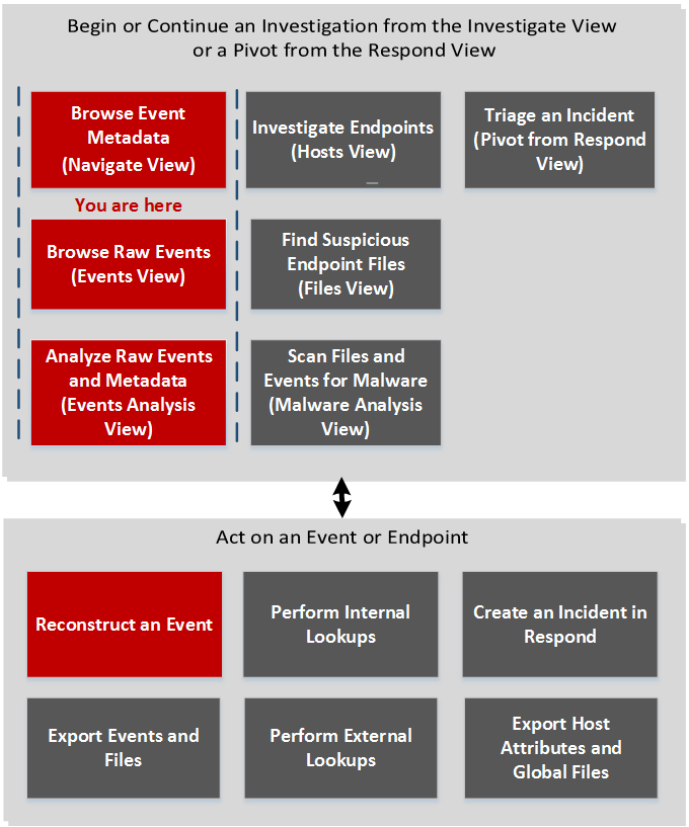
Vue Reconstruction d'événement

La vue Reconstruction d'événement fournit une reconstruction d'un événement sélectionné à partir de la Vue Événements. Par défaut, NetWitness Platform affiche la meilleure reconstruction pour l'événement déterminée par son contenu ou la reconstruction par défaut que vous avez sélectionnée dans le paramètre Vue Session par défaut pour Enquêter. Vous pouvez utiliser les options de la barre d'outils Reconstruction d'événement pour modifier la méthode de reconstruction, afficher les résultats de haut en bas ou côte à côte, sélectionner les vues de demande et de réponse, exporter un événement, exporter des métavaleurs, extraire des fichiers, ouvrir la pièce jointe d'un e-mail, et ouvrir l'événement dans un nouvel onglet.

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

- Dans la vue Événements, double-cliquez sur un événement.
- Dans la vue Événements avec la vue Détails sélectionnée, cliquez avec le bouton droit de la souris sur **Analyse d'événements** à la fin de l'événement, puis sélectionnez **Reconstruction d'événement.**
- Dans la barre d'outils Reconstruction d'événement de la reconstruction prévisualisée, cliquez sur **Ouvrir l'événement dans un nouvel onglet**.
- Dans la vue naviguer, sélectionnez **Actions > Accéder à un événement dans Reconstruction d'événement**, puis saisissez un ID d'événement.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	extraire des fichiers d'un événement reconstruit	Reconstruire un événement

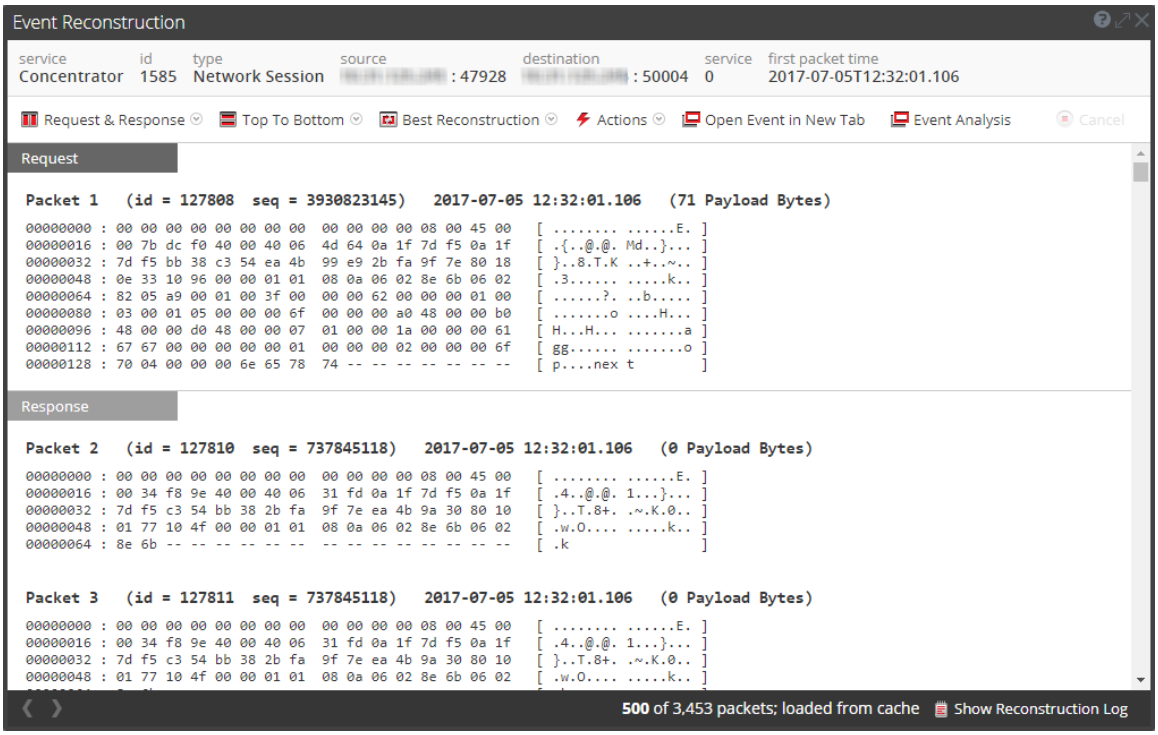
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements

Aperçu rapide

Cette figure est un exemple de la vue Reconstruction d'événement. Le tableau suivant décrit les options de la barre d'outils.



Fonctionnalité	Description
Requête et réponse	Affiche un menu déroulant permettant de sélectionner ce que la vue affiche : • Requête et réponse • Demande • Réponse
Organisation	Affiche un menu déroulant permettant d'indiquer si les informations doivent être affichées de haut en bas ou côte à côte.
Vue	Affiche un menu déroulant permettant de sélectionner les informations à afficher : Par défaut, l'option Meilleure reconstruction est activée. Autres options disponibles : • Afficher les méta • Afficher le texte • Afficher Hex • Afficher les paquets • Afficher le Web • Afficher la messagerie • Afficher les fichiers

Fonctionnalité	Description
Actions	Affiche un menu déroulant répertoriant les actions disponibles dans la vue Reconstruction d'événement.
Ouvrir l'événement dans un nouvel onglet	Ouvre l'événement dans un nouvel onglet du navigateur.

Une liste de clés méta et de valeurs apparaît sous la barre d'outils. Certaines de ces clés permet d'accéder à un menu déroulant répertoriant les actions disponibles.

La barre située sous la vue contient plusieurs options.

Fonctionnalité	Description
	Affiche l'événement précédent.
	Affiche l'événement suivant.
Afficher le log de reconstruction	Affiche le log de reconstruction au bas de la vue. Si vous cliquez sur ce bouton, son intitulé devient Masquer le log de reconstruction.

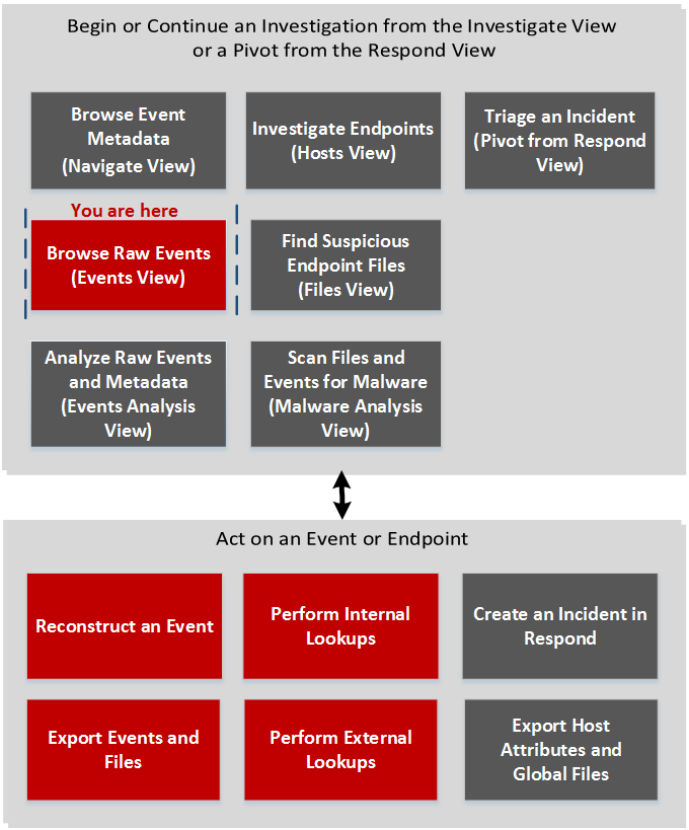
Vue Événements

Dans la vue Vue Événements, une liste d'événements associés à une session est disponible ; cette vue est optimisée pour afficher les événements bruts dans l'ordre chronologique. Vous pouvez afficher la liste des événements sous plusieurs formes, filtrer les événements, rechercher des événements et ouvrir une reconstruction d'événement.

Il existe deux façons d'afficher la vue Événements :

- Accédez à **ENQUÊTER > Événements.** NetWitness Platform exécute une requête par défaut sur les trois dernières heures pour le service par défaut (si un service est défini) ou affiche une boîte de dialogue dans laquelle vous pouvez sélectionner un service, puis exécute la requête par défaut. La requête par défaut sélectionne tous les événements et la vue Événements affiche des événements sur le service sélectionné, avec les événements les plus anciens en premier.
- Dans la vue **Naviguer**, cliquez sur un événement. La vue Événements affiche les événements sur le service sélectionné d'après le point de recherche verticale dans la vue Naviguer.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	définir les préférences utilisateur pour la vue Événements*	Configurer la vue Naviguer et la vue Événements
Responsable de la recherche des menaces	reconstruire un événement*	Reconstruire un événement
Responsable de la recherche des menaces	exporter les événements et les fichiers*	Exporter les événements dans la vue Événements
Responsable de la recherche des menaces	effectuer des recherches interne	Rechercher un contexte supplémentaire dans les vues Naviguer et Événements
Responsable de la recherche des menaces	effectuer des recherches externes	Lancer la recherche externe d'une clé méta

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces ou Responsable de la réponse aux incidents	ajouter un ou plusieurs événements à un incident existant ou à un nouvel incident*	Ajouter des événements à un incident pour obtenir une réponse

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Examiner les événements bruts dans la vue Événements
- Interrogation et action sur les données dans les vues Naviguer et Événements

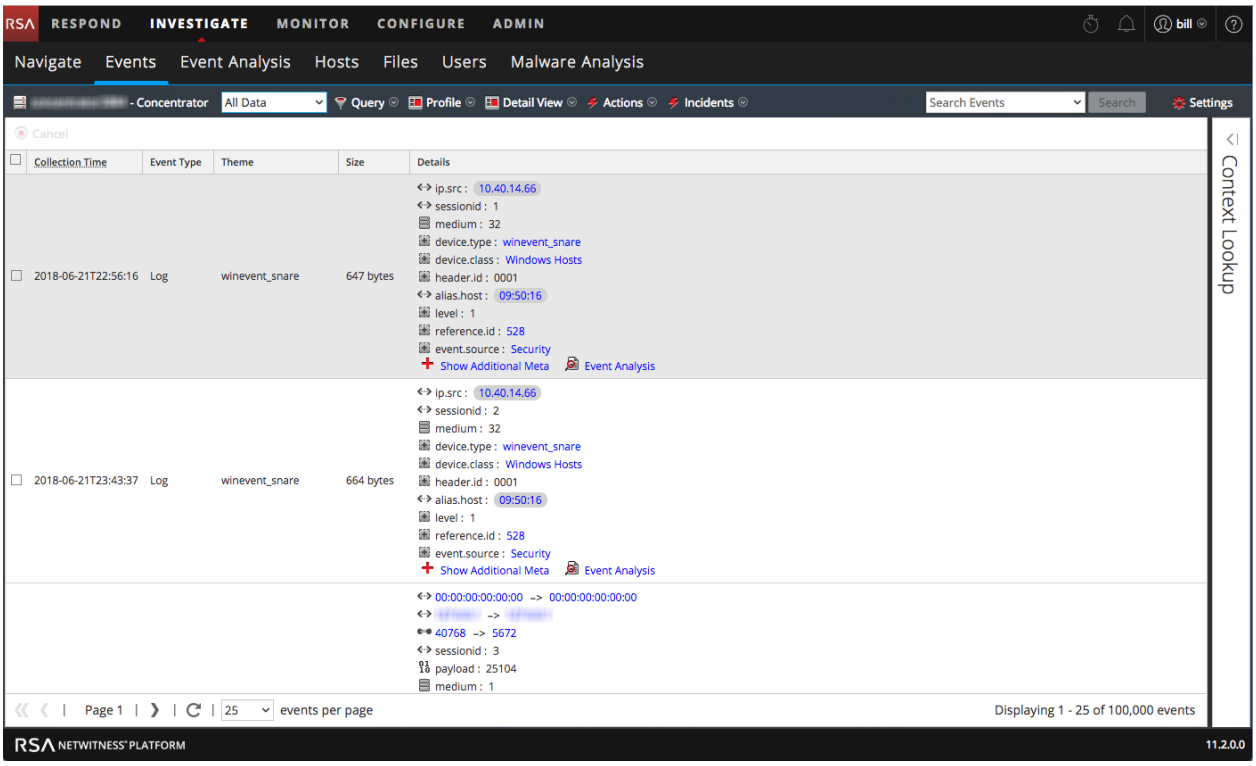
Aperçu rapide

La vue Événements fournit trois présentations intégrées des données d'événement : la vue Détails, la vue Liste et la vue Log. La vue Liste et la vue Détails sont destinées à l'affichage des événements de données de paquets. Elles fournissent plus d'informations pour chaque événement, notamment l'horodatage, le type d'événement, le thème de l'événement et la taille.

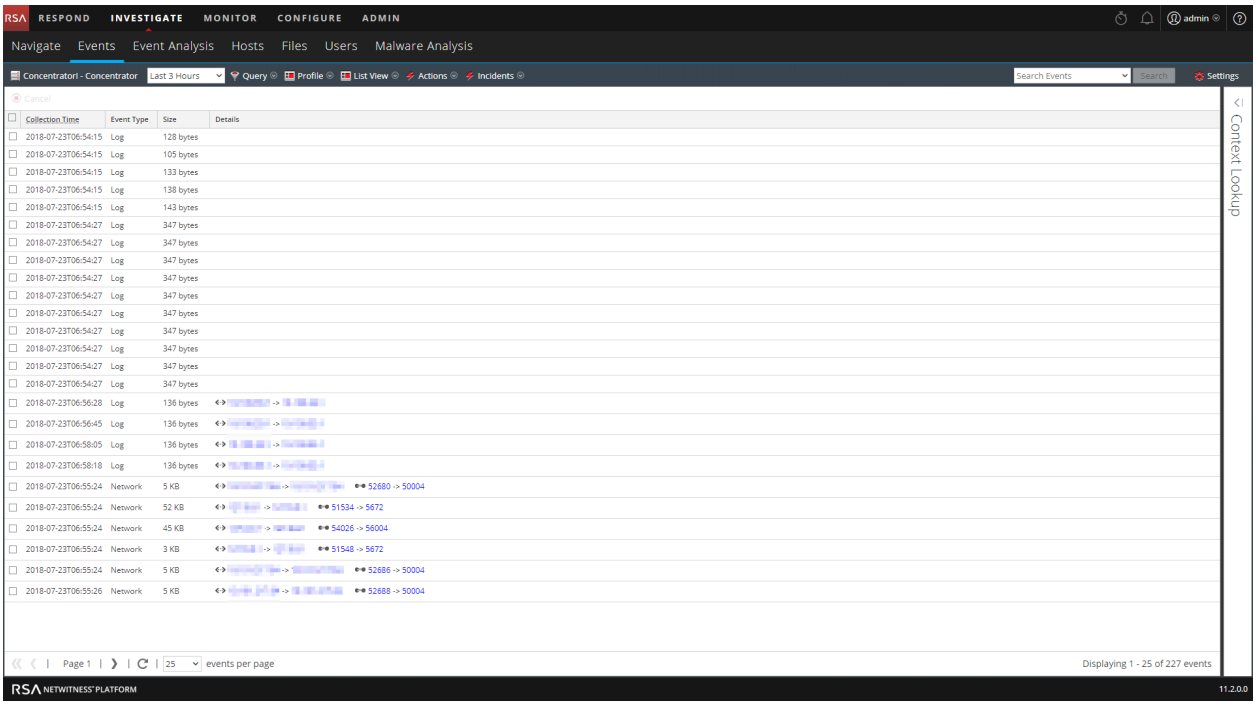
- La vue Liste affiche les informations relatives à l'adresse et au port source et de destination pour les événements sous forme de résumé dans une grille.
- La vue Détails affiche toutes les métadonnées collectées pour l'événement dans une vue de page.
- La vue Log est optimisée pour l'affichage des informations du log, et fournit plus d'informations pour chaque log, notamment l'horodatage, le type d'événement, le type de service, la classe de service et les logs.

Vous pouvez utiliser des requêtes, le paramètre de période et les profils pour filtrer les événements répertoriés dans la vue Événements. Depuis tous les types de vue dans la vue Événements, vous pouvez extraire des fichiers, exporter des événements, exporter des logs d'événements et des métavaleurs, ouvrir le panneau Reconstruction d'événement et ouvrir Analyse d'événements.

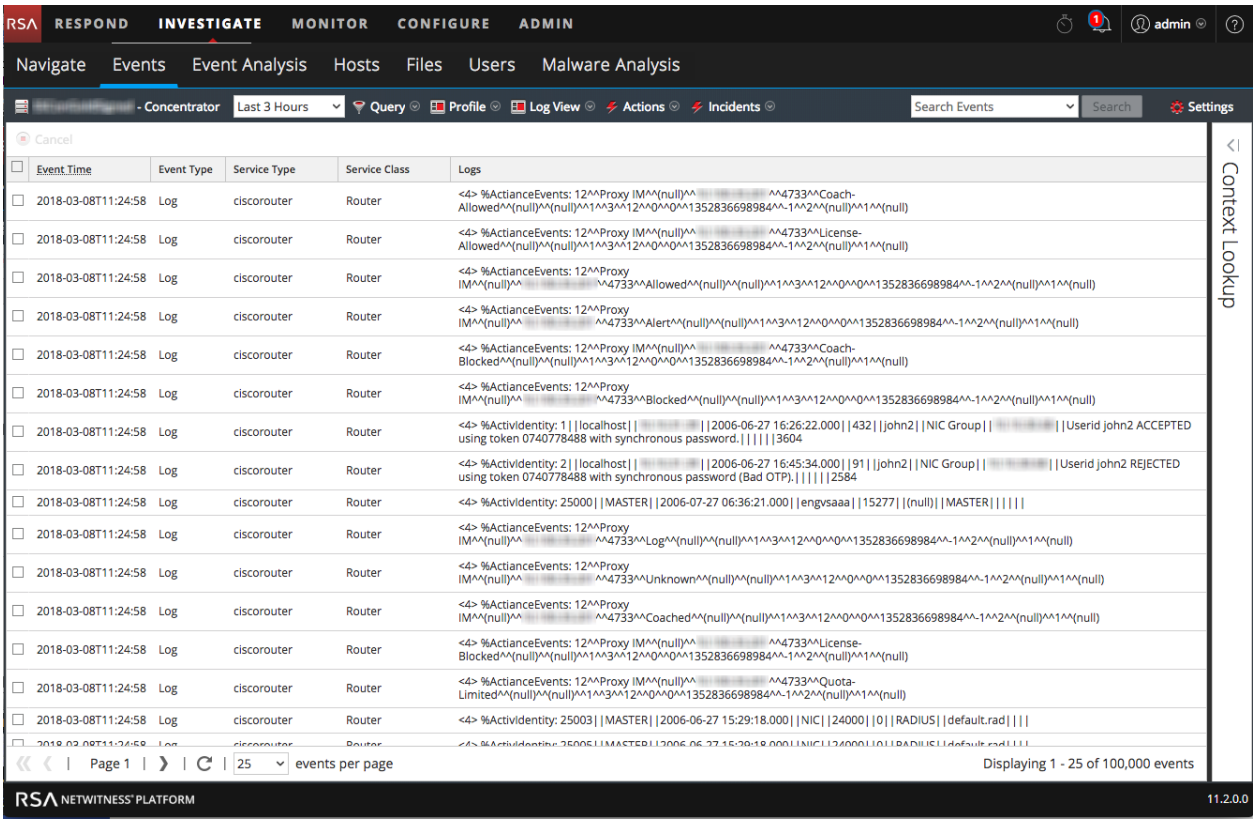
La figure suivante est un exemple d'événements de la vue Détails. Le panneau Recherche contextuelle est visible uniquement si le service Context Hub est configuré.



La figure suivante est un exemple d'événements de la vue Liste.



La figure suivante donne un exemple de la vue Log.



Description détaillée

La vue Événements contient une barre d'outils située en haut de l'écran avec les options suivantes.

Fonctionnalité	Description
Sélectionner un service	Affiche le nom de service sélectionné en regard de l'icône. Ouvre la boîte de dialogue Sélectionner un service qui vous permet de sélectionner un service pour lequel la liste des événements s'affiche.
Période	Affiche un menu déroulant pour la sélection de la période à appliquer à la liste des événements. Vous pouvez choisir une des options standard ou spécifier une période personnalisée.
Requête	Affiche la boîte de dialogue Créer un filtre qui vous permet de saisir directement une requête personnalisée au lieu d'effectuer une recherche verticale dans les données (voir Créer une requête personnalisée).

Fonctionnalité	Description
Profil	Affiche le menu Profil d'utilisation ; le profil actuellement sélectionné s'affiche dans la barre d'outils. Un profil vous permet de gérer et d'utiliser des profils qui peuvent inclure des groupes méta personnalisés, un groupe de colonne par défaut et une requête de début. Les Profils s'appliquent à la vue Naviguer (groupes et requêtes méta) et à la vue Événements (groupes et requêtes de colonne).
Afficher le menu déroulant Vue	Affiche un menu déroulant permettant de sélectionner le type de vue d'événement. • La vue Détails affiche les événements dans un format de page avec des informations détaillées pour chaque événement. • La vue Liste affiche les événements sous forme de grille avec un résumé de chaque événement sur une ligne distincte. • La vue Log affiche une grille des événements liés aux logs avec un résumé de chaque log sur une ligne distincte. • La section Groupes de colonnes personnalisées affiche la liste des événements utilisant un groupe de colonnes sélectionné dans une liste déroulante de groupes de colonnes personnalisées. • La section Gérer les groupes de colonnes affiche la boîte de dialogue permettant de créer et de modifier les groupes de colonnes personnalisées.
Actions	Affiche un menu déroulant avec des actions dans la vue Événements : • Extraire des fichiers, exporter les événements au format de fichier PCAP, exporter les logs ou exporter les métavaleurs. • Afficher une reconstruction de l'événement dans une fenêtre contextuelle ou dans un nouvel onglet. • Afficher l'analyse d'événements. • Réinitialiser tous les filtres dans la vue Événements.
Incidents	Créer un nouvel incident dans Répondre et ajouter les événements sélectionnés ou ajouter des événements sélectionnés à un incident existant dans Répondre.
Recherche	Affiche les options de recherche des événements, ce qui vous permet de spécifier le format d'exportation du log et le format d'exportation des métavaleurs avec des options supplémentaires expliquées dans Rechercher des modèles de texte

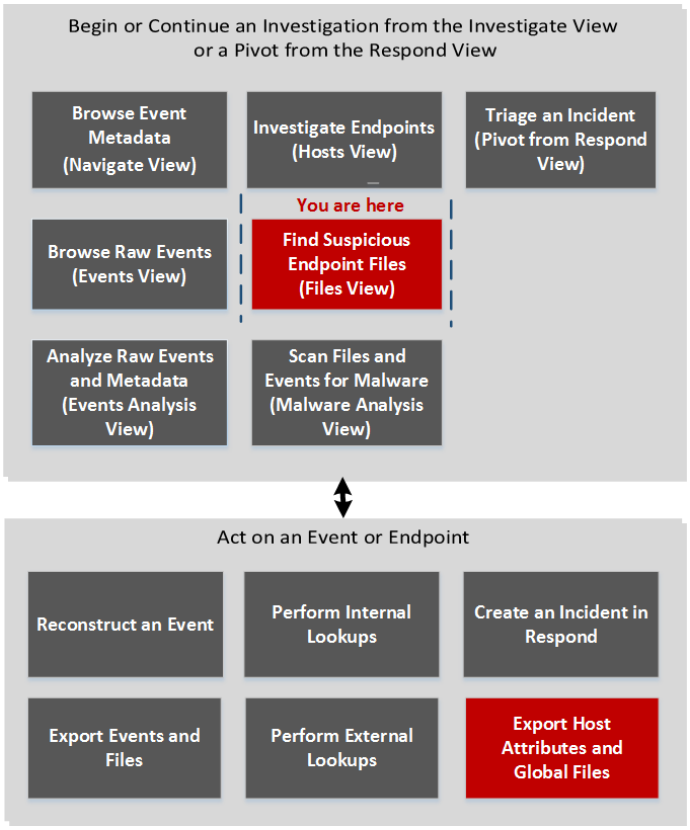
Fonctionnalité	Description
Paramètres	Affiche les paramètres de la vue Procédure d'enquête pour la vue Événements (qui sont également disponibles dans la vue Profil) pour que vous puissiez modifier les paramètres de la vue Procédure d'enquête sans avoir à naviguer hors de la vue Événements. Lorsque vous modifiez un paramètre dans la vue Événements, le paramètre est également modifié dans la vue Profil (voir Configurer la vue Naviguer et la vue Événements).

Vue Fichiers

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Dans la vue **Fichiers**, une liste de fichiers exécutables uniques figurantdans le déploiement est disponible. Pour accéder à cette vue, sélectionnez **ENQUÊTER > Fichiers**. Par défaut, la vue Fichiers affiche 100 fichiers. Pour afficher plus de fichiers, cliquez sur **Charger davantage** au bas de la page.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)*	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	exporter les attributs des hôtes et les fichiers globaux*	Examiner les fichiers

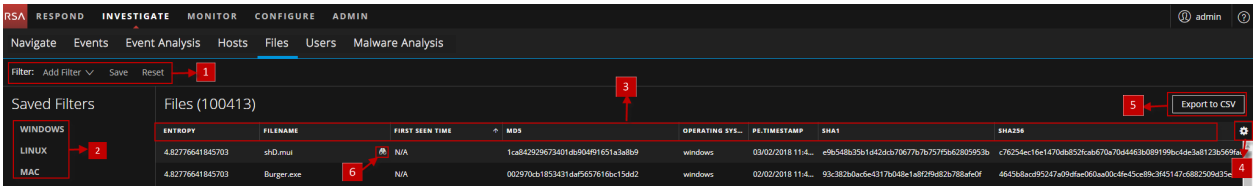
*Vous pouvez effectuer cette tâche dans la vue actuelle

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers

Aperçu rapide

Voici un exemple de la vue Fichiers.



1 **Menu déroulant Ajouter des filtres**. Vous pouvez filtrer les fichiers en choisissant un système d'exploitation (Windows, Linux ou Mac), des filtres enregistrés ou en sélectionnant les options du menu déroulant Ajouter des filtres. Pour plus d'informations, voir Filtrer les fichiers.

2 **Filtres enregistrés.** Le panneau Filtres enregistrés affiche les filtres enregistrés. Pour plus d'informations, voir Filtrer les fichiers.

3 **Trier les colonnes.** Vous pouvez trier la liste par :

Nom du fichier - Nom du fichier.

Heure de la première visualisation : La première fois que le hachage a été vu dans l'hôte.

Signature - Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires.

Taille - Taille du fichier.

Entropie - Détermine si le contenu est compressé ou chiffré.

Format - Format du fichier - Windows (PE), Linux (ELF et scripts) et Mac (Macho).

PE.Resources.Company - Nom de l'entreprise.

Remarque : Le tri des colonnes est sensible à la casse. L'ordre de tri est le suivant : nombres, majuscules et minuscules.

4 **Menu Paramètres.** Vous pouvez définir les préférences de la vue Fichiers en sélectionnant des colonnes dans le menu Paramètres. Pour plus d'informations, voir Définir les préférences de fichiers.

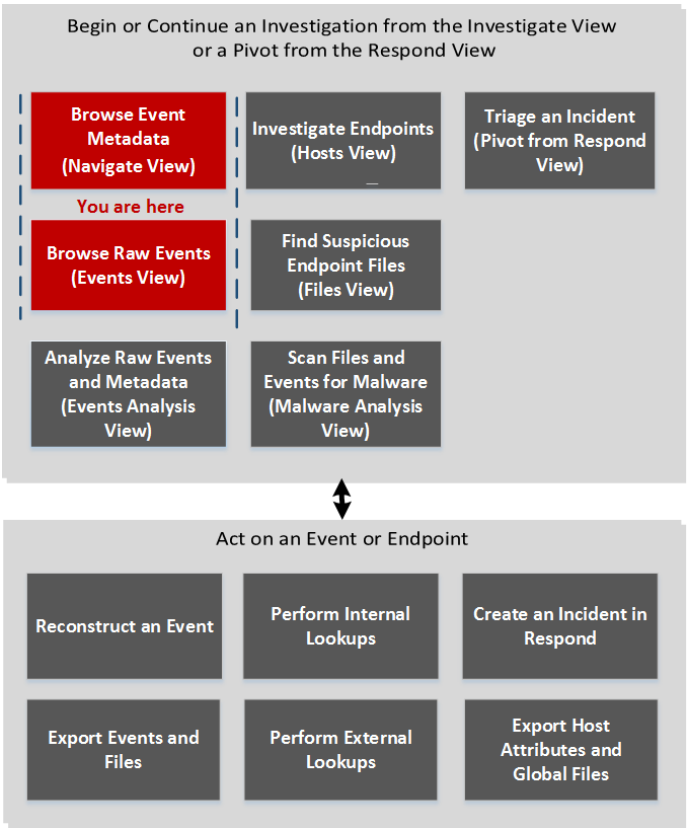
5 **Exporter dans un fichier CSV** - Extrait les fichiers globaux dans un fichier CSV. Pour plus d'informations, consultez la ressource Examiner les fichiers.

6 **Pivoter vers les vues Naviguer et Analyse d'événements.** Pour rechercher un nom de fichier ou un hachage particulier (SHA256 et MD5), vous pouvez faire pivoter les vues Naviguer et Analyse d'événements. Pour plus d'informations, voir Pivoter vers les vues Naviguer et Analyse d'événements..

