RSA NETWITNESS® SUITE

Guide d'utilisation d'Investigate et de Malware Analysis

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

Fonctionnement de NetWitness Investigate

Enquêter offre aux analystes la possibilité d'analyser des données dans RSA NetWitness® Suite 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.

Données et métadonnées

RSA NetWitness Suite 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 flux 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.

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, événements de point de terminaison ou 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.

Méthodes d'analyse

Les analystes peuvent enquêter sur les données capturées, ouvrir des résultats de requête provenant d'autres modules NetWitness Suite dans une procédure d'enquête, et importer des données en provenance d'autres sources de collecte. Au cours d'une procédure d'enquête, les analystes peuvent se déplacer de manière transparente entre les trois vues de la procédure d'enquête : Les vues Naviguer, Évènements et Malware Analysis.

Les analystes utilisent des Enquêter pour chercher 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. Un responsable de la réponse aux incidents qui travaille sur un incident dans NetWitness Respond peut ouvrir l'incident dans NetWitness Investigate et ajouter des événements à l'incident. Un chasseur de menaces qui travaille dans NetWitness Investigate peut ajouter un événement à un incident existant ou créer un nouvel incident dans NetWitness Respond. Dans les deux cas, les analystes examinent les métadonnées ou les font pivoter pour filtrer le nombre de logs et de paquets et voir ainsi les événements suspects, tout en se concentrant sur certaines combinaisons de métadonnées qui mènent à un incident.

Remarque : 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 Suite. 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.

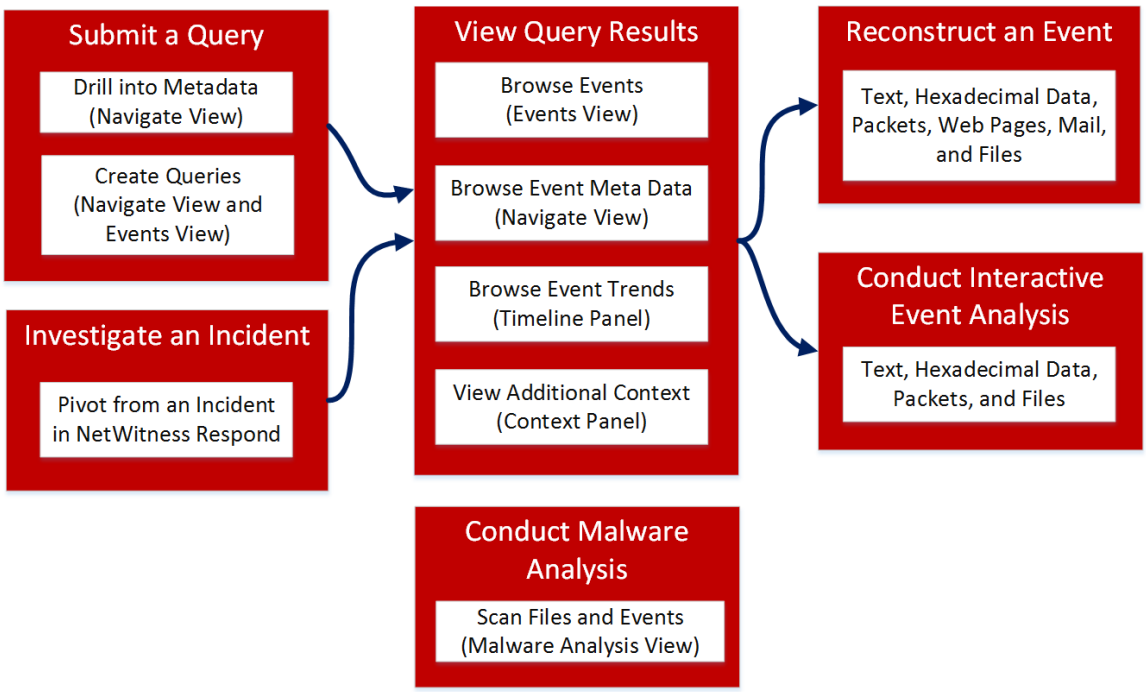
Déclencheurs pour une procédure d'enquête

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

- Vous recevez des renseignements d'un tiers sur un nouveau piratage Active Directory ; vous utilisez ces informations pour exécuter une recherche sur l'ensemble de vos données des fichiers log Active Directory brutes sur les dernières 24 heures.
- Vous êtes invité par le responsable du SOC à trouver le malware Pokemon Go en raison de sa popularité actuelle ; vous élaborer une requête pour rechercher une session HTTP à l'aide d'un agent utilisateur spécifique lié au programme malveillant qu'il a trouvé sur un blog de sécurité.
- Un responsable de la réponse aux incidents fait remonter un ticket qui présente certains indicateurs impairs associés à un hôte ; vous effectuez une association à cet hôte pour rechercher des informations spécifiques.
- Vous cherchez la prochaine attaque de type Zero Day et pivotez via les métadonnées du réseau pour trouver des sessions automatisées anormales quittant l'entreprise.
- Vous êtes invité par votre responsable du SOC à trouver les informations relatives à l'utilisateur `jarvis`, un employé qui vient d'être remercié ; vous effectuez une requête par rapport à la semaine précédente pour ce nom d'utilisateur.

Flux de travail d'une procédure d'enquête

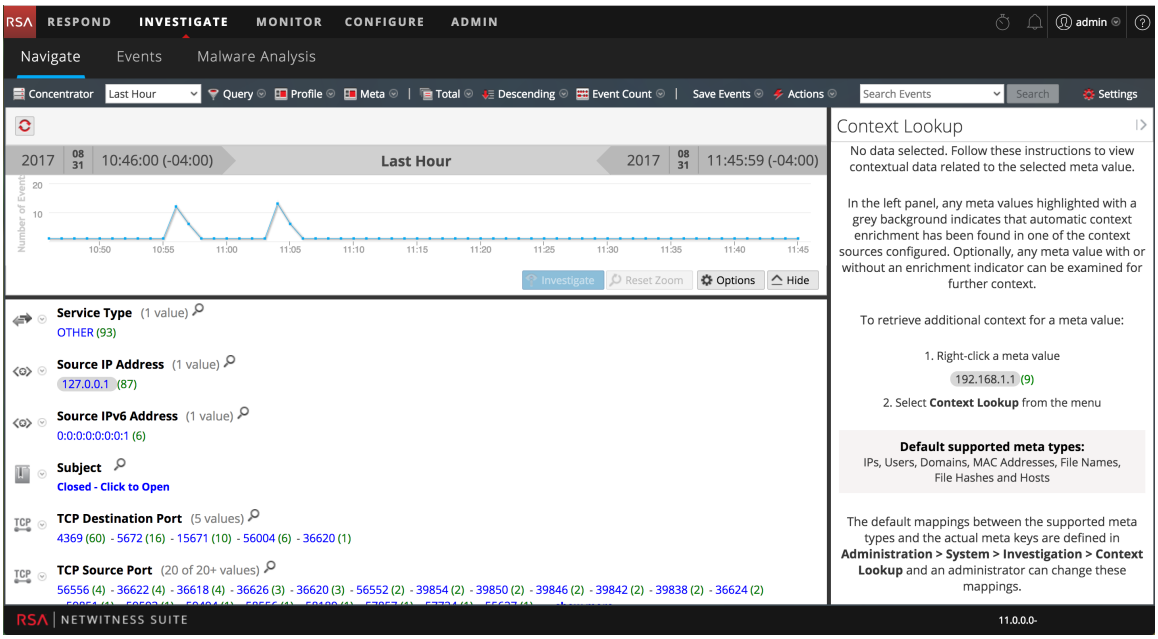
La figure suivante présente le workflow général d'une procédure d'enquête. En une journée classique, un analyste traverse les étapes du workflow général de manière circulaire. Vous commencez généralement par exécuter une requête, puis filtrez un sous-ensemble d'événements, reconstruisez ou analysez un événement et répétez ces étapes 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 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.



Une fois que vous saisissez une requête 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.

Vue Naviguer

La figure suivante illustre la vue Parcourir.



La vue Naviguer offre la possibilité d'effectuer une recherche verticale et d'interroger des données sur un Broker, un Concentrator ou un Decoder, bien que le fait de mener une procédure d'enquête sur un Decoder ne soit pas fréquent. Chaque situation est unique en termes de types d'informations que l'analyste tente de rechercher. La procédure d'enquête présente le contenu des paquets, logs et événements de point de terminaison capturés comme une collection de données extraites dans la vue Naviguer. Les clés méta définies 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.

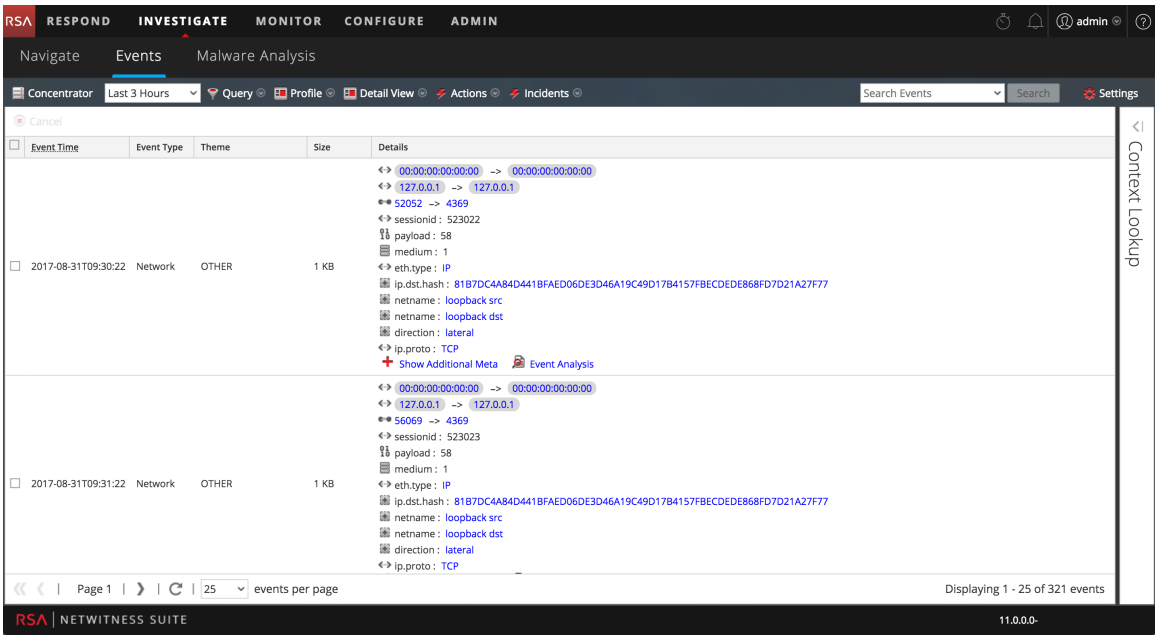
Dans la vue Naviguer, pour certaines clés méta configurées, telles que l'adresse IP ou le nom d'hôte, vous pouvez rechercher des informations contextuelles supplémentaires autour d'une valeur à l'aide du hub Context. Le contexte supplémentaire peut inclure des incidents, des alertes et d'autres sources où la valeur a été abordée.

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.

La vue Naviguer fournit également une visualisation séquentielle des données dans un calendrier. Ici, vous pouvez zoomer sur une période sélectionnée.

Vue Événements

La figure suivante illustre la 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 Événements pour une valeur méta dans un point d'extraction actuel de la vue de navigation. 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 Suite Core sans avoir à effectuer d'abord une recherche verticale à travers la méta.

La vue Événements présente des informations concernant l'événement sous trois formes standards : une simple liste restrictive d'utilisation de grille d'événements, une liste restrictive d'utilisation détaillée des événements et une vue du log. En plus des formulaires standard, vous pouvez créer un groupe de colonnes personnalisé de clés méta sélectionnées, puis attribuer le groupe de colonnes personnalisé à un profil personnalisé pour afficher la liste des événements. Une fois créés, les groupes de colonnes et les profils personnalisés peuvent être sélectionnés depuis une liste déroulante.

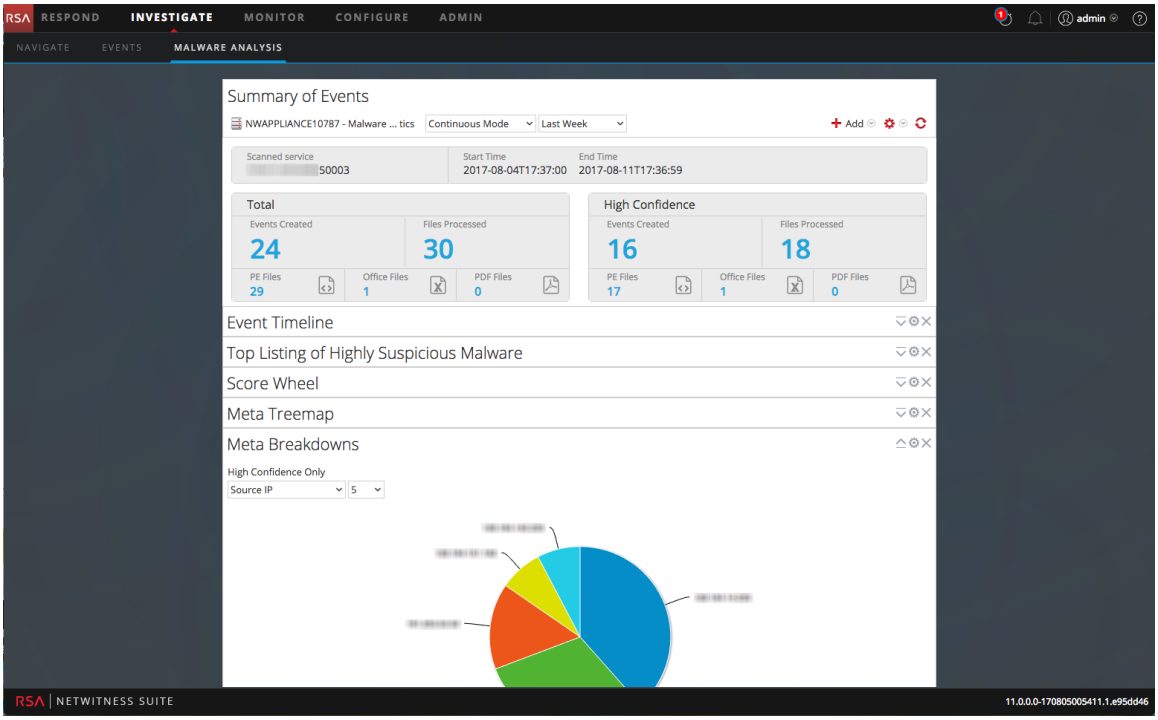
Dans la vue Événements, vous pouvez :

- Reconstruire un événement à partir de la liste des événements. Deux interfaces de reconstruction sont accessibles à partir de la vue Événements : Reconstruction d'événement et analyse d'événement.
- Utiliser les profils des procédures d'enquête pour associer les différents paramètres de ces dernières en ensembles sélectionnables, importer et exporter des métagroupes d'enquêteur, importer et exporter des groupes de colonnes d'enquêteur.
- Exporter des événements et des fichiers associés.

- Créez un incident à partir d'un événement ou modifiez un incident pour ajouter ou supprimer des événements.

Vue Malware Analysis

La figure suivante illustre la vue Malware Analysis



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. Vous pouvez ouvrir la vue Malware Analysis directement, ou vous pouvez utiliser une action de menu contextuel pour analyser des malware à partir d'une métavaleur dans un point d'extraction actuel dans la vue Naviguer. L'analyste de malware peut 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.

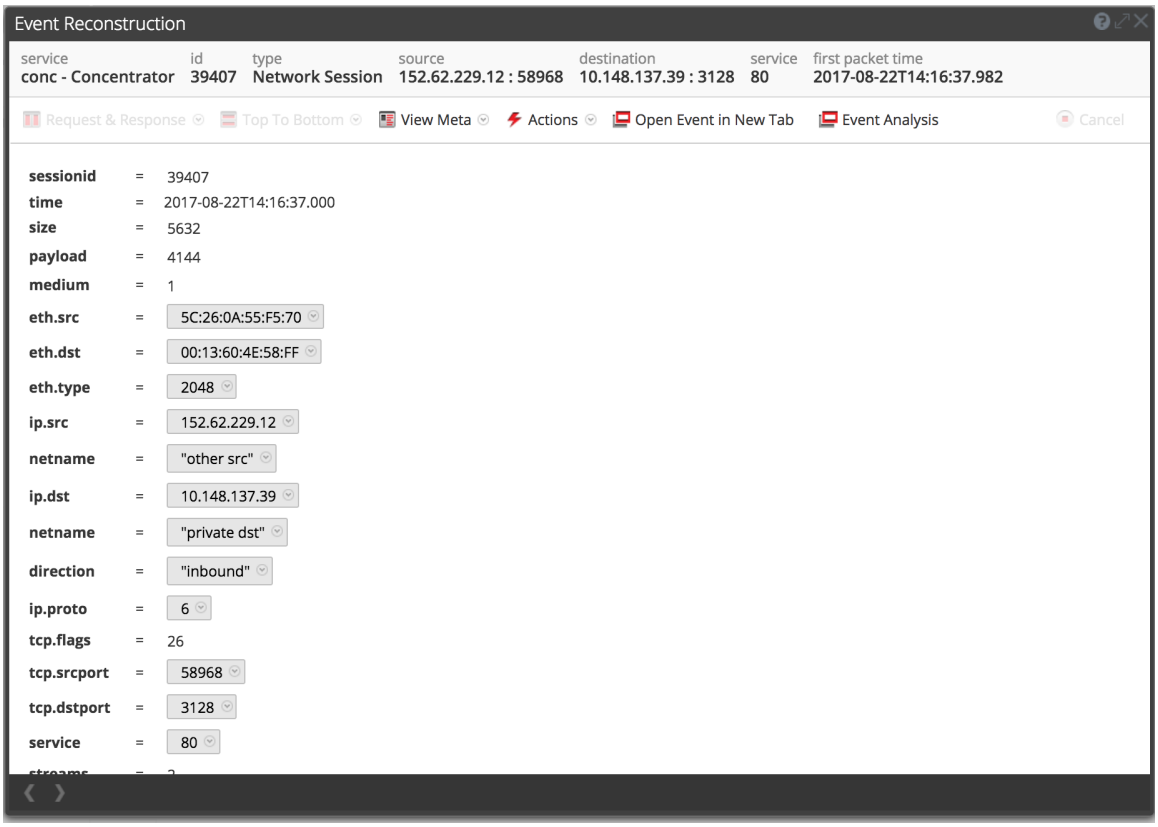
Informations contextuelles pour un événement

À partir de la vue Naviguer et de la vue Événement, vous pouvez consulter les détails à propos des éléments associés à un événement (adresse IP, utilisateur, hôte, domaine, adresse MAC, nom de fichier, hachage de fichier) dans le 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. À partir du Context Hub, vous pouvez cliquer sur un point de données pour revenir à la vue Naviguer.