Boîte de dialogue Enquêter

Dans la boîte de dialogue Procédure d'enquête, les analystes peuvent sélectionner le service ou la collection à examiner. Cette boîte de dialogue s'affiche automatiquement lorsque vous accédez pour la première fois à la vue Naviguer ou Événements et que vous n'avez sélectionné aucun service par défaut à examiner. Pour accéder à cette boîte de dialogue à partir d'une procédure d'enquête en cours, sélectionnez le nom du service actif dans la barre d'outils.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

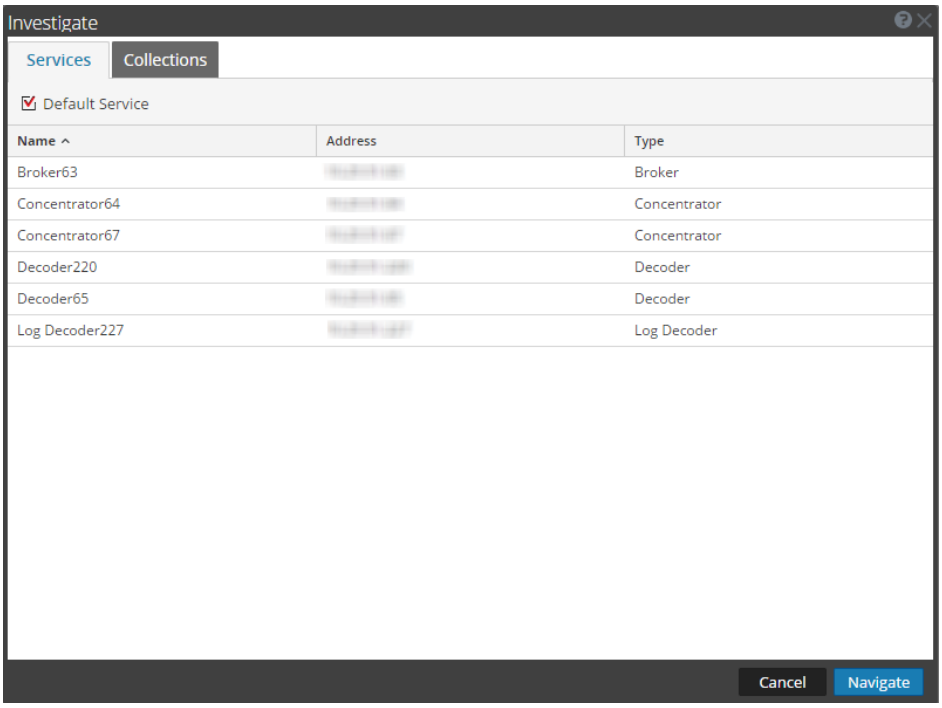
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	sélectionner un service pour enquêter*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Naviguer
- Vue Événements

Aperçu rapide



La boîte de dialogue Enquêter comporte deux onglets : Services et Collections.

Remarque : les collections sont également appelées collections Workbench. Vous ne pouvez afficher que les collections Workbench dont vous êtes l'auteur. Par ailleurs, seuls les administrateurs peuvent en créer.

L'onglet Services répertorie les services pouvant être examinés, ainsi que trois boutons. Toutes les fonctions sont décrites dans le tableau suivant.

Fonctionnalité	Description
Service par défaut	Cliquez sur ce bouton pour définir ou effacer le service par défaut à examiner. Si vous définissez un service par défaut, les termes (Par défaut) sont ajoutés au nom du service en question.
Nom	Le nom du service.
Adresse	Adresse IP du service.
Type	Type de service
Annuler	Ferme la boîte de dialogue.
Naviguer	Ouvre le service sélectionné dans la vue Naviguer ou Événements.

Cet onglet comporte deux boutons et deux panneaux : Workbench et Collections.

Le panneau Workbench répertorie les services Workbench disponibles par nom. Après avoir sélectionné un service Workbench, vous pouvez choisir une collection dans le panneau Collections.

Ces panneaux répertorient les collections qui peuvent être examinées. Après avoir sélectionné une collection, vous pouvez cliquer sur Naviguer pour l'afficher.

Le tableau suivant décrit les fonctions du panneau Collections.

Fonctionnalité	Description
Nom	Nom de la collection.
Type	Type de la collecte.
Taille	Taille de la collection.
Type de données	Type des données de la collection.
Date de création	Date de création de la collection.

Onglet Procédure d'enquête - Panneau Préférences utilisateur

Dans la vue Profil > panneau Préférences > onglet Procédure d'enquête, les utilisateurs peuvent définir plusieurs préférences qui affectent les performances et le comportement de NetWitness Platform lors de l'analyse de données, de l'affichage des événements et de la reconstruction d'événements dans NetWitness Investigate. Pour accéder à cet onglet, sélectionnez  > Profile. Lorsque la vue Profil s'affiche, sélectionnez **Préférences > Procédure d'enquête**. Vous pouvez modifier les préférences utilisateur à tout moment lorsque vous travaillez dans NetWitness Platform.

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	afficher et modifier les préférences utilisateur pour Enquêter*	Configurer la vue Naviguer et la vue Événements

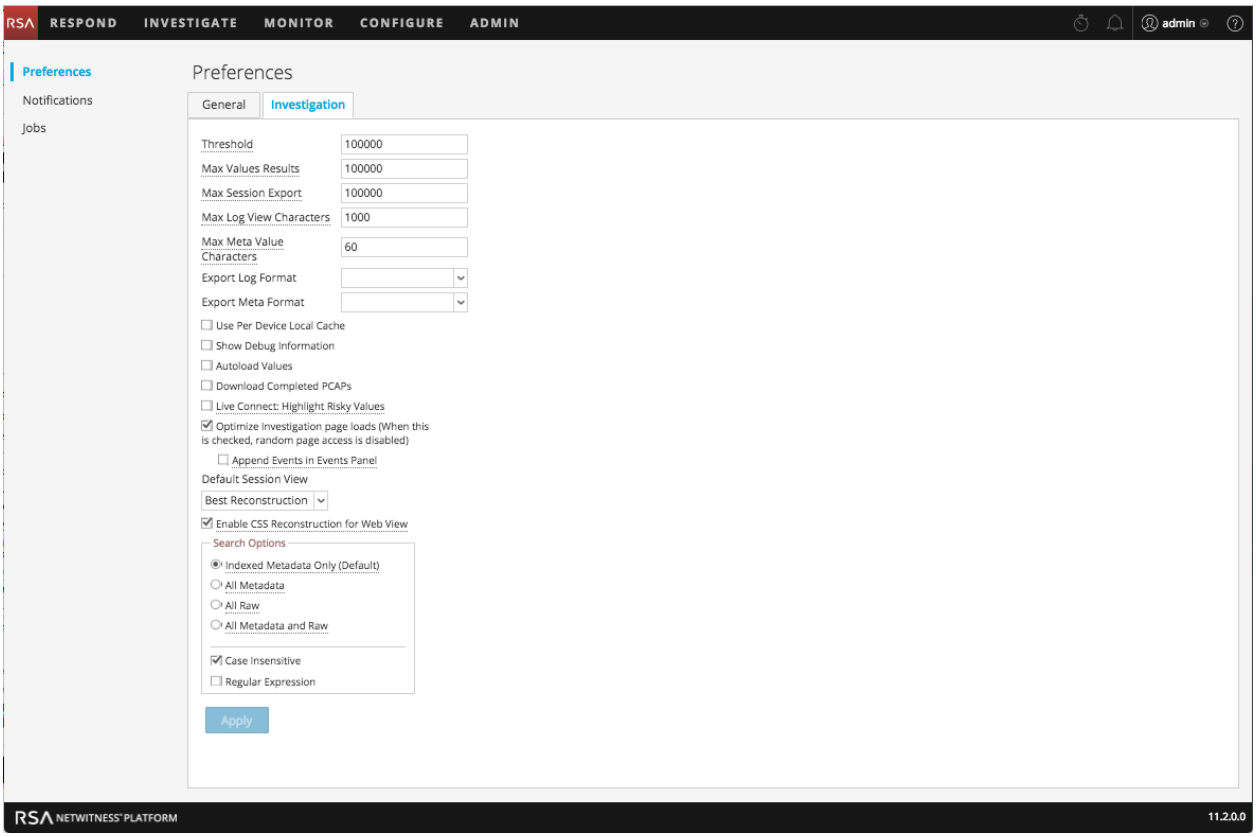
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Naviguer
- Vue Événements

Aperçu rapide

La figure suivante est un exemple de l'onglet Procédure d'enquête, et le tableau suivant décrit les préférences de Procédure d'enquête qui ont un impact sur cette fonction. Il existe de légères différences entre les versions 11.1 et 11.2 des paramètres de recherche et celles-ci sont expliquées dans Rechercher des modèles de texte.



Fonctionnalité	Description
Seuil	Ce paramètre contrôle le nombre indiqué pour une valeur de clé méta dans la vue Naviguer pendant la charge. Un seuil plus élevé autorise des chiffres plus précis pour une valeur. Toutefois, un seuil plus élevé provoque plus de temps de charge. Lorsque le seuil est atteint, NetWitness Platform affiche le nombre et le pourcentage de temps utilisé pour atteindre le nombre par rapport au temps nécessaire pour charger toutes les sessions avec cette valeur. Par exemple, **(>100 000 - 18 %)** indique que le seuil a été fixé à 100 000 et que cette charge a pris uniquement 18 % du temps qu'il aurait fallu sans fixer de seuil. La valeur par défaut est **100 000**.
Nb max résultats de valeurs	Ce paramètre contrôle le nombre maximal de valeurs à charger dans la vue Naviguer lorsque l'option Résultats maximum est sélectionnée dans le menu Clé méta pour ouvrir une clé méta. La valeur par défaut est **1 000**.
Nb max exports de session	Ce paramètre contrôle le nombre maximum de sessions qui peuvent être exportées. La valeur par défaut est **100 000**.
Caractères max affichage logs	Ce paramètre contrôle le nombre maximal de caractères à afficher sous **Procédure d'enquête > Événements > Texte du log**. La valeur par défaut est **1 000**.

Fonctionnalité	Description
Format du log d'exportation	Ce paramètre spécifie le format par défaut pour l'exportation des logs à partir de Procédure d'enquête. Les options disponibles sont **Texte**, **XML**, **CSV** et **JSON**. Il n'existe pas de valeur par défaut intégrée pour le format d'exportation de log. Si vous ne sélectionnez pas de format ici, NetWitness Platform affiche une boîte de dialogue de sélection lorsque vous invoquez l'exportation des logs. Lorsque vous sélectionnez l'une des options dans le menu déroulant Format du log d'exportation et cliquez sur Appliquer, le paramètre prend effet immédiatement.
Exporter le format de métadonnées	Ce paramètre spécifie le format par défaut pour l'exportation des métavaleurs à partir de Procédure d'enquête. Les options disponibles sont Texte, XML, CSV et JSON. Il n'existe pas de valeur par défaut intégrée pour le format d'exportation de métavaleurs. Si vous ne sélectionnez pas de format ici,NetWitness Platform affiche une boîte de dialogue de sélection lorsque vous invoquez l'exportation des méta. Lorsque vous sélectionnez l'une des options dans le menu déroulant Exporter le format de métadonnées et cliquez sur Appliquer, le paramètre prend effet immédiatement.
Utiliser le cache local par appareil	
Afficher les informations de débogage	Lorsque cette option est sélectionnée,NetWitness Platform affiche la clause `where` sous le fil d'Ariane dans la vue Naviguer. Le temps de chargement s'affiche pour chaque charge de métavaleur. Si le service est un Broker, le temps écoulé pour chaque service agrégé est signalé. La valeur par défaut est **Off**.
Ajouter des événements dans le panneau Événements	Lorsque cette option est sélectionnée, les événements affichés dans le **panneau Événements** sont ajoutés de manière incrémentielle plutôt que d'écraser les événements actuellement affichés. Chaque fois que vous cliquez sur l'icône de la page suivante, les événements supplémentaires sont ajoutés aux événements précédents ; 1 à 25, puis 1 à 50, puis 1 à 75, et ainsi de suite. **Remarque :** cette option est uniquement disponible si l'option Optimiser les charges de la page Procédure d'enquête est activée.
Charger automatiquement les valeurs	Lorsque cette option est sélectionnée, les valeurs du service sont automatiquement chargées dans la vue Naviguer. Lorsqu'elle n'est pas sélectionnée, NetWitness Platform affiche un bouton **Charger les valeurs**, ce qui donne à l'utilisateur l'opportunité de modifier des options. La valeur par défaut est **Off**.
Téléchargement des PCAP terminés	Ce paramètre automatise le téléchargement des PCAP extraits dans Enquêter pour que vous n'ayez pas à télécharger et ouvrir manuellement les fichiers PCAP extraits dans une application, telle que Wireshark, qui peut gérer l'affichage des données dans un format PCAP.
Live Connect : Mettre en évidence les valeurs risquées	

Fonctionnalité	Description
Optimiser les charges de la page Procédure d'enquête	Cette option est activée par défaut (cochée) et contrôle la façon dont la vue Événements récupère les événements. Lorsqu'ils sont optimisés, les résultats sont renvoyés le plus rapidement possible. La fonction de base qui permet de se rendre à une page spécifique dans la liste des événements est annulée. Désactiver cette case modifie la pagination de la liste Événements pour vous permettre d'accéder à une page spécifique de la liste (ou à la dernière page). Être en mesure de se rendre à une page de la liste fait perdre un peu de vitesse pour renvoyer des résultats en raison de temps système supplémentaire qui détermine les événements à l'avance.
Visualisation des sessions par défaut	Ce paramètre sélectionne le type de reconstruction par défaut pour la vue initiale de reconstruction. Par défaut, les événements sont reconstruits à l'aide du type de reconstruction le plus approprié pour l'événement.
Activer la vue CSS Reconstruction pour le Web	Ce paramètre contrôle la réalisation de la reconstruction de contenu Web. Si elle est activée, la reconstruction Web comprend des styles avec feuille de style en cascade (CSS) et des images pour que son apparence soit identique à celle de la vue originale dans un navigateur Web. Elle inclut l'analyse et la reconstruction des événements connexes, et la recherche de feuilles de style et d'images utilisées dans l'événement cible. Cette option est activée par défaut. Désactivez cette option en cas de problèmes avec l'affichage de sites Web spécifiques. **Remarque :** l'apparition du contenu reconstitué peut ne pas correspondre parfaitement à la page Web d'origine si les images et les feuilles de style sont introuvables ou si elles ont été chargées à partir de la mémoire cache du navigateur Web. De plus, tout style ou mise en page effectué dynamiquement via le javascript côté client ne sera pas rendu dans la reconstruction, car tout le javascript côté client est supprimé pour des raisons de sécurité.
Options de recherche	Ce paramètre définit les options de recherche par défaut à appliquer à une recherche dans les vues Naviguer et Événements. Rechercher des modèles de texte fournit des informations détaillées.
Appliquer	Enregistre vos préférences et les applique immédiatement.

Vue Enquêter

La vue Investigate (ENQUÊTER) est le point d'entrée principal dans NetWitness Investigate. La vue Examiner comporte six sous-menus, qui ouvrent différentes vues vous permettant d'analyser des événements de différentes perspectives. Les sous-menus sont les suivants : Naviguer, Événements, Analyse d'événements, Hôtes, Fichiers, Utilisateurs et Malware Analysis.

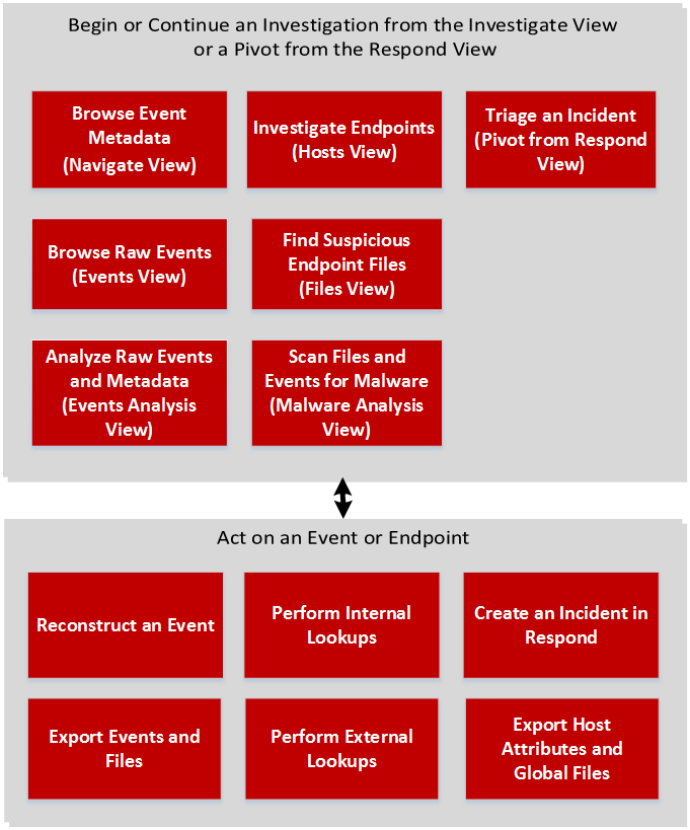
Remarque : Les sous-menus Analyse d'événements, Hôtes et Fichiers sont disponibles dans la version 11.1 ou supérieure. Le menu Utilisateurs est disponible dans la version 11.2 et versions ultérieures. Les autorisations configurées par rôle d'utilisateur et utilisateur déterminent les sous-menus affichés.

Vous pouvez utiliser les options de sous-menu pour vous déplacer entre les différentes vues.

- La vue Naviguer, la vue Événements et la vue Analyse d'événements offrent des liens les uns aux autres pour examiner les résultats actuels sous un angle différent, ce qui offre une certaine continuité à la procédure d'enquête lorsque vous passez d'une vue à l'autre.
- La vue Hôtes et la vue Fichiers intègrent NetWitness Endpoint à Investigate, et fournissent une vue de tous les hôtes avec un agent NetWitness Endpoint installé et une vue des fichiers exécutables uniques dans l'environnement déployé.
- La vue Utilisateurs fournit une visibilité sur les comportements des utilisateurs à risque dans votre entreprise à l'aide de NetWitness UEBA. Vous pouvez afficher une liste d'utilisateurs à haut risque et un récapitulatif des alertes principales pour le comportement risqué de votre environnement, puis sélectionner un utilisateur ou une alerte et afficher des détails sur le comportement risqué et une chronologie pendant laquelle les comportements se sont produits.
- La vue Analyse de malware offre la possibilité d'analyser les fichiers trouvés dans l'une des autres vues ou collectés par analyse continue du trafic réseau.

Workflow

Le workflow ci-dessous décrit les tâches générales lors de l'analyse des événements.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts*	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)*	Examiner les fichiers

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants*	Mener une analyse de malware

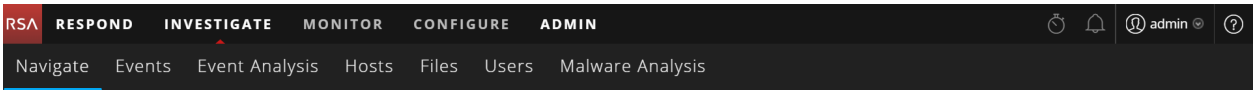
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Commencer une procédure d'enquête
- Configuration des vues et des préférences de NetWitness Investigate
- Vue Naviguer
- Vue Événements
- Vue Analyse d'événements
- Vue Hôtes
- Vue Fichiers
- Vue Analyse de malware
- *Guide de l'utilisateur de NetWitness UEBA*

Aperçu rapide

La vue Enquêter se compose de six vues, chacune représentant une approche différente d'analyse des données. Par défaut, la procédure d'enquête s'ouvre dans la vue Naviguer. Vous pouvez remplacer la vue par défaut par l'une des autres vues. Voir Fonctionnement de NetWitness Investigate pour une introduction à l'utilisation de chaque vue. La figure suivante montre les sous-menus sous la vue ENQUÊTER.



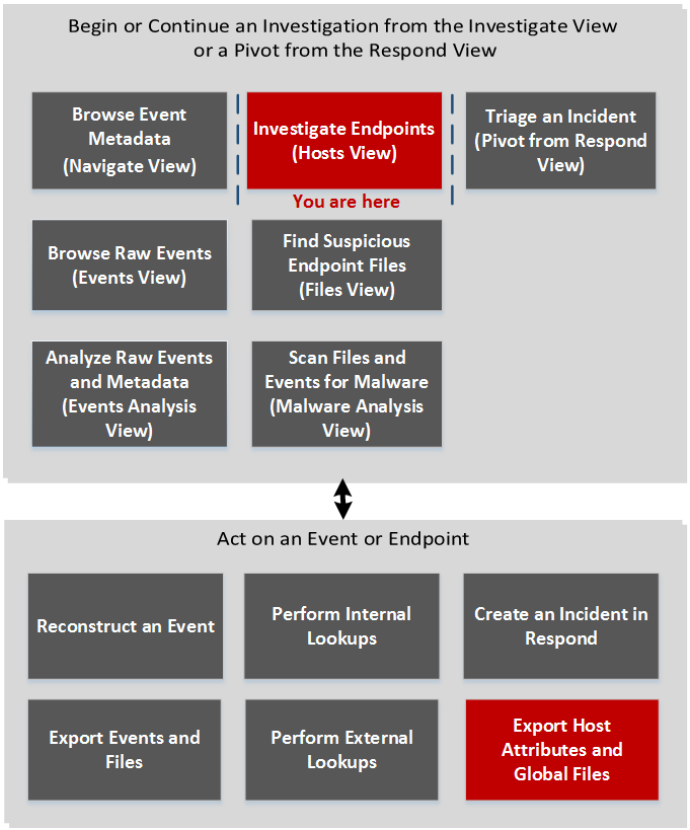
Vue Hôtes

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Dans NetWitness Investigate, la vue Hôtes fournit la liste de tous les hôtes dotés d'un agent Endpoint. Le tableau affiche un ensemble de colonnes par défaut pour l'hôte. Vous pouvez personnaliser cette vue en définissant les préférences d'hôtes. Pour accéder à cette vue, sélectionnez **ENQUÊTER > Hôtes**.

Workflow

La figure suivante montre une vue générale du workflow Enquêter avec les tâches Examiner les points de terminaison mises en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	exporter les attributs des hôtes et les fichiers globaux*	Examiner les hôtes

*Vous pouvez effectuer cette tâche dans la vue actuelle.

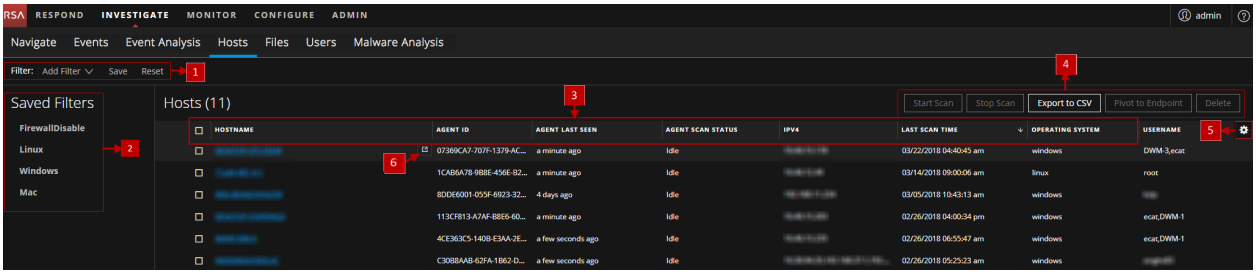
Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes - Onglet Présentation
- Vue Hôtes - Onglet processus
- Vue Hôtes - Onglet Exécutions automatiques
- Vue Hôtes - Onglet Fichiers
- Vue Hôtes - Onglet Pilotes
- Vue Hôtes - Onglet Bibliothèques
- Vue Hôtes - Onglet Informations du système

Aperçu rapide

La vue Hôtes vous permet d'exporter les attributs des hôtes et les fichiers globaux, d'effectuer une analyse à la demande, de définir les préférences de l'hôte, d'afficher la liste des hôtes et d'enquêter dans la vue Naviguer ou Événements.

Voici un exemple de la vue Hôtes :



1 **Menu déroulant Ajouter des filtres**. Vous pouvez filtrer les hôtes en choisissant un système d'exploitation (Windows, Linux ou Mac), des filtres enregistrés ou en sélectionnant les options du menu déroulant Ajouter des filtres. Pour plus d'informations, reportez-vous à la section Filtrer les hôtes.

2 **Filtres enregistrés.** Le panneau Filtres enregistrés affiche les filtres enregistrés. Pour plus d'informations, reportez-vous à la section Filtrer les hôtes.

3 **Trier les colonnes**. Permet de trier les colonnes.

> **Remarque :** Le tri des colonnes est sensible à la casse. L'ordre de tri est le suivant : nombres, majuscules et minuscules.
> Le tri dans les champs État d'analyse de l'agent et Dernière consultation de l'agent n'affiche pas le bon ordre.

4 **Actions disponibles dans la barre d'outils :**
Démarrer l'analyse - Démarre une analyse pour les hôtes sélectionnés.
Arrêter l'analyse - Arrête une analyse pour les hôtes sélectionnés.
Exporter dans un fichier CSV - Extrait les attributs des hôtes dans un fichier CSV. Pour plus d'informations, voir Exporter les attributs de l'hôte.
Pivoter vers Endpoint - Permet d'examiner l'hôte NetWitness Endpoint (version 4.4.0.2 ou version supérieure). Pour plus d'informations, voir Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure.
Supprimer - Permet de supprimer manuellement des hôtes à partir de l'interface utilisateur. Une fois la suppression effectuée, le serveur Endpoint ne traite plus les demandes émanant de cet hôte.

> **Remarque :** Assurez-vous que l'agent est désinstallé de l'hôte avant de supprimer l'interface utilisateur. Pour plus d'informations, voir Supprimer un hôte.

5 **Menu Paramètres** Vous pouvez définir les préférences de la vue Hôtes en sélectionnant des colonnes dans le menu Paramètres. Pour plus d'informations, voir Définir les Préférences d'hôtes.

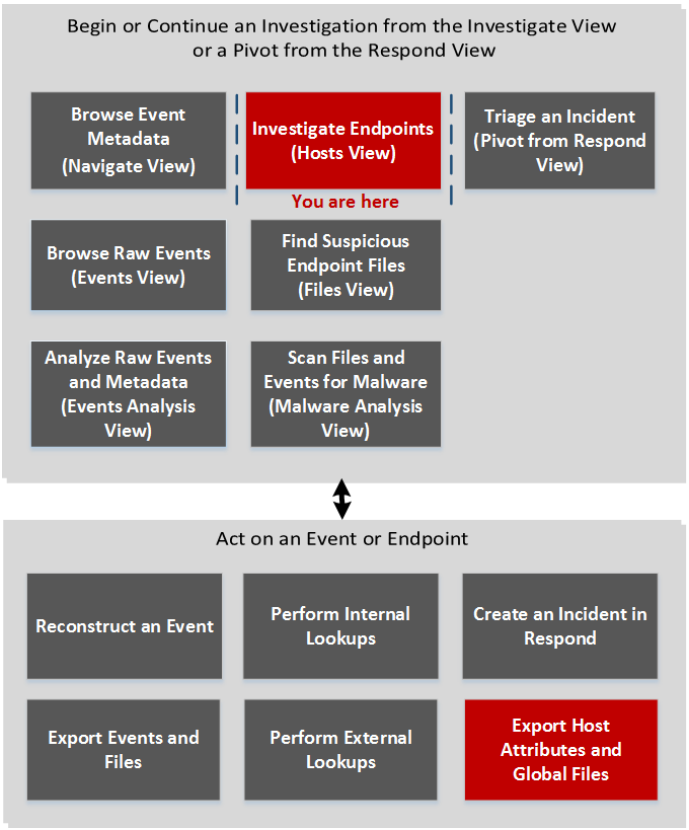
6 **Pivoter vers les vues Naviguer et Analyse d'événements**. Pour rechercher un hôte, une adresse IP ou un nom d'utilisateur spécifique, vous pouvez faire pivoter les vues Naviguer et Analyse d'événements. Pour plus d'informations, voir Pivoter vers les vues Naviguer et Analyse d'événements..

Vue Hôtes - Onglet Exécutions automatiques

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Le panneau Exécutions automatiques fournit la liste des exécutions automatiques, des services, des tâches et des tâches cron s'exécutant sur l'hôte. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Exécutions automatiques**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Evénements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les exécutions automatiques, services et tâches cron en cours d'exécution sur l'hôte*	Analyser les exécutions automatiques

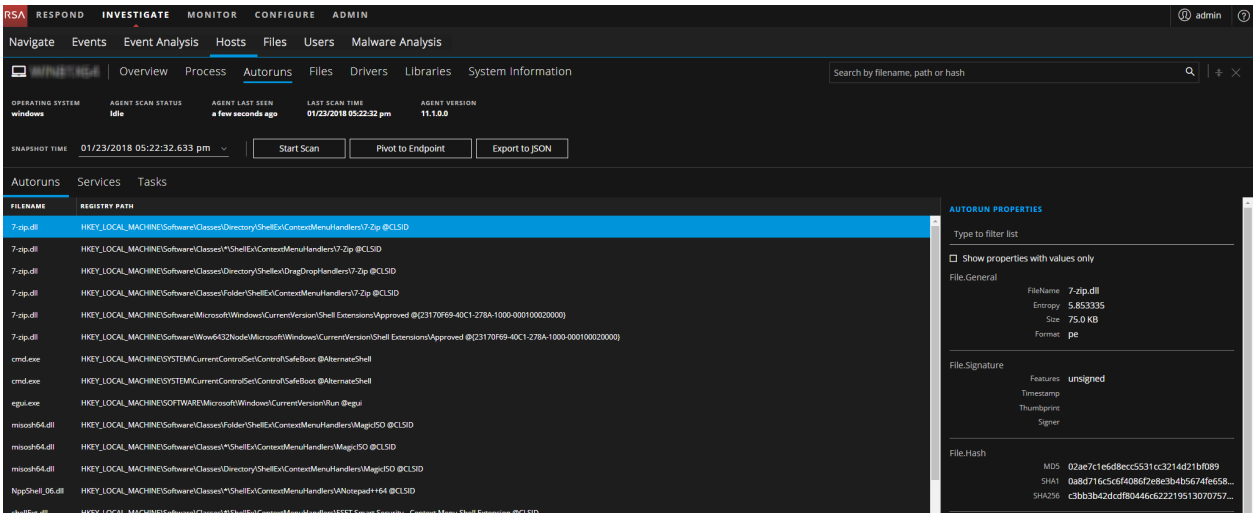
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Exécutions automatiques :



Catégorie	Description
Exécutions automatiques	Fichiers qui sont exécutés au démarrage. Il affiche les colonnes suivantes : • Nom de fichier - `cmd.exe` • Chemin de registre - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot @AlternateShell`
Services	Fichiers qui s'exécutent en tant que service pour l'hôte sélectionné. Il affiche les colonnes suivantes : • Nom du service - `acsock` • État en cours d'exécution :`stopped` • Heure de création du fichier - `07/11/2017 11:47:00 am` • Signature - `Microsoft, signed, valid` • Chemin d'accès du fichier - `C:\Windows\System32\drivers`
Tâches/tâches Cron	Fichiers configurés pour s'exécuter en tant que tâches planifiées avec le déclencheur. Il affiche les colonnes suivantes : • Nom - `shell32.dll` • Hachage - `cafa6e7b6a9220e7c805ea476a89a78800f48bb48c66fe5f935057940df3909c` • Dernière heure d'exécution - `01/19/2018 05:34:50 pm` • Prochaine heure d'exécution - `12/30/1899 05:30:00 am` • Déclencheur - `No Trigger`

Panneau Propriétés des exécutions automatiques

Ce panneau affiche toutes les propriétés du fichier sélectionné. Il se présente comme suit :

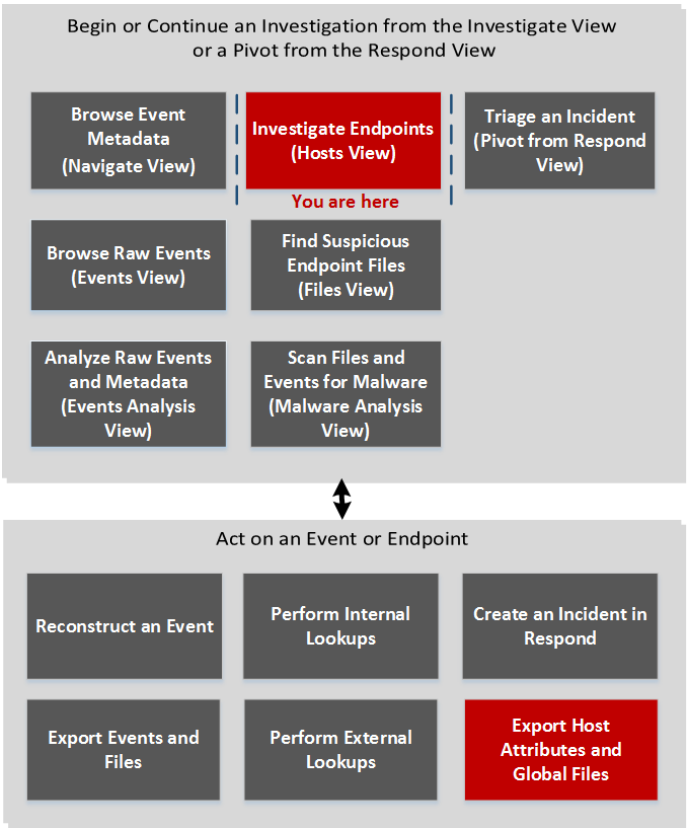
Catégorie	Description
Signature	Fournit des informations sur le signataire.
Hachage	Type de hachage du fichier (MD5, SHA256 et SHA1).
Heure	Heure à laquelle le fichier a été créé, modifié ou ouvert.
Lieu	Emplacement du fichier.
Image	Charger l'image

Vue Hôtes - Onglet Pilotes

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

L'onglet Pilotes répertorie les pilotes en cours d'exécution sur les hôtes au moment de l'analyse. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Pilotes**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les pilotes en cours d'exécution sur l'hôte*	Examiner les hôtes

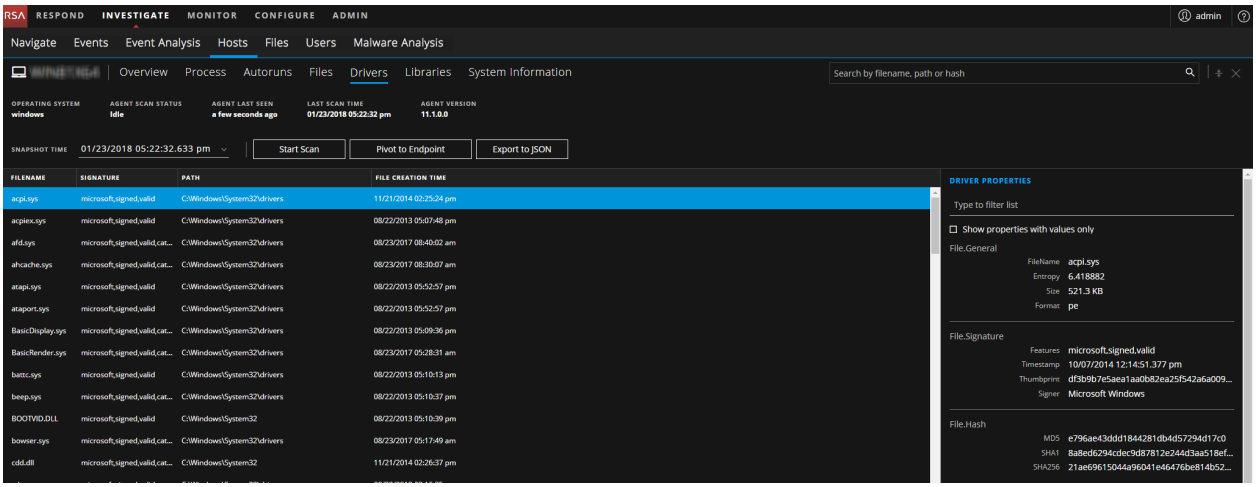
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Pilotes :



Champ	Description
Nom du fichier	Nom du fichier. Par exemple, `acpi.sys`.
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires.
Chemin	Chemin du fichier. Par exemple, `C:\Windows\System32\drivers`.
Heure de création du fichier	Heure à laquelle le fichier a été créé.

Panneau Propriétés du pilote

Ce panneau affiche toutes les propriétés du fichier sélectionné. Il se présente comme suit :

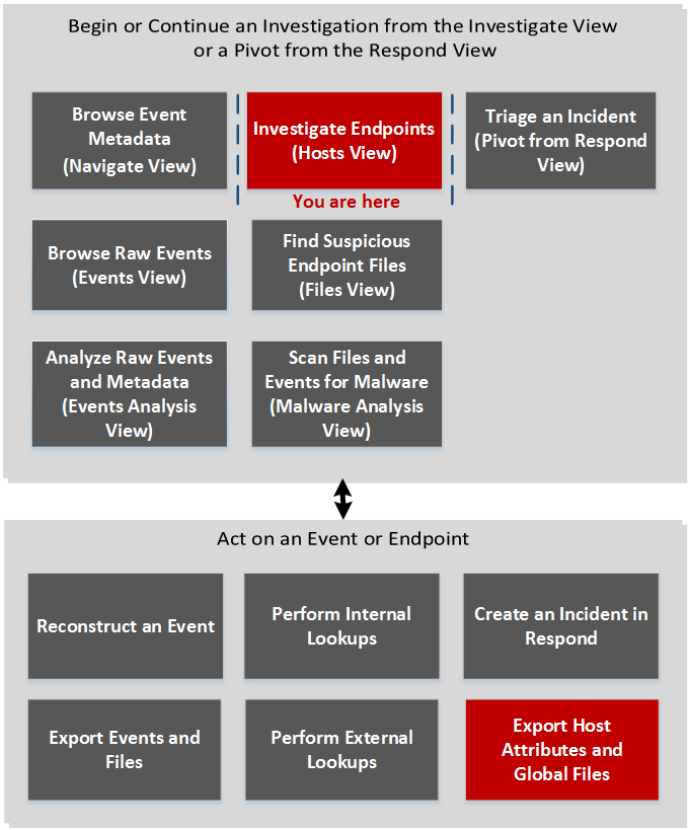
Catégorie	Description
Général	Informations générales sur le fichier, telles que le nom de fichier, l'entropie, la taille et le format.
Signature	Fournit des informations sur le signataire.
Hachage	Type de hachage du fichier (MD5, SHA256 et SHA1).
Heure	Heure à laquelle le fichier a été créé, modifié ou ouvert.
Lieu	Emplacement du fichier.
Image	Image chargée.

Vue Hôtes - Onglet Fichiers

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

L'onglet Fichiers affiche tous les fichiers analysés sur l'hôte. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Fichiers**. Par défaut, 100 fichiers sont affichés. Pour afficher plus de fichiers, cliquez sur **Charger davantage** au bas de la page.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les fichiers analysés sur l'hôte*	Analyser les fichiers

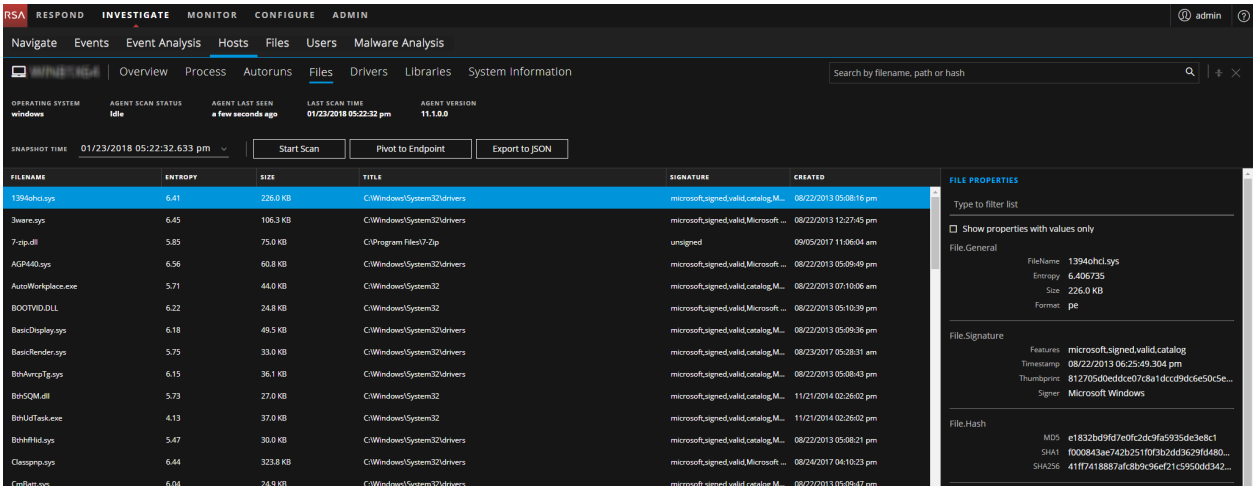
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Fichiers :



Champ	Description
Nom du fichier	Nom du fichier. Par exemple, `7-zip.dll`.
Entropie	Entropie des données d'image, à l'exclusion des en-têtes PE. Détermine si le contenu est compacté (compressé ou chiffré).
Taille	Taille du fichier. Peut être un indicateur lors de l'accès à un fichier.
Chemin	Chemin du fichier. Parfois, les auteurs de programmes malveillants placent le fichier dans des répertoires où il n'y a généralement pas de fichiers de ce type. Les fichiers malveillants sont généralement des fichiers autonomes (par exemple, un fichier à la racine `C:\ProgramData`) par rapport à un groupe de fichiers dans un dossier légitime (par exemple, les fichiers figurant dans `C:\Program Files\<folder name>\`).
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires.
Créé	Horodatage du fichier.
Nom d'utilisateur	Utilisateur du fichier (pour Linux). Par exemple, `root`.
Nom du groupe	Groupe auquel appartient l'utilisateur (pour Linux). Par exemple, `root (0)`.

Panneau Propriétés du fichier

Ce panneau affiche toutes les propriétés du fichier sélectionné. Il se présente comme suit :

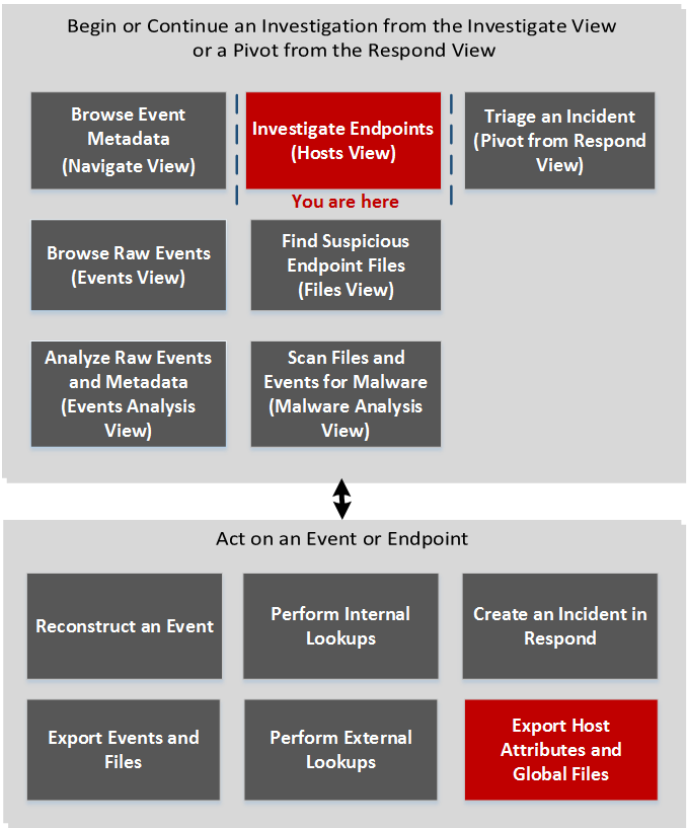
Catégorie	Description
Général	Informations générales sur le fichier, telles que le nom de fichier, l'entropie, la taille et le format.
Signature	Fournit des informations sur le signataire.
Hachage	Type de hachage du fichier (MD5, SHA256 et SHA1).
Heure	Heure à laquelle le fichier a été créé, modifié ou ouvert.
Lieu	Emplacement du fichier.

Vue Hôtes - Onglet Bibliothèques

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

L'onglet Bibliothèques répertorie les bibliothèques chargées au moment de l'analyse. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Bibliothèques**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les bibliothèques chargées*	Analyse des bibliothèques

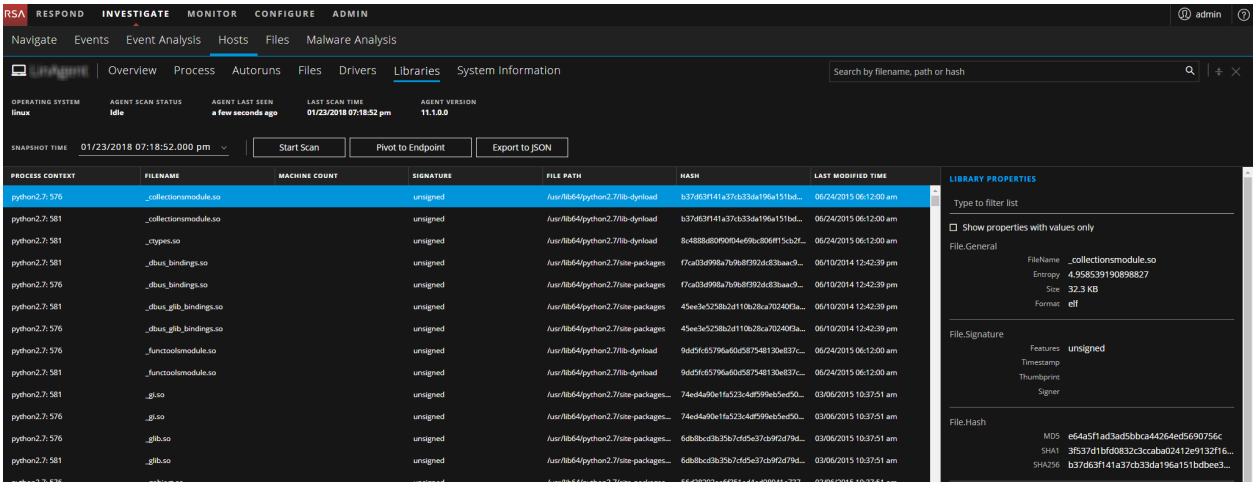
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Bibliothèques :



Champ	Description
Contexte du processus	Nom et PID du processus ayant chargé la bibliothèque dans la mémoire. Par exemple, `explorer.exe: 1916`.
Nom du fichier	Nom du fichier. Par exemple, `7-zip.dll`.
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires. Par exemple, `signed, valid`.
Chemin de fichier	Chemin du fichier. Par exemple, `C:\Program Files\7-Zip`.
Hachage	Fonction SHA256 du fichier. Par exemple, `c3bb3b42dcdf80446c622219513070757e618c06afd9ee0ac37cbce5befcb897`.
Heure de création du fichier	Heure à laquelle le fichier a été créé.
Heure de la dernière modification	Heure de modification du fichier.

Panneau Propriétés de la bibliothèque

Ce panneau affiche toutes les propriétés du fichier sélectionné. Il se présente comme suit :

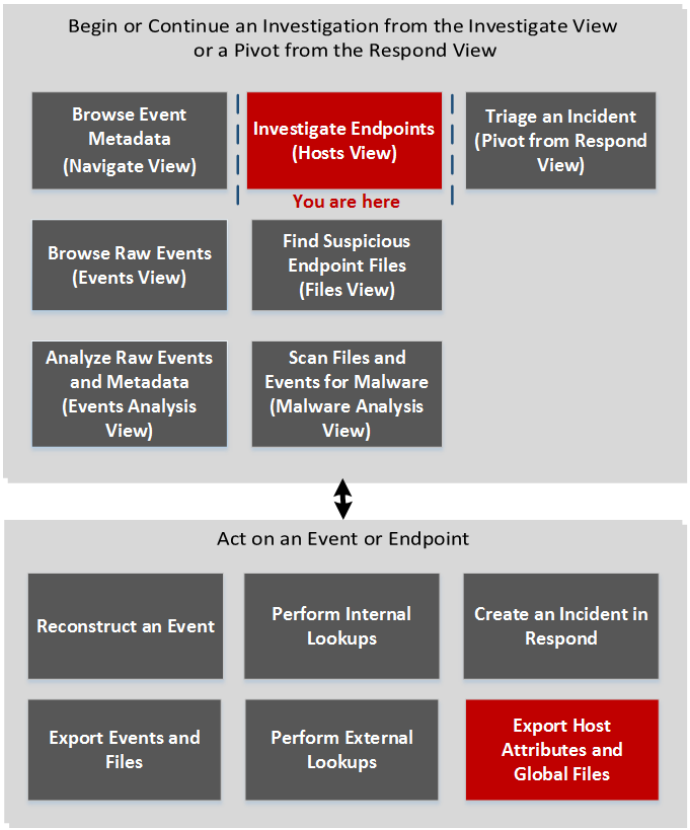
Catégorie	Description
Général	Informations générales sur le fichier, telles que le nom de fichier, l'entropie, la taille et le format.
Signature	Fournit des informations sur le signataire.
Hachage	Type de hachage du fichier (MD5, SHA256 et SHA1).
Heure	Heure à laquelle le fichier a été créé, modifié ou ouvert.
Lieu	Emplacement du fichier.
Processus	Détails du processus : taille de l'image et PID.

Vue Hôtes - Onglet Présentation

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

L'onglet Présentation fournit les résultats détaillés de l'analyse de l'hôte sélectionné. Par défaut, les résultats de la dernière analyse s'affichent. Pour accéder à cette vue, accédez à **ENQUÊTER > Hôtes**, puis sélectionnez un hôte dans la vue **Hôtes**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher un résumé de l'hôte*	Examiner les hôtes

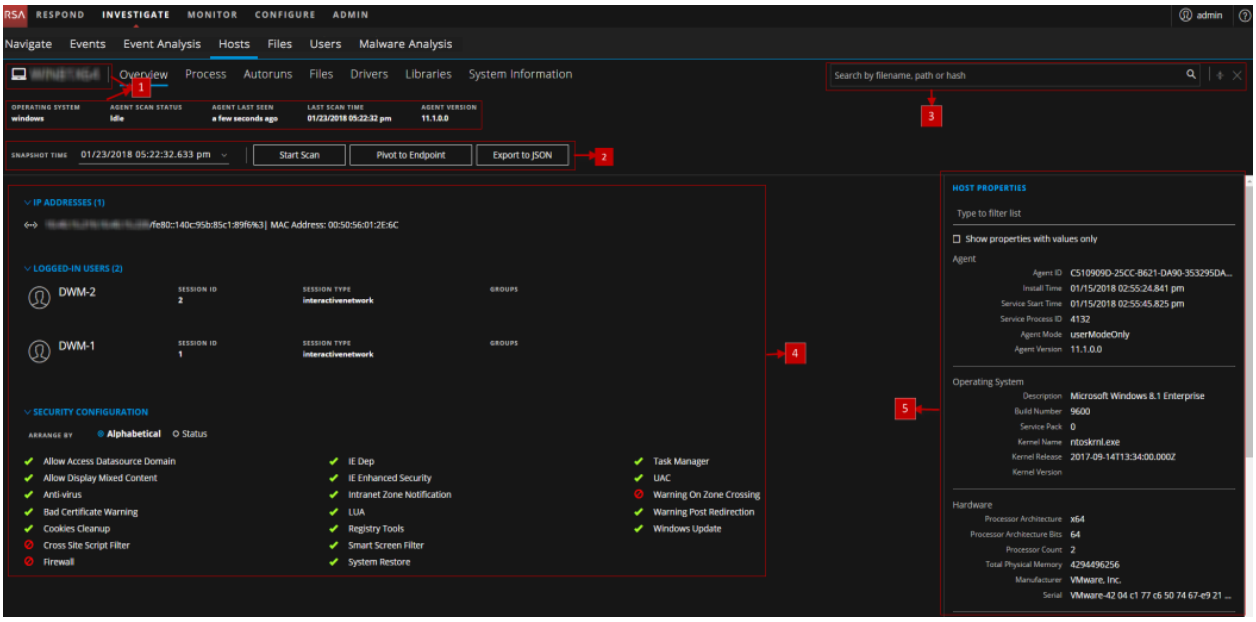
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Présentation :



1	**Détails de l'agent et de l'analyse**. Vous pouvez afficher les détails suivants relatifs à l'agent et à l'analyse pour l'hôte sélectionné : **Nom d'hôte** : Nom de l'hôte Par exemple, `WIN-ABC`. **Système d'exploitation** - Système d'exploitation sur lequel l'agent est en cours d'exécution (Linux, Windows ou Mac). **État d'analyse de l'agent** - État actuel de l'analyse - Inactif, Analyse en cours, Démarrage de l'analyse ou Arrêt de l'analyse. Pour plus d'informations, voir Examiner les hôtes. **Dernière consultation de l'agent** - Heure de la dernière communication de l'agent avec le serveur. **Heure de la dernière analyse** - Dernière fois que l'agent a été analysé. La date et l'heure correspondent au fuseau horaire défini dans les préférences utilisateur et sont locales au serveur. **Version d'agent** : Version de l'agent. Par exemple, `11.1.0.0`.
2	**Actions disponibles dans la barre d'outils :** **Date du snapshot** - Indique les horodatages analysés. Pour afficher l'historique d'analyse, sélectionnez le snapshot dans le menu déroulant. **Démarrer l'analyse** - Démarre une analyse pour les hôtes sélectionnés. Pour plus d'informations, voir Examiner les hôtes. **Exporter dans un fichier CSV** - Extrait les attributs des hôtes dans un fichier CSV. Pour plus d'informations, voir Exporter les attributs de l'hôte. **Pivoter vers Endpoint** - Permet d'examiner l'hôte NetWitness Endpoint (version 4.4.0.2 ou version supérieure). Pour plus d'informations, voir Enquêter sur les hôtes NetWitness Endpoint 4.4.0.2 ou version ultérieure. **Exporter dans un fichier JSON** - Extrait les attributs de l'hôte et les données de point de terminaison dans un fichier JSON du snapshot sélectionné.
3	**Recherche dans les snapshots**. Permet d'effectuer une recherche sur tous les snapshots (nom de fichier, chemin de fichier et somme de contrôle SHA-256). Pour plus d'informations, voir Recherche dans les snapshots.

4 **Récapitulatif de l'hôte sélectionné**. Affiche les champs suivants :

Adresses IP - Adresses IP associées à l'hôte. Par exemple, `10.10.10.3`.

Utilisateurs connectés - Utilisateurs connectés à l'hôte. Par exemple, `abc`.

Configuration de la sécurité - Détails de configuration de la sécurité sur l'hôte. Par exemple, pare-feu désactivé ou activé, filtre d'écran intelligent désactivé ou activé. Ce champ s'applique uniquement à Windows et Mac.

Remarque : Version d'agent, Adresses IP, Utilisateurs connectés et Configuration de la sécurité peuvent changer pour chaque analyse.

5 **Panneau Propriétés de l'hôte**. Affiche toutes les propriétés de l'hôte sélectionné. Il se présente comme suit :

Agent - Informations relatives à l'agent, telles que l'ID de l'agent, le code d'erreur du pilote, l'heure d'installation et le mode de l'agent.

Système d'exploitation : version du système d'exploitation et informations sur la build.

Matériel - Informations relatives à l'architecture.

Interfaces réseau - Informations sur la carte réseau, notamment l'adresse Mac et la passerelle.

Utilisateur - Informations relatives à l'utilisateur.

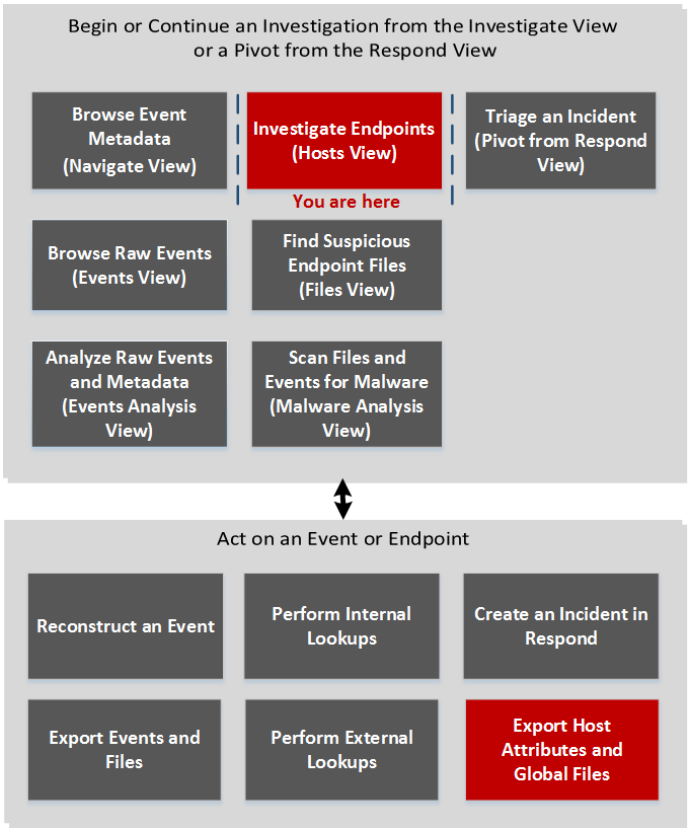
Paramètres régionaux - Fuseau horaire et langue locale de l'hôte.

Vue Hôtes - Onglet processus

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

Le panneau de processus fournit la liste des processus en cours d'exécution sur l'hôte. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Processus**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les processus en cours d'exécution sur l'hôte*	Examiner les hôtes

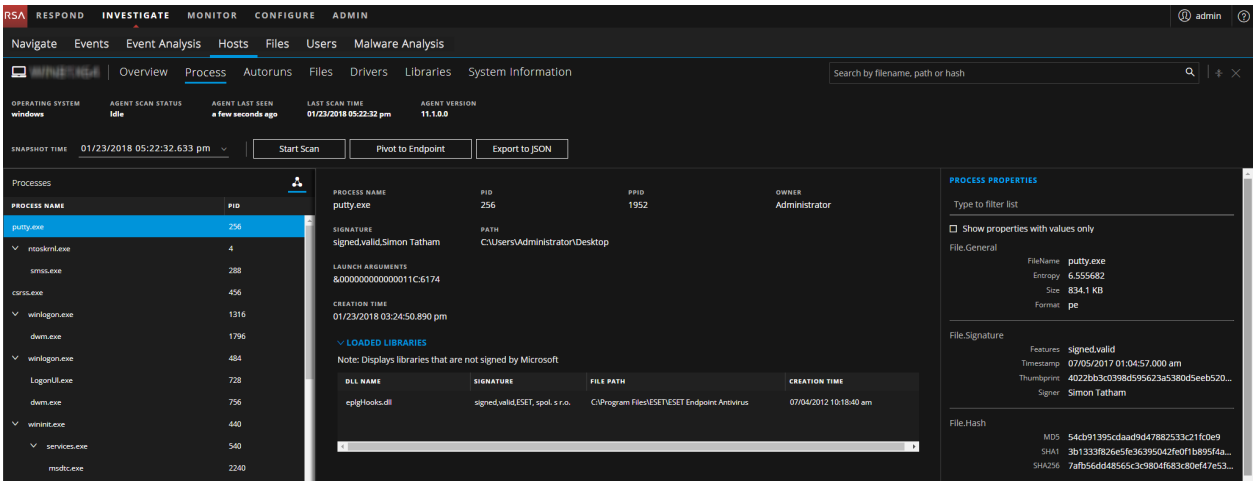
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Voici un exemple de l'onglet Processus :



Le panneau Processus affiche les informations suivantes sous Détails du processus :

Champ	Description
Nom du processus	Nom du processus. Par exemple, `server.exe`.
PID	ID du processus. Par exemple, `492`.
Processus parent (PPID)	Nom et ID du processus du parent. Par exemple, `4`.
Propriétaire	Propriétaire du processus. Par exemple, `SYSTEM`.
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires.
Chemin	Chemin du fichier associé au processus sur le disque. Par exemple, `C:\Windows\System32`.
Arguments de lancement	Arguments de ligne de commande transmis au processus lorsqu'il est lancé. Par exemple, `-k LocalServiceNoNetwork`.
Date et heure de création	Moment auquel le processus a été créé. Par exemple, `01/19/2018 11:32:29.908 am`.

- Liste des bibliothèques chargées pour le processus sélectionné, telles que les DLL (pour Windows), Dylibs (pour Mac) ou .SO (pour Linux).
- Liste des exécutions automatiques (si configuré).

Panneau Propriétés du processus

Ce panneau affiche toutes les propriétés du processus sélectionné. Il se présente comme suit :

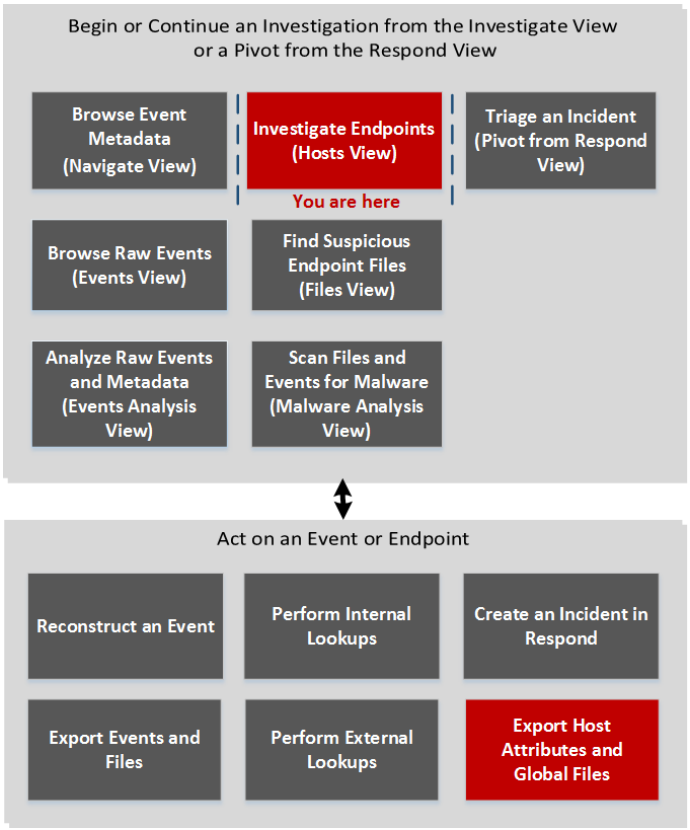
Catégorie	Description
Général	Informations générales sur le fichier, telles que le nom de fichier, l'entropie, la taille et le format.
Signature	Fournit des informations sur le signataire.
Hachage	Type de hachage de fichier (MD5, SHA1 et SHA256).
Heure	Heure à laquelle le fichier a été créé, modifié ou ouvert.
Lieu	Emplacement du fichier.
Processus	Détails du processus : taille de l'image et PID.
Image	Détails de l'image chargés par le processus.

Vue Hôtes - Onglet Informations du système

Remarque : Les informations de cette rubrique s'appliquent à RSA NetWitness® Platform version 11.1 ou ultérieure.