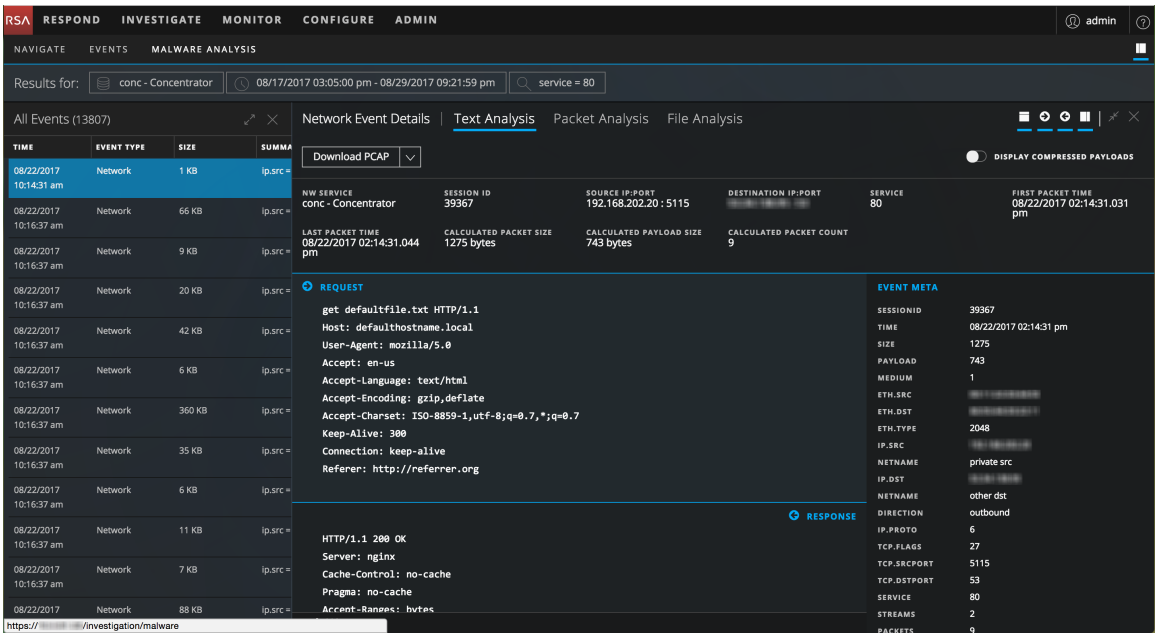
Reconstruction d'événement et analyse d'événement

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, à l'aide de la Reconstruction d'événement ou de l'analyse interactive des événements. 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 s'ouvre dans une fenêtre en haut de la vue Événements. Vous pouvez voir les clés méta et les valeurs méta sous forme de liste et sur une page 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. Cette figure est un exemple de la Reconstruction d'événement.



La vue Analyse des 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 certains types d'informations. Selon le type de reconstruction, par exemple, les paquets, le texte ou les fichiers, des informations différentes sont appropriées. 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 des événements.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
NAVIGATE
EVENTS
MALWARE ANALYSIS
Results for:
conc - Concentrator
08/17/2017 03:05:00 pm - 08/29/2017 09:21:59 pm
service = 80
All Events (13807)
TIME
EVENT TYPE
SIZE
Network Event Details
Text Analysis
Packet Analysis
File Analysis
Download PCAP
DISPLAY COMPRESSED PAYLOADS
NW SERVICE
conc - Concentrator
SESSION ID
39367
SOURCE IP:PORT
192.168.202.20 : 5115
SERVICE
80
FIRST PACKET TIME
08/22/2017 02:14:31.031 pm
LAST PACKET TIME
08/22/2017 02:14:31.044 pm
CALCULATED PACKET SIZE
1275 bytes
CALCULATED PAYLOAD SIZE
743 bytes
CALCULATED PACKET COUNT
9
REQUEST
get defaultfile.txt HTTP/1.1
Host: defaulthostname.local
User-Agent: mozilla/5.0
Accept: en-us
Accept-Language: text/html
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://referrer.org
RESPONSE
HTTP/1.1 200 OK
Server: nginx
Cache-Control: no-cache
Pragma: no-cache
EVENT META
SESSIONID 39367
TIME 08/22/2017 02:14:31 pm
SIZE 1275
PAYLOAD 743
MEDIUM 1
ETH.TYPE 2048
NETNAME private src
NETNAME other dst
DIRECTION outbound
IP.PROTO 6
TCP.FLAGS 27
TCP.SRCPORT 5115
TCP.DSTPORT 53
SERVICE 80
STREAMS 2
/investigation/malware

Fonctions Malware Analysis

NetWitness Suite 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.

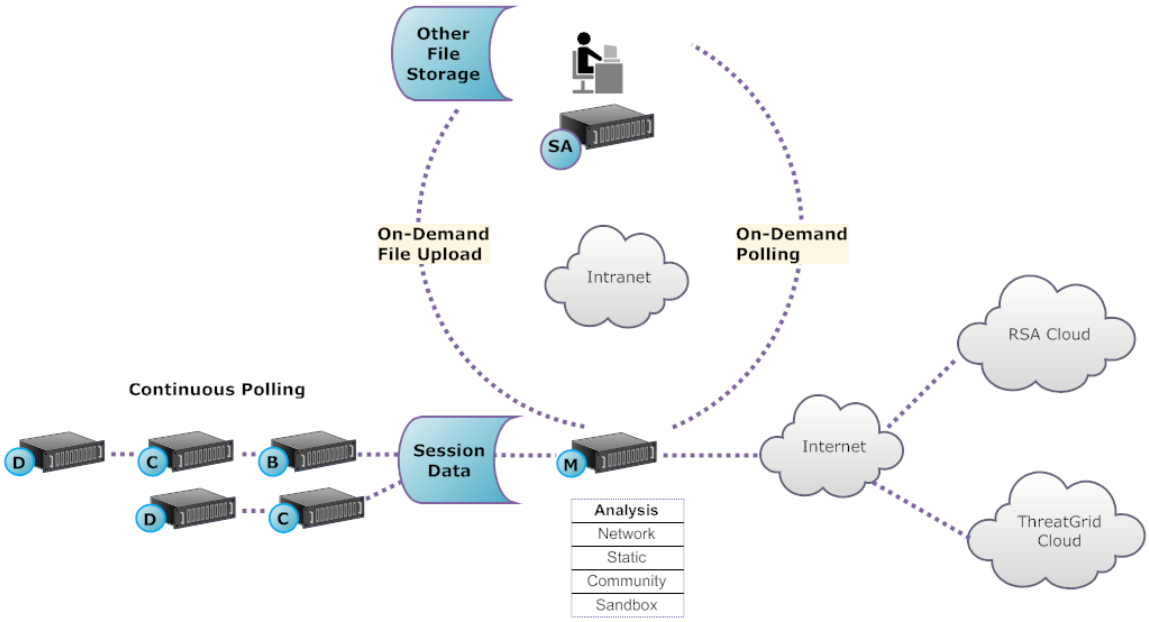
En plus des indicateurs de compromission intégrés, Malware Analysis prend également en charge les indicateurs de compromission écrits en langage YARA. YARA est un langage de règles qui permet aux chercheurs spécialisés d'identifier et de classer les échantillons de programmes malveillants. Cela permet 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 Serveur NetWitness.

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.

Serveur NetWitnessAccédez au service Malware Analysis

Le Serveur NetWitness 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 Suite 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 compromis (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 Suite 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 Suite, toutes les fonctionnalités d'affichage et d'analyse dans Investigation sont disponibles pour poursuivre l'analyse des Indicateurs de compromis. 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 Suite 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.

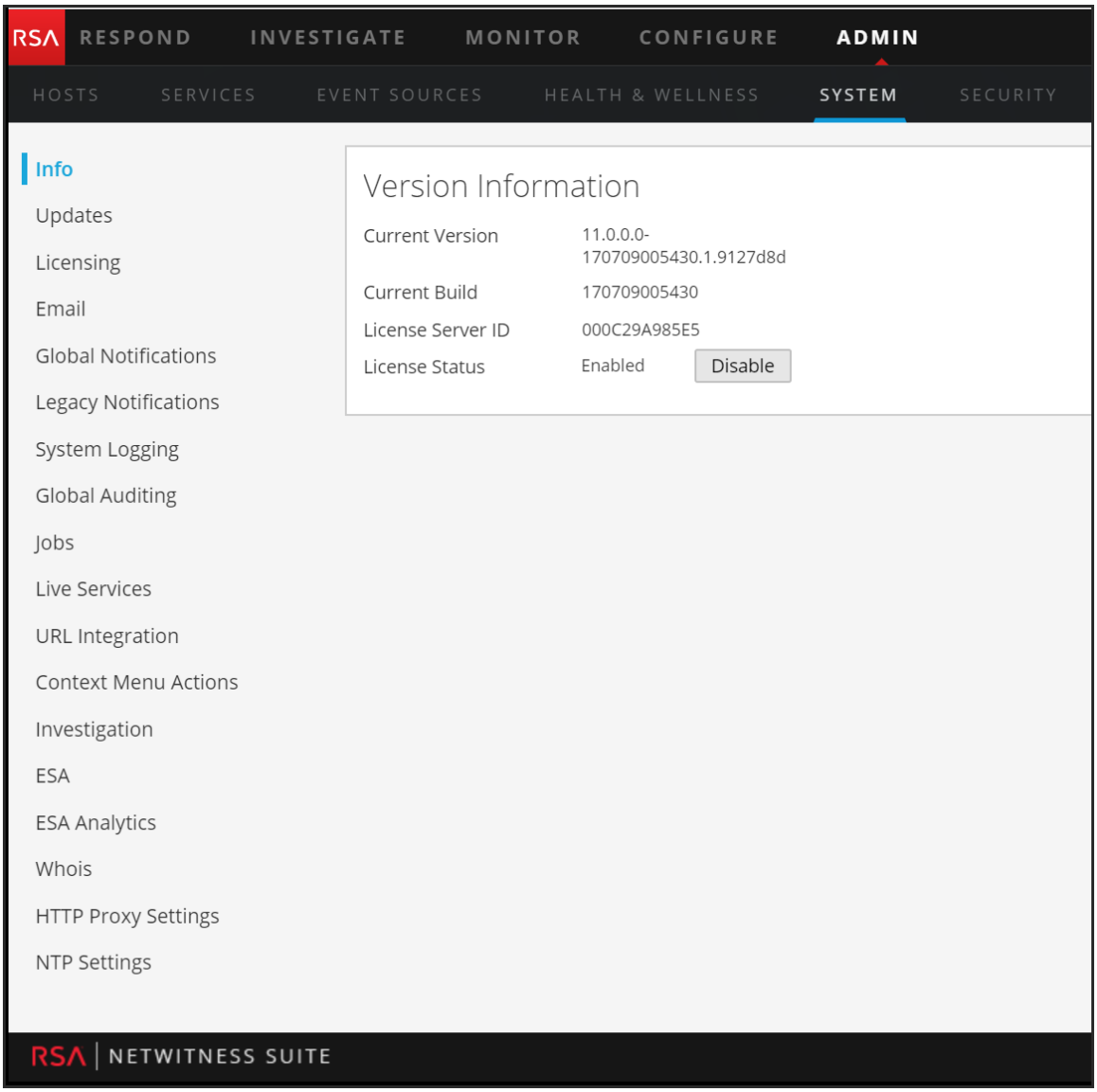
Rôles et autorisations pour les analystes Malware

Cette rubrique identifie les rôles d'utilisateur et les autorisations nécessaires pour qu'un utilisateur effectue une analyse de malware dans NetWitness Suite. 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.

Rôles et autorisations nécessaires

RSA NetWitness Suite gère la sécurité en autorisant l'accès aux vues et fonctions au moyen d'autorisations système et d'autorisations sur les différents services.

Au niveau du système, l'utilisateur doit être associé à un rôle système dans la vue Administration > Système pour pouvoir accéder à certaines vues et fonctions.



Dans NetWitness Suite 11.0, le rôle `Malware_Analysts` par défaut est attribué à toutes les autorisations ci-dessous. Si nécessaire, un administrateur peut créer un rôle personnalisé combinant plusieurs des autorisations suivantes :

- Accéder au module Investigation (obligatoire)
- Investigation - Parcourir les événements
- Investigation - Parcourir les valeurs
- Accéder au module Incident
- Afficher et gérer les incidents
- Afficher les événements de malware (pour consulter les événements)

- Téléchargement de fichiers (pour télécharger des fichiers à partir du service Malware Analysis)
- Lancer une analyse de malware (pour lancer une analyse de service ou un téléchargement de fichier unique)
- Autorisations de dashlet pour des questions pratiques : Dashlet - Dashlet Valeurs principales d'investigation, Dashlet - Dashlet Liste des services d'investigation, Dashlet - Dashlet Tâches d'investigation, Dashlet - Dashlet Raccourcis d'investigation.

Vous pouvez par exemple créer le rôle personnalisé Analyste du malware Junior et l'associer à des autorisations limitées excluant l'autorisation Téléchargement de fichiers.

Pour certains services, un analyste du malware doit être membre du groupe **Analystes** ou d'un groupe disposant des deux autorisations associées par défaut au groupe Analyste : **sdk.meta** et **sdk.content**. Les utilisateurs disposant de ces autorisations peuvent se servir d'applications spécifiques, lancer des requêtes et afficher des contenus à des fins d'analyse du service.

Configurer les vues et préférences de procédure d'enquête

Les analystes peuvent configurer certains aspects des vues et du comportement de NetWitness Suite Investigation. 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 des rôles et des autorisations conformément à la description de la rubrique Rôles et autorisations pour les analystes Malware.

Ces rubriques fournissent des détails :

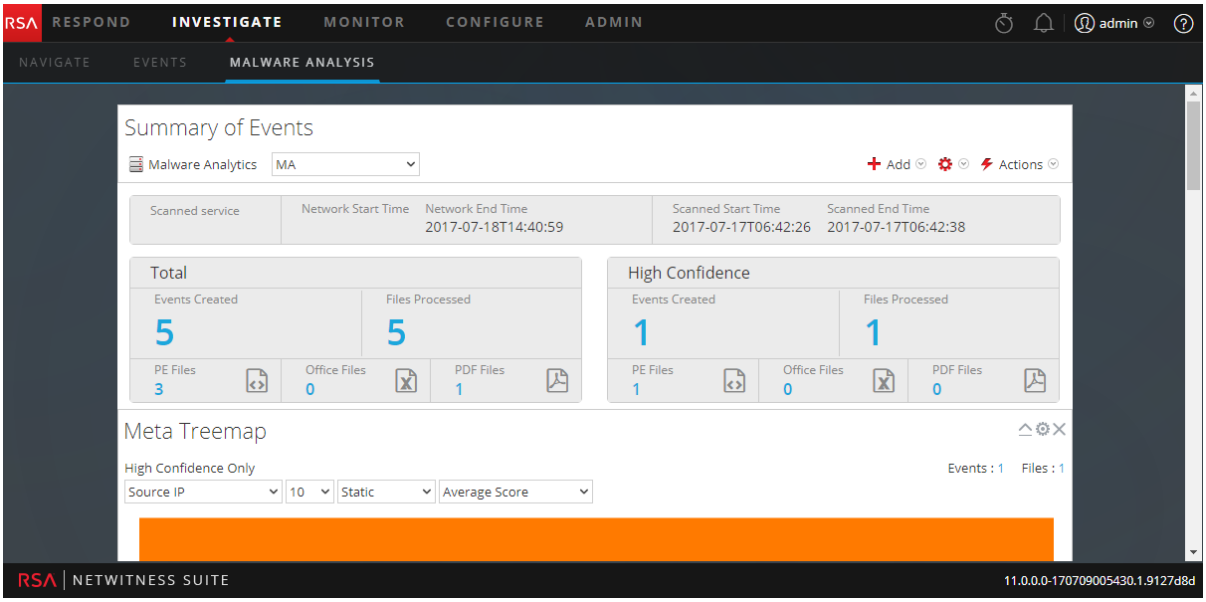
- Configurer la vue Parcourir et la vue Événements
- Vue Configurer le récapitulatif des événements de malware

Vue Configurer le récapitulatif des événements de malware

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 Suite : 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 RSA NetWitness Suite.
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.

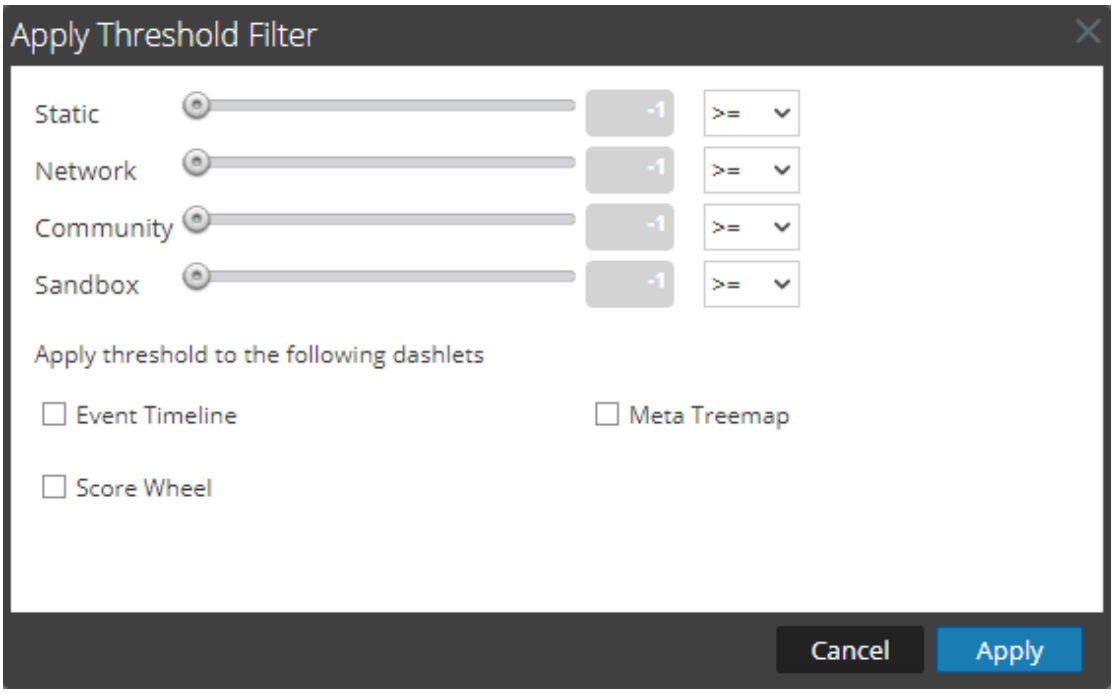
Pour utiliser les options de la barre d'outils :

- 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 Méta Treemap. Vous pouvez également définir le seuil pour des dashlets individuels.