L'onglet Informations du système répertorie les informations du système de l'agent. Pour accéder à cet onglet, sélectionnez un hôte dans la vue **Hôtes**, puis cliquez sur l'onglet **Informations du système**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)*	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	afficher les informations du système de l'agent*	Analyser les informations du système

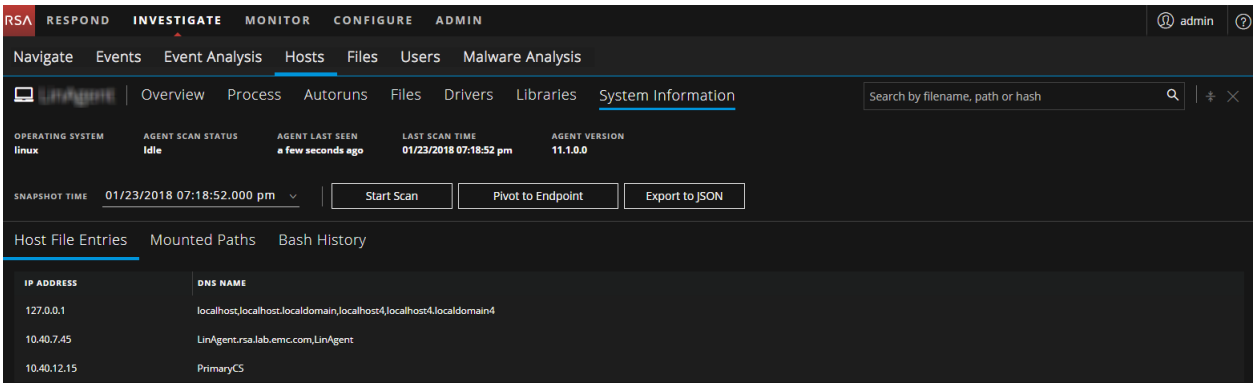
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Enquête sur les hôtes et les fichiers
- Vue Hôtes

Aperçu rapide

Vous trouverez ci-dessous un exemple de l'onglet Informations du système :



Champ	Description
Entrées de fichiers hôtes	Toutes les redirections réseau écrites dans le fichier hôte. Par exemple, l'adresse IP - `10.10.10.3` et un nom DNS - `localhost,localhost.localdomain,localhost4,localhost4.localdomain4`
Partages réseau	Nom du réseau de la ressource partagée (pour Windows uniquement). Par exemple, Nom - `Admin$`, Description - `Remote Admin`, Chemin - `C:\`, Autorisations - `None`, Type - `disk, special`, Utilisateurs max. - `4294967295`, Utilisateurs actuels - `0`.
Produits de sécurité	Produits de sécurité installés (pour Windows uniquement). Par exemple, Nom d'affichage - `Windows Defender`, Instance - `D68DDC3A-831F-4FAE-9E44-DA132C1ACF46`, Fonctions - `Enabled`, Type - `antiVirus`.
Correctifs Windows	Liste complète des correctifs appliqués par Windows Update (pour Windows uniquement). Par exemple, `KB2959936`.
Chemins d'accès montés	Chemin d'accès monté. Par exemple, Chemin - `/`, Système de fichiers - `rootfs`, Chemin d'accès distant - `rootfs`, Options - `rw`.
Historique de bash	Nom d'utilisateur et exécution de commande. Par exemple, Nom d'utilisateur - `root` et commande - `ls`.

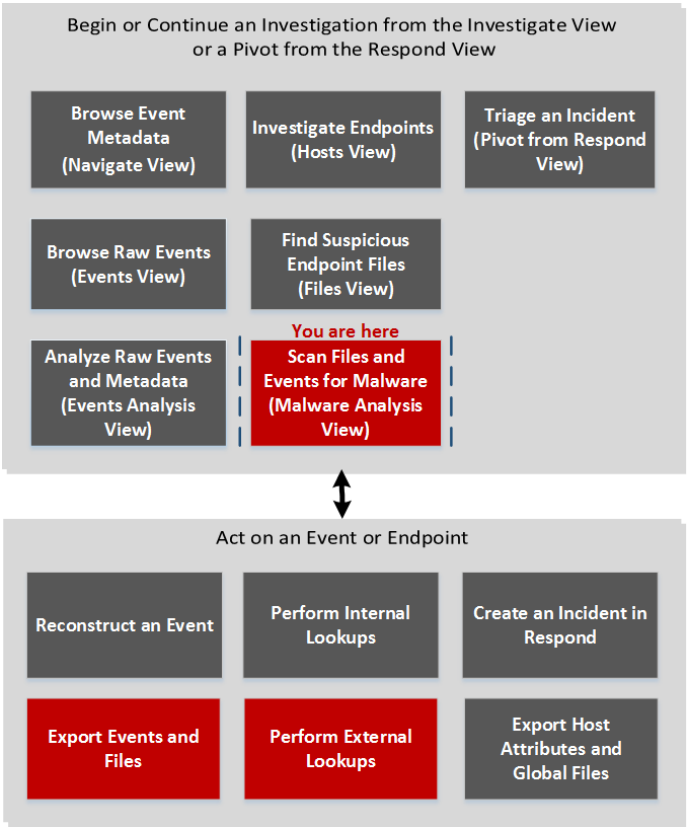
Remarque : Pour les hôtes Mac, les champs Chemins d'accès montés et Historique de bash sont vides.

Vue Analyse de malware

Dans NetWitness Investigate, la vue Malware Analysis fournit l'interface utilisateur permettant d'effectuer une analyse des malware. La vue Malware Analysis se présente sous la forme d'un tableau de bord personnalisable, dans lequel les dashlets par défaut de la vue initiale sont basés sur le rôle de l'utilisateur (administrateur ou analyste) et les personnalisations de l'utilisateur. Initialement, le dashlet Récapitulatif des événements s'affichait dans la vue Malware Analysis. D'autres dashlets présentent des visualisations différentes des événements en cours d'affichage, et chaque représentation est configurable pour affiner votre vue lorsque vous recherchez des indicateurs de compromission. Les dashlets Malware Analysis disponibles dans le tableau de bord sont également disponibles dans la vue Malware.

Pour accéder à cette vue, sélectionnez **ENQUÊTER > Malware Analysis.** Si aucun service par défaut n'est sélectionné, la boîte de dialogue Sélectionner un service Malware Analysis. Sélectionnez un service, puis cliquez sur **Afficher le mode continu**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants*	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	exporter les événements et les fichiers*	Examiner les fichiers et événements d'analyse dans le formulaire de liste
Responsable de la recherche des menaces	effectuer des recherches externes*	Afficher l'analyse Malware Analysis détaillée d'un événement

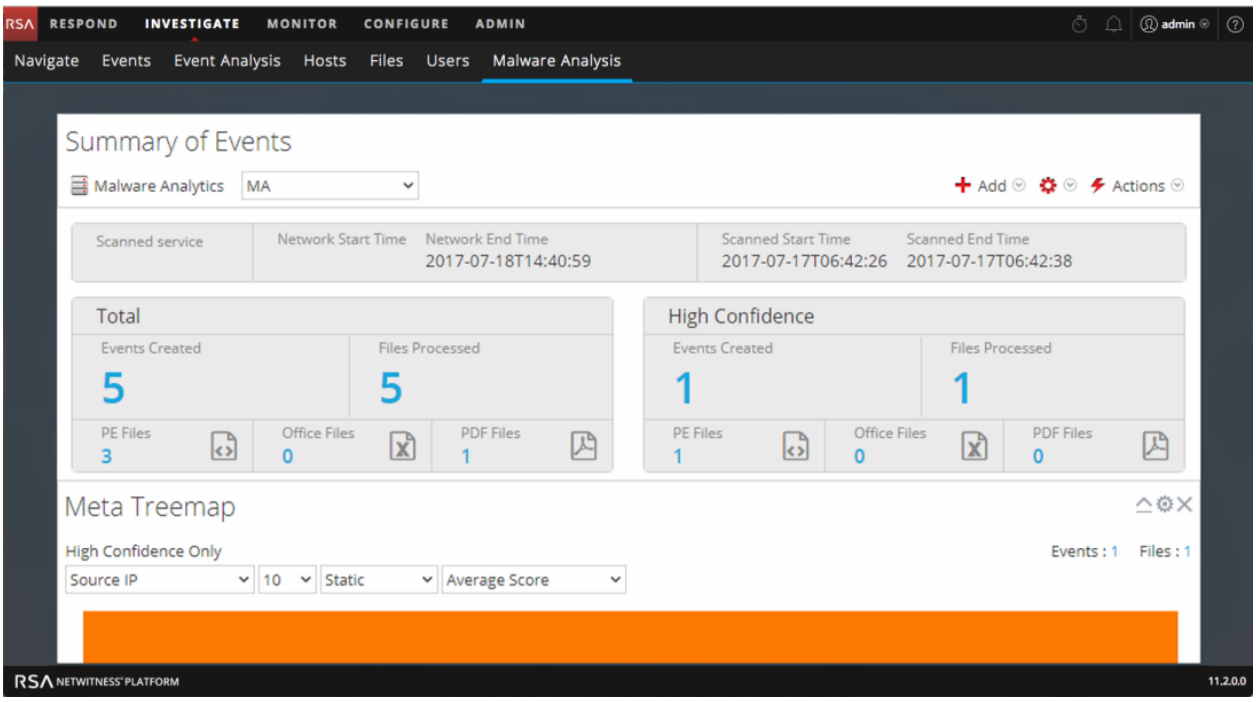
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Lancer une analyse Malware Analysis à partir de la vue Naviguer

Aperçu rapide

Voici un exemple de la vue Malware Analysis.



La vue Malware Analysis se compose du panneau Récapitulatif des événements et de quatre dashlets. Chacun des dashlets uniques contient des boîtes de dialogue d'options. Les dashlets Malware Analysis dans le tableau de bord SURVEILLER sont également disponibles et sont décrites dans la rubrique Dashlets au sein de l'espace Contenu RSA de RSANetWitness Platform.

Panneau Récapitulatif des événements

Dans le panneau Récapitulatif des événements, vous pouvez sélectionner le service, le mode d'analyse et la période. De plus, vous pouvez sélectionner un point de données et afficher les événements associés à l'événement.

Le tableau suivant décrit toutes les fonctionnalités du panneau Récapitulatif des événements.

Fonctionnalité	Description
	Sélectionne un service à afficher.
Mode d'analyse	Affiche la liste déroulante des modes d'analyse disponibles.
Période	Affiche la liste déroulante des périodes pour visualiser les événements.
Date de début	Lorsque la période est définie sur Personnalisé, fournit un calendrier à partir duquel choisir la date de début de la période.
Date de fin	Lorsque la période est définie sur Personnalisé, fournit un calendrier à partir duquel choisir la date de fin de la période.
	Affiche la liste déroulante des dashlets que vous pouvez ajouter à la vue.

Fonctionnalité	Description
	Affiche la liste déroulante des actions que vous pouvez effectuer dans cette vue : • Restaurer la configuration par défaut • Organiser les dashlets • Appliquer le filtre de seuil
	Actualise la vue Malware Analysis.

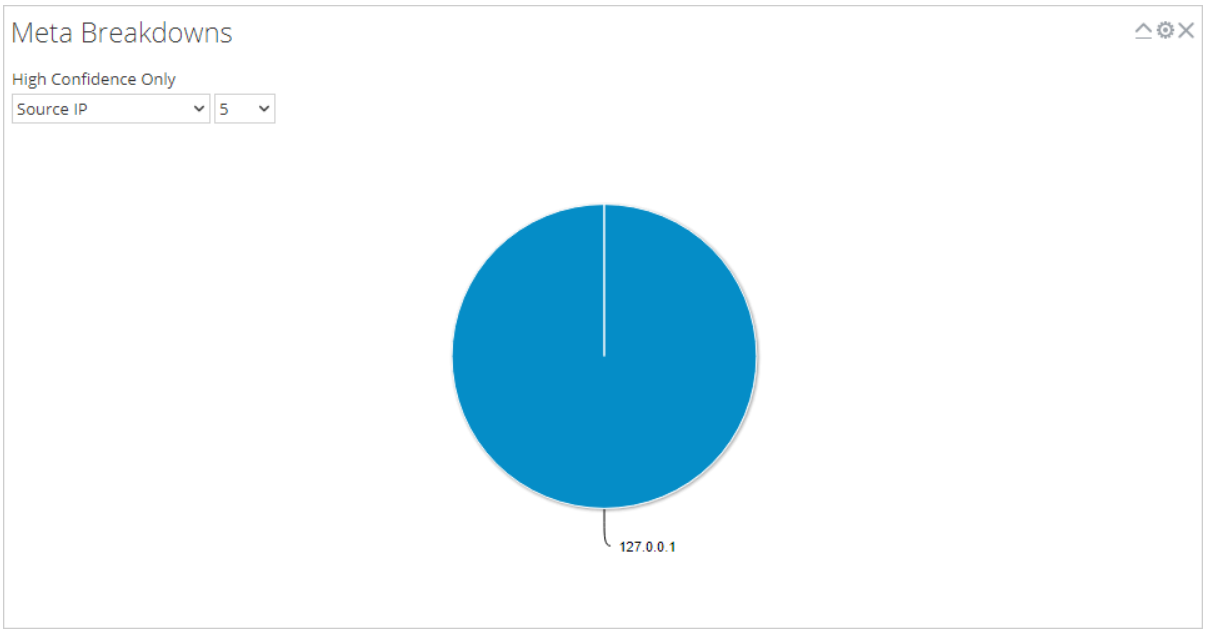
Boîte de dialogue Options

La boîte de dialogue Options vous permet de personnaliser les résultats affichés dans le dashlet. Elle est accessible en cliquant sur l'icône située dans l'angle supérieur droit de chaque dashlet. Le tableau suivant décrit les fonctions de la boîte de dialogue Options.

Fonctionnalité	Description
Titre	Indique si les données affichées sont limitées aux événements indiqués en tant que confiance élevée ou non. Si les données ne sont pas limitées, cette ligne ne s'affichera pas.
Influencé par la forte probabilité uniquement	Indique si les données affichées sont limitées aux événements indiqués en tant que confiance élevée.
Statique, Réseau, Communauté, Sandbox	Vous permet de filtrer les résultats en fonction des notes dans les modules de notation.
Annuler	Ferme la boîte de dialogue sans enregistrer les modifications.
Appliquer	Applique immédiatement les modifications au dashlet et ferme la boîte de dialogue.

Répartition des méta

Le dashlet Répartition des méta présente les événements sous la forme d'un graphique circulaire, avec chaque tranche représentant une métavaleur pour la clé méta spécifiée. Vous pouvez sélectionner la clé méta et le nombre de métavaleurs pour cette clé à afficher dans le graphique, en commençant par la valeur méta ayant le plus d'événements. Le pointage de la souris sur un événement permet d'en afficher le nombre.

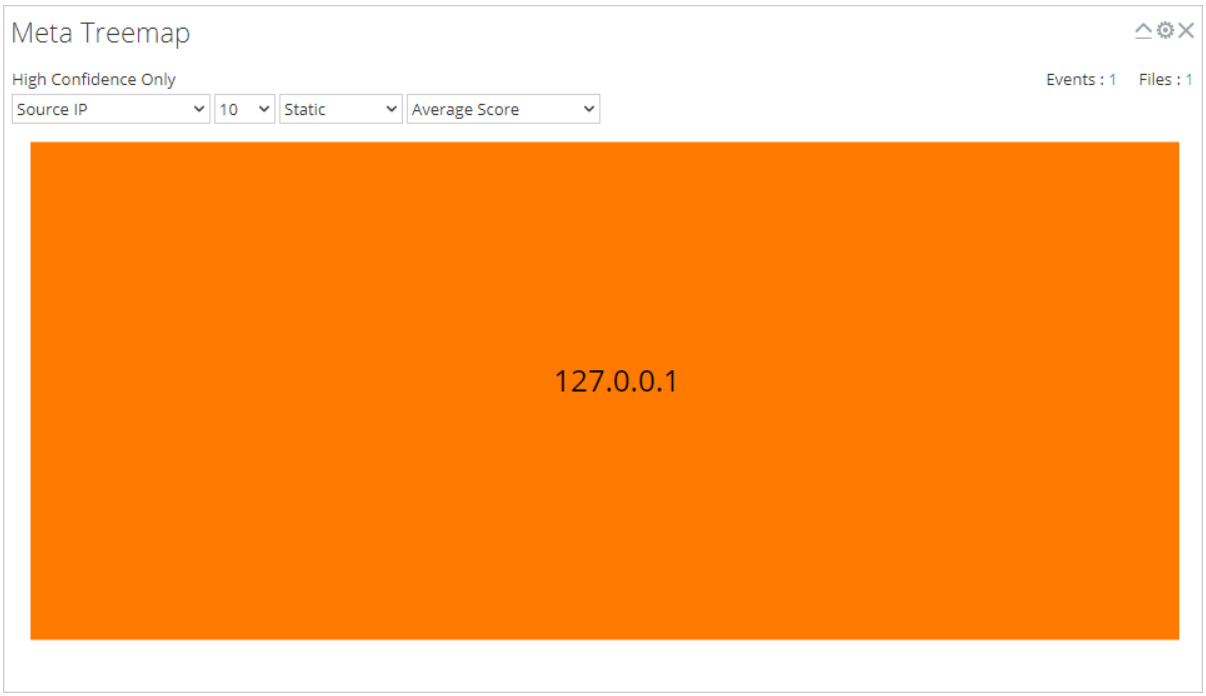


Le tableau suivant décrit les options du dashlet Répartition des méta.

Fonctionnalité	Description
Forte probabilité uniquement	Indique si les données affichées sont limitées aux événements indiqués en tant que confiance élevée ou non. Si les données ne sont pas limitées, cette ligne ne s'affichera pas.
Clé méta	Liste déroulante des clés méta disponibles.
Nombre	Liste déroulante indiquant combien de résultats supérieurs sont affichés.

Compartimentage des méta

Compartimentage des méta présente les événements sous la forme d'une carte d'utilisation. Vous pouvez sélectionner la clé meta et le nombre de valeurs méta pour cette clé à afficher dans le graphique, en commençant par les métavaleurs ayant le plus d'événements. En outre, vous pouvez sélectionner le module qui a détecté la métavaleur dans les événements : statique, réseau, communauté ou sandbox.

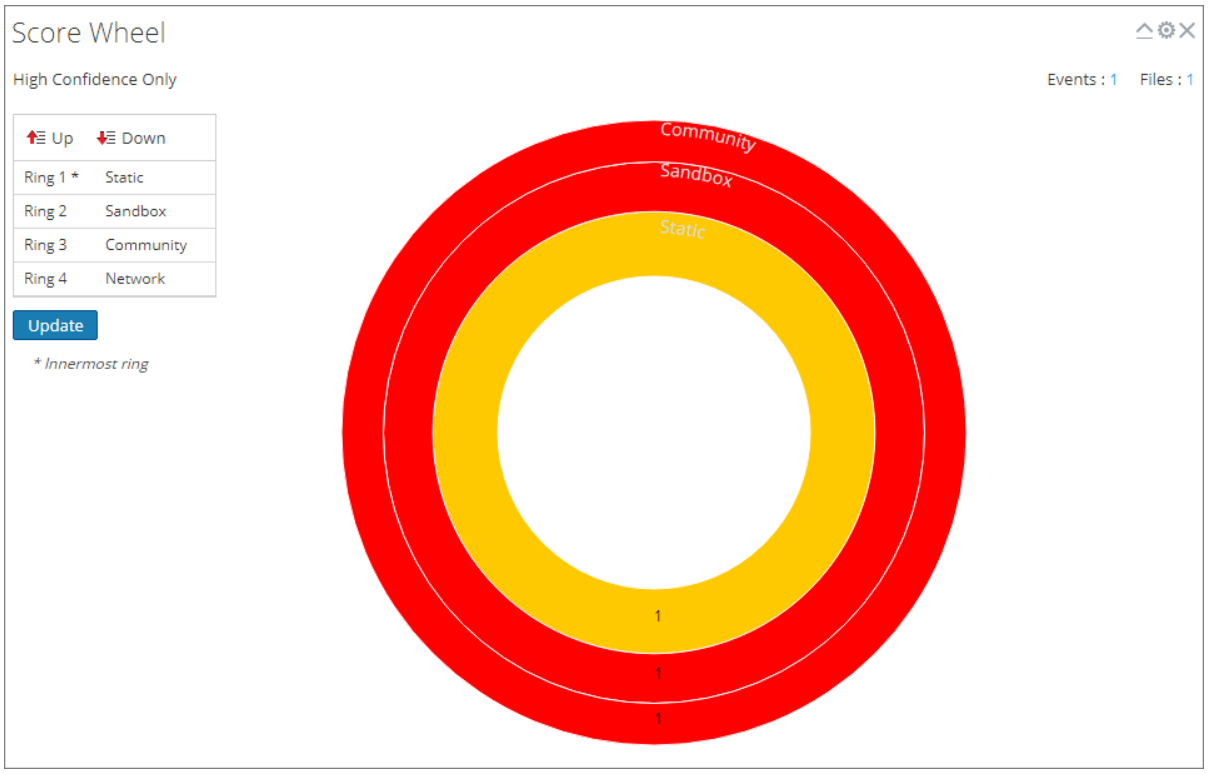


Le tableau suivant décrit les options du dashlet Compartimentage des méta.

Fonctionnalité	Description
Forte probabilité uniquement	Indique si les résultats sont limités aux événements indiqués en tant que confiance élevée ou non. Si les résultats ne sont pas restreints, cette ligne ne s'affiche pas.
Clé méta	Liste déroulante des clés méta pouvant être sélectionnées en tant que filtre.
Nombre	Liste déroulante indiquant combien de résultats supérieurs sont affichés.
Module	Liste déroulante spécifiant les résultats du module qui seront extraits.
Valeur	Liste déroulante spécifiant les informations qui s'afficheront lorsque la souris est positionnée sur un résultat (par exemple, Score moyen).

Roue des scores

La roue des scores offre une vue des événements sous la forme d'anneaux concentriques avec des couleurs représentant les scores des événements basés sur les indicateurs de compromission et le module de notation. Vous pouvez organiser la position des anneaux à l'aide des flèches vers le haut et vers le bas pour obtenir une vue qui met en lumière les événements qui ont été détectés par un module de notation (rouge) et non détectés par les autres modules de notation.

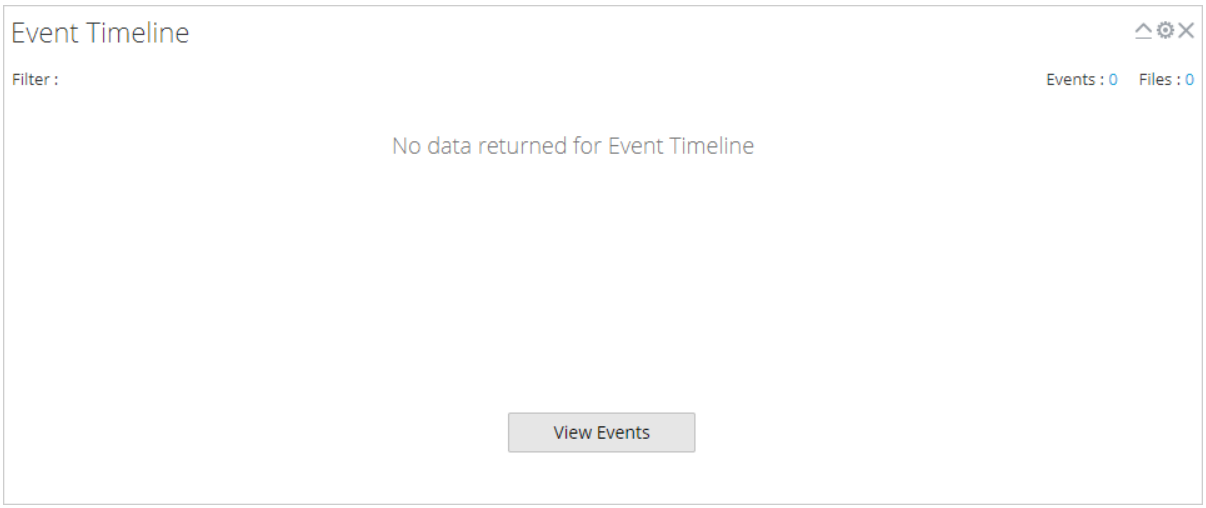


Le tableau suivant décrit les fonctionnalités du dashlet Roue des scores.

Fonctionnalité	Description
Forte probabilité uniquement	Indique si les résultats sont limités aux événements indiqués en tant que confiance élevée ou non. Si les résultats ne sont pas restreints, cette ligne ne s'affiche pas.
Grille Ordre des modules	Affiche l'ordre des anneaux dans la roue des scores, l'anneau 1 étant l'anneau le plus à l'intérieur et l'anneau 4 étant l'anneau le plus à l'extérieur. Vous pouvez cliquer sur les boutons **Haut** et **Bas** pour réorganiser les modules. Cliquez ensuite sur **Mettre à jour** pour appliquer les modifications.

Chronologie d'événements

Chronologie d'événements offre une vue des événements organisés par heure d'apparition dans un graphique à barres. Cliquer et faire glisser une période dans le graphique permet de zoomer sur l'heure sélectionnée.



Le tableau suivant décrit les fonctionnalités du dashlet Chronologie d'événements.

Fonctionnalité	Description
Forte probabilité uniquement	Indique si les résultats sont limités aux événements indiqués en tant que confiance élevée ou non. Si les résultats ne sont pas restreints, cette ligne ne s'affiche pas.
Affichage des événements	Affiche la vue Procédure d'enquête > Événements.

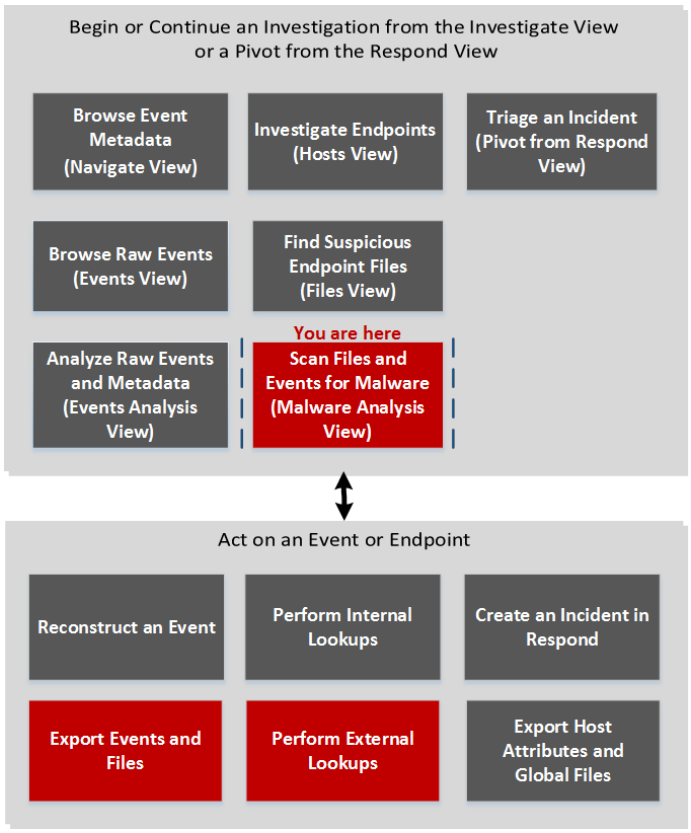
Liste d'événements d'analyse de malware et liste Fichiers

La liste d'événements Malware Analysis et la liste Fichiers présentent une vue détaillée des événements ou des fichiers. Vous pouvez double-cliquer sur un événement ou un fichier dans l'une des listes pour afficher la vue des résultats de l'analyse dans un nouvel onglet du navigateur.

Pour accéder à cette vue, allez à **ENQUÊTER > Malware Analysis** > boîte de dialogue **Sélectionner un service Malware Analysis**. Sélectionnez un service dans le panneau de gauche, puis choisissez une tâche dans le panneau de droite, puis cliquez sur **Afficher l'analyse**. Pour afficher la vue Récapitulatif des événements, procédez de l'une des façons suivantes :

- Dans le panneau **Total** ou dans le panneau **Forte probabilité**, cliquez sur le numéro dans la section **Événements créés**.
- Si vous souhaitez afficher la liste Fichiers, cliquez sur le numéro dans la section **Fichiers traités**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants*	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	exporter les événements et les fichiers*	Examiner les fichiers et événements d'analyse dans le formulaire de liste
Responsable de la recherche des menaces	effectuer des recherches externes*	Afficher l'analyse Malware Analysis détaillée d'un événement

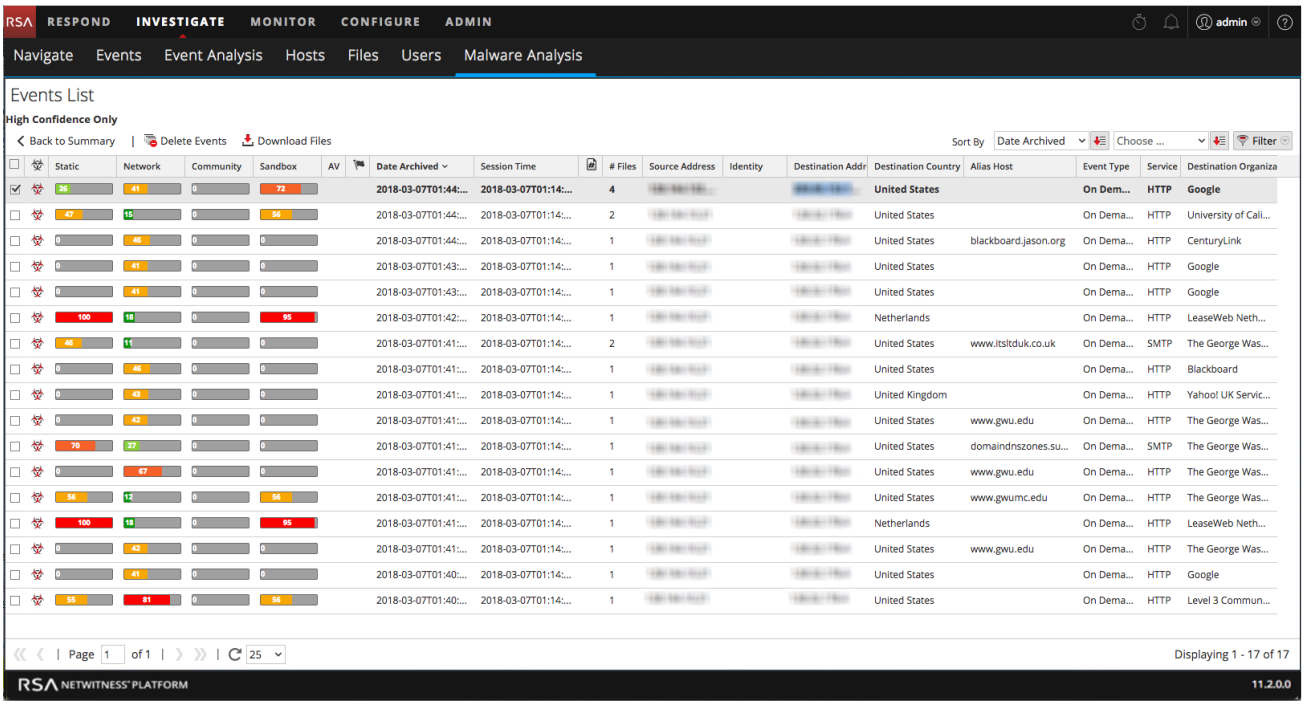
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

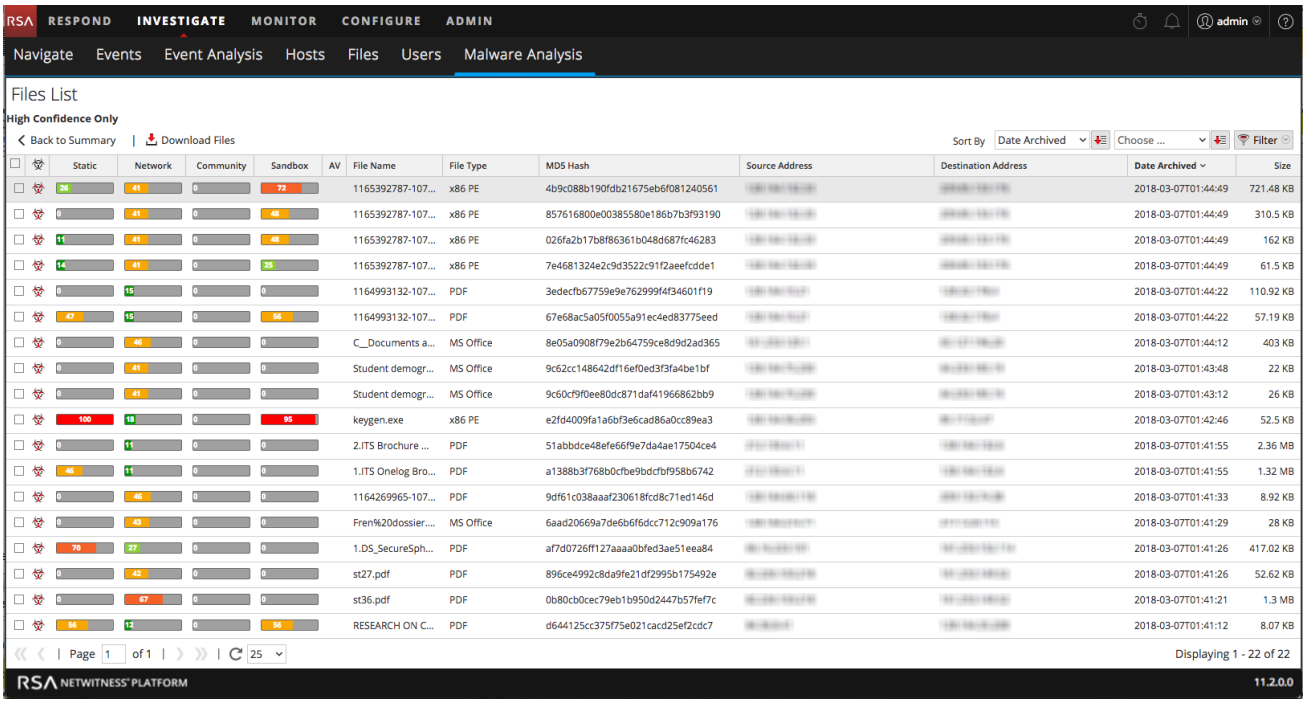
- Fonctionnement de NetWitness Investigate

Aperçu rapide

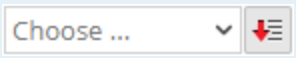
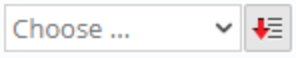
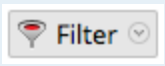
Il s'agit d'un exemple de la vue Liste des événements.