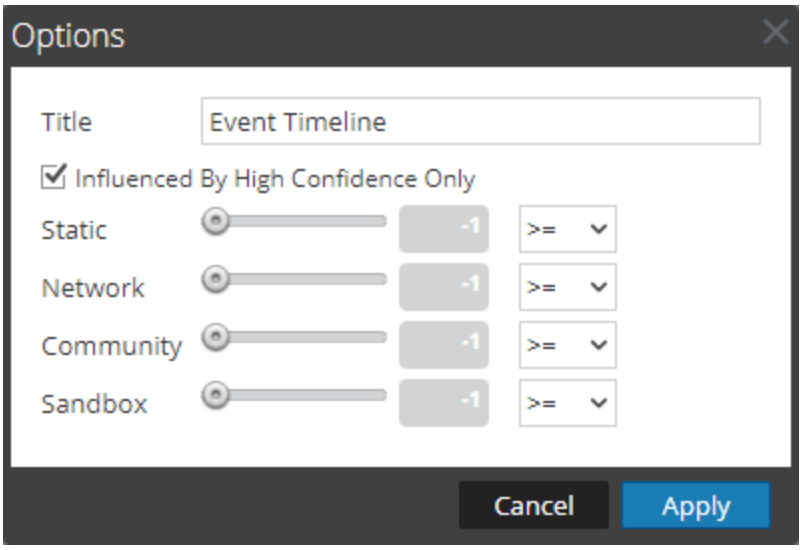
1. Dans la barre d'outils, sélectionnez > **Appliquer le filtre de seuil**.
   La boîte de dialogue Appliquer le filtre de seuil s'affiche.



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.

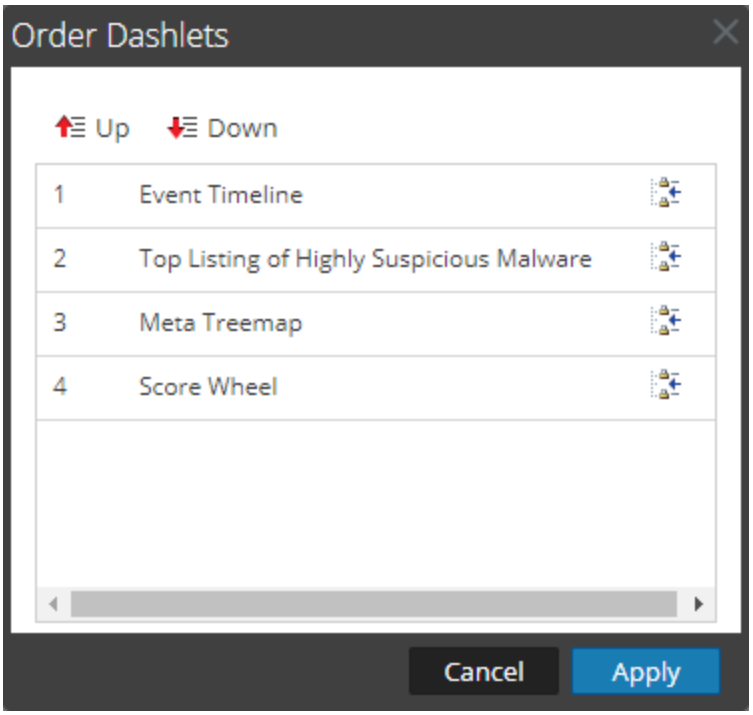


2. Saisissez un nouveau titre pour le dashlet dans le champ **Titre**.
3. Si vous voulez voir uniquement les événements qui sont influencés par une balise de forte probabilité, ce qui signifie qu'il y une grande probabilité que l'événement contienne un code malveillant, cochez l'option **Influencé par 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 Résumé 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 Résumé 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.

Configurer la vue Parcourir et la vue Événements

Les analystes peuvent configurer des préférences affectant les performances et le comportement de NetWitness Suite lors de l'analyse de données avec la vue Enquêter > Naviguer et la vue Événements.

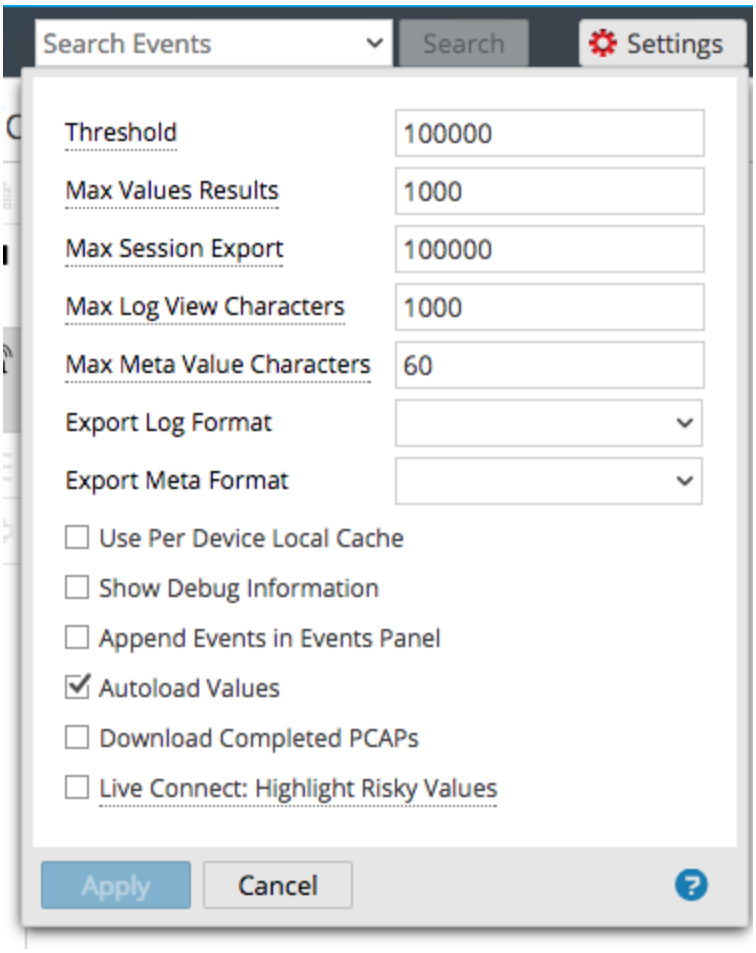
Ces paramètres sont disponibles à deux emplacements dans NetWitness Suite et les modifications effectuées dans l'un ou l'autre des emplacements sont répercutées dans l'autre vue :

- Vue Enquêter > boîte de dialogue Paramètres et champ Rechercher pour la vue Naviguer et la vue Événements.
- Profils > panneau Préférences > onglet Procédures d'enquête.

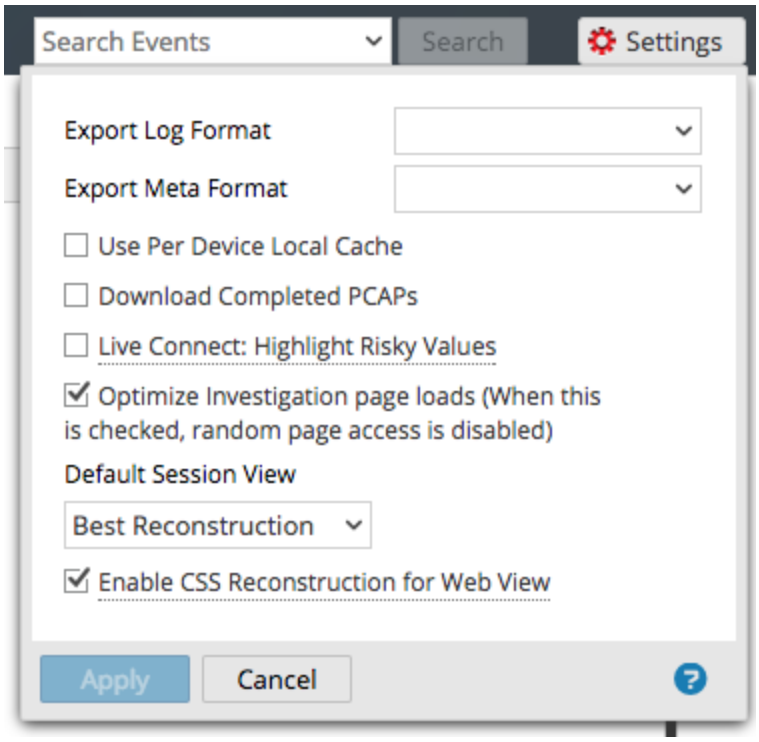
Accès aux paramètres de la procédure d'enquête

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.

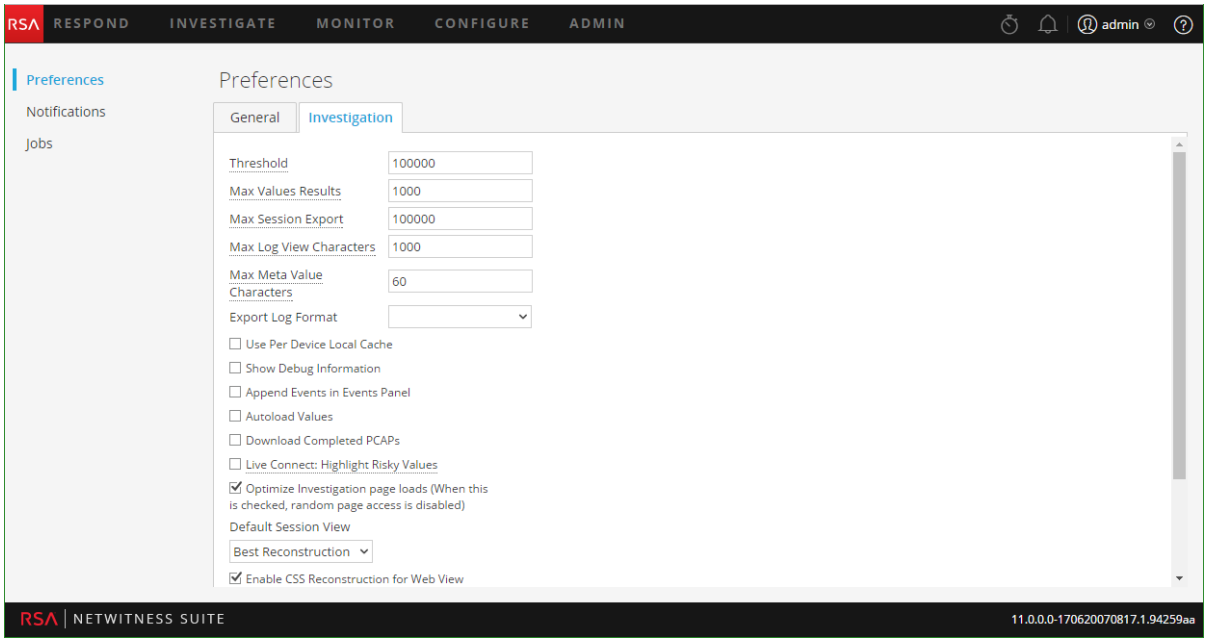


- Dans la barre d'outils de la vue **Événements**, sélectionnez l'option **Paramètres**.
  La boîte de dialogue Paramètres de la vue Événements s'affiche.



- Dans le coin supérieur droit de NetWitness Suite, sélectionnez **Profil** dans le menu contextuel de l'utilisateur, puis cliquez sur **Préférences**. Cliquez sur l'onglet **Procédure d'enquête**.

  L'onglet Procédure d'enquête s'affiche.



Calibrer les paramètres de chargement des valeurs de la vue Naviguer

Plusieurs paramètres de procédure d'enquête influencent les performances de NetWitness Suite 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** pour afficher la vue Naviguer.
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 max 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 **Investigation Événements > Texte du log**. La valeur par défaut est **1000**.
- Afficher les informations de débogage Si vous souhaitez que NetWitness Suite 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**.
- Charger automatiquement les valeurs : Si vous souhaitez que NetWitness Suite charge automatiquement les valeurs pour le service sélectionné dans la vue Naviguer, cochez cette option. Lorsqu'elle n'est pas sélectionnée, NetWitness Suite affiche un bouton **Charger les valeurs**, qui donne l'opportunité à l'utilisateur de modifier des options. La valeur par défaut est **Off**.
- Live Connect : Mettre en évidence les IP risquées : Si vous souhaitez que NetWitness Suite 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 Suite affiche toutes les adresses IP. Par défaut, cette option n'est pas activée (**Désactivée**).

3. Cliquez sur **Appliquer**.

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

Configurer le comportement du téléchargement PCAP dans Procédure d'enquête

Vous pouvez automatiser le téléchargement des fichiers PCAP extraits du module Investigation 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.

Pour procéder à la configuration :

1. 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.
2. Accédez à l'onglet **Procédure d'enquête** ou à la boîte de dialogue **Paramètres** pour afficher la vue Naviguer ou la vue Événements.
3. Cochez l'option **Téléchargement des PCAP terminés**.
4. Cliquez sur **Appliquer**.
   Le paramètre prend effet immédiatement.

Configurer le format d'export de log par défaut dans Procédure d'enquête

Vous pouvez exporter des logs dans Procédure d'enquête dans différents formats. Les options disponibles sont : Texte, XML, CSV, 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 Suite 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 afficher la vue Naviguer.
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'export de méta par défaut dans Procédure d'enquête

Vous pouvez exporter des valeurs méta dans Procédure d'enquête dans différents formats. Les options disponibles sont : Texte, XML, CSV, 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 Suite 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 afficher la vue Naviguer.
2. Sélectionnez l'une des options du menu déroulant **Format méta d'exportation**.
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 Suite 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**.
- **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 page suivante, le prochaine incrément d'événements 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.

- **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. 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 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. L'option est activée par défaut. Désactivez cette option en cas de problèmes avec l'affichage de sites Web spécifiques.

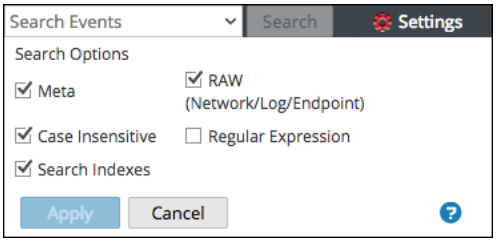
Remarque : L'apparition du contenu reconstitué peut ne pas correspondre parfaitement à la page Web d'origine si les images et les feuilles de style sont introuvables ou si elles ont été chargées à partir de la mémoire cache du navigateur Web. De plus, tout style ou mise en page effectué dynamiquement via le javascript côté client ne sera 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. Accédez à l'onglet **Procédure d'enquête**.
2. Cochez la case **Activer la vue CSS Reconstruction pour le Web**.
3. Cliquez sur **Appliquer**.
   Le paramètre devient effectif immédiatement mais ne sera visible que dans la prochaine reconstruction de contenu Web.

(Optional) Configure Search Options

1. Cliquez dans le champ **Rechercher** pour afficher le menu déroulant Rechercher des événements.



2. Sélectionnez une ou plusieurs options de recherche à appliquer à la recherche. Rechercher des modèles de texte dans la vue Enquêter 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.

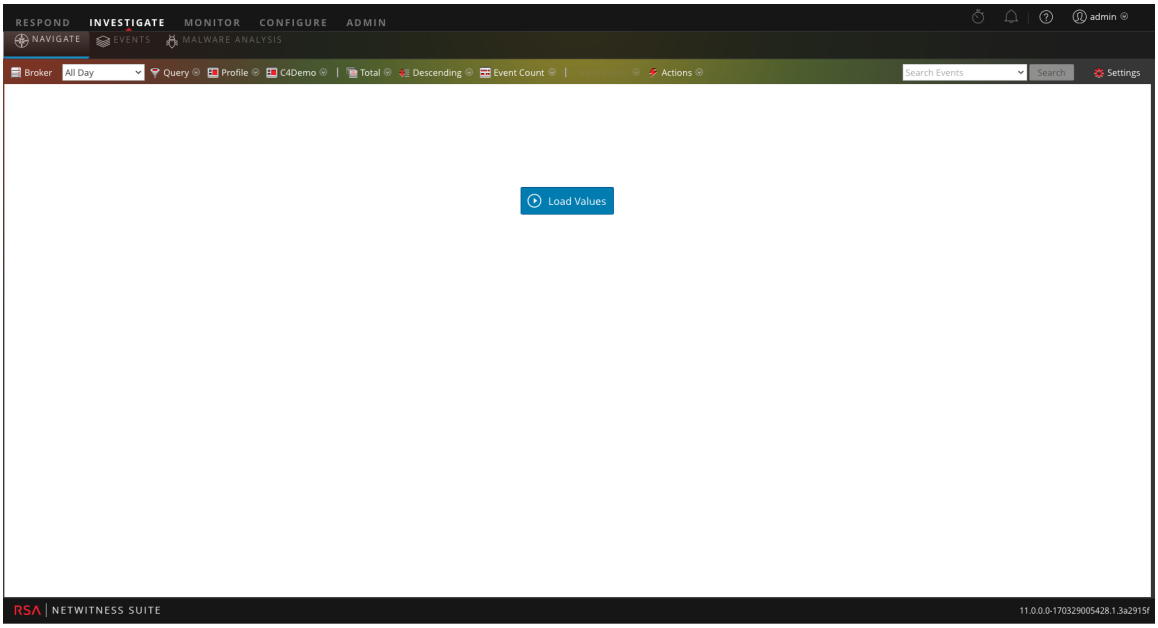
Mener une procédure d'enquête

Vous pouvez commencer une procédure d'enquête de différentes manières dans NetWitness Suite ; pour les procédures détaillées, consultez Commencer une procédure d'enquête d'un service ou d'une collection. Une procédure d'enquête ne nécessite pas de respecter un ordre spécifique lors de sa conduite. Au lieu de cela, NetWitness Suite offre différentes méthodes d'affichage, de filtrage et d'interrogation des données, d'action sur un point d'extraction verticale et d'inspection sur des événements spécifiques.

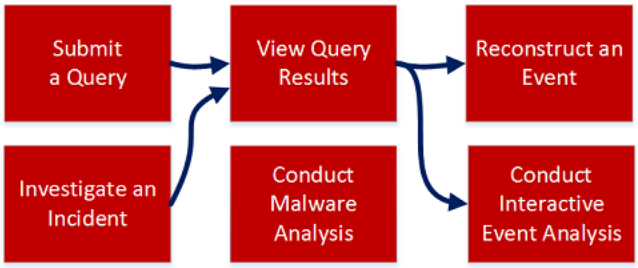
Les analystes qui utilisent NetWitness Suite Investigation doivent disposer des rôles et autorisations du système appropriés pour leur compte utilisateur. Voir Rôles et autorisations pour les analystes Malware. Un administrateur doit configurer des rôles et des autorisations.

Remarque : Si vous enquêtez sur un service 10.6 à partir d'un serveur 11.0 NetWitness, le comportement de téléchargement varie pour les fichiers, PCAP, logs, charges utiles et valeurs méta. Vous pouvez voir une charge utile d'événement sur un service 10.6 pour lequel vous n'avez pas d'autorisation, mais vous ne serez pas en mesure de télécharger des fichiers ou des charges utiles.

Pour effectuer une procédure d'enquête, connectez-vous à NetWitness Suite et accédez à ENQUÊTER. La vue Procédure d'enquête s'affiche avec les champs dans lesquels vous sélectionnez le service, la plage de temps et une requête facultative pour des métadonnées spécifiques. Sélectionnez un service, puis cliquez sur **ChargerValeurs**.



Voici les étapes de base pour mener une procédure d'enquête.



1. Envoyer une requête ou pivotez vers Enquêter à partir d'une entité Répondre (reportez-vous à la section Commencer une procédure d'enquête d'un service ou d'une collection).
2. Affichez les résultats de la requête dans la vue Naviguer (reportez-vous à la section Affiner les résultats affichés dans la vue Naviguer) et la vue Événements (reportez-vous à la section Examiner des événements).
3. 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 Analyser les événements dans la vue Analyse d'événements).
4. Agissez sur un point de recherche verticale ou un événement (reportez-vous à la section Agir sur un point de recherche verticale dans la vue Parcourir et Examiner des événements. Par exemple, vous pouvez Afficher un contexte supplémentaire pour un point de données, Lancer une analyse Malware Analysis à partir de la vue Naviguer ou Ajouter des événements à un incident pour obtenir une réponse.

Commencer une procédure d'enquête d'un service ou d'une collection

Les analystes peuvent commencer une procédure d'enquête sur les données d'un service ou d'une collection NetWitness Suite, ce qui entraîne le chargement de valeurs.

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 Suite. Si vous ne pouvez pas réaliser de tâche d'analyse ou afficher une vue, l'administrateur a peut-être besoin d'ajuster les rôles et autorisations configurés pour vous.

Pour commencer une procédure d'enquête dans NetWitness Suite, un service doit être spécifié.

- NetWitness Suite ouvre la vue Naviguer 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 Suite 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, vous pouvez modifier le service ou la collection à examiner en sélectionnant le nom du service dans la barre d'outils. NetWitness Suite 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 Suite est prêt à charger les données du service ou de la collection. 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 Configurer les vues et préférences de procédure d'enquête).

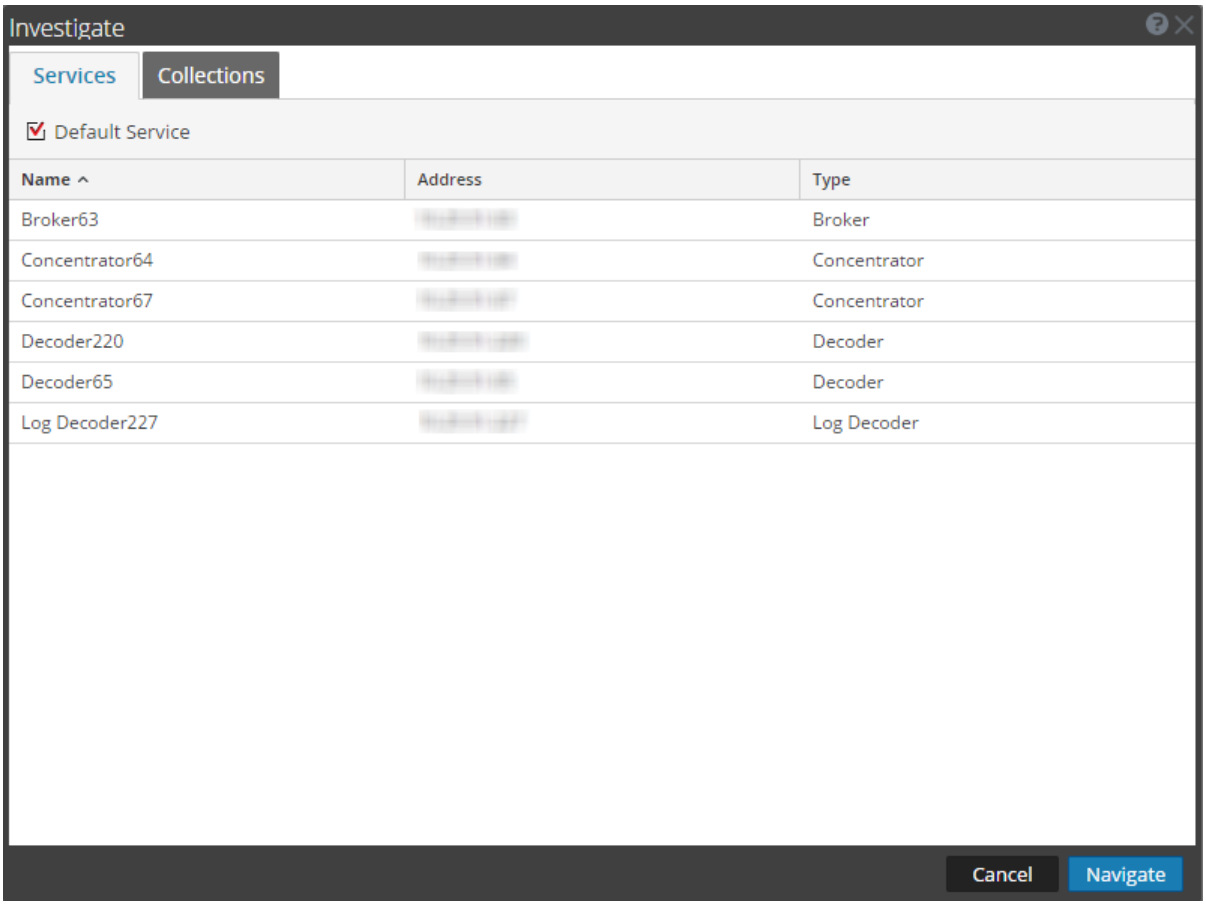
Remarque : Si vous avez indiqué Charger automatiquement les valeurs, NetWitness Suite remplit automatiquement les données. Sinon, vous devez sélectionner le bouton Charger. NetWitness Suite remplit les métadonnées dans le panneau Valeurs de la vue Naviguer et les résultats deviennent visibles presque 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.

Commencer une procédure d'enquête dans la vue Enquêter (aucun service par défaut)

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

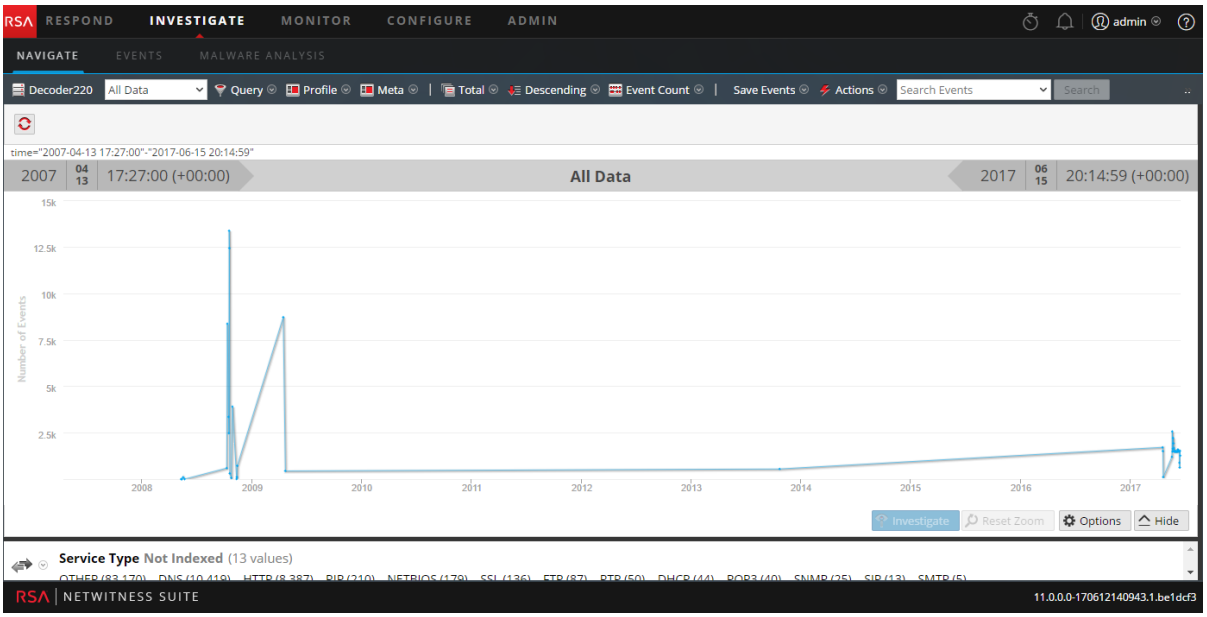


2. Double-cliquez sur un service ou sélectionnez un service, en général un Concentrator, puis cliquez sur **Naviguer**.
   Le panneau qui en résulte affiche l'activité pour le service sélectionné.
3. Si vous souhaitez modifier les options de procédure d'enquête avant le chargement, vous pouvez créer 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 Affiner les résultats affichés dans la vue Naviguer Vous pouvez également modifier les options à tout moment pendant la procédure d'enquête.

4. Lorsque vous êtes prêt, cliquez sur Load Values.

   Les données du service sélectionné commencent à se charger.



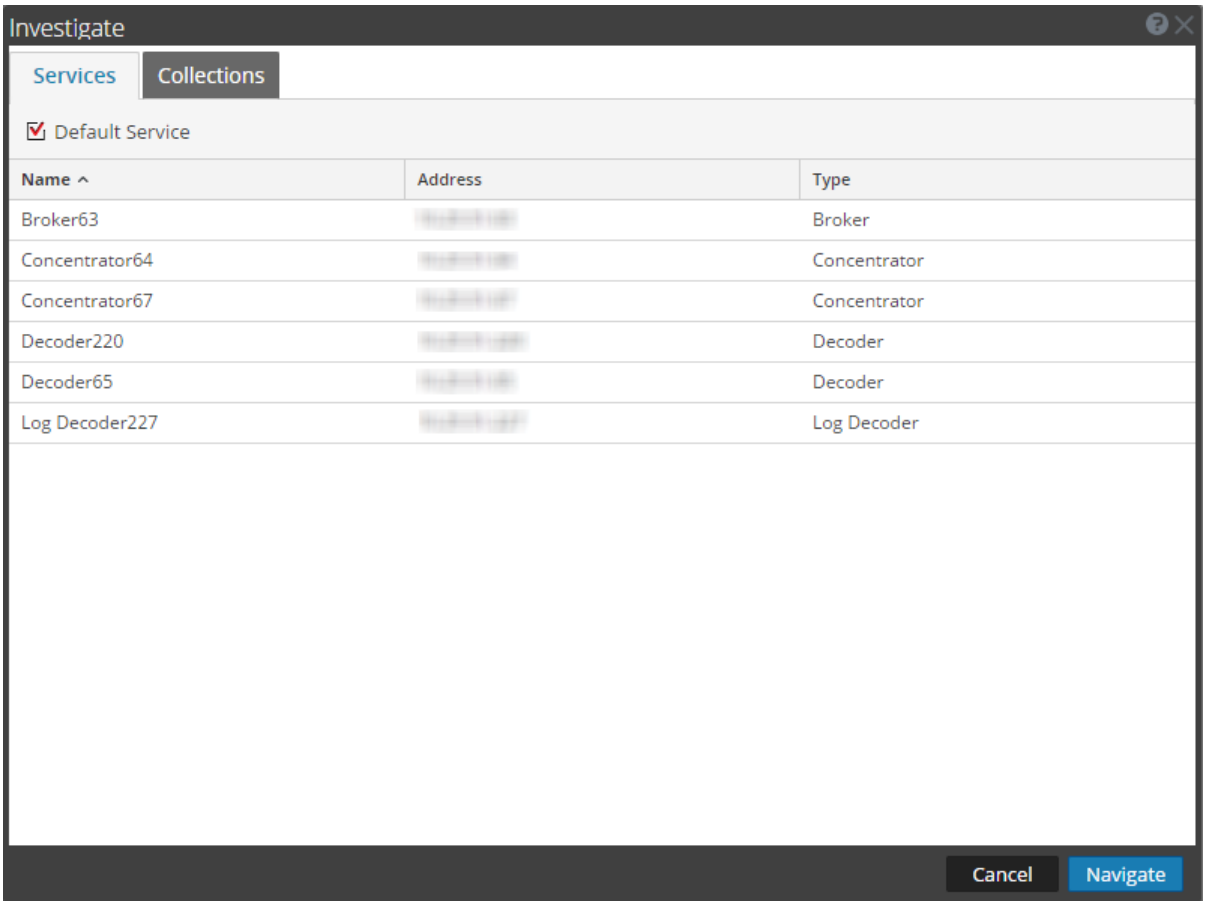
Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données.

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.

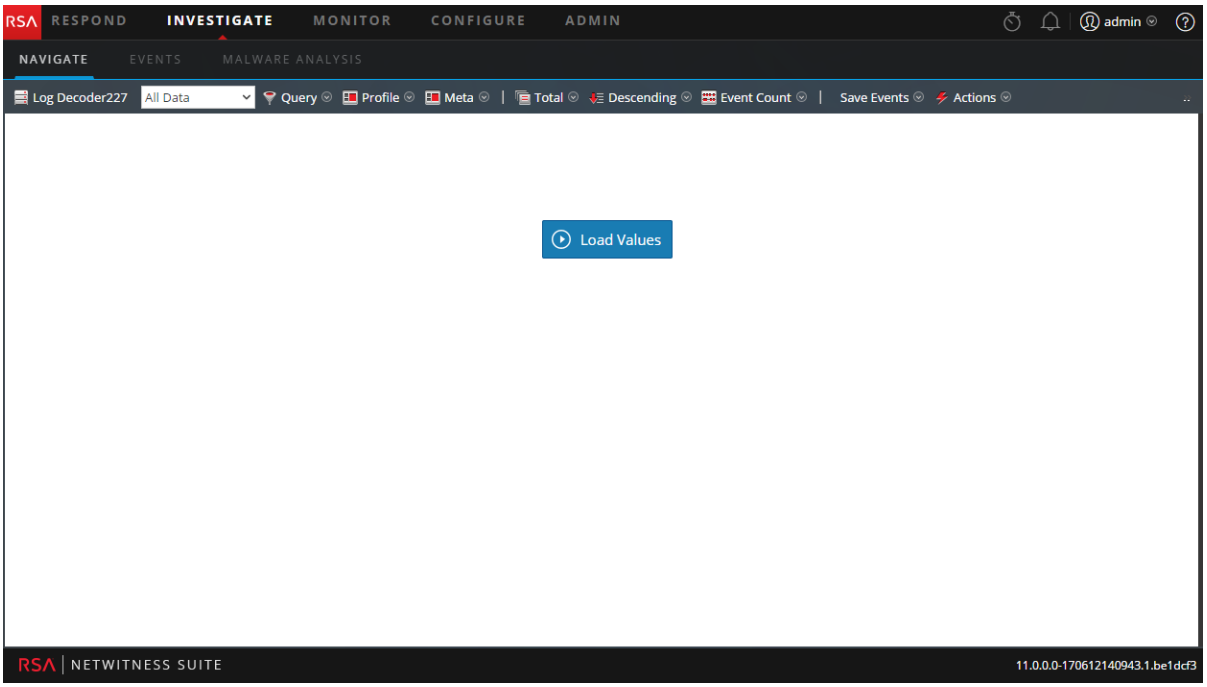
> **Remarque :** Le bouton Annuler n'annule pas votre sélection du service par défaut. Il ferme simplement la boîte de dialogue sans avoir à naviguer vers le service actuellement sélectionné dans la grille. La définition d'un service par défaut, différent du service actuellement à l'étude, n'actualise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

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

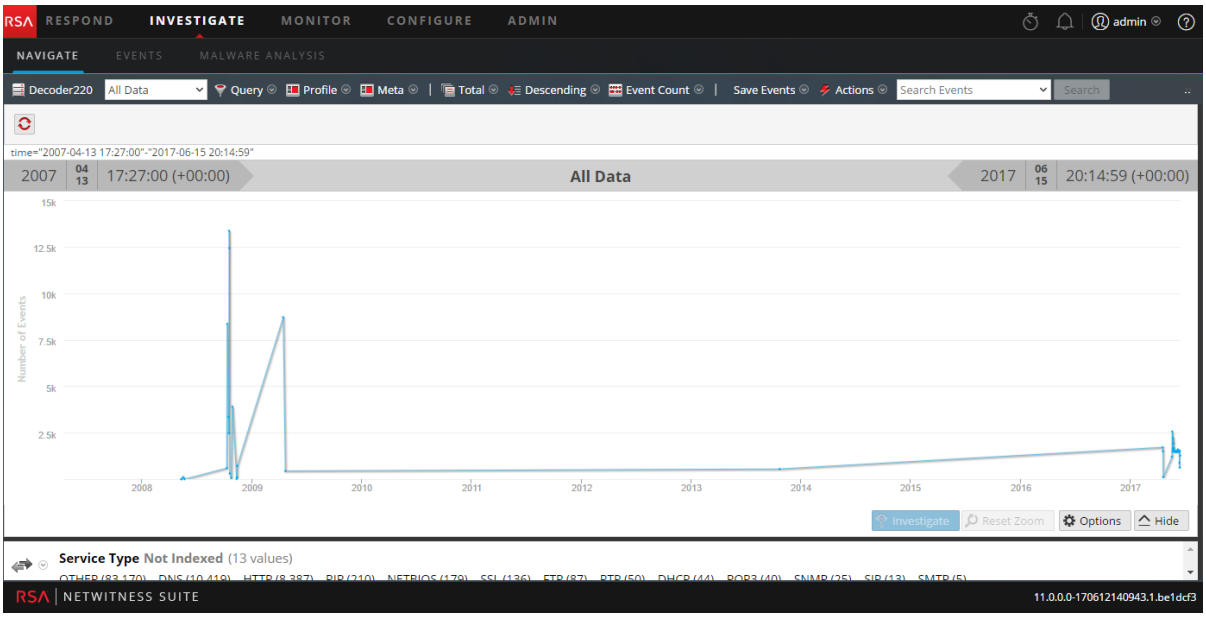
1. Accédez à **ENQUÊTER** > Naviguer

   .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.