Il s'agit d'un exemple de la vue Liste de fichiers.



Voici les fonctions dans la barre d'outils de la liste d'événements. La barre d'outils de la liste des fichiers est identique, à ceci près qu'elle ne contient aucune option pour supprimer des événements.

Fonctionnalité	Description
Retour au récapitulatif	Retourne à la vue Récapitulatif des événements.
Supprimer des événements	Supprime les événements sélectionnés de la liste des événements actuels.
Télécharger les fichiers	Affiche la boîte de dialogue Téléchargement de fichier de malware, qui vous permet de télécharger les fichiers disponibles.
	Affiche un menu déroulant à partir duquel vous pouvez décider de l'ordre de tri de la liste. Les options de tri sont les suivantes : • Forte probabilité • Statique • Réseau • Communauté • Sandbox • AV • Nom de fichier • Type de fichier • Hachage • Date de l'archivage • Taille Le bouton juste à droite de cette liste déroulante indique si la liste sera triée par les valeurs croissante ou décroissante.
	Affiche un menu déroulant à partir duquel vous pouvez sélectionner un ordre de tri secondaire. Ce menu comprend une option pour NetWitness Platform**Aucun**, la sélection d'un ordre de tri secondaire n'est donc pas nécessaire.
	Affiche une fenêtre déroulante dans laquelle vous pouvez filtrer la liste par nom de fichier ou Hâchage MD5.

Voici les fonctions de la liste d'événements.

Fonctionnalité	Description
	Indique si l'événement est influencé parl'indicateur de forte probabilité.
Statique, Réseau, Communauté, Sandbox	Affiche les notes pour chaque module de note.

Fonctionnalité	Description
AV	Indique si l'AV a indiqué cet événement comme suspect.
	Indique si l'événement est influencé par une règle personnalisée.
Date de l'archivage	Affiche la date et l'heure d'archivage de l'événement.
Heure de la session	Affiche la durée de la session de l'événement.
	Indique si la valeur de hachage est marquée comme fiable.
Nombre de fichiers	Affiche le nombre de fichiers inclus dans l'événement.
Adresse source	Affiche l'adresse de la source d'événement.
Identity	Recherche l'identité de la source d'événement.
Adresse de destination	Affiche l'adresse de destination de l'événement.
Pays de destination	Affiche le pays de destination de l'événement.
Hôte de l'alias	Affiche le nom d'hôte de l'alias.
Type d'événement	Affiche le type d'événement. Par exemple, Téléchargement manuel.
Service	Affiche le service sur lequel l'événement s'est produit.
Organisation de destination	Affiche l'organisation de la destination.

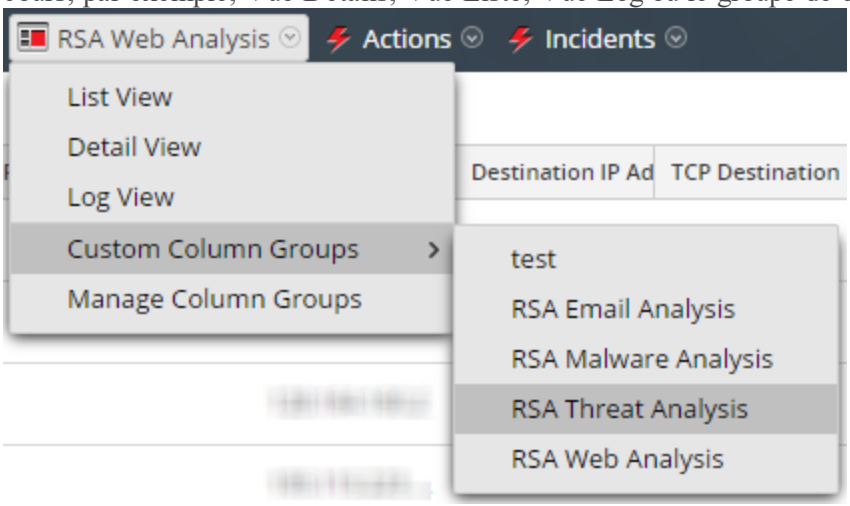
Voici les fonctions de la grille de la liste Fichiers.

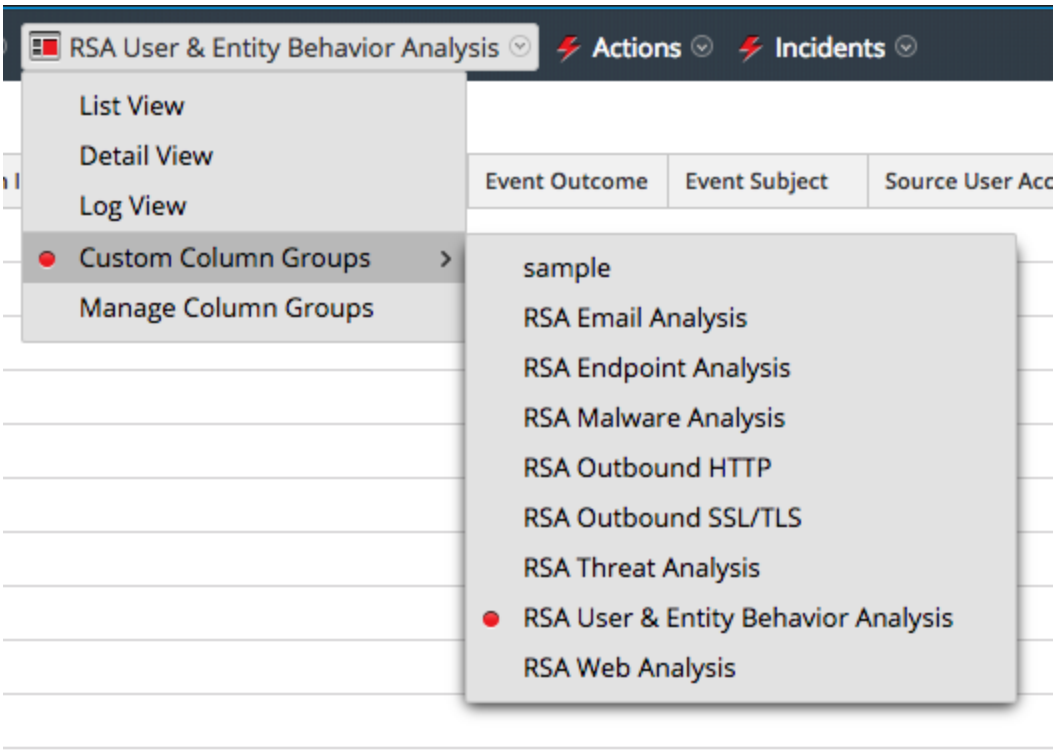
Fonctionnalité	Description
	Indique si l'événement est influencé parl'indicateur de forte probabilité.
Statique, Réseau, Communauté, Sandbox	Affiche les notes pour chaque module de note.
AV	Indique si l'AV a indiqué cet événement comme suspect.
Nom de fichier	Affiche le nom du fichier.
Type de fichier	Affiche le type de fichier (par exemple, PDF ou x86 PE)
Hachage MD5	Affiche le hachage MD5.
Adresse source	Affiche l'adresse de la source du fichier.
Adresse de destination	Affiche l'adresse de destination du fichier.
Date de l'archivage	Affiche la date et l'heure d'archivage du fichier.
Taille	Indique la taille du fichier.

Boîte de dialogue Gérer les groupes de colonnes

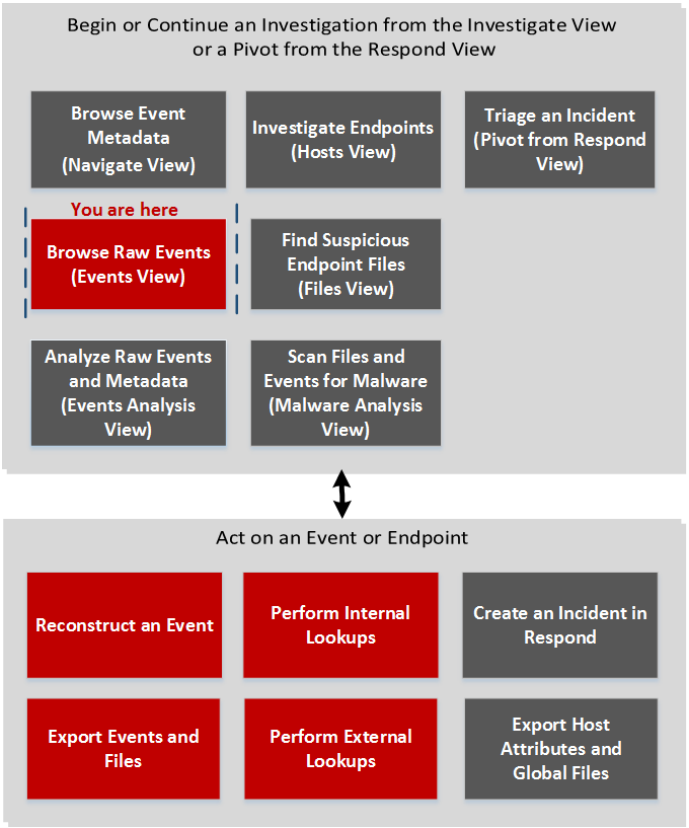
Vous pouvez personnaliser la façon dont les données s'affichent en définissant l'affichage des métadonnées dans une colonne, la position de la colonne dans la grille et la largeur par défaut de la colonne. Dans la boîte de dialogue Gérer les groupes de colonnes, vous pouvez ajouter, supprimer, importer, exporter et modifier des groupes de colonnes pour afficher des clés méta spécifiques. Lors d'une nouvelle installation, des groupes de colonnes prêts à l'emploi sont disponibles à l'utilisation dans la boîte de dialogue Gérer les groupes de colonnes. Les groupes de colonnes prêts à l'emploi sont précédés de RSA pour leur identification. Ils peuvent être dupliqués, mais pas modifiés ou supprimés. Vous pouvez également créer des groupes de colonnes personnalisés.

Pour accéder à cette boîte de dialogue, allez à **ENQUÊTER > Événements** et dans la liste déroulante **Afficher**, sélectionnez **Gérer les groupes de colonnes**. L'option **Vue** porte le nom de la valeur en cours, par exemple, Vue Détails, Vue Liste, Vue Log ou le groupe de colonnes sélectionné.




RSA User & Entity Behavior Analysis
Actions
Incidents
List View
Detail View
Log View
Custom Column Groups
Manage Column Groups
Event Outcome
Event Subject
Source User Acc
sample
RSA Email Analysis
RSA Endpoint Analysis
RSA Malware Analysis
RSA Outbound HTTP
RSA Outbound SSL/TLS
RSA Threat Analysis
RSA User & Entity Behavior Analysis
RSA Web Analysis

Workflow


Begin or Continue an Investigation from the Investigate View or a Pivot from the Respond View
Browse Event Metadata (Navigate View)
Investigate Endpoints (Hosts View)
Triage an Incident (Pivot from Respond View)
You are here
Browse Raw Events (Events View)
Find Suspicious Endpoint Files (Files View)
Analyze Raw Events and Metadata (Events Analysis View)
Scan Files and Events for Malware (Malware Analysis View)
Act on an Event or Endpoint
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files

Que voulez-vous faire ?

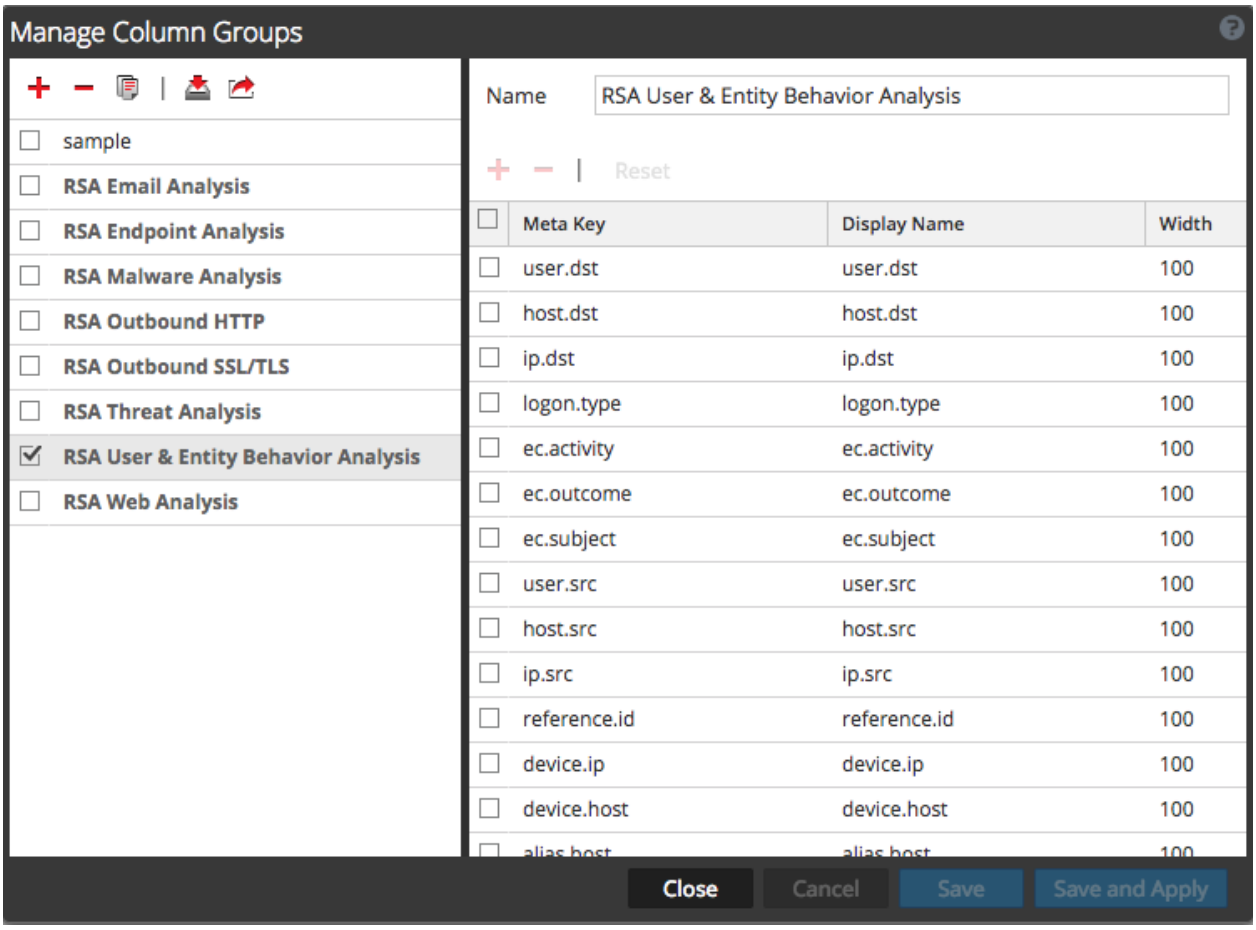
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	configurer les groupes de colonnes	Gérer des groupes de colonnes dans la vue Événements

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Événements

Aperçu rapide



La boîte de dialogue Gérer les groupes de colonnes comporte deux panneaux : Groupes et Paramètres.

Quatre boutons se trouvent en bas de cette boîte de dialogue : Fermer, Annuler, Enregistrer, et Enregistrer et appliquer. Le tableau suivant fournit une description de ces boutons.

Fonctionnalité	Description
Fermer	Ferme la boîte de dialogue sans enregistrer.
Annuler	Annule toutes les modifications non enregistrées.
Enregistrer	Enregistre toutes vos modifications sans fermer la boîte de dialogue.
Enregistrer et appliquer	Enregistre et applique immédiatement toutes les modifications, et ferme la boîte de dialogue.

Panneau Groupes

Le panneau gauche s'intitule Groupes. Vous pouvez y ajouter, supprimer, importer ou exporter des groupes de colonnes. En haut du panneau se trouve une barre d'outils qui fournit des actions. Sous la barre d'outils se trouve une liste de groupes de colonnes ajoutés, où vous pouvez sélectionner un ou plusieurs groupes.

Le tableau suivant répertorie les actions de la barre d'outils.

Action	Description
	Ajoute un groupe de colonnes. Le fait de cliquer sur ce bouton met en évidence le panneau Paramètres sur la droite, où vous pouvez nommer le groupe de colonnes et ajouter ou supprimer les métaclés. Au moins une métaclé est requise pour l'ajout d'un groupe.
	Supprime un groupe de colonnes. Une boîte de dialogue de confirmation s'affiche avant la suppression du groupe sélectionné.
	Affiche la boîte de dialogue Importer des groupes de colonnes, où vous pouvez sélectionner un fichier à télécharger.
	Exporte un ou plusieurs groupes sélectionnés sur votre ordinateur.

Panneau Paramètres

Le panneau de droite est le panneau Paramètres. Vous pouvez y créer et modifier des groupes de colonnes. Ce panneau contient le champ Nom, une barre d'outils et une grille.

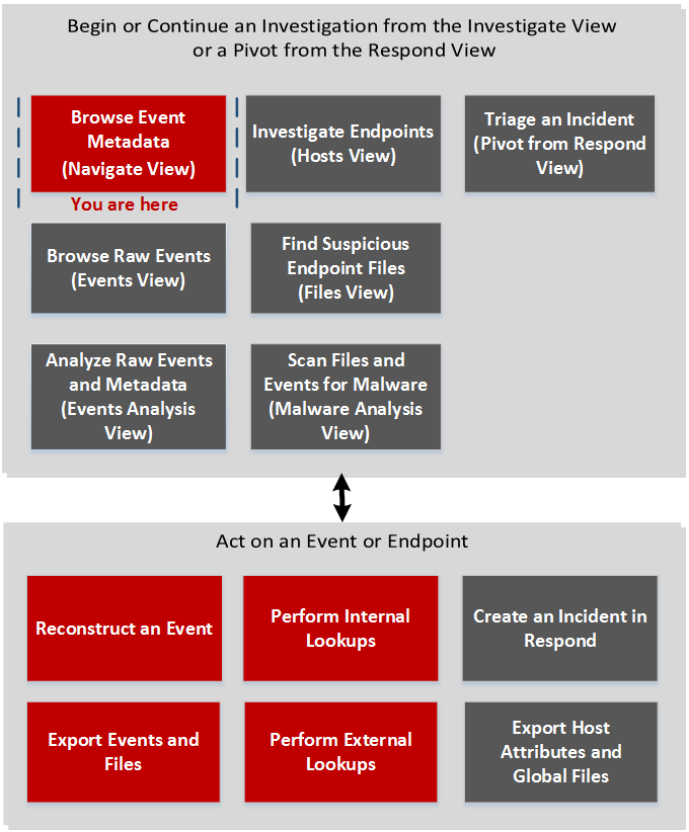
Le tableau suivant décrit les fonctions du panneau Paramètres.

Fonctionnalité	Description
Nom	Nom du groupe de colonnes sélectionné.
	Ajoute une nouvelle ligne dans la liste de métaclés, où vous pouvez ouvrir un menu déroulant pour sélectionner une nouvelle métaclé.
	Permet de supprimer une ou plusieurs métaclés sélectionnées. Affiche une boîte de dialogue de confirmation avant de supprimer.
Réinitialiser	Rétablit le groupe de colonnes à ses derniers paramètres sauvegardés.
Clé méta	Répertorie les métaclés ajoutées au groupe de colonnes sélectionné.
Nom d'affichage	Répertorie les noms des métaclés tels qu'ils seront affichés dans la vue Événements.
Largeur	Spécifie la largeur de chaque colonne de métaclés. La largeur peut être définie entre **10** et **1000**. La largeur par défaut est **100**.

Boîte de dialogue Gérer les clés méta par défaut

Dans la boîte de dialogue Gérer les clés méta par défaut, les analystes peuvent spécifier les métaclés à afficher pendant la navigation pour un service spécifique. Ceci peut vous aider à trouver les données souhaitées plus rapidement et cela empêche le chargement des métadonnées inutiles. Pour accéder à cette boîte de dialogue, dans la barre d'outils de la **vue Naviguer**, sélectionnez **Méta > Gérer les clés méta par défaut**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	configurer les clés méta par défaut pour un service*	Filtrer les résultats dans la vue Naviguer

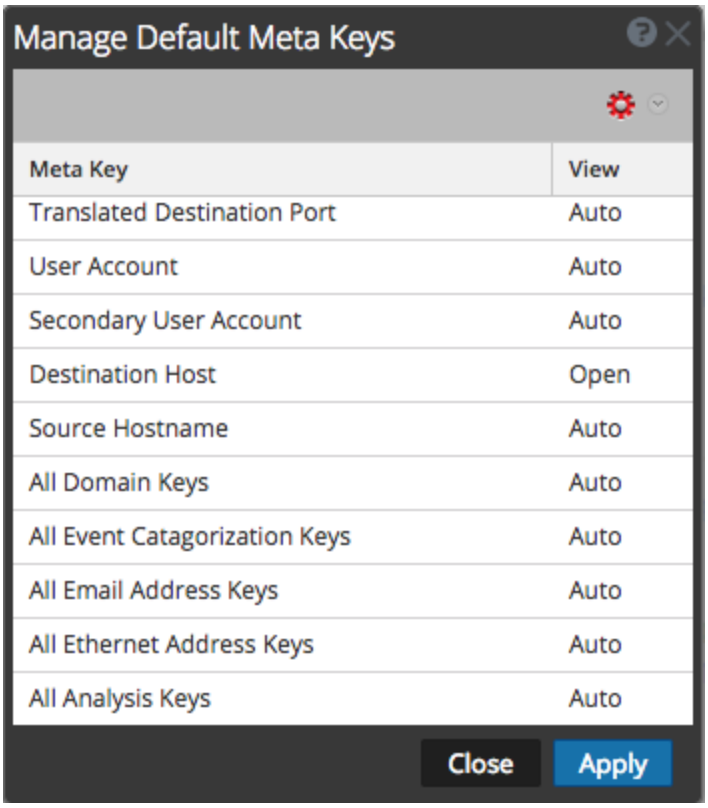
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Gérer les groupes méta
- Gérer les groupes méta

Aperçu rapide

La figure suivante illustre la boîte de dialogue Gérer les clés méta par défaut, qui contient une liste des clés méta, une barre d'outils, un bouton Fermer et un bouton Appliquer. Dans la liste, vous pouvez afficher, trier et gérer les clés méta par défaut. Vous pouvez réorganiser les clés méta en cliquant dessus et en les faisant glisser. Le tableau suivant décrit les colonnes de la liste.



Colonne	Description
Clé méta	Cette colonne affiche les métaclés disponibles pour le service. Dans la version 11.1 ou supérieure, les entités méta par défaut sont également incluses, par exemple Toutes les clés de domaine et Toutes les clés d'adresse e-mail.

Colonne	Description
Vue	Cette colonne affiche le type de vue attribué à chaque métaclé. Cliquez sur la vue dans chaque ligne pour attribuer une vue par défaut différente à la métaclé. Quatre vues sont disponibles : • Auto : Retourne à la vue par défaut pour les clés méta, comme l'indique le fichier d'index de service. • Fermé : Les valeurs de cette clé méta sont fermées par défaut et peuvent être ouvertes manuellement. • Masqué : Ces clés méta sont masquées par défaut et ne sont pas affichées dans Investigation. • Ouvert : Les valeurs de cette clé méta s'affichent par défaut. Lorsque vous modifiez les métaclés par défaut pour une métaclé non indexée, vous ne pouvez pas définir la clé sur **Ouvert**. Si vous modifiez la vue par défaut d'un groupe de clés méta sur **Ouvert** et si certaines des clés méta ne sont pas indexées, ces dernières reprennent la valeur **Auto**. La clé méta est donc automatiquement chargée uniquement si elle est indexée, et les clés méta non indexées adoptent l'état **Fermé** jusqu'à ce qu'elles soient ouvertes manuellement.

Le tableau suivant décrit les options et les boutons de la barre d'outils.

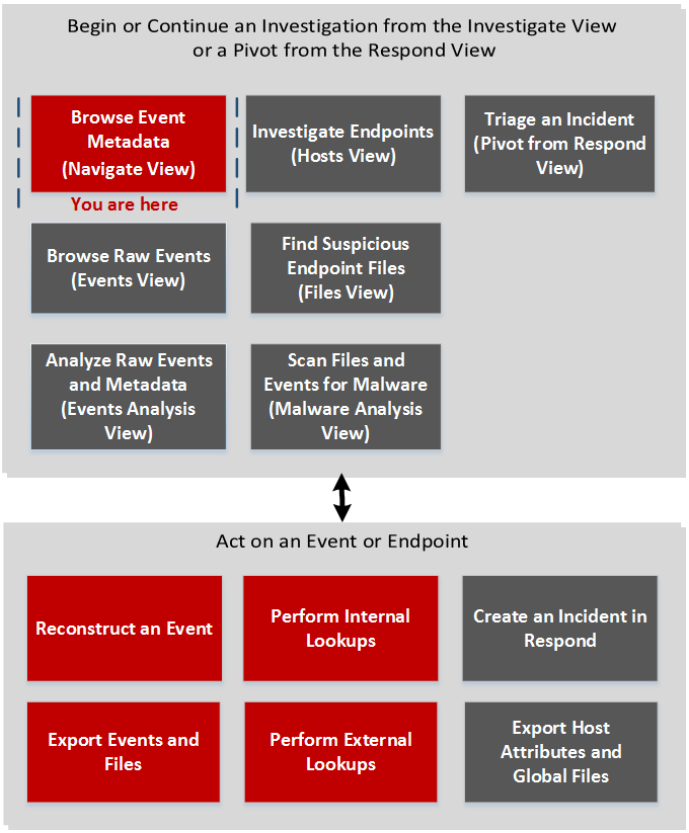
Fonctionnalité	Description
	Le fait de cliquer sur le menu Actions vous permet de modifier la vue par défaut de toutes les métaclés. Quatre vues sont disponibles : • Auto : Retourne à la vue par défaut pour les clés méta, comme l'indique le fichier d'index de service. • Fermé : Les valeurs de cette clé méta sont fermées par défaut. • Masqué : Les valeurs de cette clé méta sont masquées par défaut. • Ouvert : Les valeurs de cette clé méta s'affichent par défaut.
Fermer	Ferme la boîte de dialogue. Toutes les modifications non sauvegardées sont perdues.
Appliquer	Applique les modifications, qui prennent effet immédiatement.

Boîte de dialogue Gérer les groupes méta

Lors d'une nouvelle installation, des groupes méta prêts à l'emploi sont disponibles dans la boîte de dialogue Gérer les groupes méta. Les groupes méta prêts à l'emploi sont précédés de RSA pour leur identification. Ils peuvent être dupliqués, mais pas modifiés ou supprimés. Dans la boîte de dialogue Gérer les groupes méta, vous pouvez ajouter, supprimer, importer et exporter des métagroupes.

Pour accéder à cette boîte de dialogue, dans la barre d'outils **Procédure d'enquête > vue Naviguer**, sélectionnez **Méta > Gérer les groupes méta**

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	ajouter, modifier et supprimer des groupes de méta*	Gérer les groupes méta

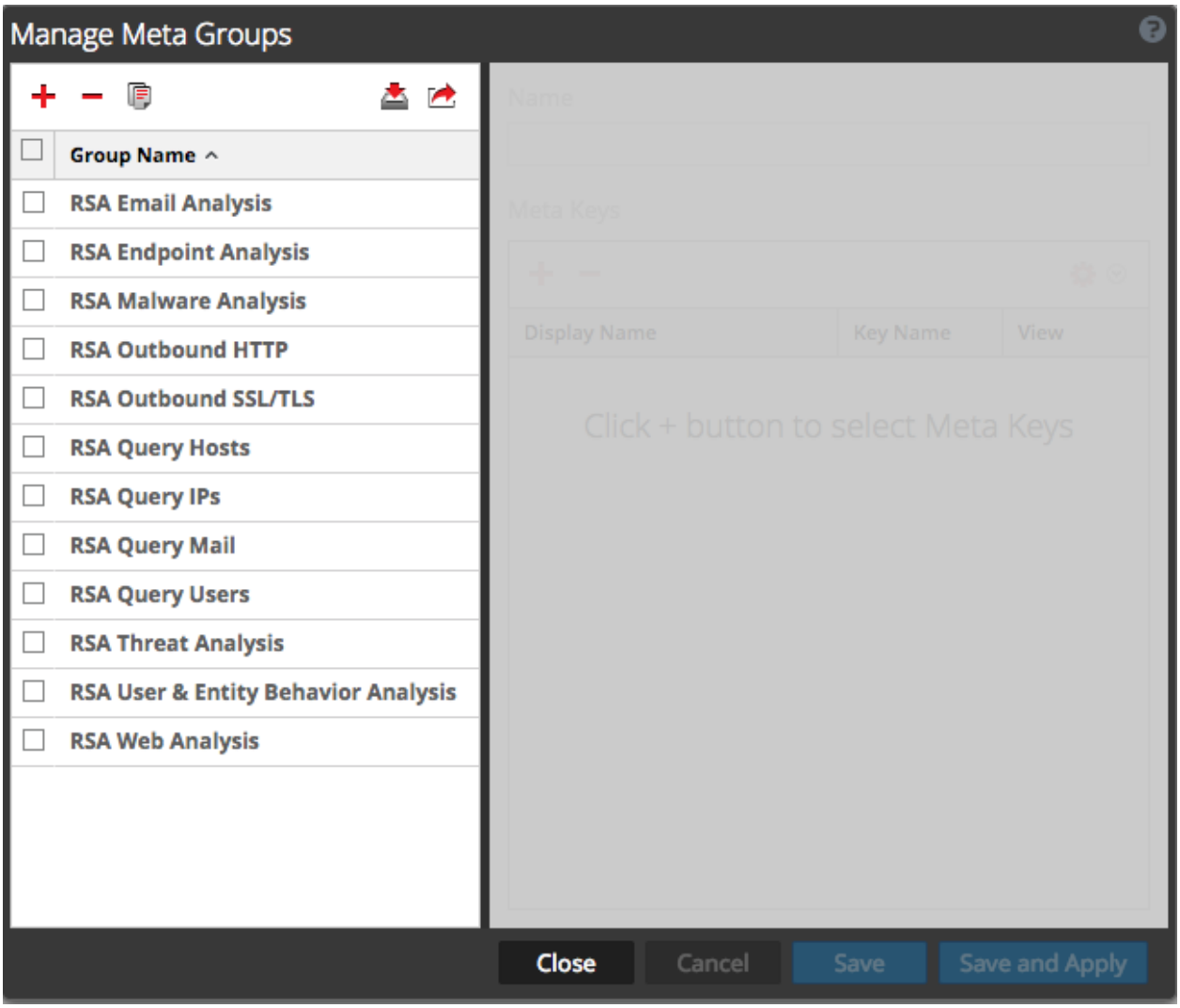
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Filtrer les résultats dans la vue Naviguer
- Fonctionnement de NetWitness Investigate

Aperçu rapide

Voici un exemple de la boîte de dialogue de la version 11.1, dans laquelle des groupes méta OOTB supplémentaires sont disponibles : RSA Endpoint Analysis, RSA Outbound HTTP et RSA Outbound SSL/TLS. La boîte de dialogue Gérer les groupes méta contient deux panneaux. Le tableau suivant décrit les boutons situés en bas de la boîte de dialogue.