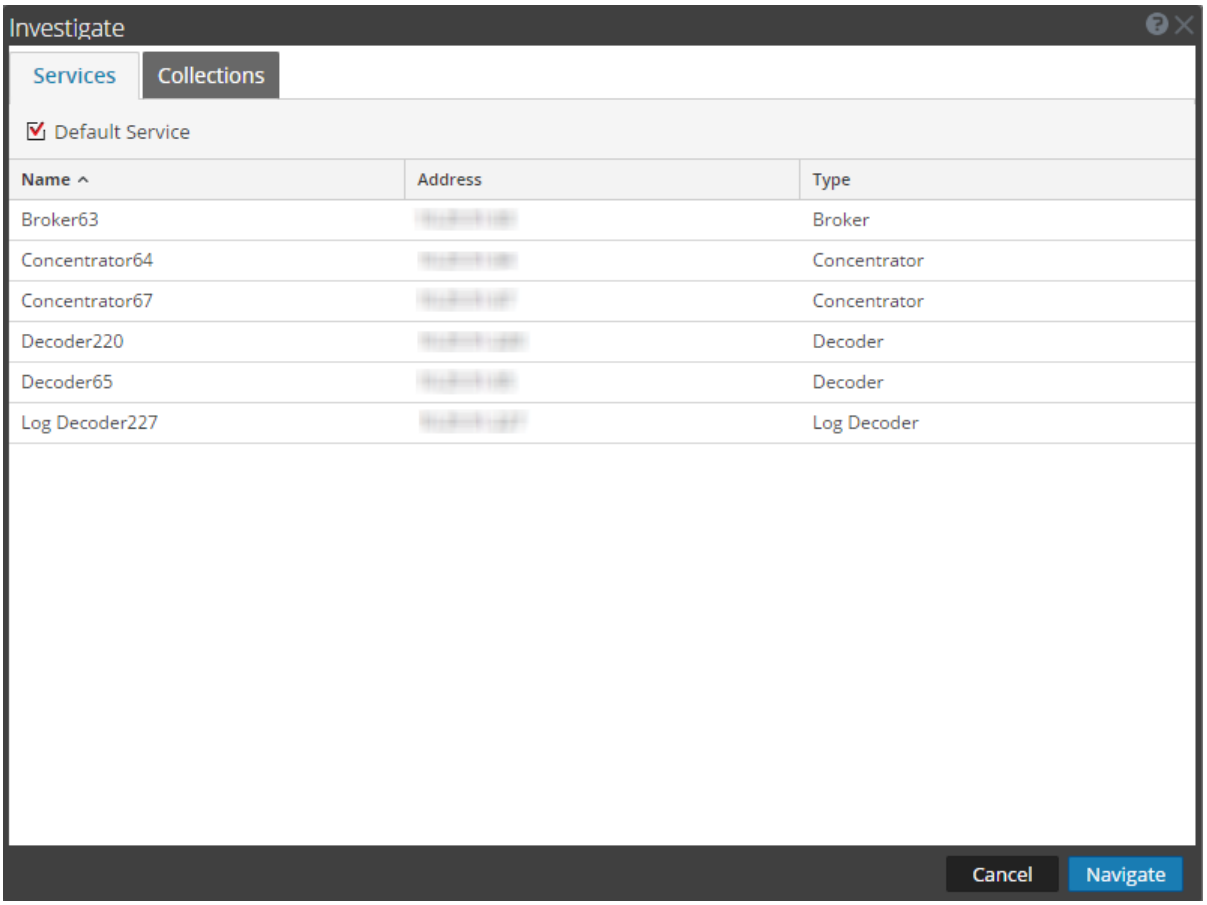
2. Si vous souhaitez modifier les options de procédure d'enquête avant le chargement, vous pouvez créer ou modifier un profil personnalisé, appliquer une période différente, créer ou appliquer un groupe méta, et effectuer une requête personnalisée.
3. Lorsque vous êtes prêt, cliquez sur Load Values.
   Les valeurs du service sont chargées selon les options choisies.



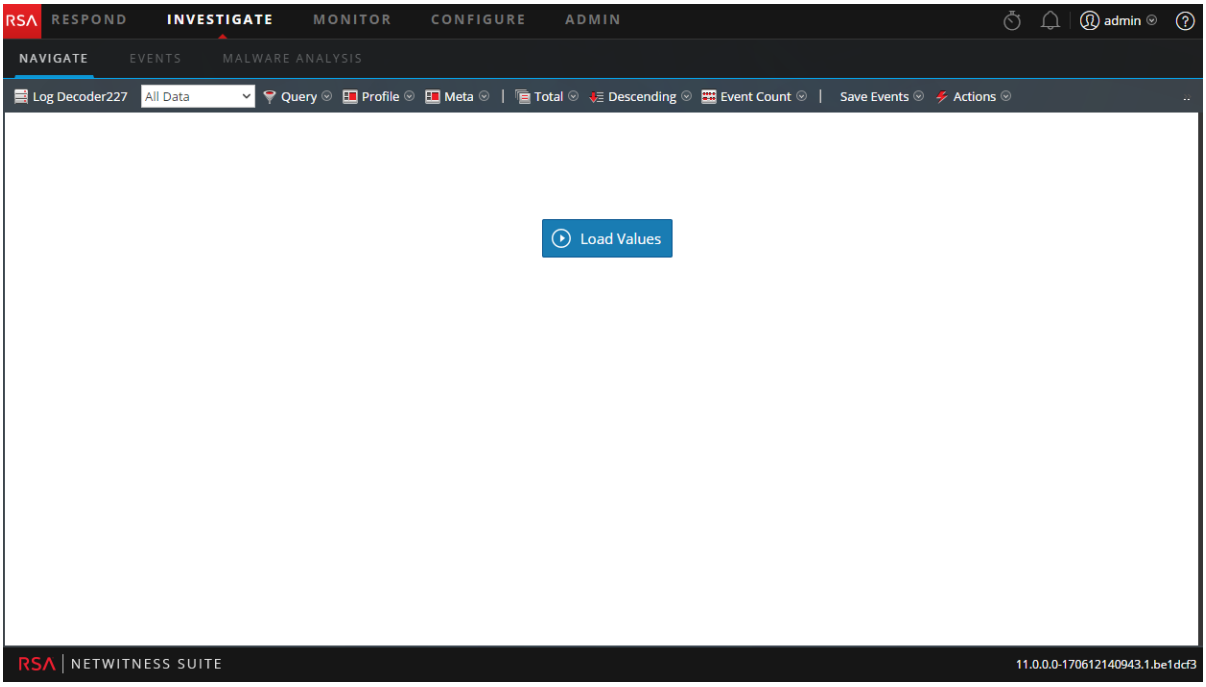
Avec le service sélectionné et les données chargées, vous êtes prêt à commencer à analyser les données.

Modifier le service ou la collecte à examiner

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

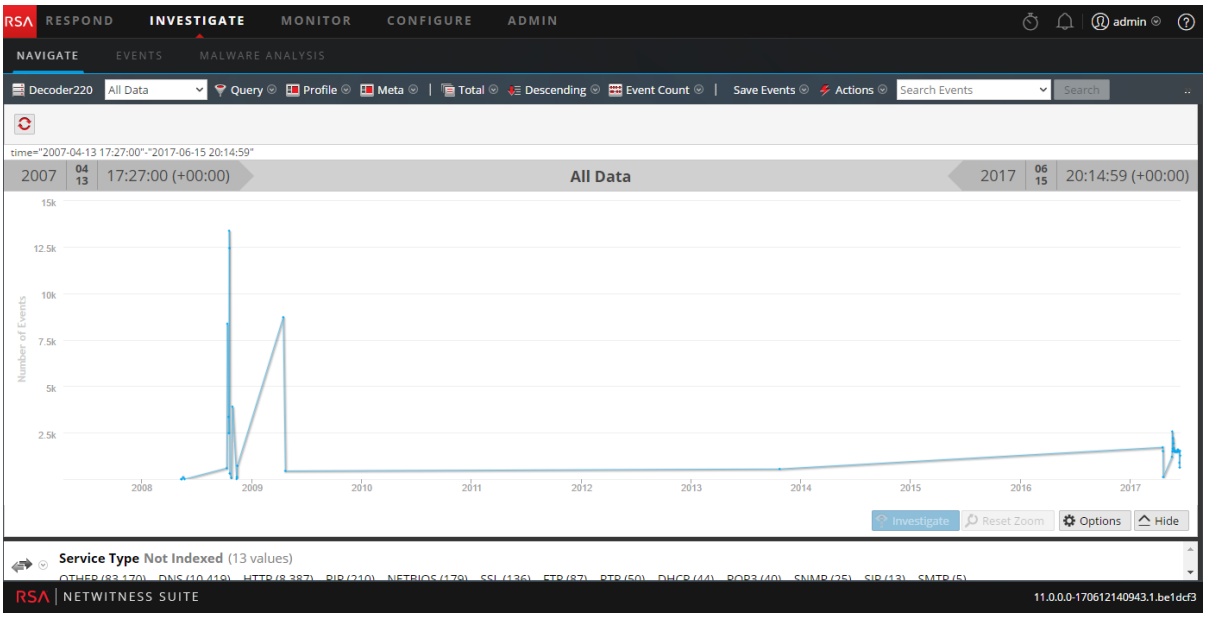


2. Double-cliquez sur un service ou sélectionnez un service, puis cliquez sur **Naviguer**. Le panneau résultant affiche l'activité pour le service sélectionné.
   Si le paramètre Charger automatiquement les valeurs est activé, les valeurs sont chargées comme indiqué à l'étape 3. Dans le cas contraire,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



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.

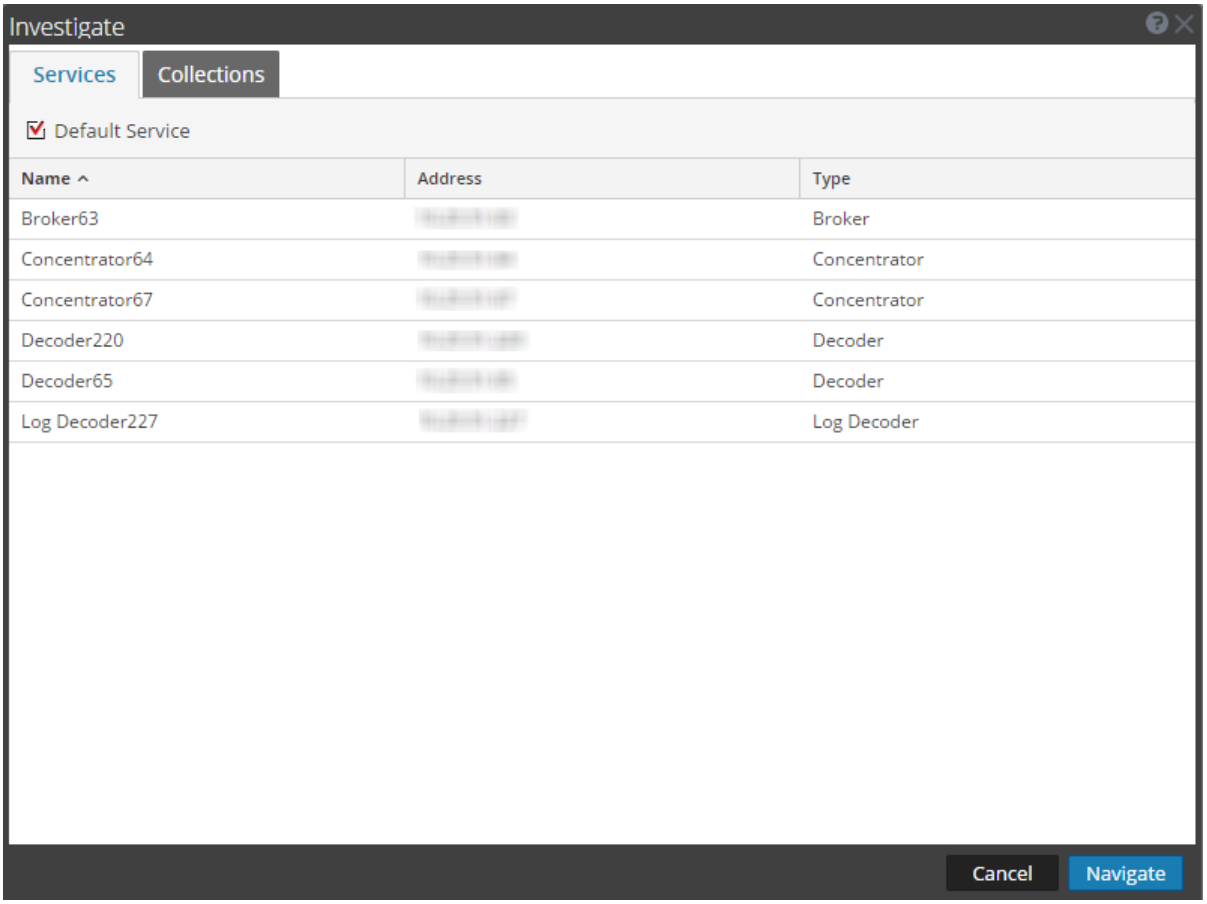
Examiner des collections de restauration Workbench

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
   . 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.

Affiner les résultats affichés dans la vue Naviguer

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

- Définir la période d'investigation (vue Rechercher ou vue Événements)
- Définir la méthode de quantification et trier la séquence des résultats de clé méta (vue Naviguer)
- Gérer et appliquer des clés méta par défaut dans une procédure d'enquête (vue Naviguer)
- Gérer les groupes méta (vue Naviguer)
- Visualiser des métadonnées en tant que coordonnées parallèles(vue Naviguer)
- Utiliser des profils d'investigation pour encapsuler les vues personnalisées (vue Naviguer et vue Événements)

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 ont été trouvées. 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 Suite inclut les groupes méta prêts à l'emploi que les développeurs de contenu RSA ont mis au point pour vous aider à trouver des jeux de données intéressants dans Enquêter. 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 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 groupes méta prêts à l'emploi sont intégrés à la Suite RSA NetWitness. Les groupes méta 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.

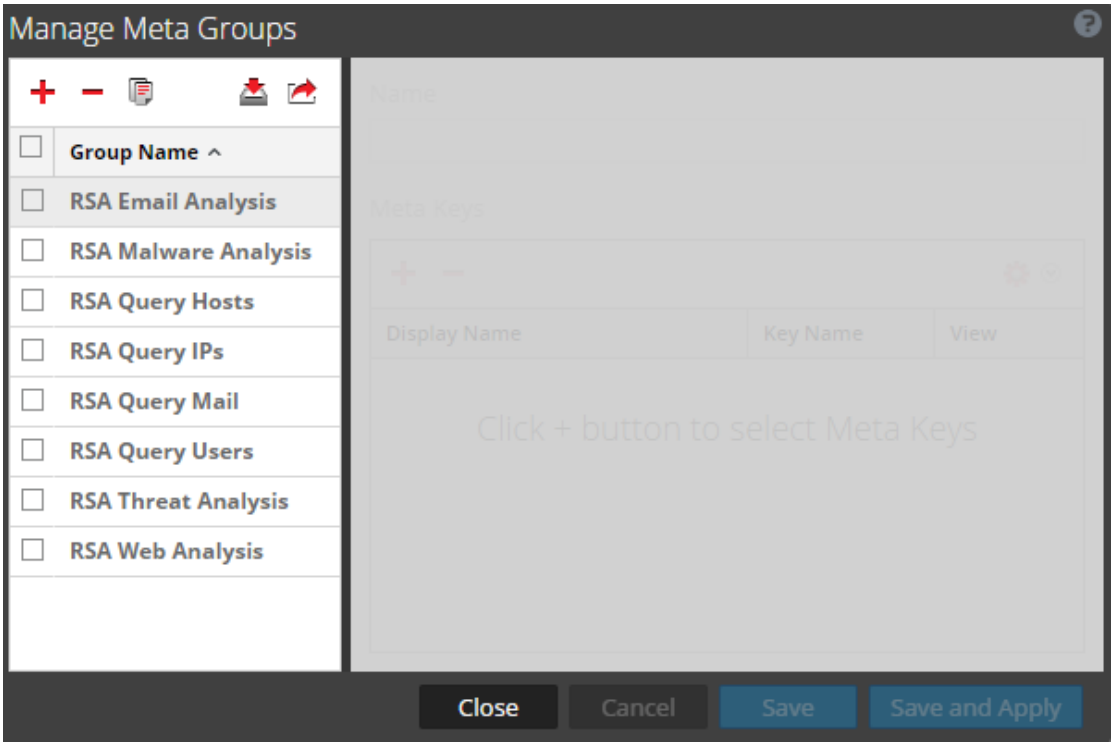
Voici les groupes méta prêts à l'emploi :

- 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.
- RSA Web Analysis comprend des clés méta qui marquent des anomalies dans le trafic web.

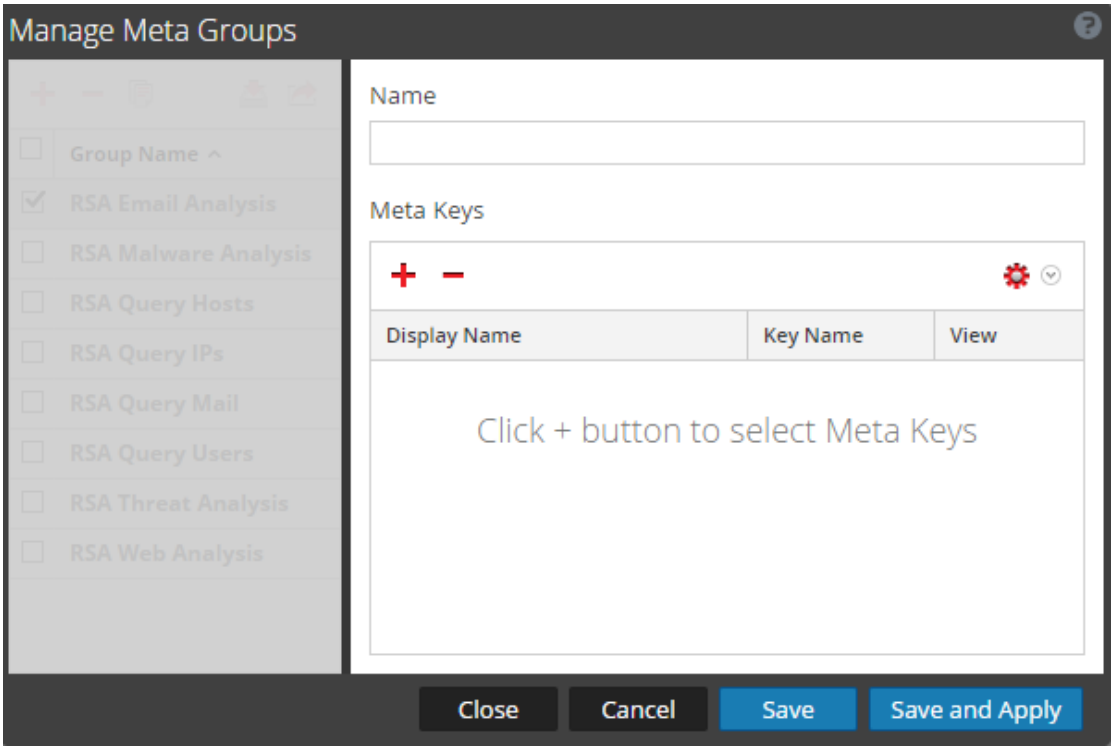
Créer un métagroupe et ajouter des clés méta

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

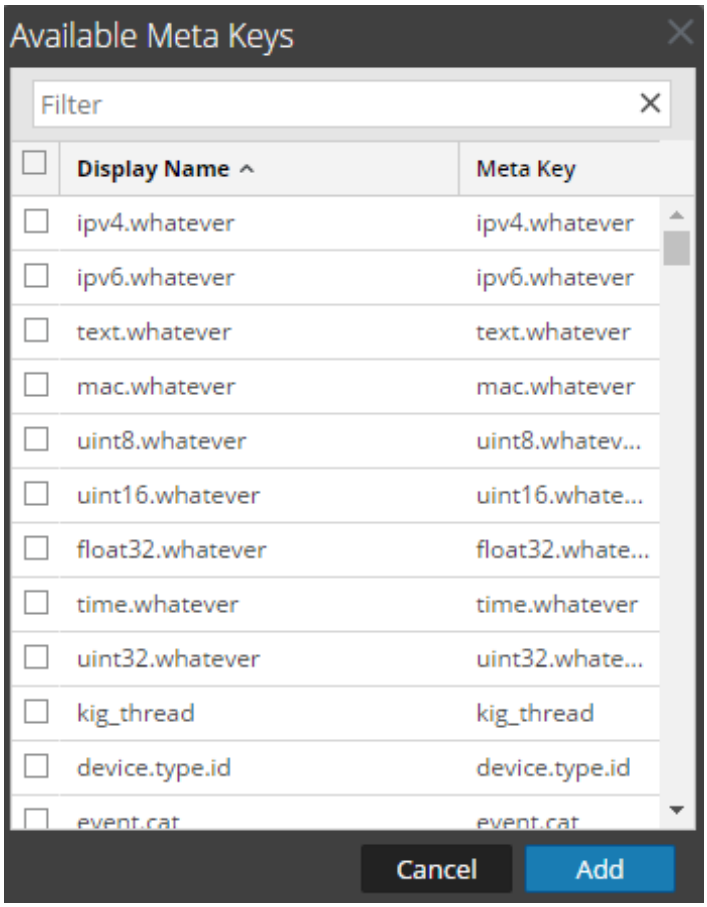
groupes personnalisés ont été configurés, ils apparaissent également sous le nom du groupe.