Fonctionnalité	Description
Fermer	Ferme la boîte de dialogue.
Annuler	Annule toutes les modifications.
Enregistrer	Enregistre toutes les modifications.
Enregistrer et appliquer	Enregistre et applique immédiatement toutes les modifications.

Le panneau Groupes méta se trouve à gauche de la boîte de dialogue Gérer les groupes méta. C'est à cet emplacement que vous pouvez ajouter, supprimer, importer et exporter des métagroupes.

Le tableau suivant décrit les fonctions du panneau Groupes méta.

Fonctionnalité	Description
	Ajoute un métagroupe à l'aide du panneau Paramètres situé à droite de la boîte de dialogue Gérer les groupes méta.
	Supprime le métagroupe sélectionné. Une fenêtre de confirmation s'affiche avant la suppression du métagroupe.
	Affiche la boîte de dialogue Importation du groupe méta dans laquelle vous pouvez télécharger un fichier en amont.
	Exporter le métagroupe sélectionné vers votre ordinateur.
Nom du groupe	Affiche tous les noms de métagroupes.

Le panneau Paramètres se trouve à gauche de la boîte de dialogue Gérer les groupes méta. C'est à cet emplacement que vous pouvez créer et modifier des métagroupes. Sous le champ Nom figure la grille Clés méta.

Le tableau suivant décrit les fonctions du panneau Paramètres.

Fonctionnalité	Description
Nom	Affiche le nom du métagroupe sélectionné.
	Affiche la boîte de dialogue Clés méta disponibles dans laquelle vous pouvez sélectionner les clés méta à ajouter au groupe.
	Supprime les clés méta sélectionnées.
	Affiche un menu déroulant qui vous permet de sélectionner la vue de toutes les clés méta. Il existe quatre options basées sur les valeurs possibles pour la propriété `defaultAction` permettant de définir une clé dans le fichier d'index personnalisé relatif au service : • Masqué : Ces clés méta sont masquées par défaut et ne sont pas affichées dans Investigation. • Ouvert : Les valeurs de cette clé méta s'affichent par défaut. • Fermé : Les valeurs de cette clé méta sont fermées par défaut et peuvent être ouvertes manuellement. • Auto : Retourne à la vue par défaut pour les clés méta, comme l'indique le fichier d'index de service.
Nom d'affichage	Désigne le nom qui est affiché pour la clé dans les vues Investigation. Ce nom est défini par la propriété `description` pour la clé dans le fichier d'index personnalisé du service.
Nom de clé	Désigne le `name` de la clé méta telle que définie dans le fichier d'index personnalisé du service.

Fonctionnalité	Description
Vue	Indique sur quelle vue la clé méta est définie. Vous pouvez modifier ce paramètre de l'une des manières suivantes : • En cliquant sur **v** dans l'en-tête de colonne Vue, puis en sélectionnant une vue pour changer toutes les vues de clés méta. • En cliquant sur une clé méta unique dans la colonne Vue, puis en ouvrant le menu déroulant dans lequel toutes les vues disponibles sont affichées, afin de changer une seule vue de clé méta.

Boîte de dialogue Gérer les profils

Les profils vous permettent de configurer des vues personnalisées dans la vue Naviguer et la vue Événements. Lors d'une nouvelle installation, des profils prêts à l'emploi sont disponibles dans la boîte de dialogue Gérer les profils. Les groupes de profils prêts à l'emploi sont précédés de RSA pour leur identification. Ils peuvent être dupliqués, mais pas modifiés ou supprimés. Dans la boîte de dialogue Gérer les profils, vous pouvez configurer, ajouter, supprimer, importer et exporter des profils. Dans la version 11.2 et versions ultérieures, vous pouvez organiser des profils dans des groupes de profil.

Pour accéder à cette boîte de dialogue, dans **Procédure d'enquête > barre d'outils de la vue Naviguer** ou **Événements**, sélectionnez **Profil > Gérer les profils**.

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	configurer des profils pour la vue Naviguer ou la vue Événements*	Utiliser des profils pour encapsuler les vues personnalisées

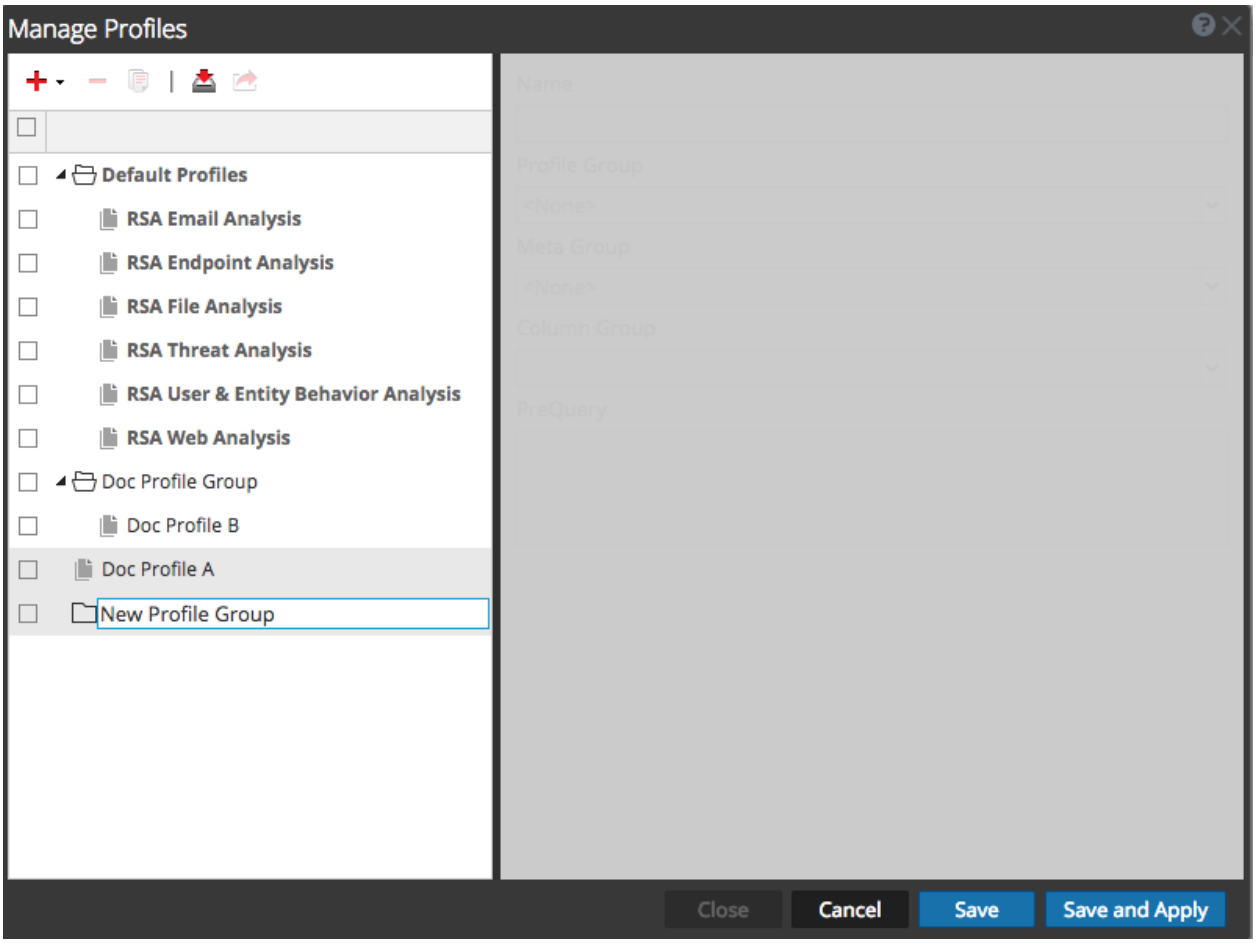
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Naviguer
- Vue Événements

Aperçu rapide

Il s'agit d'un exemple de la boîte de dialogue Gérer les profils affichant plusieurs profils.



La boîte de dialogue Gérer les profils comporte deux panneaux. Une rangée de boutons se trouve dans la partie inférieure de la boîte de dialogue. Le tableau suivant décrit ces boutons.

Champ	Description
Fermer	Ferme la boîte de dialogue.
Annuler	Annule toutes les modifications.
Enregistrer	Enregistre toutes les modifications.

Champ	Description
Enregistrer et appliquer	Enregistre et applique immédiatement toutes les modifications.

Sur la gauche de la boîte de dialogue, ce panneau répertorie les profils disponibles. Vous pouvez en ajouter, supprimer, importer et exporter. Le tableau suivant décrit les champs du panneau Profil.

Champ	Description
	Ajoute un profil via le panneau Paramètres situé sur la droite de la boîte de dialogue Gérer les profils.
	Supprime le profil sélectionné. Une fenêtre de confirmation s'affiche avant la suppression du profil.
	Affiche la boîte de dialogue Importation du profil depuis laquelle vous pouvez télécharger un fichier.
	Exporte le profil sélectionné vers votre ordinateur.
Nom du profil	Répertorie les noms de profils.

Sur la droite de la boîte de dialogue, le panneau Paramètres contient des options permettant de configurer les profils. Ces options sont accessibles uniquement quand un profil est sélectionné. Le tableau suivant décrit les champs du panneau Paramètres.

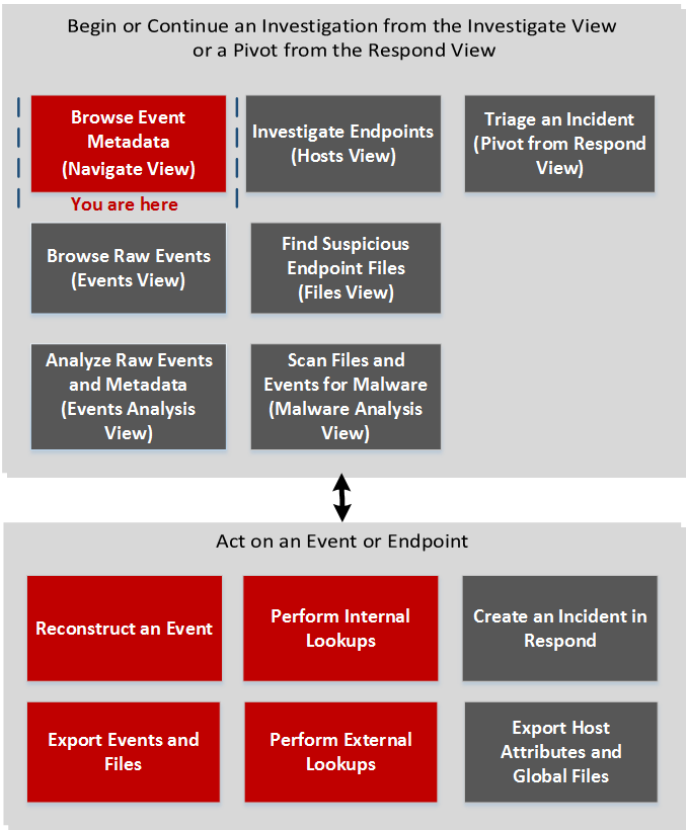
Fonctionnalité	Description
Nom	Affiche le nom du profil.
Groupe méta	Affiche un menu déroulant répertoriant les groupes méta disponibles.
Groupe de colonnes	Affiche un menu déroulant répertoriant les groupes de colonnes disponibles. Par défaut, trois groupes sont disponibles : • Vue Liste • Vue Détails • Vue Log
Requête préalable	Définit une requête restrictive permettant de filtrer les résultats de la procédure d'enquête. Cette requête est utilisée lorsque le profil associé est activé. Elle s'applique aux requêtes utilisées dans les vues Naviguer et Événements (Procédure d'enquête). Voici un exemple de requête préalable : `'service=80,25,110'`.

Vue Naviguer

La vue Vue Naviguer (**ENQUÊTER** > Parcourir) affiche les métadonnées d'événement--les clés méta et les valeurs méta-- ayant été trouvés dans les données capturées pour le service sélectionné. Les données sont filtrées et affichées conformément aux options que vous avez définies pour le profil, la période, le groupe méta et la requête. Vous pouvez aussi explorer les données en cliquant sur les clés méta et les valeurs méta. La vue Naviguer est le point d'entrée par défaut dans NetWitness Investigate ; vous pouvez modifier le point d'entrée par défaut à l'une des autres vues dans les préférences du profil.

Workflow

La figure ci-dessous illustre le workflow général pour l'examen des métadonnées d'événement.



Voici les tâches que vous pouvez effectuer dans Vue Naviguer :

- Sélectionner un service pour enquêter et charger des données.
- Afficher les résultats d'une requête et les filtrer par période, profil, groupe méta.
- Trier les résultats et sélectionner une méthode de quantification.
- Enregistrer les événements, accéder à un événement à l'aide de l'ID d'événement, visualiser un événement et imprimer l'événement.
- Afficher des données contextuelles supplémentaires pour des clés méta et des valeurs spécifiques.

- Accéder à Vue Événements ou à la vue Analyse d'événements, où vous pouvez voir une liste chronologique des événements, reconstruire un événement et réaliser l'analyse interactive d'un événement. Lors de l'affichage et l'analyse des événements, vous pouvez exporter des événements, des fichiers et des logs vers votre système de fichiers local.

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	définir les préférences utilisateur pour la vue Naviguer*	Configurer la vue Naviguer et la vue Événements
Responsable de la recherche des menaces	envoyer une requête ou effectuer une recherche verticale dans le jeu de données*	Procédure d'enquête relative aux métadonnées dans la vue Naviguer
Responsable de la recherche des menaces	affiner les résultats de la requête*	Interrogation et action sur les données dans les vues Naviguer et Événements
Responsable de la recherche des menaces	effectuer des recherches interne*	Rechercher un contexte supplémentaire dans les vues Naviguer et Événements

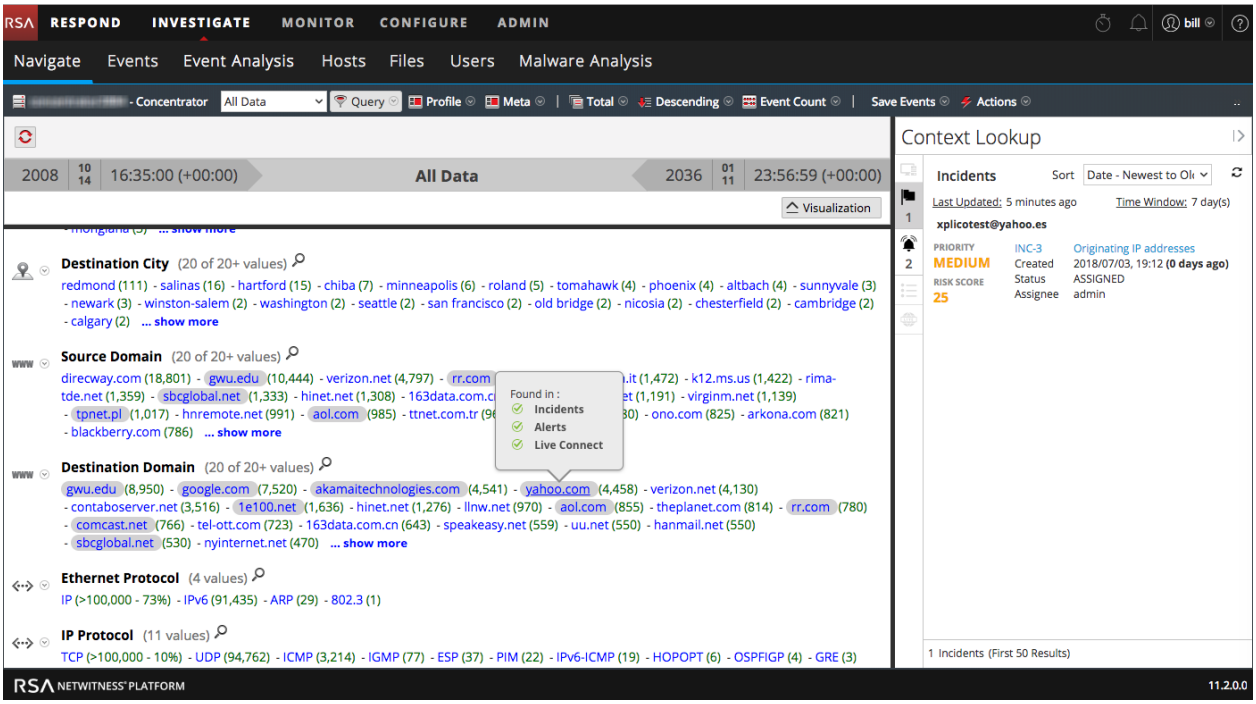
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	effectuer des recherches externes*	Lancer la recherche externe d'une clé méta

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Événements
- Vue Analyse d'événements
- Vue Analyse de malware

Aperçu rapide



La vue Naviguer se compose des fonctions suivantes :

- Barre d'outils
- Bouton Suspendre/Recharger et fil d'Ariane
- Bannière Temps
- Informations de débogage facultatives.
- Panneau Visualisation réductible

- Panneau Valeurs
- Panneau Recherche contextuelle
- Menus contextuels

Barre d'outils

La barre d'outils permet d'effectuer les opérations suivantes :

- Modifier le service en cours de recherche.
- Contrôler la plage des données affichées : vous pouvez sélectionner des profils d'utilisation, définir une période, utiliser des groupes méta et créer des requêtes à appliquer aux données.
- Définir la méthode de quantification et la méthode de tri des données dans le panneau Valeurs.
- Effectuer des actions sur les résultats. Vous pouvez exporter et imprimer les résultats, accéder à un événement pour lequel vous avez un ID d'événement dans la vue Événements ou la vue Analyse d'événements, et transmettre une requête à Informer.
- Configurer les paramètres d'investigation sans avoir à naviguer hors des vues Investigation.

Certaines options de la barre d'outils sont libellées avec la valeur par défaut ou la valeur sélectionnée plutôt que d'afficher le nom de l'option. Ainsi, l'option de période dans l'exemple ci-dessus est libellée **5 dernières minutes** afin de refléter la valeur actuellement sélectionnée. Voici les options de la barre d'outils :

Option	Description
	Affiche le nom de service sélectionné en regard de l'icône. Cliquer sur l'icône permet d'ouvrir la boîte de dialogue Rechercher un service, dans laquelle vous pouvez sélectionner un service à rechercher et définir le service par défaut à rechercher (voir Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements). La modification du service ne provoque pas un rechargement des données.

Option	Description
Période	Affiche les options Période ; l'option actuellement sélectionnée s'affiche dans la barre d'outils (voir Filtrer les résultats dans la vue Naviguer). Les choix possibles sont les suivants : • Toutes les données • 5, 10, 15 ou 30 dernières minutes • Dernière heure, 3, 6, 12 ou 24 dernières heures • 2 ou 5 derniers jours • Début de matinée • Matin • Après-midi • Soir • Toute la journée • Hier • Cette semaine • La semaine dernière • Personnalisé **Remarque :** si vous spécifiez une heure de début ou de fin personnalisée en secondes, l'heure de début en secondes a toujours la valeur par défaut :00, alors que l'heure de fin en secondes a toujours la valeur par défaut :59. Par exemple, si vous utilisez du temps de recherche verticale dans un problème, la durée de la recherche sera interprétée en tant que `HH:MM:00 - HH:MM:59`. Les secondes s'affichent dans ce format dans les fonctions Procédure d'enquête.
Requête	Affiche la boîte de dialogue Requête qui vous permet de saisir directement une requête personnalisée au lieu d'effectuer une recherche verticale dans les données. Voir la rubrique Boîte de dialogue Requête pour une description de la boîte de dialogue.
Profil	Affiche le menu Profil ; le profil actuellement sélectionné s'affiche dans la barre d'outils. Un profil vous permet de gérer et d'utiliser des profils qui peuvent inclure des groupes méta personnalisés, un groupe de colonne par défaut et une requête de début. Les Profils s'appliquent à la vue Naviguer (groupes et requêtes méta) et à la vue Événements (groupes et requêtes de colonne). Pour plus d'informations, voir la rubrique Utiliser des profils pour encapsuler les vues personnalisées.
Méta	Affiche le menu Groupe méta. Vous pouvez utiliser la fonctionnalité Clés méta par défaut ou un groupe méta personnalisé. Vous disposez également de l'option permettant de modifier les deux types de groupes (voir la rubrique Gérer les groupes méta).

Option	Description
Champ Trier	Affiche le menu du champ Trier ; l'option actuellement sélectionnée s'affiche dans la barre d'outils. Le menu dispose de deux options : Classer par total et Classer par valeur. Le champ Trier est un complément de l'option Ordre de tri, les données de chaque clé méta sont classées en fonction du total (nombre en vert) ou de la valeur méta (texte en bleu) (voir Filtrer les résultats dans la vue Naviguer).
Ordre de tri	Affiche le menu Ordre de tri ; l'option actuellement sélectionnée s'affiche dans la barre d'outils. Le menu dispose de deux options : Trier par ordre croissant et Trier par ordre décroissant. Le champ Ordre de tri est un complément de l'option de tri d'un champ ; le champ sélectionné pour chaque clé méta est trié par ordre croissant ou décroissant (voir Filtrer les résultats dans la vue Naviguer).
Méthode de quantification	Affiche le menu Méthode de quantification ; l'option actuellement sélectionnée s'affiche dans la barre d'outils. La méthode de quantification s'applique uniquement aux résultats de clé méta dans le panneau Valeurs. Cela ne s'applique pas à la chronologie. Le menu déroulant contient trois options pour le calcul de la quantité (nombre en vert entre parenthèses) pour une valeur méta : Quantifier par nombre d'événements, Quantifier par taille d'événement et Quantifier par nombre de paquets (voir Filtrer les résultats dans la vue Naviguer). Ces options sont appliquées différemment en fonction du type de données affichées. Pour les données de paquets : • L'option Quantifier par nombre d'événements affiche le nombre de sessions. • L'option Quantifier par taille d'événement affiche la taille en octets. • L'option Quantifier par nombre de paquets affiche le nombre de paquets. Pour les données de log : • L'option Quantifier par nombre d'événements affiche le nombre de logs. • L'option Quantifier par taille d'événement affiche la taille en octets. • L'option Quantifier par nombre de paquets affiche le nombre de logs.
Enregistrer les événements	Affiche le menu Enregistrer les événements dans lequel vous pouvez utiliser les options permettant d'effectuer les tâches suivantes : extraire les fichiers associés à un événement, exporter le point de recherche verticale actif en tant que fichier PCAP, et exporter le point de recherche verticale actif en tant que fichier log (voir la rubrique Exporter un point de recherche verticale).
Actions	Le menu Actions contient des actions que vous pouvez effectuer dans la vue Naviguer (voir Procédure d'enquête relative aux métadonnées dans la vue Naviguer). Dans la Version 11.0.0.x, les options sont : Visualiser, Accéder à un événement et Imprimer. Dans la version 11.1 ou supérieure, les options sont Visualiser, Accéder à un événement dans Reconstruction d'événement, Accéder à un événement dans Analyse d'événements et Imprimer).

Option	Description
Rechercher des événements	Permet de rechercher des modèles de texte dans l'ensemble des événements en cours. Si vous cliquez dans le champ Rechercher, un menu déroulant affiche les options de recherche. Si vous cliquez sur Appliquer, les options sélectionnées sont enregistrées et les options de recherche sont mises à jour dans la vue Événements et le profil Procédures d'enquête (voir la rubrique Rechercher des modèles de texte).
Paramètres	Affiche les paramètres de la vue Naviguer (qui sont également modifiables dans la vue Profil) pour que vous puissiez modifier les paramètres d'enquête sans avoir à naviguer hors de la vue Naviguer. Lorsque vous modifiez un paramètre dans la vue Naviguer, le paramètre est également modifié dans la vue Profil (voir la rubrique Configurer la vue Naviguer et la vue Événements).

Bouton Suspendre/Recharger et fil d'Ariane

Le fil d'Ariane fait le suivi de chaque requête pour laquelle vous effectuez une recherche verticale via les métadonnées du service. Chaque requête est répertoriée avec un menu déroulant dans une chaîne séparée par des traits verticaux. Le dernier point correspond au point actuel, aussi appelé extrémité. L'icône en regard du fil d'Ariane vous permet d'interrompre le chargement des valeurs méta ou de recharger les valeurs méta.

Le fil d'Ariane ne comprend pas le nom du service et apparaît uniquement si une requête est active. Si un nombre trop important de recherches verticales doit être affiché, le dépassement de capacité s'affiche sous la forme de doubles crochets, >>, à la fin du fil d'Ariane.

Chaque menu déroulant dans le fil d'Ariane est identique, avec une légère variation en fonction de la position du fil.

Le tableau suivant décrit les commandes et options de menu du fil d'Ariane.

Fonctionnalité	Description
Pause	Bouton Suspendre et Recharger. Contrôle le chargement des données dans la vue. Trois fonctions sont disponibles : la suspension du chargement, la poursuite du chargement et le rechargement.
Naviguer ici	Ouvre le point de recherche verticale sélectionné dans le panneau Valeurs actuel.
Naviguer ici (nouvel onglet)	Ouvre le point de recherche verticale sélectionné dans un nouvel onglet.
Insérer avant	Insère une requête avant le point de recherche verticale actif. La boîte de dialogue Créer un filtre s'ouvre pour vous permettre de définir une requête personnalisée à insérer dans le fil d'Ariane (voir la rubrique Créer une requête personnalisée).
Ajouter	Ajoute une requête après le point de recherche verticale actif. La boîte de dialogue Créer un filtre s'ouvre pour vous permettre de définir une requête personnalisée à ajouter à la fin du fil d'Ariane (voir la rubrique Créer une requête personnalisée).

Fonctionnalité	Description
Supprimer	Supprime le point de recherche verticale sélectionné du fil d'Ariane.
Modifier	Ouvre le point de recherche verticale sélectionné dans la boîte de dialogue Créer un filtre afin que vous puissiez modifier la requête.
>>	Cliquer sur les crochets permet d'afficher le menu déroulant du dépassement de capacité du fil d'Ariane.

(Facultatif) Informations de débogage

Si vous avez activé le paramètre Afficher les informations de débogage et que le service dans lequel vous vous trouvez est un Broker 10.4, NetWitness Platform affiche les informations de débogage en dessous du fil d'Ariane.

Les informations de débogage correspondent à la clause `where` de la requête actuelle. Le seul cas où il n'y a pas de clause `where` , c'est lorsque la période s'applique à toutes les données et qu'il n'y a aucun point de recherche verticale. Si le Broker dispose au minimum d'un service agrégé en ligne, les informations de débogage afficheront également le service hors ligne.

Par exemple :

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

De plus, le temps de chargement s'affiche à la fin de chaque clé méta dans le panneau Valeurs.

Bannière Temps

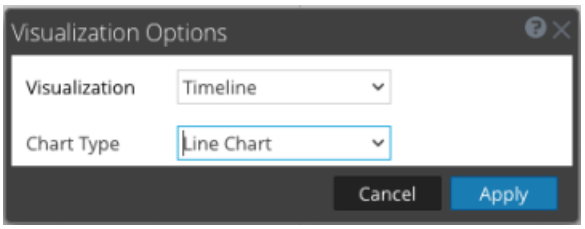
Juste en dessous du fil d'Ariane et des informations de débogage, (si disponibles), la bannière Temps affiche la période utilisée pour créer le graphique.

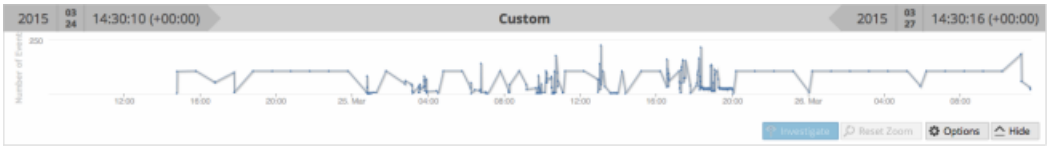
Visualisation

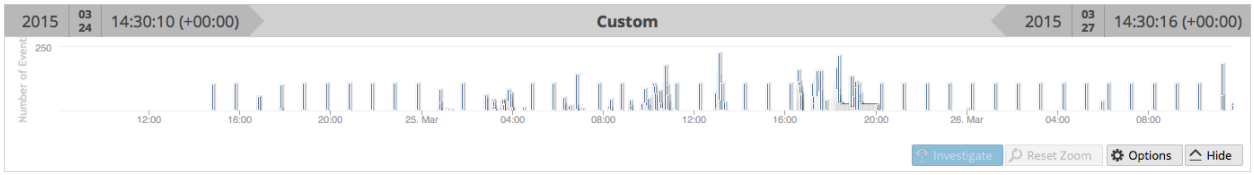
La visualisation du point de recherche verticale actif figure en haut de la vue Naviguer. Vous pouvez l'utiliser pour effectuer une recherche verticale dans les données du panneau Visualisation (voir Filtrer les résultats dans la vue Naviguer). Vous pouvez afficher ou masquer la visualisation, et choisir une des options de visualisation suivantes : Chronologie ou Coordonnées. La fonctionnalité Visualisation s'ouvre généralement à la dernière visualisation.

Graphique chronologique

La chronologie est le décompte du nombre d'événements qui se produisent à une instance spécifique. La chronologie fournit les nombres d'événements afin que vous pouvez voir si le nombre d'événements augmente considérablement à un point donné dans le temps. La chronologie affiche une activité pour le service et la période spécifiés, comme un graphique linéaire ou un graphique à barres en fonction de votre choix dans le menu Options. La deuxième figure illustre un graphique linéaire et la troisième figure illustre un graphique à barres.