2. Dans la barre d'outils de la grille, cliquez sur +.
   Une nouvelle ligne est insérée en haut de la grille 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.

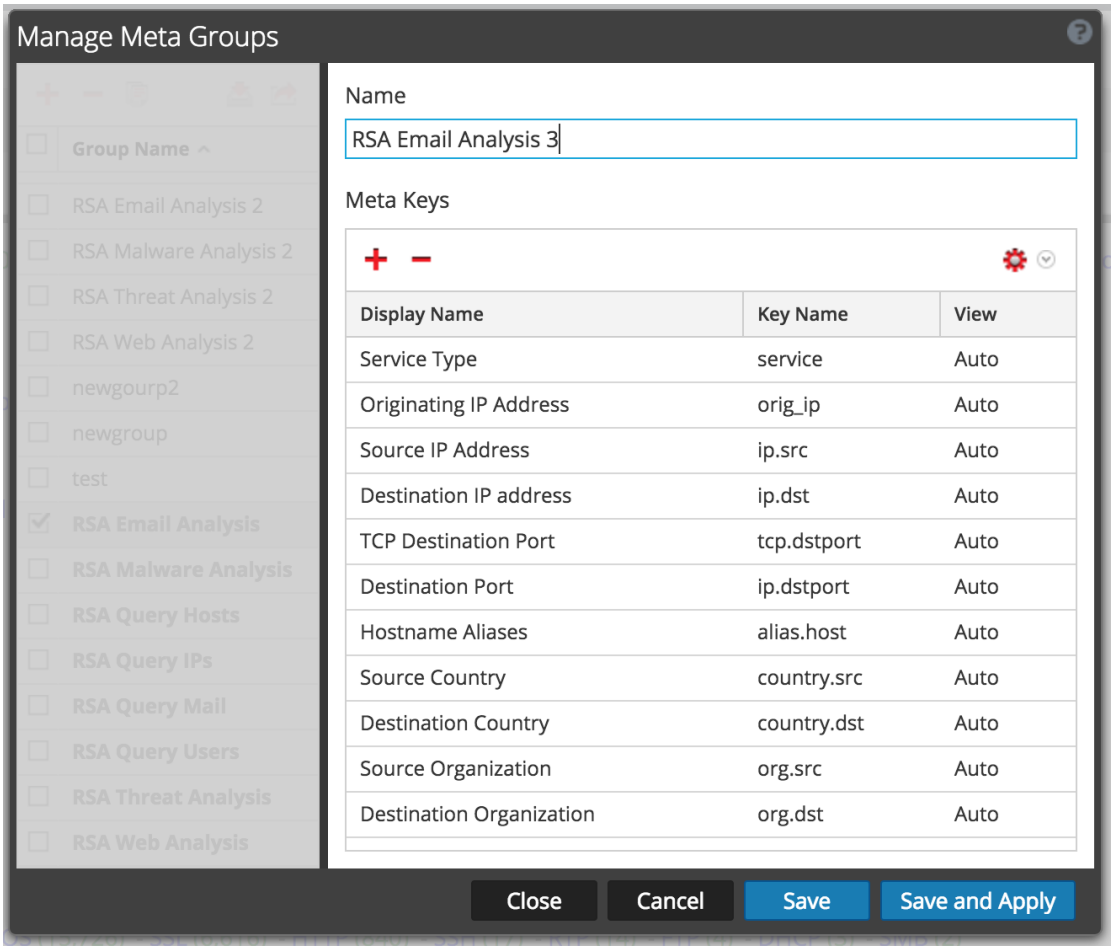
10. Cliquez sur **Fermer**.

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 grille Groupes méta, puis cliquez sur .

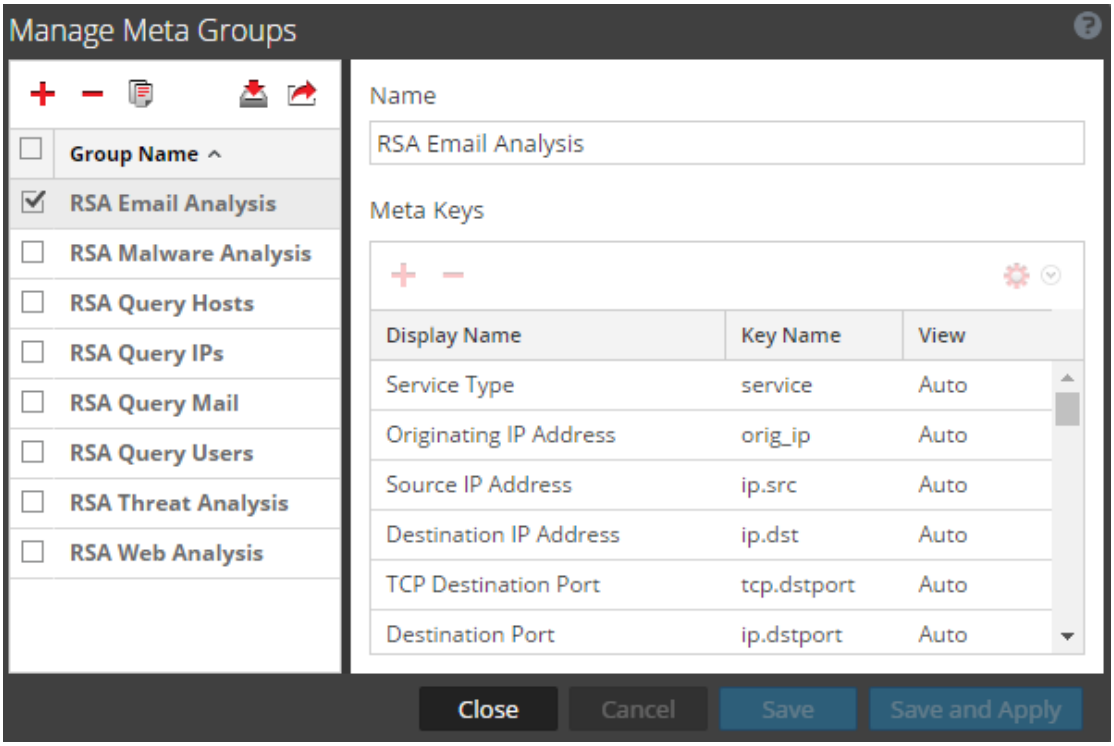
   Le formulaire à droite s'ouvre pour modification avec toutes les clés méta telles qu'elles sont dans le groupe prêt à l'emploi.



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 grille **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 métagroupe 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 Navigation active, cliquez sur **Enregistrer et appliquer**.

Supprimer un métagroupe

1. Dans la grille **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 grille **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 dans NetWitness Suite, NetWitness Suite affiche un message d'erreur si l'un des groupes existe déjà dans. 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 grille **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 grille Groupe méta. Si le fichier est un doublon d'un métagroupe existant, une fenêtre vous indique que le métagroupe existe déjà.

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.

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 Suite n'ouvre pas les clés méta non indexées par défaut. Lorsque vous ouvrez une clé méta non indexée dans la vue Valeurs, NetWitness Suite 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 définies par l'utilisateur, appelé métagroupe.

Remarque : 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.

Utiliser les clés méta par défaut

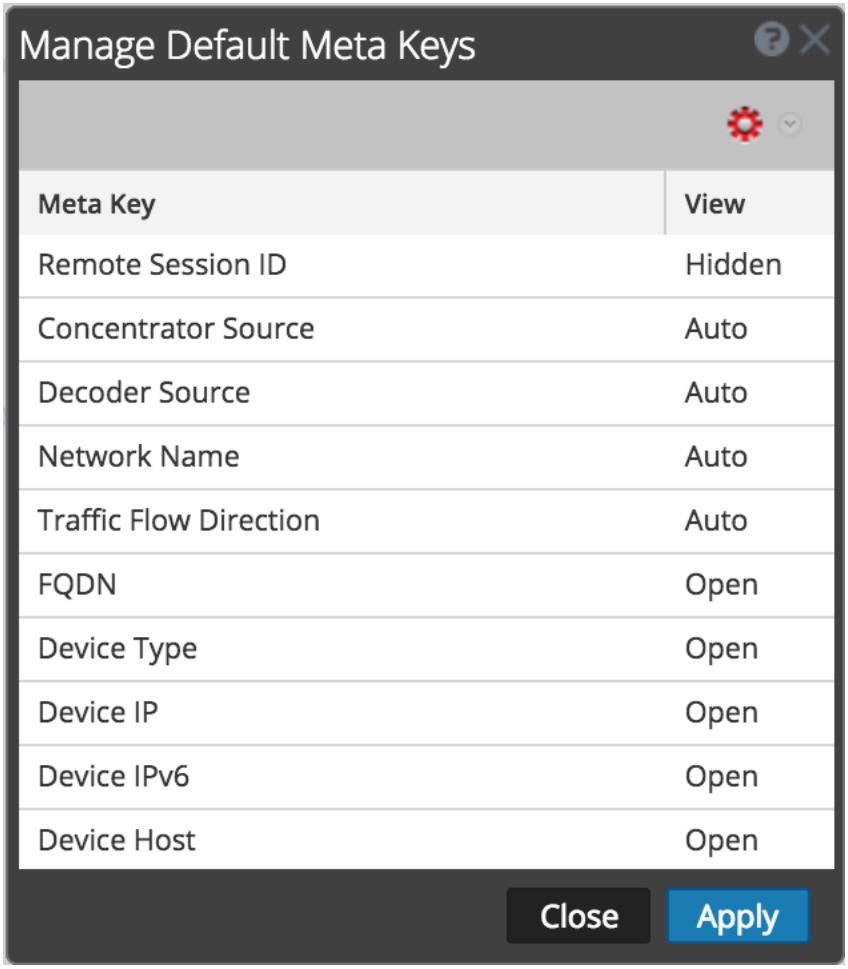
Pour spécifier que la vue Naviguer initiale s'ouvre à l'aide des clés méta par défaut :

1. Accédez à ENQUÊTER > **Parcourir.**
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.

Configurer les clés méta par défaut

Pour configurer la vue par défaut des clés méta dans la vue Procédure d'enquête > 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 les clés méta 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.

Rechercher des modèles de texte dans la vue Enquêter

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.

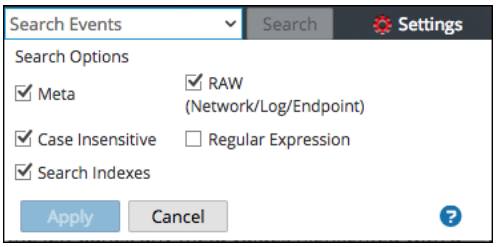
Options de contrôle du comportement de recherche

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 Rechercher des options.



Les options sélectionnées dans cette zone modifient la manière dont la recherche et exécutée. Le mode de recherche par défaut consiste à utiliser les index de recherche des mots-clés de texte dans les métadonnées et les données brutes.

Remarque : Étant donné que la case à cocher Index de recherche 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 Index de recherche. La recherche est plus longue, mais elle ne contiendra un ensemble plus complet de données.

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

Fonction	Description
Index de recherche	Commence par rechercher dans les index avant de rechercher dans les métadonnées ou les données brutes. 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 :** - La recherche dans l'index ne renvoie que les résultats obtenus avec les données indexées. - 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.
Meta	Recherche dans les métadonnées. Votre mot-clé ou votre modèle Regex est mis en correspondance avec les métadonnées analysées.
RAW (Réseau/Log/Point de terminaison)	Recherche le texte du log ou de l'événement. 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 générateur d'archive, 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.
Non sensible à la casse	Ignore la casse lors de la recherche.

Fonction	Description
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.
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.

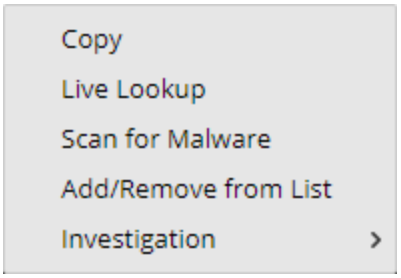
Exemples de recherche

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 valeur méta, par exemple HTTP, dans le panneau Naviguer.



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 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.
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 le **X** dans la zone de recherche.

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 Enquêter > Naviguer.

Chaque section de clé méta dans la vue Enquêter > Naviguer contient une liste classée des valeurs, 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**.

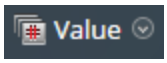
Pour sélectionner la méthode de quantification du nombre de clés méta et l'ordre des résultats de clé méta affichés dans la vue Naviguer :

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.

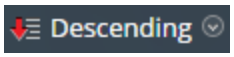
   L'affichage actuel est rechargé selon votre sélection.

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.

Définir la période d'investigation

Lorsque vous menez une procédure d'enquête dans la vue Enquêter > 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 (type) 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 affiche les premier et dernier horodatages pour la période utilisée pour les métadonnées.

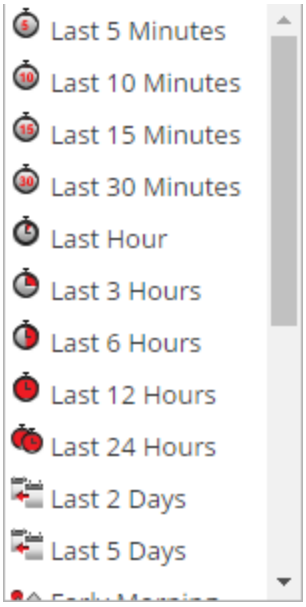
Remarque : La période est basée sur le fuseau horaire configuré dans le panneau Préférences du profil, comme indiqué dans « Définir les préférences utilisateur » dans le *Guide de mise en route de RSA NetWitness Suite*.

Sélectionner une période intégrée pour la procédure d'enquête

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**.
   - Si vous souhaitez définir une période relative au jour actuel, sélectionnez **Hier**, **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.

Spécifier une période personnalisée pour une procédure d'enquête

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, Minute et Seconde, ou cliquez sur **Maintenant**. La sélection de l'heure est l'heure actuelle par défaut.

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 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 ». Les secondes s'affichent dans ce format dans les fonctions **Procédure d'enquête > Naviguer**.

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

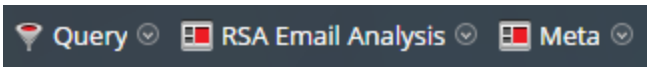
Utiliser des profils d'investigation pour encapsuler les vues personnalisées

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 Suite. 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.

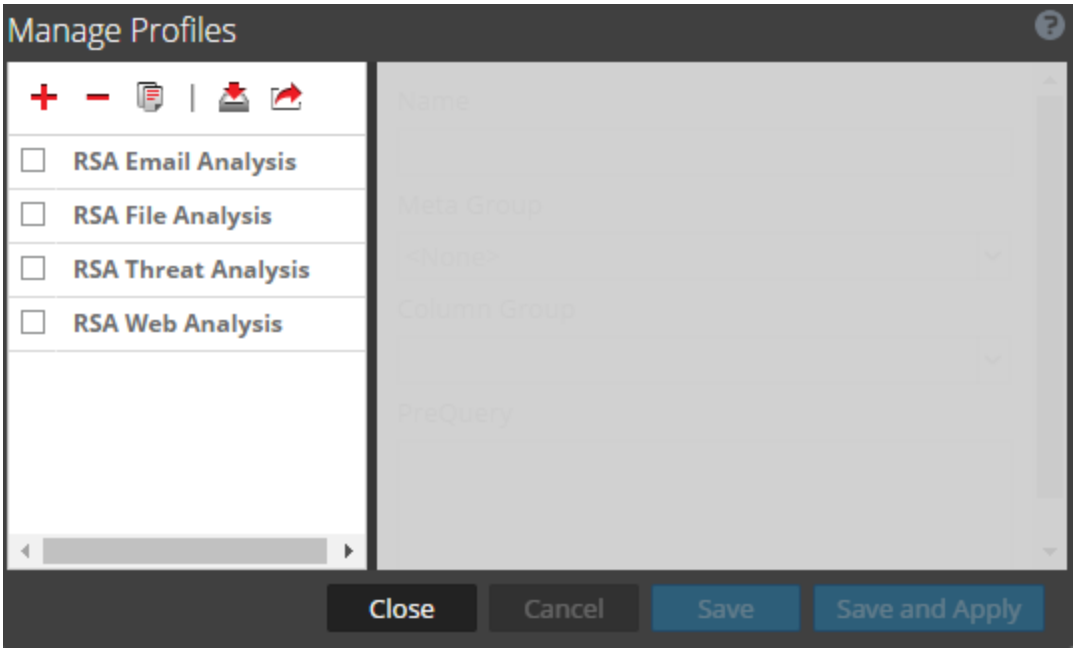
La figure suivante l'illustre dans la vue Naviguer. Le nom du profil s'affiche entre Requête et Méta. Dans la vue Événements, le nom du profil s'affiche entre Requête et Vue.



Parcourir la boîte de dialogue Gérer les profils

1. Accédez à **ENQUÊTER > Naviguer** ou ENQUÊTER **> Événements**.
2. Si la boîte de dialogue **Examiner** s'affiche, sélectionnez un service, puis cliquez sur **Naviguer**.

3. Dans la barre d'outils, sélectionnez **Profil > Gérer les profils**.
   La boîte de dialogue Gérer les profils s'affiche.



Créer et modifier des profils

1. Dans la boîte de dialogue **Gérer les profils**, sélectionnez un profil existant en cliquant sur la case à cocher en regard du nom, ou cliquez sur + pour créer un nouveau profil.
   Le panneau droit est disponible.
2. Modifiez ou saisissez le nom du profil dans le champ **Nom**. Ce nom doit comprendre entre 2 et 80 caractères.
3. Sélectionnez un métagroupe dans la liste déroulante **Groupe méta**. Vous pouvez ajouter des métagroupes personnalisés comme décrit dans la rubrique Gérer les groupes méta.
4. 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.
5. Saisissez des requêtes pour filtrer les résultats dans le champ **PreQuery**. PreQuery applique la même syntaxe que le Générateur de requête. Dans la figure, PreQuery utilise un groupe méta nommé **crypto exists**.
6. 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 de configurer le profil sélectionné comme étant actif.

Modifier un 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. 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.

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.

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.

Le graphique de coordonnées parallèles est une façon de visualiser le point actuel de recherche verticale dans Investigation 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 dans la vue Naviguer, 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 dans NetWitness Suite, NetWitness Suite affiche un message d'erreur 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 Suite 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.

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

Un ensemble de groupes méta prédéfinis est inclus avec NetWitness Suite. 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 :

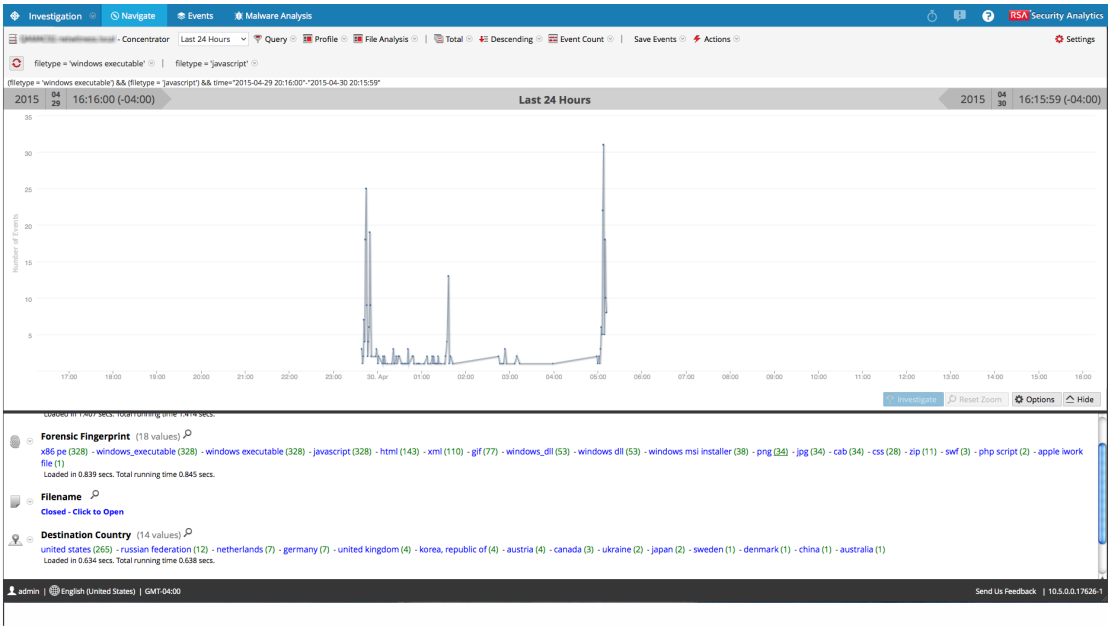
- Balisage de botnets
- Canaux de conversion
- E-mail
- Sessions chiffrées
- Analyse des points de terminaison
- Analyse de fichiers
- Malware Analysis
- Trafic HTTP sortant
- Trafic SSL/TLS sortant
- Attaques d'injection SQL
- Analyse des menaces
- Analyse Web

Afficher la visualisation des coordonnées parallèles

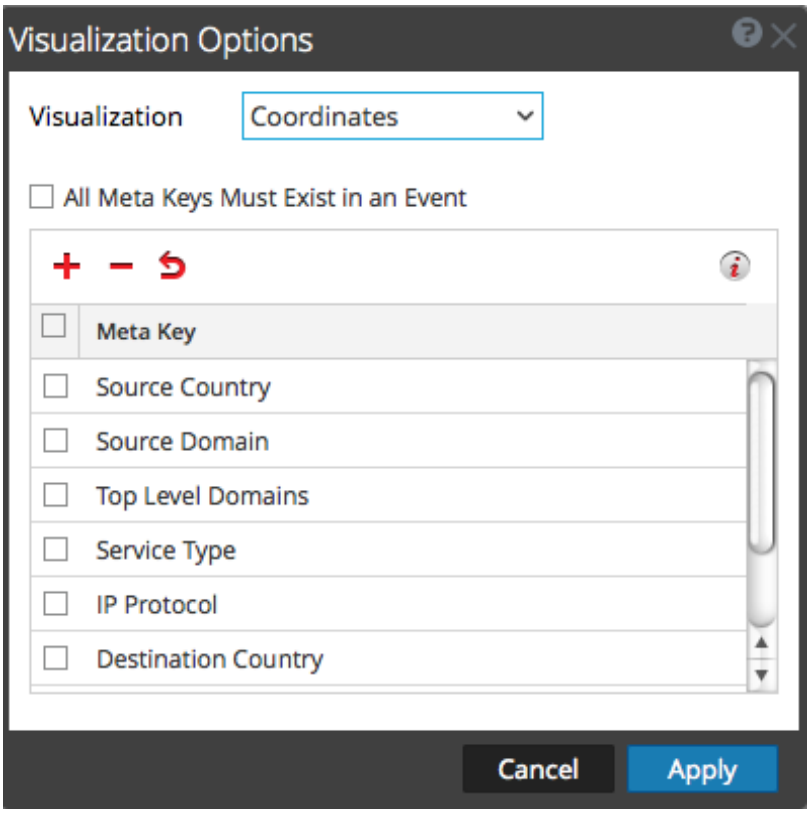
À partir d'une procédure d'enquête dans Procédure d’enquête > vue Naviguer :

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

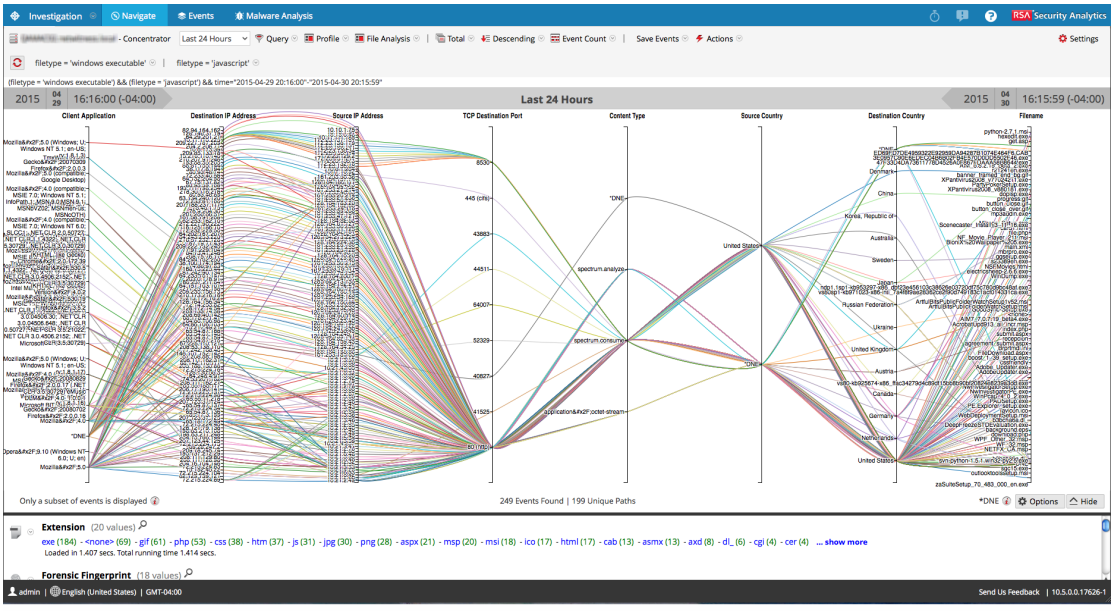
4. La visualisation par défaut pour le point actuel de recherche verticale s'affiche sous forme de chronologie.



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**.



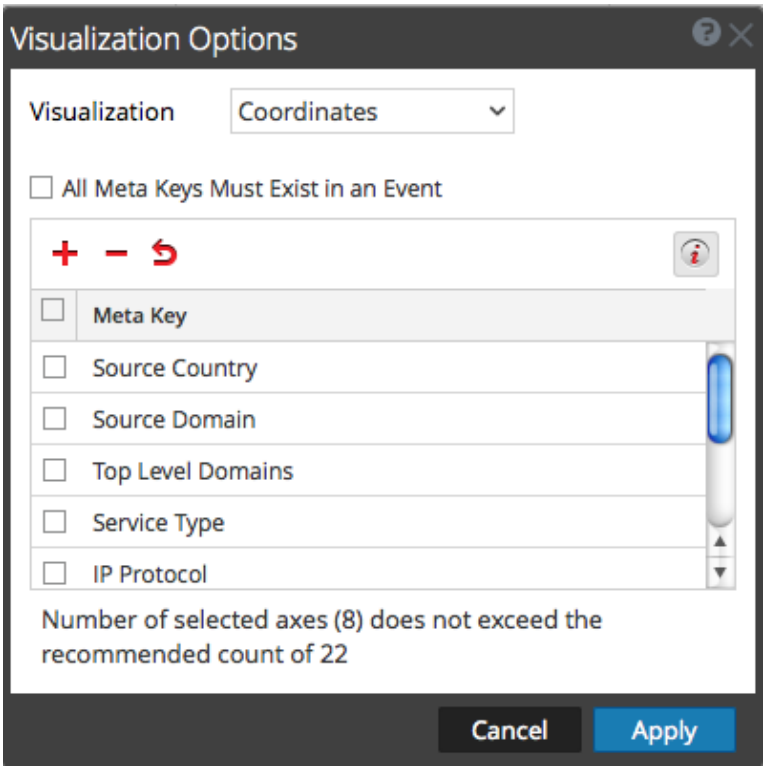
La visualisation est chargée. Dans cet exemple, 249 événements sont trouvés et 199 chemins uniques sont visualisés.



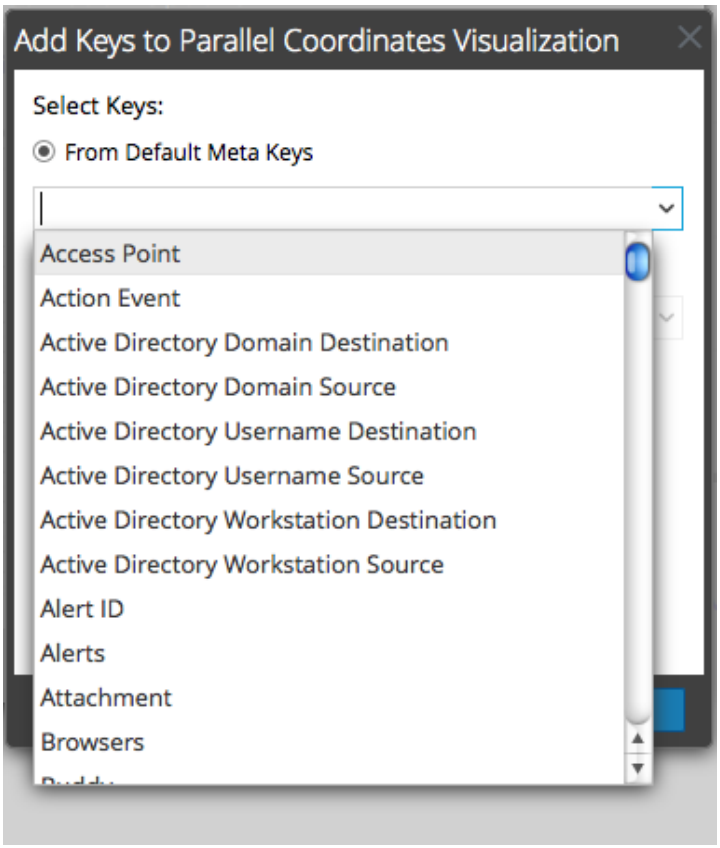
Sélectionner des clés méta pour la visualisation de coordonnées parallèles

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

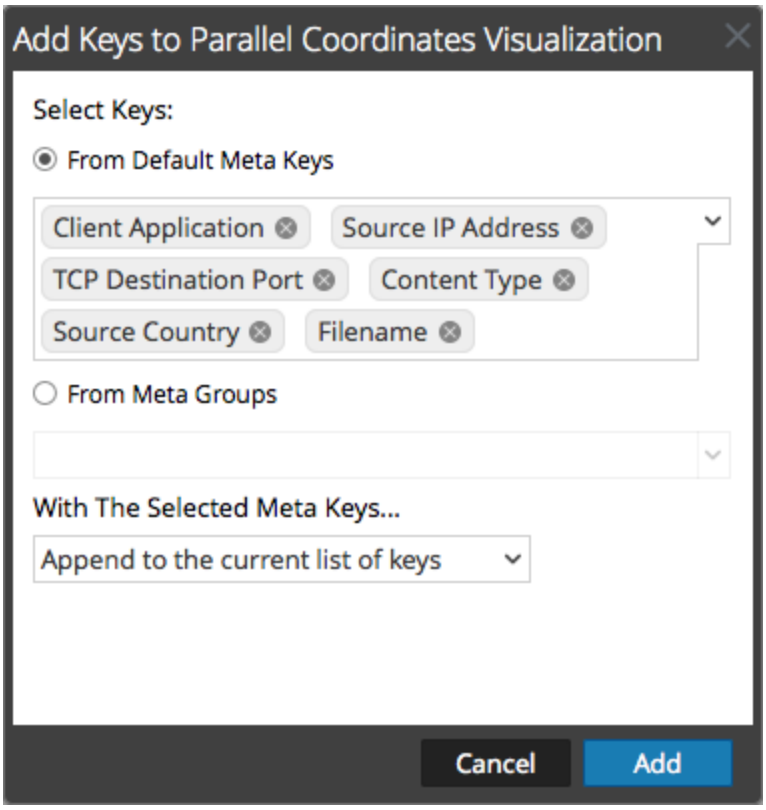
1. Dans le panneau Visualisation, sélectionnez **Options**.
   La boîte de dialogue Options de visualisation s'affiche. Dans la barre d'outils, cliquez sur pour afficher le nombre d'axes recommandé afin que la visualisation soit lisible. Lorsque le nombre recommandé de clés s'affiche, le nombre change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



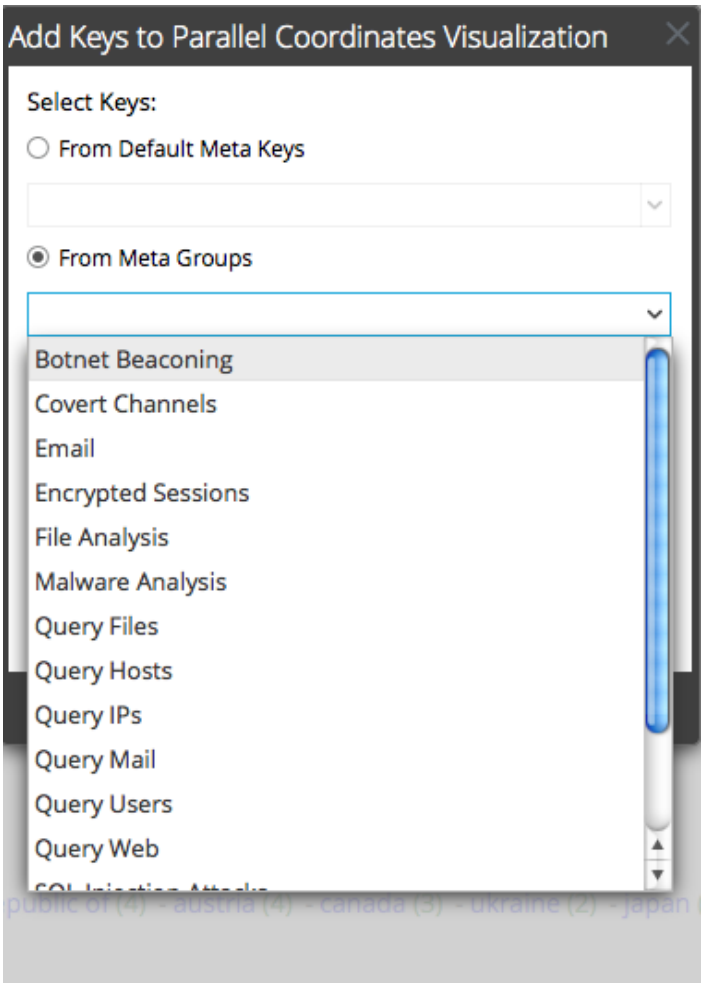
2. Si vous souhaitez modifier la séquence des clés méta, faites glisser les clés méta vers le haut ou vers le bas, selon la séquence souhaitée.
3. Si vous souhaitez supprimer des clés méta, cliquez dans la boîte de sélection, puis cliquez sur .
   Les clés méta sont supprimées, mais la modification n'a 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.

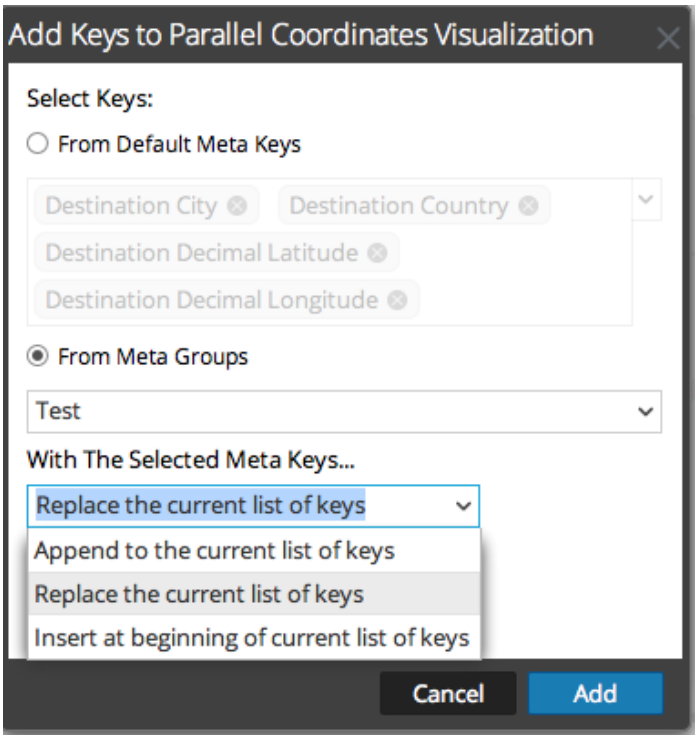


6. Si vous souhaitez ajouter toutes les clés au groupe méta, vous ne pouvez pas ajouter de clés méta individuelles. Sélectionnez **À partir des groupes méta**, et sélectionnez un groupe dans la liste déroulante.