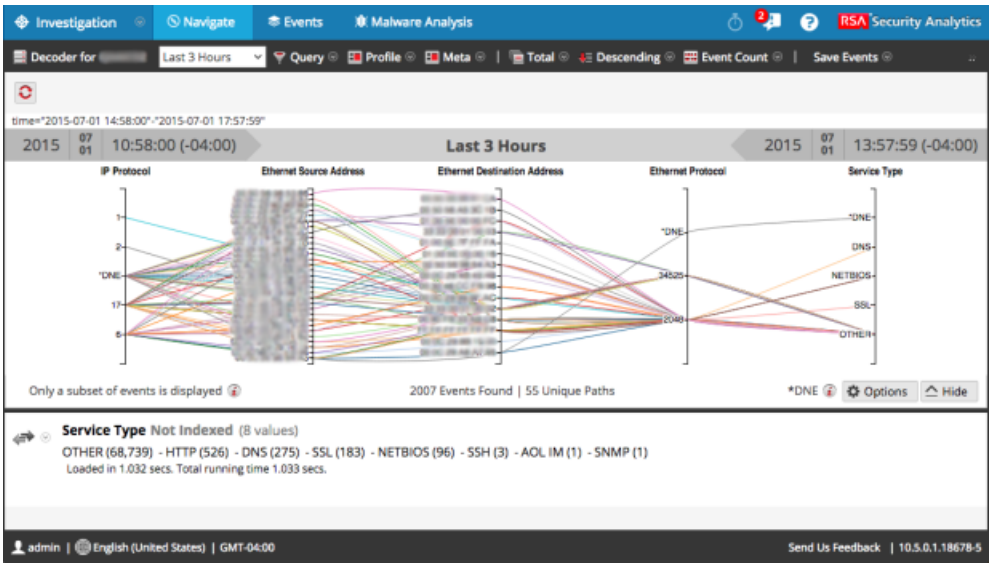


La chronologie affiche une activité pour le service et la période spécifiés, comme un graphique linéaire ou un graphique à barres en fonction de votre choix dans le menu Options.

Fonctionnalité	Description
Nombre d'événements (Chronologie)	Axe Y du graphique basé sur des milliers d'événements.
Chronologie	Axe X du graphique basé sur l'heure à laquelle les événements se sont produits.
Point d'événement (Chronologie)	Si vous souhaitez explorer une section spécifique, sélectionnez simplement la plage correspondante dans le graphique. La nouvelle période sera reflétée dans le graphique.
Examiner (Chronologie)	Affiche les valeurs méta du sous-ensemble sélectionné.
Réinitialiser le zoom (Chronologie)	Pour revenir à la période d'origine, cliquez sur Réinitialiser le zoom.
Options	Affiche la boîte de dialogue Options de visualisation. Les points de données peuvent être affichés sous la forme d'un graphique linéaire (par défaut), d'un graphique à barres ou d'un graphique de coordonnées. Lorsqu'un type de graphique est sélectionné, les options correspondantes s'affichent.
Masquer	Réduit le graphique.

Graphique de coordonnées parallèles

Le graphique de coordonnées parallèles est l'un des choix du menu Options pour visualiser le point de recherche verticale actif. Avec le paramètre Coordonnées sélectionné dans la boîte de dialogue Options de visualisation, vous pouvez sélectionner les métadonnées à afficher (voir Visualiser des métadonnées en tant que coordonnées parallèles).



Fonctionnalité	Description
Axes	Chaque axe est une clé méta. Le nombre de clés méta affecte le temps de charge du graphique. Toutes les clés méta sont chargées, mais le nombre d'événements par clé méta est limité.
Lignes	Les lignes représentent des événements, qui relient des valeurs sur les axes pour montrer la corrélation entre plusieurs clés méta.
Options	Affiche la boîte de dialogue Options de visualisation. Les points de données peuvent être affichés sous la forme d'un graphique linéaire (par défaut), d'un graphique à barres ou d'un graphique de coordonnées. Lorsqu'un type de graphique est sélectionné, les options correspondantes s'affichent.
Seul un sous-ensemble d'événements s'affiche.	Ce message est une notification indiquant que tous les événements du panneau Valeurs sont tracés dans le graphique. La suppression des axes ou le filtrage des données dans le panneau Valeurs permet d'afficher tous les événements.
Événements trouvés | Chemins uniques	Affiche le nombre total d'événements représentés dans le graphique par rapport au nombre de chemins uniques représentés dans le graphique. La définition de l'option Toutes les clés méta doivent exister dans un événement retrace le graphique afin qu'il soit plus ciblé et lisible.
Inexistant	Indique que l'événement ne contient aucune valeur pour cette clé méta.

Dans la boîte de dialogue Options de visualisation pour les coordonnées, vous pouvez sélectionner les clés méta à représenter dans le graphique.

Fonctionnalité	Description
Sélection de visualisations	Affiche une liste déroulante des types de visualisation : Chronologie et coordonnées

Fonctionnalité	Description
Toutes les clés méta doivent exister dans un événement	Limite les données représentées dans la visualisation à uniquement ces événements qui incluent toutes les clés méta sélectionnées. Il en résulte une visualisation plus nette et plus ciblée.
	Affiche la boîte de dialogue Ajouter des clés à la visualisation des coordonnées parallèles afin de pouvoir ajouter des axes à la visualisation. Cela est utile si vous recherchez des relations entre les clés méta par défaut et les autres.
	Supprime les clés sélectionnées afin qu'elles n'apparaissent pas sous la forme d'axes dans la visualisation. Ainsi, la visualisation apparaît moins encombrée et peut inclure plus de points de données.
	Rétablit les clés méta par défaut de la visualisation, se composant de toutes les clés méta dans le point de recherche verticale actif.
	Contrôle l'affichage d'informations supplémentaires relatives au nombre d'axes sélectionnés par rapport au nombre recommandé. Cela vous permet de prendre conscience des améliorations de performances en supprimant les axes.
Axes	Affiche les clés méta sélectionnées en tant qu'axes dans la visualisation.
Annuler	Annule les modifications appliquées aux options de visualisation.
Appliquer	Enregistre les modifications effectuées dans les options de visualisation et les applique à la visualisation actuelle.

Dans la boîte de dialogue Ajouter des clés à la visualisation des coordonnées parallèles, vous pouvez sélectionner les clés méta ou les groupes méta à utiliser en tant qu'axes dans la visualisation des coordonnées parallèles.

Fonctionnalité	Description
Sélection de visualisations	Sélectionner les clés : Les deux options qui permettent de sélectionner les clés méta sont les suivantes : • À partir des clés méta par défaut • À partir des groupes méta Chaque option fournit une liste déroulante à partir de laquelle effectuer la sélection.
Avec les clés méta sélectionnées...	Les options de la méthode d'ajout des clés méta vous permettent d'effectuer les opérations suivantes : • Remplacer la liste actuelle de clés • Ajouter à la liste actuelle de clés • Insérer au début de liste actuelle de clés
Annuler	Ferme la boîte de dialogue et n'ajoute aucune clé.
Ajouter	Ferme la boîte de dialogue et ajoute les clés sélectionnées comme spécifié.

Panneau Valeurs

La fonctionnalité principale de la vue Naviguer est le panneau Valeurs, que vous pouvez utiliser pour analyser les données (voir Filtrer les résultats dans la vue Naviguer).

La vue par défaut concerne les 3 dernières heures de collecte, en utilisant les clés méta par défaut et les clés méta non indexées fermées. Les clés méta au sein des groupes méta sont affichées dans l'ordre dans lequel NetWitness Platform interroge les clés. Au fur et à mesure que le chargement des données s'effectue dans le panneau Valeurs, NetWitness Platform est optimisé pour afficher les résultats partiels, la progression du chargement et l'état du service au moment du chargement des données.

Le comportement du chargement est déterminé par plusieurs paramètres de configuration. Les paramètres de niveau les plus élevés sont configurés par l'administrateur pour chaque utilisateur. Elles sont les suivantes :

- La durée maximale autorisée pour l'exécution d'une requête par cet utilisateur (Délai d'expiration de la requête).
- La limite à laquelle NetWitness Platform cesse de compter le nombre de métavaleurs dans une session (Seuil de session). Si un seuil est défini pour une session, la vue Naviguer montre que le seuil a été atteint et affiche le pourcentage de résultats chargés. Toute session qui n'affiche pas un pourcentage est exacte et a été traitée jusqu'à la fin. S'il existe un pourcentage, il reflète la quantité de traitement effectuée. Le pourcentage affiché est estimé en extrapolant à partir de la valeur à la fin du traitement, compte tenu du volume de travail restant. Des pourcentages plus élevés sont généralement plus précis, car ils nécessitent moins d'extrapolation.
- La limite à laquelle NetWitness Platform cesse de compter le nombre de métavaleurs dans une session (Seuil de session). Si un seuil est défini pour une session, la vue Naviguer montre que le seuil a été atteint et affiche le pourcentage de temps de requête utilisé pour atteindre le seuil.

Remarque : les valeurs des clés méta non indexées prennent plus de temps à se charger dans le panneau Valeurs. Pour optimiser le chargement, NetWitness Platform n'ouvre pas les clés méta non indexées par défaut. Pour une description détaillée des clés méta non indexées dans Procédure d'enquête, reportez-vous à la rubrique Gérer et appliquer des clés méta par défaut dans une procédure d'enquête.

Lorsque vous avez lancé une procédure d'enquête de service, NetWitness Platform affiche les résultats dans le panneau Valeurs.

1. NetWitness Platform charge les clés méta et les métavaleurs dans le panneau Valeurs. Pour chaque chargement de clé méta, les étapes de chargement sont les suivantes :
    a. **En attente de chargement** ou **Fermé**. Si le paramètre Fermé est défini, aucune donnée relative à cette clé ne sera chargée.
    b. **Chargement**
        i. **Progression du chargement** : NetWitness Platform reçoit et affiche les messages de progression.
        ii. **Résultats partiels** : NetWitness Platform reçoit des messages de valeurs et des résultats partiels sont affichés dans le panneau Valeurs.

c. **Chargement terminé** : Le chargement de tous les résultats est terminé.

2. À la fin du chargement d'une clé méta et de l'affichage de ses valeurs finales, le chargement de la clé méta suivante est lancé. Le nombre et les valeurs affichés pour chaque clé méta sont spécifiés par la valeur Générer des threads dans les paramètres de préférences de procédure d'enquête. Le chargement se poursuit jusqu'à ce que toutes les clés soient complètement chargées.
3. Si l'option **Afficher les informations de débogage** est active et que le service utilisé est un service Broker 10.4 ou de version ultérieure, NetWitness Platform affichera les informations de temps de chargement sous les valeurs de chaque clé méta, ainsi que d'autres détails de chargement relatifs aux services agrégés. NetWitness Platform affiche également les informations de débogage sous le fil d'Ariane.

Résultats itératifs

Les résultats itératifs contiennent des commentaires sur l'état des requêtes au sein des interfaces afin de fournir un contexte supplémentaire quant à la durée de chargement des données et l'absence de données de service. Par exemple, si vous interrogez un service Broker qui agrège deux services Concentrator, NetWitness Platform commence à afficher les résultats du premier service Concentrator dès qu'ils sont disponibles, même si le second service Concentrator attend toujours les résultats.

Les résultats itératifs comprennent également une notification indiquant que des données de service sont manquantes parce que le service est inaccessible.

Résultats partiels

Lorsque les valeurs partielles du service Core sont retournées mais non terminées, un message à la fin de la liste des clés méta indique la progression des valeurs chargées. Par exemple, Currently looking at 38 ip.src values 71% indique que le chargement des valeurs de la clé méta est exécuté à 71 %.

Informations de débogage

Si le paramètre Afficher les informations de débogage est activé, un champ à la fin des valeurs affiche l'état des différents systèmes que vous interrogez dans NetWitness Platform. Par exemple, lorsque vous interrogez un service Broker 10.4 extrayant ses données de plusieurs services Concentrator, NetWitness Platform affiche l'état de la requête sur chacun des services Concentrator, ce qui donne un aperçu de la vitesse relative du chargement des données de chacun des services Concentrator. Chaque service ayant participé à la requête est indiqué avec la durée d'exécution totale de la requête.

Chaque service ayant participé à la requête est indiqué avec la durée d'exécution totale de la requête. Dans l'exemple ci-dessus, deux services ont indiqué 3,207 secondes, localhost:50005 a pris 2 secondes pour retourner les résultats. En outre, la clause where de la requête est affichée sous le fil d'Ariane. Vous pouvez copier cette syntaxe directement dans la clause where d'une règle d'application ou du Reporting.

Chargement terminé

Pour chaque clé méta, il y a une liste de valeurs (texte en bleu) et des nombres (texte en vert) trouvés au niveau du point de recherche verticale actif. Lorsque vous cliquez sur une valeur pour effectuer une recherche verticale dans un sous-ensemble de données sélectionnées, l'affichage est mis à jour et le nouveau point de recherche verticale est enregistré dans le fil d'Ariane. Vous pouvez spécifier les méthodes de tri et de quantification pour la liste des valeurs en utilisant les options correspondantes dans la barre d'outils.

Remarque : le titre, les valeurs et les chiffres relatifs aux clés méta non indexées ne peuvent pas faire l'objet d'une recherche verticale ; les valeurs et les chiffres sont en noir.

Fonctionnalité	Description
Clé méta	Nom de la clé méta qui est affiché. Par exemple, **Type de service** est une clé méta.
Nombre de valeurs affichées par rapport aux nombres de valeurs disponibles pour le chargement	Le nombre et les valeurs affichés sont spécifiés par la valeur Générer des threads dans les paramètres de préférences de procédure d'enquête. Dans l'exemple ci-dessus, la clé méta est **Type de service** et les valeurs 20 sur 20+ correspondent aux valeurs actuellement affichées. Vous pouvez afficher d'autres valeurs en cliquant sur **...show more**.
	Cliquer sur  sur une clé méta indexée permet d'ouvrir la boîte de dialogue Rechercher dans laquelle vous pouvez sélectionner un filtre pour la clé méta actuelle. La fonction de recherche n'est pas disponible pour les clés méta non-indexées, et elle est basée sur la valeur méta plutôt que sur l'alias. La recherche verticale dans la boîte de dialogue Rechercher en utilisant des alias n'est pas prise en charge. REMARQUE : contactez votre administrateur pour obtenir la liste des alias pouvant être utilisés avec une clé méta dans Procédure d'enquête. Lorsqu'un alias est utilisé, cette boîte de dialogue de recherche ne fournit pas de résultats. En revanche, vous devez interroger la clé méta à l'aide de la fonctionnalité de requête accessible par clic droit ou à l'aide de la boîte de dialogue Requête.
Services hors ligne : xxx.xxx.xxx.xxx:50004	Indique les services hors ligne interrogés par un service Broker 10.4.
Nombre de méta, par exemple (3)	Nombre d'instances trouvées pour un méta particulier dans la session.
Valeur méta, par exemple other src	Nom spécifique associé aux méta trouvés.
...show more	Si le nombre de valeurs méta a été limité (par exemple, 20), cliquer sur cette fonctionnalité permet d'afficher d'autres valeurs méta pour la clé méta sélectionnée.
Loaded in 0.418 secs. Durée totale en cours d'exécution 0,434 secondes. (localhost:50005 loaded in 1 secs...	Les statistiques de débogage affichent les durées de chargement en fonction du paramètre Afficher les informations de débogage.

Menu déroulant Clé méta

Les clés méta contenues dans le panneau Valeurs fournissent des menus déroulants. En regard de chaque libellé de méta, une flèche déroulante affiche les options qui peuvent être appliquées à cet élément. Vous pouvez les utiliser pour modifier le mode d'affichage des résultats de la clé méta dans la vue actuelle. Les modifications apportées aux clés méta s'affichent dans la vue active, sauf si vous actualisez la page ou sélectionnez un nouveau service dans la barre d'outils de la vue Naviguer. Voir Effectuer une recherche verticale dans les données dans le panneau Valeurs

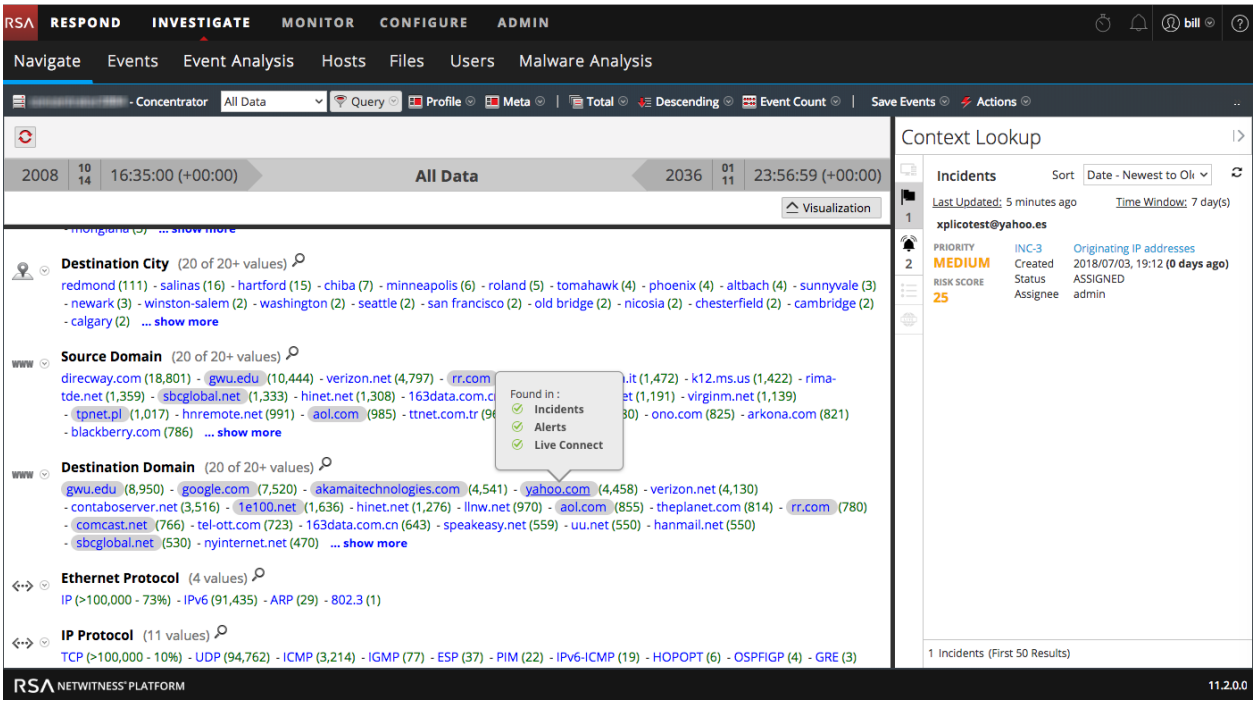
L'actualisation rétablit la vue actuelle des clés méta, telle que définie dans la boîte de dialogue Gérer les clés méta par défaut (voir la rubrique Gérer et appliquer des clés méta par défaut lors d'une procédure d'enquête). Si vous n'avez effectué aucune modification dans la boîte de dialogue Gérer les clés méta par défaut, NetWitness Platform restaure les clés méta par défaut à partir du service de base.

- Autres résultats
- Résultats maximum
- Masquer les résultats
- Info sur la clé méta
- Afficher au format CSV (version 11.0.0.x) ou Exporter des valeurs (version 11.1 et ultérieure)

Panneau Recherche contextuelle

La vue Naviguer et la vue Événements disposent d'un panneau Recherche contextuelle sur le côté droit. Le panneau Recherche contextuelle ne s'affiche que si vous avez installé et configuré le service Context Hub. Pour plus d'informations sur la configuration du service Context Hub, reportez-vous au *Guide de configuration du service Context Hub*.

Le panneau Recherche contextuelle affiche les données pertinentes lorsqu'un analyste recherche des données contextuelles pour une valeur méta dans le panneau Valeurs.

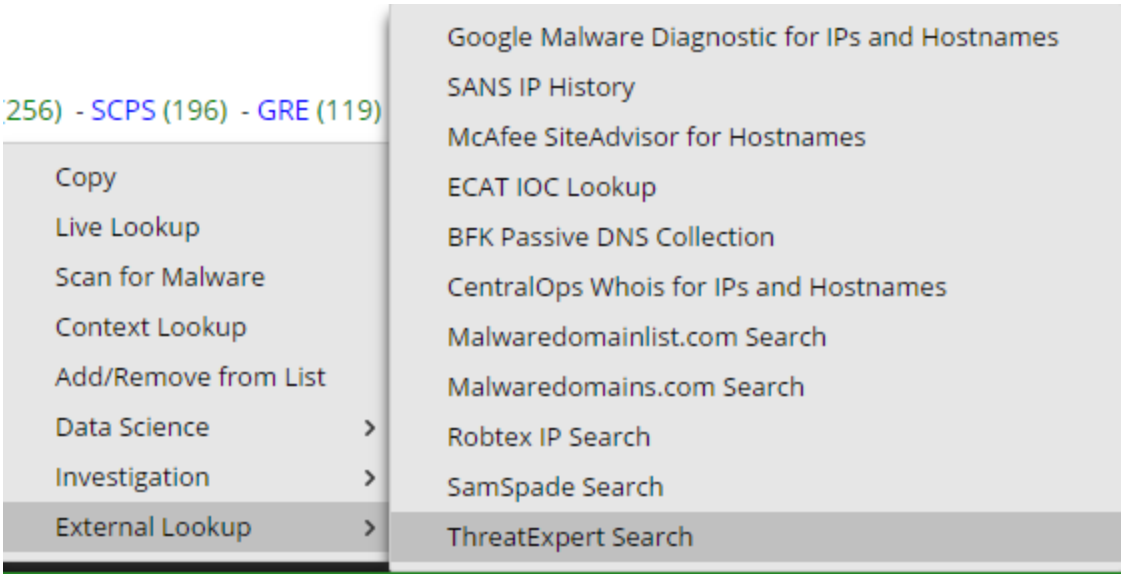


Une fois que l'administrateur a configuré le service Context Hub, vous pouvez afficher les informations contextuelles des métavaleurs dans la vue Naviguer et la vue Événements. Pour plus d'informations sur la configuration du service Context Hub, reportez-vous au *Guide de configuration du service Context Hub*. Pour plus d'informations sur l'exécution de la recherche contextuelle des valeurs méta, consultez la rubrique Rechercher un contexte supplémentaire dans les vues Naviguer et Événements.

Le service Context Hub est pré-configuré avec un adressage du type de méta et de la clé méta par défaut. Pour plus d'informations sur l'adressage de la métavaleur du service Context Hub avec une clé méta de procédure d'enquête, consultez la rubrique « Gérer l'adressage du type de méta » et de la clé méta du *Guide de configuration de Context Hub*

Vous pouvez afficher le type de données contextuelles disponible pour une valeur méta en surbrillance en positionnant le pointeur de la souris sur une valeur méta mise en surbrillance. Un indicateur en ligne affiche le type de données contextuelles disponible pour la méta : Point de terminaison, Incidents, Alertes ou Listes.

En cliquant sur une valeur méta avec le bouton droit de la souris, un menu s'affiche avec l'option de recherche contextuelle. La figure suivante illustre l'option Recherche contextuelle lorsque vous cliquez sur une valeur méta avec le bouton droit de la souris.



Pour les clés méta comme IP, Hôte et Adresse Mac, les détails des valeurs qui sont marqués sont collectés à partir de Point de terminaison, Incident, Alertes et Listes.

Pour les clés méta comme Fichier, Hachage de fichier, Domaine, Utilisateur, les détails des valeurs qui sont signalés sont collectés à partir de Point de terminaison, Incident, Alertes et Listes.

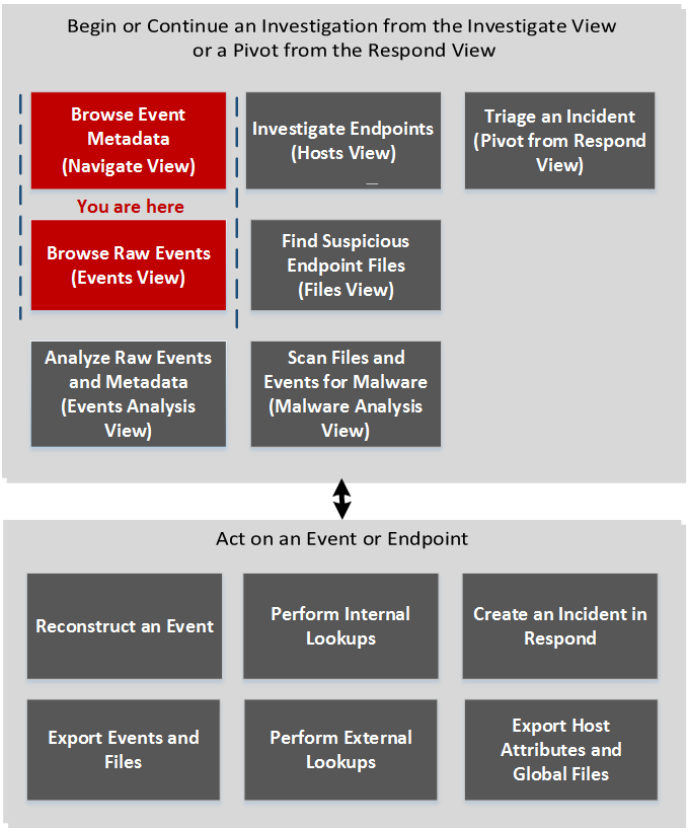
Les données sont affichées dans le panneau Contexte, uniquement si des données sont disponibles.

Pour plus d'informations sur les résultats des recherches et les données contextuelles pour différentes sources de données, consultez la rubrique Panneau Recherche contextuelle.

Boîte de dialogue Requête

Dans la vue Naviguer ou Événements, vous pouvez créer une requête au lieu de cliquer sur les clés méta et les métavaleurs pour accéder aux métadonnées. Les boîtes de dialogue pour créer une requête offrent une aide à la syntaxe grâce à des listes déroulantes de clés méta applicables et d'opérateurs. Pour accéder à cette boîte de dialogue dans la barre d'outils de la vue**Naviguer** ou **Événements**, sélectionnez **Requête**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts*	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

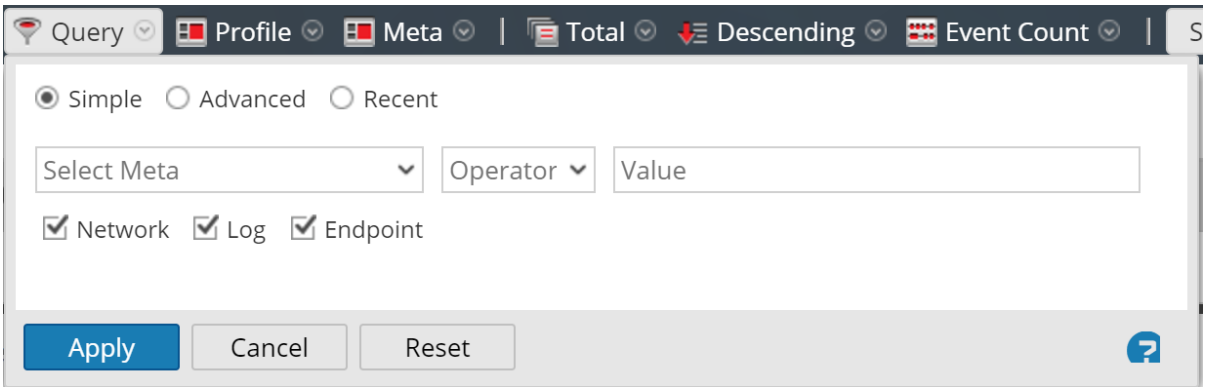
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	créer une requête personnalisée*	Créer une requête personnalisée

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Naviguer
- Vue Événements

Aperçu rapide

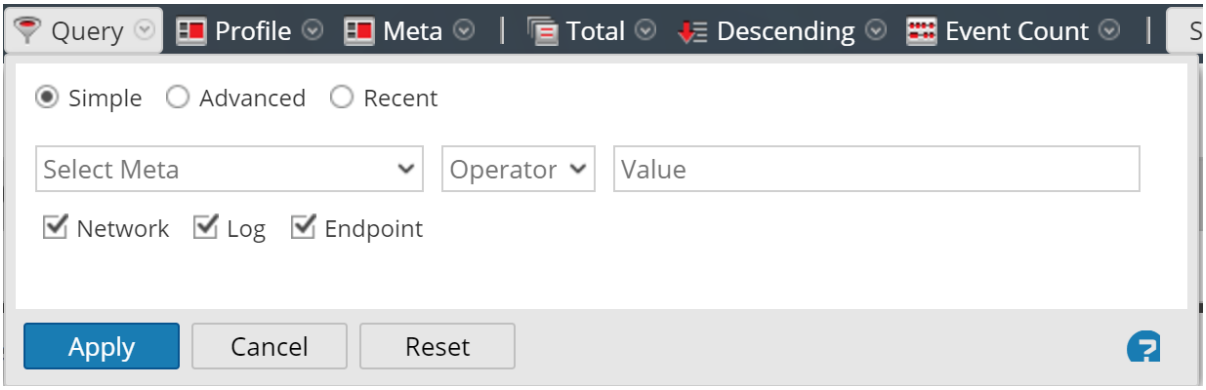


La boîte de dialogue Requête propose trois vues :

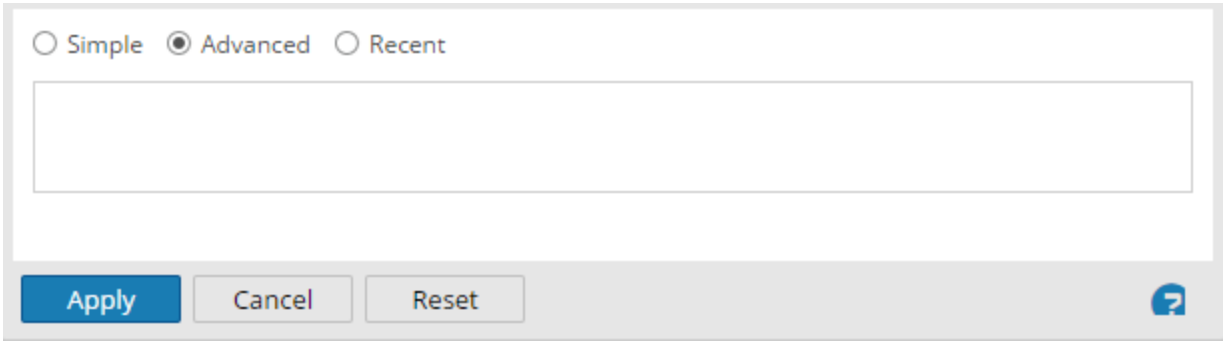
- Simple
- Avancé
- Récente

Dans la vue Simple, vous pouvez créer une requête à l'aide des options affichées dans la boîte de dialogue. Dans la vue Avancé, vous pouvez créer une requête en toute autonomie. Dans la vue Récente, vous pouvez sélectionner une requête dans la liste déroulante des requêtes les plus récentes.

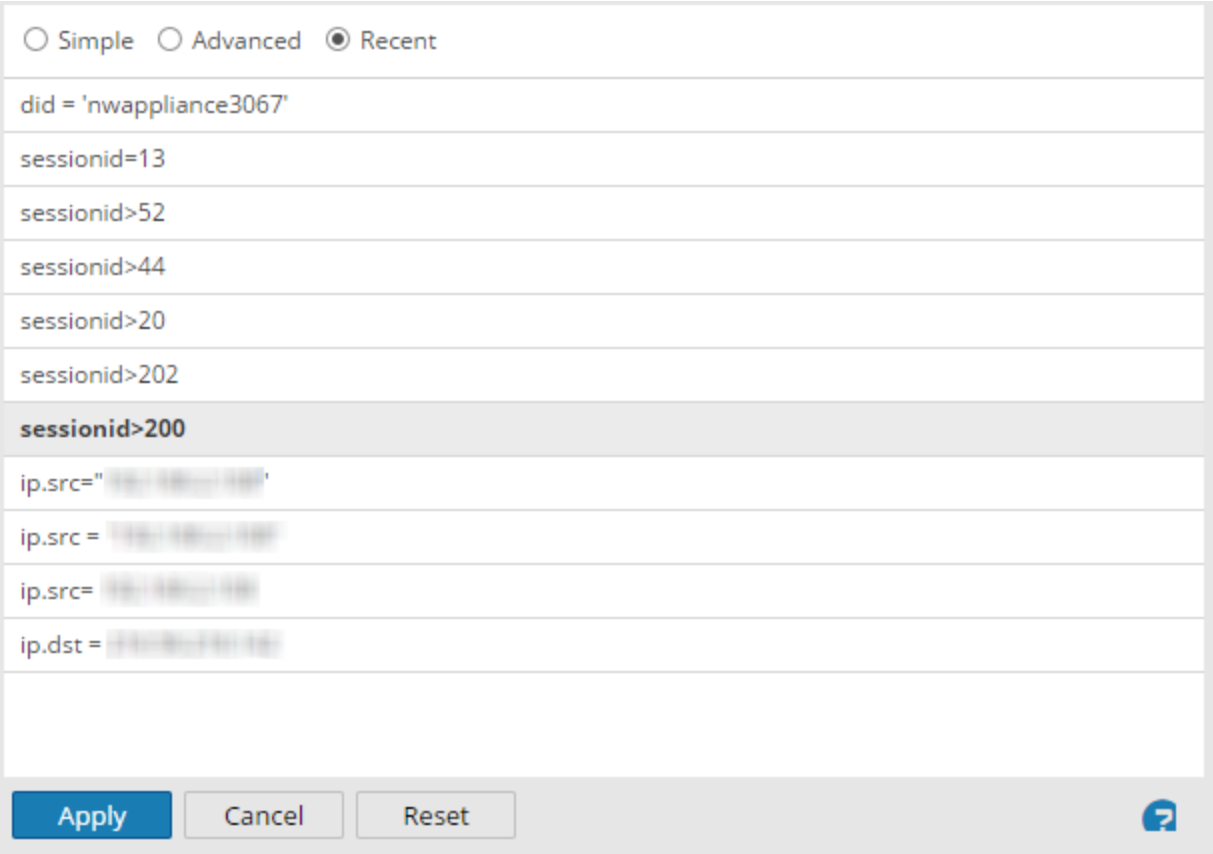
Vue Simple



Vue Avancé



Vue Récente



Le tableau suivant décrit les fonctions de la boîte de dialogue Requête.

Fonctionnalité	Description
Sélectionner les méta	Affiche une liste déroulante de métagroupes.
Opérateur	Affiche une liste déroulante d'opérateurs `(=,NetWitness Platform!=,NetWitness Platformexists,NetWitness Platform!exists)`
Valeur	Vous permet de saisir une valeur pour compléter la requête.
Réseau	Limite la requête aux paquets si l'option Log n'est pas sélectionnée.
Log	Limite la requête aux journaux si l'option Réseau n'est pas sélectionnée.
Zone de requête	Permet de saisir une requête dans la vue Avancé. Au début de la saisie, une liste déroulante répertoriant les clés méta disponibles pour le service s'affiche, suivie d'une liste d'opérateurs. Si l'expression saisie dans la zone de recherche n'est pas valide, un message d'avertissement s'affiche à côté. Lorsque la requête est valide, cet avertissement disparaît.

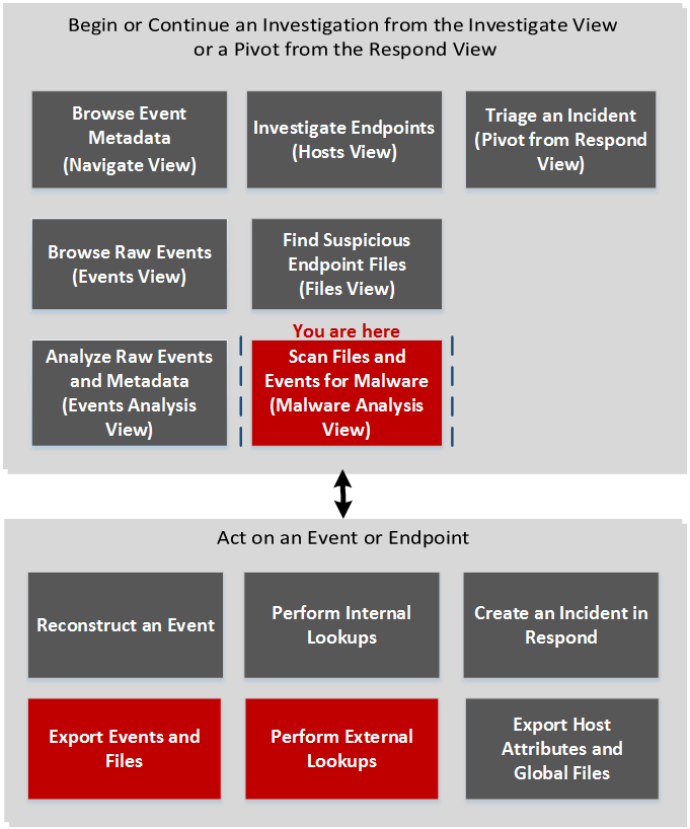
Fonctionnalité	Description
Liste de requête	Vous permet de sélectionner une requête parmi les dernières requêtes effectuées dans la vue Récente. Double-cliquez sur une requête pour l'appliquer automatiquement.
Appliquer	Applique la nouvelle requête à la vue Investigation actuelle.
Annuler	Ferme la boîte de dialogue sans appliquer les modifications.
Réinitialiser	Réinitialiser tous les champs.

Boîte de dialogue Analyser les malwares

Dans la boîte de dialogue Analyser les malwares, les analystes Malware Analysis peuvent télécharger des fichiers à étudier dans Malware Analysis.

Pour accéder à cette boîte de dialogue, allez à la vue **Malware Analysis**. Dans la boîte de dialogue**Sélectionner un service Malware Analysis**, sélectionnez un service dans le panneau de gauche, puis cliquez sur Scan Files dans le panneau de droite.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants*	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

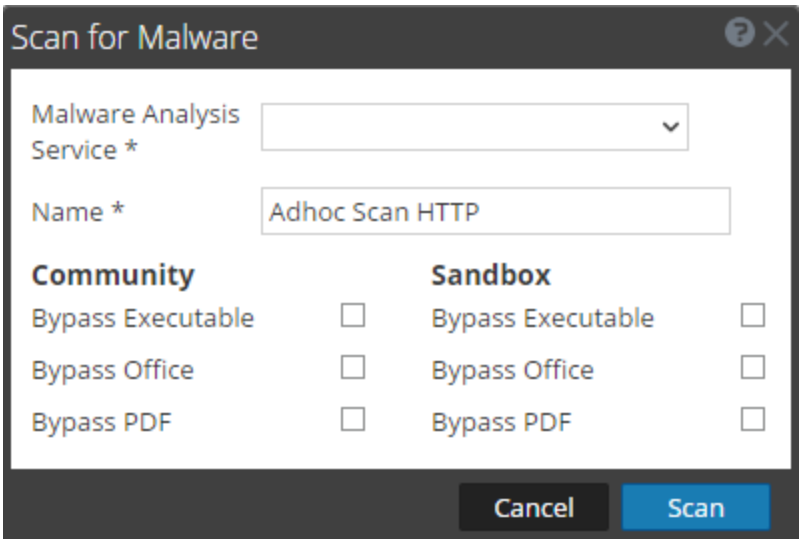
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Lancer une procédure d'enquête Malware Analysis
- Lancer une analyse Malware Analysis à partir de la vue Naviguer

Aperçu rapide

La figure ci-dessous illustre la boîte de dialogue Analyser les malwares et le tableau suivant décrit les fonctions disponibles dans la boîte de dialogue Analyser les malwares.

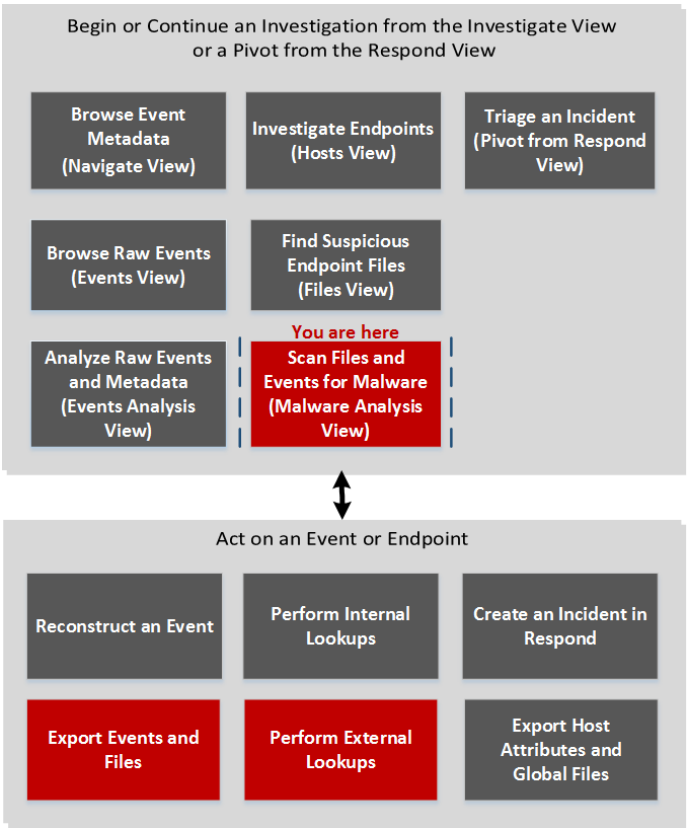


Fonctionnalité	Description
	Télécharge un fichier depuis votre ordinateur.
	Supprime un fichier de la liste.
Nom de fichier	Affiche les noms des fichiers ajoutés à la liste.
Nom	Vous permet de nommer la tâche d'analyse.
Communauté	Affiche des options pour la communauté pour contourner ou ignorer certains types de fichiers : • Ignorer les fichiers exécutables • Ignorer les fichiers Office • Ignorer les fichiers PDF
Sandbox	Affiche des options pour Sandbox pour contourner ou ignorer certains types de fichiers : • Ignorer les fichiers exécutables • Ignorer les fichiers Office • Ignorer les fichiers PDF
Annuler	Ferme la boîte de dialogue sans effectuer d'actions.
Scan	Analyse les fichiers téléchargés.

Boîte de dialogue Sélectionner un service Malware Analysis

La boîte de dialogue Sélectionner un service Malware Analysis est accessible dans la vue Malware Analysis. Dans cette boîte de dialogue, les analystes Malware Analysis peuvent sélectionner un service pour enquêter, choisir une analyse sur ce service pour enquêter, télécharger un fichier à analyser et commencer une analyse continue du service.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements

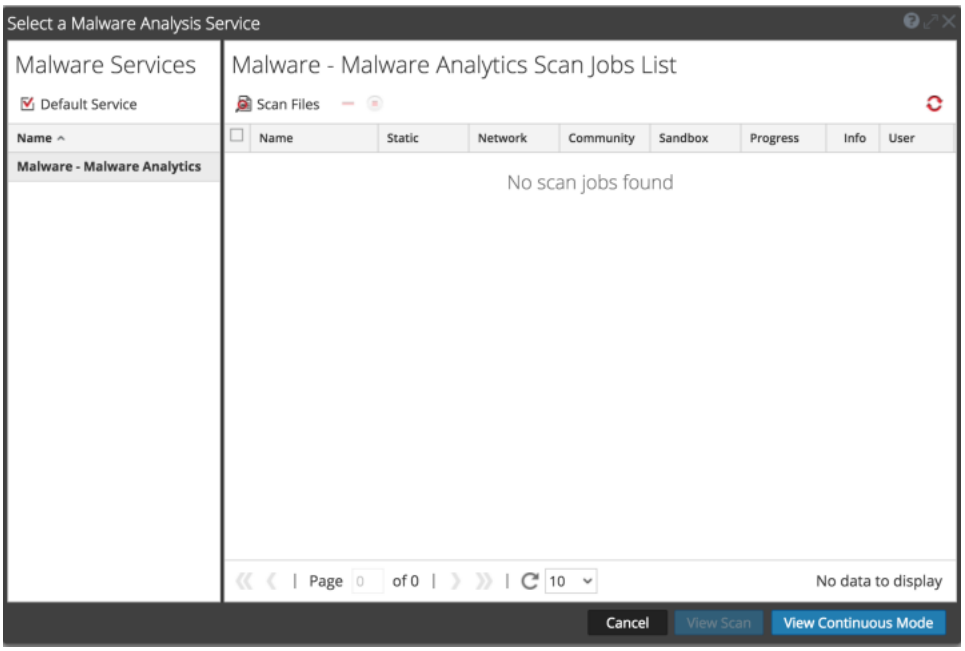
Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants*	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Lancer une procédure d'enquête Malware Analysis
- Lancer une analyse Malware Analysis à partir de la vue Naviguer

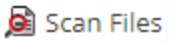
Aperçu rapide



La boîte de dialogue Sélectionner un service Malware Analysis possède un panneau Services Malware sur la gauche et une Liste des tâches d'analyse sur la droite. Le panneau Liste des tâches d'analyse possède une barre d'outils, une liste et des boutons pour afficher les analyses.

Le panneau Services Malware présente la liste des services disponibles pour l'analyse de malware. Dans ce panneau, vous pouvez sélectionner le service sur lequel mener la procédure d'enquête et définissez un service par défaut à l'aide de l'icône Service par défaut. Lorsque vous sélectionnez un service, les tâches d'analyse disponibles pour ce service sont répertoriées dans la Liste des tâches d'analyse.

Voici les fonctions de la barre d'outils Liste des tâches d'analyse.

Fonctionnalité	Description
	Affiche la boîte de dialogue Analyser les malwares, dans laquelle vous pouvez télécharger un fichier vers le service d'analyse.
Supprimer la tâche d'analyse ()	Supprime une ou plusieurs des tâches d'analyse sélectionnées. NetWitness Platform affiche une boîte de dialogue de confirmation avant de supprimer des tâches d'analyse.
Annuler la tâche d'analyse ()	Met en pause ou poursuit une ou plusieurs tâches d'analyse.
Actualiser ()	Actualise la liste des tâches d'analyse.

Il s'agit des colonnes de la Liste des tâches d'analyse. Cette liste est également disponible dans le Dashlet Liste des tâches d'analyse des malware.

Fonctionnalité	Description
Nom	Affiche le nom de la tâche.
Statique, Réseau, Communauté, Sandbox	Filtre les résultats en fonction des scores de chaque module de notation.
Progression	Affiche la progression actuelle effectuée sur la tâche. • Vert : La tâche est terminée. • Noir : La tâche est en cours. • Rouge: Une erreur s'est produite :
Info	Fournit des informations supplémentaires. Affiche la requête de la tâche. Si la tâche n'est pas terminée, elle affiche également une description plus détaillée de l'état.
Utilisateur	Affiche le nom de l'utilisateur qui a créé la tâche.
Événements	Compte le nombre d'événements pour la tâche.
Abandonné	Compte le nombre de fichiers/événements dans la tâche qui ont été abandonnés car les scores étaient inférieurs à leur seuil configuré.
Type d'événement	Affiche le type de la tâche : Téléchargement manuel, À la demande ou Resoumettre.

Fonctionnalité	Description
Planifiée	Affiche la date et l'heure auxquelles la tâche a été exécutée.

Les actions disponibles dans la boîte de dialogue sont les suivantes.

Fonctionnalité	Description
Bouton Annuler	Annule la tâche d'analyse sélectionnée.
Bouton Afficher l'analyse	Affiche le Récapitulatif des événements pour l'analyse sélectionnée avec les dashlets par défaut affichés.
Bouton Afficher le mode continu	Affiche le Récapitulatif des événements pour l'analyse sélectionnée avec les dashlets par défaut affichés.

Boîte de dialogue Paramètres pour les vues Enquêter

NetWitness PlatformVersion 11.0 dispose de deux boîtes de dialogue de paramétrage, l'une pour la vue Naviguer et l'autre pour la vue Événements. Avec l'ajout de la boîte de dialogue Paramètres de la vue Analyse d'événements dans la version 11.1, Investigate dispose de trois boîtes de dialogue de paramétrage.

Les paramètres des boîtes de dialogue Paramètres pour les vues Naviguer et Événements sont un sous-ensemble des paramètres de Procédure d'enquête définis dans Profils > panneau Préférences > onglet Procédures d'enquête. En fournissant les paramètres dans la vue Procédure d'enquête, NetWitness Platform est un gain de temps pour les analystes. Si vous modifiez un paramètre ici, le même paramètre est modifié dans la vue Profils et si vous changez un paramètre dans cette même vue, le même paramètre est modifié ici.

Pour accéder à cette boîte de dialogue, accédez à la vue **Naviguer** ou **Événements** et sélectionnez l'option **Paramètres** dans la barre d'outils.

Les paramètres de la vue Analyse d'événements n'ont pas de paramètres correspondants dans le panneau Profils > Préférences.

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	parcourir les métadonnées d'événement	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	parcourir les événements bruts	Commencer une procédure d'enquête dans la vue Naviguer ou la vue Événements
Responsable de la recherche des menaces	analyser les métadonnées et événements bruts	Commencer une procédure d'enquête dans la vue Analyse d'événements
Responsable de la recherche des menaces	examiner les points de terminaison (Version 11.1)	Examiner les hôtes
Responsable de la recherche des menaces	rechercher des fichiers de point de terminaison suspects (Version 11.1)	Examiner les fichiers
Responsable de la recherche des menaces	analyser les fichiers et les événements des programmes malveillants	Mener une analyse de malware
Responsable de la réponse aux incidents	triage d'un incident dans Investigate	*Guide d'utilisation de NetWitness Respond*

Rôle d'utilisateur	Je souhaite...	Me montrer comment
Responsable de la recherche des menaces	configurer les préférences pour Investigate*	Configuration des vues et des préférences de NetWitness Investigate

*Vous pouvez effectuer cette tâche dans la vue actuelle.

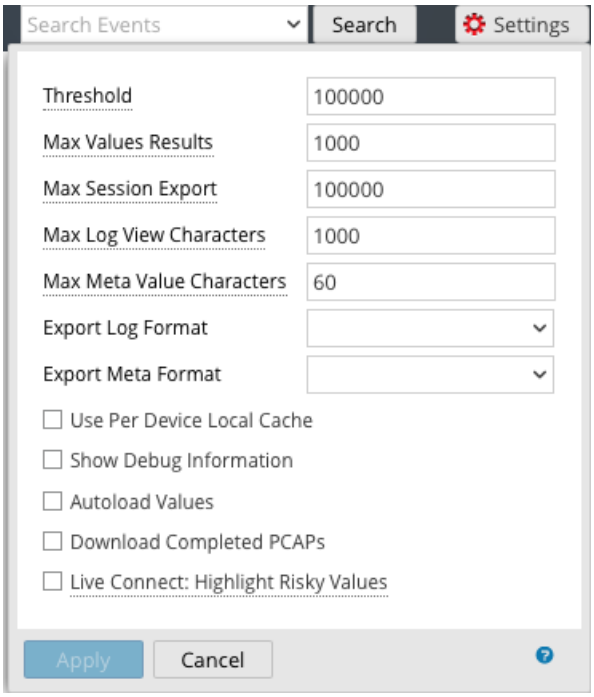
Rubriques connexes

- Fonctionnement de NetWitness Investigate

Aperçu rapide

Les boîtes de dialogue Paramètres des vues Naviguer et Événements ont plusieurs fonctions en commun.

Plusieurs paramètres de procédure d'enquête de la vue Naviguer influencent les performances lors du chargement de valeurs dans le panneau Valeurs. Les valeurs par défaut sont définies d'après l'usage commun. Les analystes individuels peuvent ajuster ces paramètres selon leurs propres procédures d'enquêtes. L'illustration ci-dessous est un exemple de la boîte de dialogue et le tableau suivant décrit les fonctions.



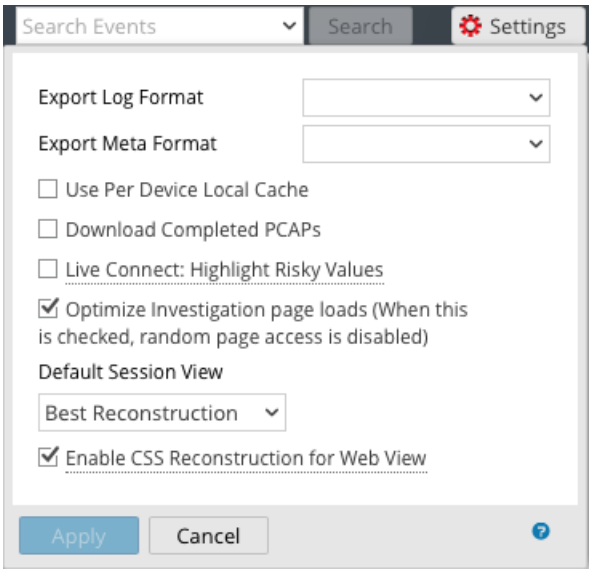
Fonctionnalité	Description
Seuil	Définit le seuil du nombre maximum de sessions chargées pour une valeur de clé meta dans le panneau Valeurs. Un seuil supérieur offre des décomptes précis pour une valeur, et cause également des temps de charge plus longs. La valeur par défaut est **100000**.

Fonctionnalité	Description
Nb max résultats de valeurs	Définit le nombre maximal de valeurs à charger dans la vue Naviguer lorsque l'option Résultats maximum est sélectionnée dans le menu Clé méta pour ouvrir une clé méta. La valeur par défaut est **1 000**.
Nb max exports de session	Définit le nombre maximum de sessions pouvant être exportées. La valeur par défaut est **100000**.
Format du log d'exportation	Définit le format des logs exportés. Quatre formats sont disponibles : • Text • SML • CSV • JSON
Exporter le format de métadonnées	Définit le format de fichier des métavaleurs exportées. Quatre formats sont disponibles : • Text • SML • CSV • JSON
Utiliser le cache local par appareil	Lorsque cette option est désactivée, Enquêter envoie une nouvelle requête à la base de données plutôt que d'afficher les données mises en cache dans les vues d'Enquêter après le chargement initial. Si elle est activée, Enquêter utilise les données provenant du cache local.
Afficher les informations de débogage	Cette option contrôle l'affichage de la clause `where` sous le fil d'Ariane dans la vue Naviguer, ainsi que le temps de charge écoulé pour chaque service agrégé sur un Broker, cochez cette option. Si elle est activée, les informations de débogage sont affichées. Par défaut, l'option est **Off** (désactivée)**.**
Ajouter des événements dans le panneau Événements	Cette option n'affecte la pagination dans le panneau Événements. Lorsqu'elle est activée, le groupe d'événements suivant est ajouté aux événements déjà affichés. Lorsque cette option est désactivée, la page précédente des événements est remplacée par la page suivante. Par défaut, l'option est **Off** (désactivée)
Charger automatiquement les valeurs	Cette option contrôle le chargement automatique des valeurs du service sélectionné dans la vue Naviguer. Lorsqu'elle est activée, les valeurs sont automatiquement chargées quand vous sélectionnez un service à examiner. Lorsqu'elle n'est pas activée, Enquêter affiche un bouton **Charger les valeurs**, qui vous offre l'opportunité de modifier des options. La valeur par défaut est **Off**.

Fonctionnalité	Description
Téléchargement des PCAP terminés	Ce paramètre automatise le téléchargement des PCAP extraits dans le module Investigation pour que vous n'ayez pas à télécharger et ouvrir manuellement les fichiers PCAP extraits dans une application, telle que Wireshark, qui peut gérer l'affichage des données dans un formulaire PCAP.
Live Connect : Mettre en évidence les IP risquées	Si cette option est désactivée, toutes les métavaleurs qui disposent d'un contexte disponible dans Live Connect sont mises en surbrillance dans la vue Naviguer du panneau Valeurs. Si l'option est activée, parmi les valeurs qui disposent d'un contexte dans Live Connect, seules les valeurs jugées risquées/suspectes/dangereuses par la communauté sont mises en surbrillance. Par défaut, cette option est désactivée (**Off**).
Appliquer	Applique les paramètres immédiatement. Ils seront visibles la prochaine fois que vous chargerez les valeurs. Les mêmes modifications sont également appliquées dans la vue Profils.
Annuler	Annule l'opération de modification et ferme la boîte de dialogue, en laissant les paramètres non modifiés.

Boîte de dialogue Paramètres - Vue Événements

L'illustration suivante est un exemple de la boîte de dialogue Paramètres pour la vue Événements et le tableau suivant décrit les fonctions.

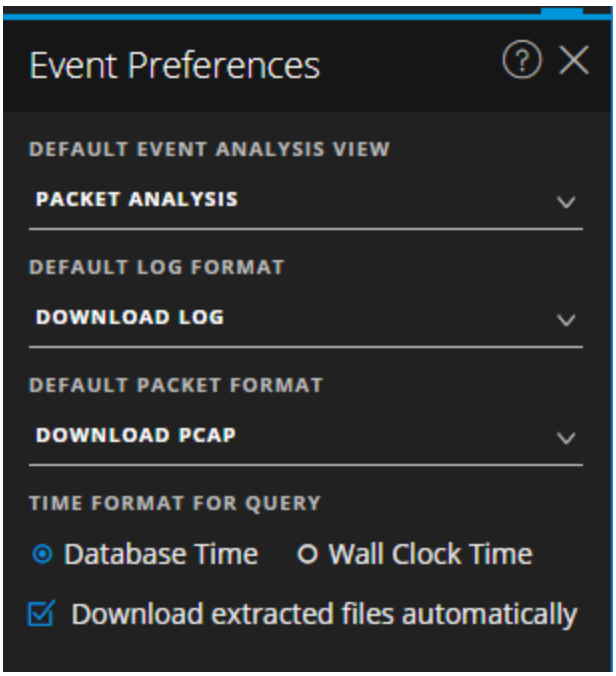


Fonctionnalité	Description
Format du log d'exportation	Définit le format des logs exportés. Quatre formats sont disponibles : • Text • SML • CSV • JSON
Exporter le format de métadonnées	Définit le format de fichier des métavaleurs exportées. Quatre formats sont disponibles : • Text • SML • CSV • JSON
Téléchargement des PCAP terminés	Ce paramètre automatise le téléchargement des PCAP extraits dans le module Investigation pour que vous n'ayez pas à télécharger et ouvrir manuellement les fichiers PCAP extraits dans une application, telle que Wireshark, qui peut gérer l'affichage des données dans un formulaire PCAP.
Live Connect : Mettre en évidence les IP risquées	Lorsque cette option est activée, Enquêter utilise un filtre pour extraire uniquement les adresses IP considérées comme présentant des risques par la communauté RSA. Lorsqu'elle n'est pas sélectionnée, NetWitness Platform affiche toutes les adresses IP. Par défaut, cette option n'est pas sélectionnée (**Off**).
Optimiser les charges de la page Procédure d'enquête	Définit une option de pagination. Lorsqu'ils sont optimisés, les résultats sont renvoyés aussi rapidement que possible, en sacrifiant la capacité originale à accéder à une page spécifique dans la liste des événements. Désactiver cette case modifie la pagination de la liste Événements pour vous permettre d'accéder à une page spécifique de la liste (ou à la dernière page). La valeur par défaut est **activé**.
Vue Session par défaut	Sélectionne le type de reconstruction par défaut pour la reconstruction initiale dans la vue Événements. La valeur par défaut est **Meilleure reconstruction**, dans laquelle les événements sont reconstruits à l'aide de la méthode de reconstruction la plus appropriée pour l'événement.
Activer la vue CSS Reconstruction pour le Web	Ce paramètre contrôle la réalisation de la reconstruction de contenu Web. Si elle est activée, la reconstruction Web comprend des styles avec feuille de style en cascade (CSS) et des images pour que son apparence soit identique à celle de la vue originale dans un navigateur Web. Elle inclut l'analyse et la reconstruction des événements connexes, et la recherche de feuilles de style et d'images utilisées dans l'événement cible. Cette option est activée par défaut. Désactivez cette option en cas de problèmes avec l'affichage de sites Web spécifiques.

Fonctionnalité	Description
Appliquer	Applique les paramètres immédiatement. Ils seront visibles la prochaine fois que vous afficherez les événements. Les mêmes modifications sont également appliquées dans la vue Profils.
Annuler	Annule l'opération de modification et ferme la boîte de dialogue, en laissant les paramètres non modifiés.

Vue Analyse d'événements - Panneau Préférences

À partir de la version 11.1, la vue Analyse d'événements dispose des préférences utilisateur que vous pouvez configurer dans la vue Analyse d'événements > panneau Préférences de l'événement. Ces paramètres sont conservés afin d'être appliqués chaque fois que vous vous connectez et accédez à la vue Analyse d'événements. L'illustration ci-dessous est un exemple de la boîte de dialogue et le tableau suivant décrit les fonctions.



Fonctionnalité	Description
Vue Analyse d'événements par défaut	Sélectionne la vue d'analyse d'événements par défaut qui s'affiche chaque fois que vous ouvrez la vue Analyse d'événements. Par exemple, si vous sélectionnez Analyse de fichiers, le panneau Analyse de fichiers est mis en surbrillance et affiché chaque fois que vous examinez un événement dans la vue Analyse d'événements. Ces options sont les suivantes : • **Analyse de texte** : Affiche et analyse la charge utile de texte brut d'un événement. • **Analyse de paquets** : Affiche et analyse de façon interactive les paquets et la charge utile d'un événement. • **Analyse de fichiers** : Affiche la liste des fichiers et télécharge un ou plusieurs fichiers dans un événement.
Format de log par défaut	Sélectionne le format par défaut pour le téléchargement des logs : • **Télécharger le fichier log** : Log brut (log) utilisant cette option. • **Télécharger le fichier CSV** : Valeurs séparées par des virgules (CSV) utilisant cette option. • **Télécharger le fichier XML** : Fichier XML (Extensible Markup Language) utilisant cette option. • **Télécharger JSON** : Fichier JSON (JavaScript Object Notation) utilisant cette option.
Format de paquet par défaut	Sélectionne le format de paquet par défaut pour le téléchargement des paquets. • **Télécharger le PCAP** : Télécharge l'événement entier en tant que fichier de capture de paquets (*.pcap). • **Télécharger toutes les charges utiles** : Télécharge la charge utile en tant que fichier *.payload. • **Télécharger la charge utile de la demande** : Télécharge la charge utile de la demande en tant que fichier *.payload1. • **Télécharger la charge utile de la réponse** : Télécharge la charge utile de la réponse en tant que fichier *.payload2.

Fonctionnalité	Description
Format d'heure pour la requête	La vue Analyse d'événements peut afficher les résultats en fonction de l'heure de la base de données ou de l'heure actuelle de l'horloge. Le paramètre par défaut pour cette préférence est Heure de la base de données, qui est le même format que celui utilisé pour afficher les résultats de la requête dans la vue Naviguer et dans la vue Événements. Lorsque le paramètre **Heure de la base de données** est sélectionné, l'heure de début et l'heure de fin d'une requête se basent sur l'heure à laquelle l'événement a été capturé. Lorsque **Temps Horloge** est sélectionné, la requête est exécutée en utilisant l'heure de fin en fonction de l'heure actuelle du navigateur. L'heure de début est calculée en fonction de cette heure de fin et de la période.
Télécharger automatiquement les fichiers extraits	Permet le téléchargement automatique des fichiers s'ils sont au format par défaut sélectionné dans les champs **Format de log par défaut** et **Format de paquet par défaut** dans le panneau Préférences de l'événement. Cochez la case pour activer le téléchargement automatique du format sélectionné dans le dossier local. Sinon, la tâche de téléchargement est placée en file d'attente, ce qui vous permet de le télécharger manuellement.