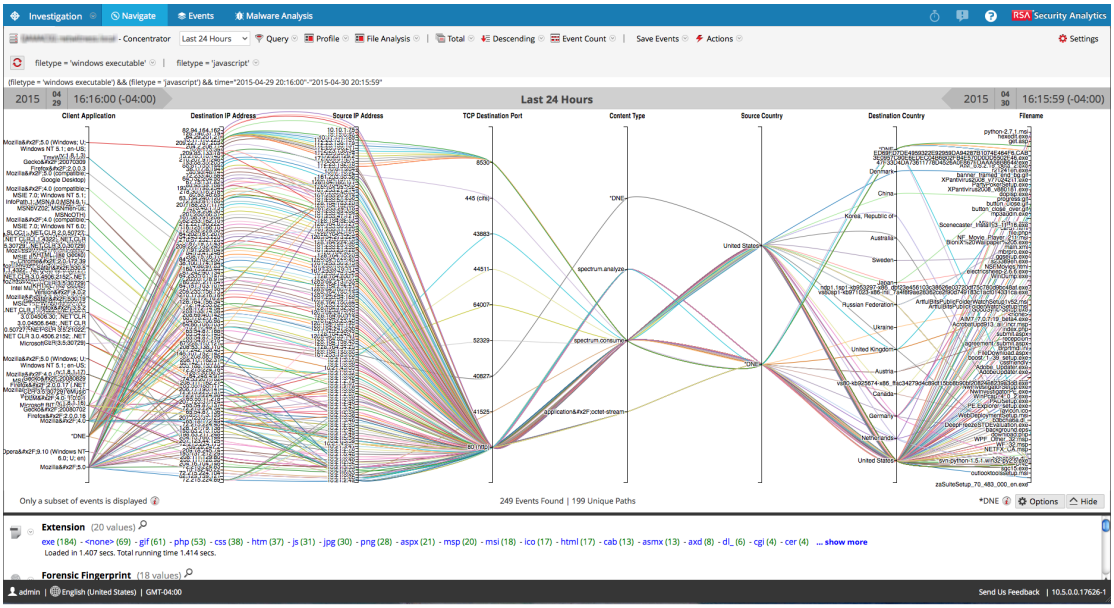


Les groupes méta sélectionnés sont répertoriés dans le champ.

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

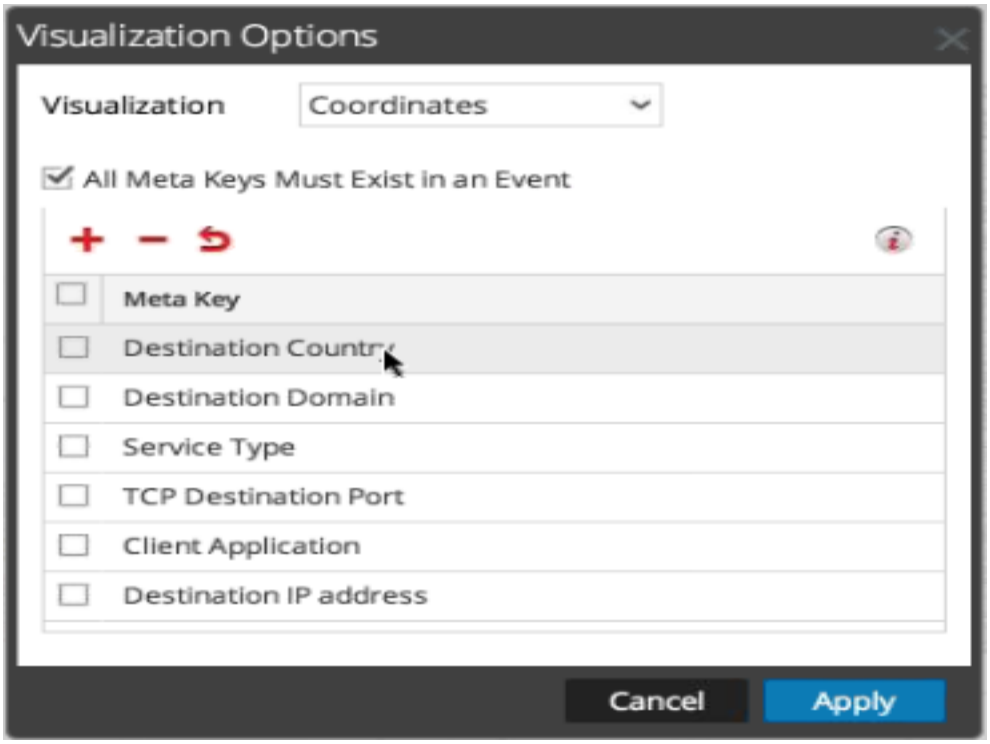


8. Pour terminer la procédure, cliquez sur **Ajouter**.
   La boîte de dialogue Options de visualisation s'affiche avec les clés méta ou groupes que vous avez sélectionnés.
9. Pour afficher le nouveau graphique de visualisation, cliquez sur **Appliquer**.

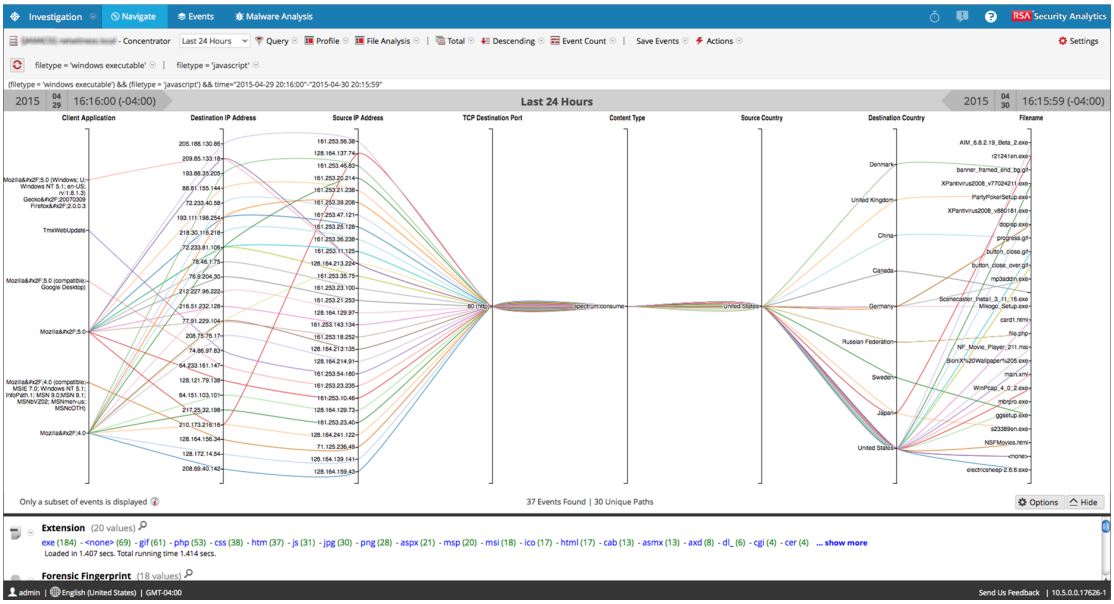


Optimiser la visualisation des coordonnées parallèles

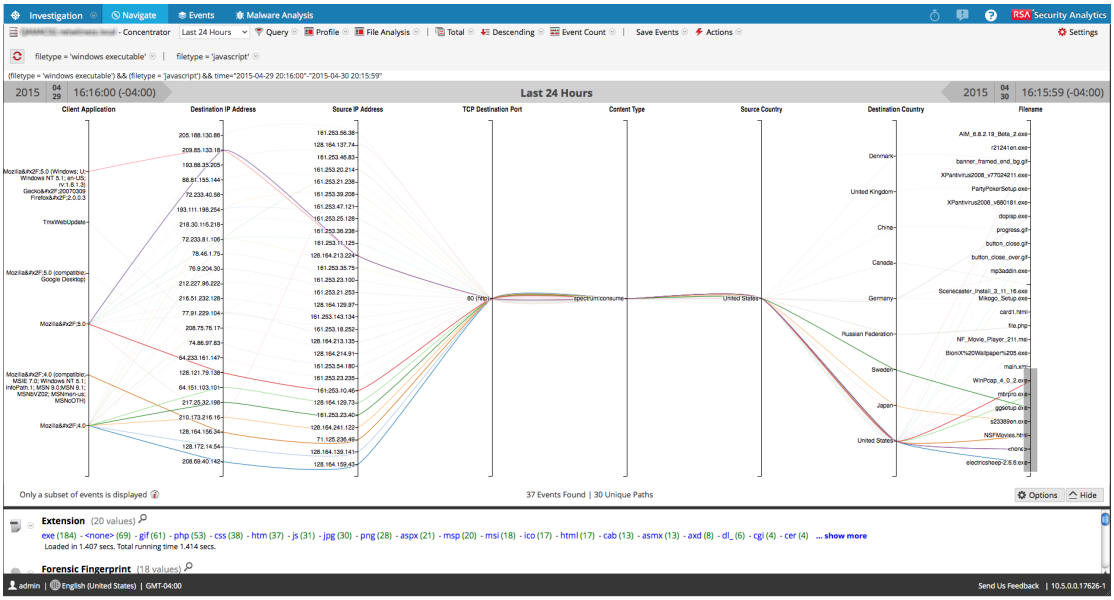
1. Pour optimiser la visualisation en supprimant des événements pour lesquels toutes les clés méta n'existent pas, sélectionnez **Options.**



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 généralement 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.

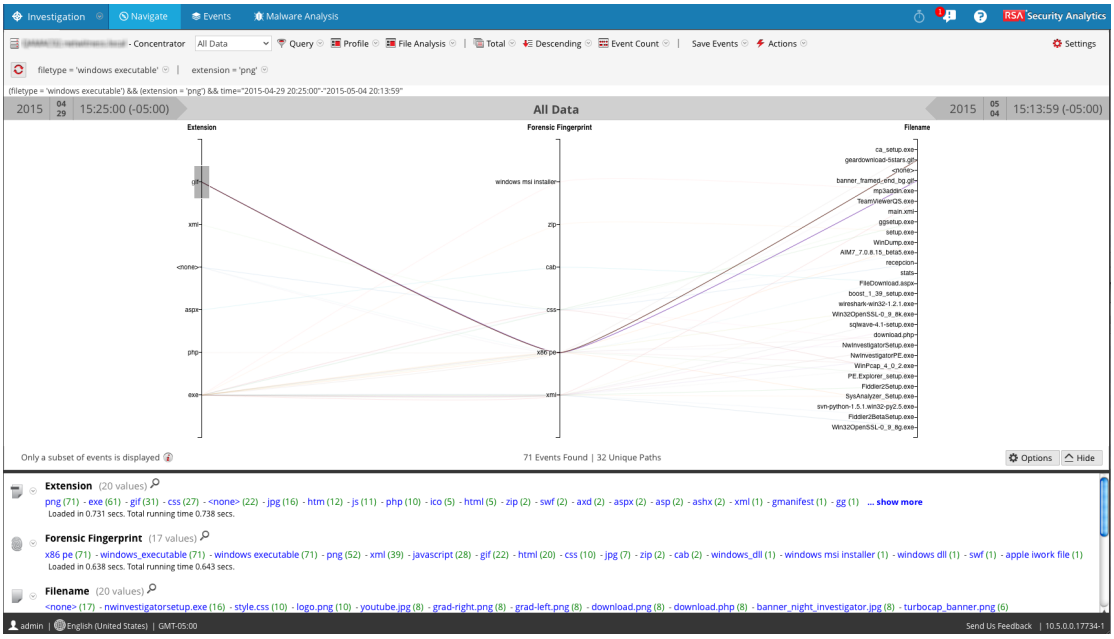
Exemple de cas d'utilisation

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.

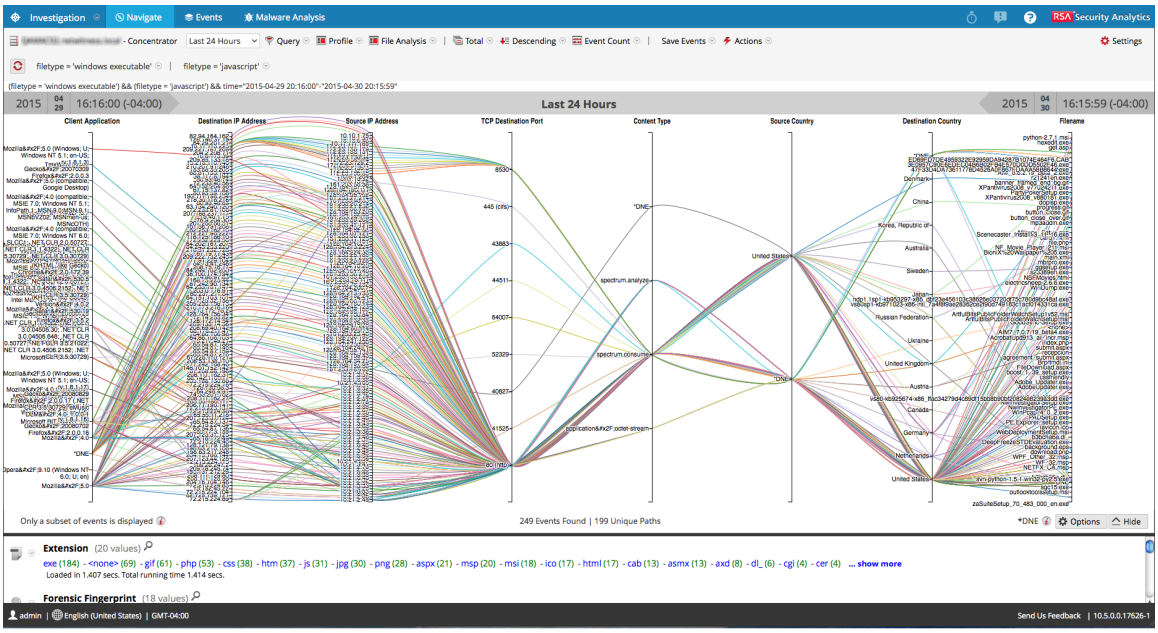
3. Configurez un graphique de coordonnées parallèles en choisissant trois axes : `file extension`, `forensic fingerprint` et `filename`.



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 Suite 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 Suite 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 Suite 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 Suite 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 Suite 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.

Interroger les données dans la vue Parcourir

Cette rubrique décrit les méthodes disponibles pour interroger les données dans la vue Procédure d'enquête > Naviguer.

Lors d'une procédure d'enquête dans NetWitness Suite, il existe plusieurs méthodes pour demander des résultats et rechercher plus précisément une zone d'intérêt dans la vue Naviguer. Les analystes peuvent :

- Créer une requête personnalisée, plutôt que de cliquer sur les valeurs et les clés méta (vue Naviguer et vue Événements)
- Effectuer une recherche verticale dans les données au sein du graphique chronologique de la vue Naviguer (vue Naviguer)
- Effectuer une recherche verticale dans les données dans le panneau Valeurs (vue Naviguer)
- Afficher et modifier des requêtes avec l'intégration d'URL (vue Naviguer et vue Événements)

Créer une requête personnalisée

Dans le panneau des options de la vue Enquêter > Naviguer, 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. 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.

Lorsque vous sélectionnez un groupe méta, NetWitness Suite 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 :

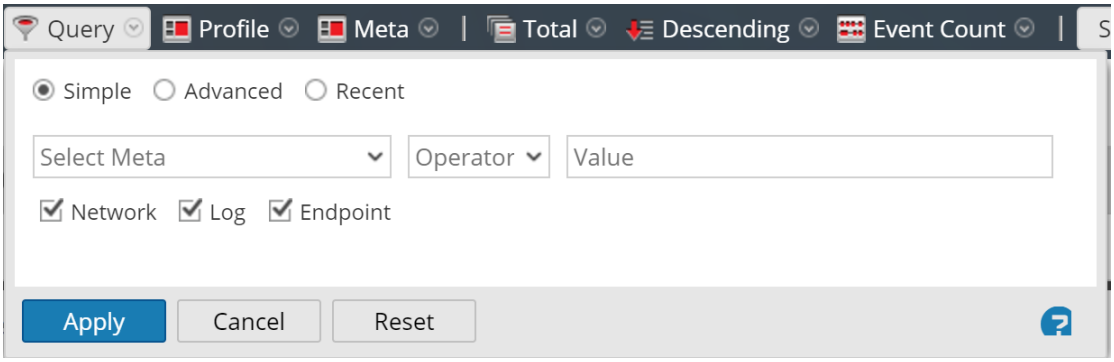
```
action exists
action = 'get'
alias.host = '10.25.55.115'
```

```
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 Suite fournit des listes déroulantes de métadonnées et d'opérateurs.

1. Dans la barre d'outils de la **vue Naviguer**, 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**.

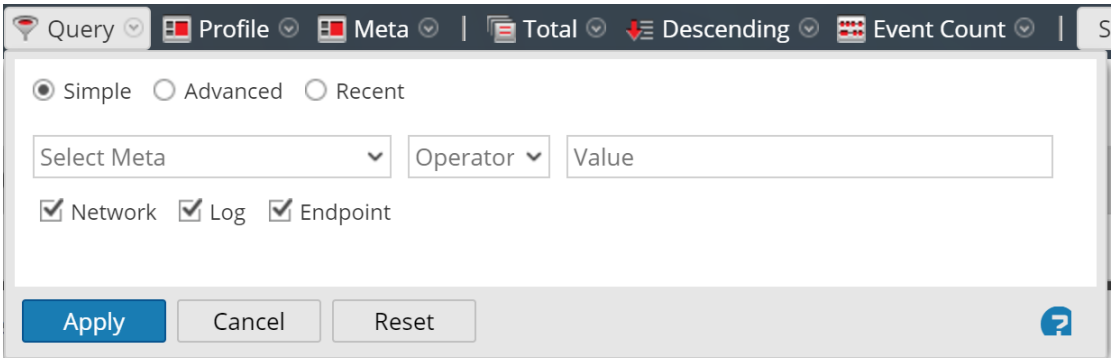
7. Exécutez l'une des opérations suivantes :

a. Cliquez sur **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.

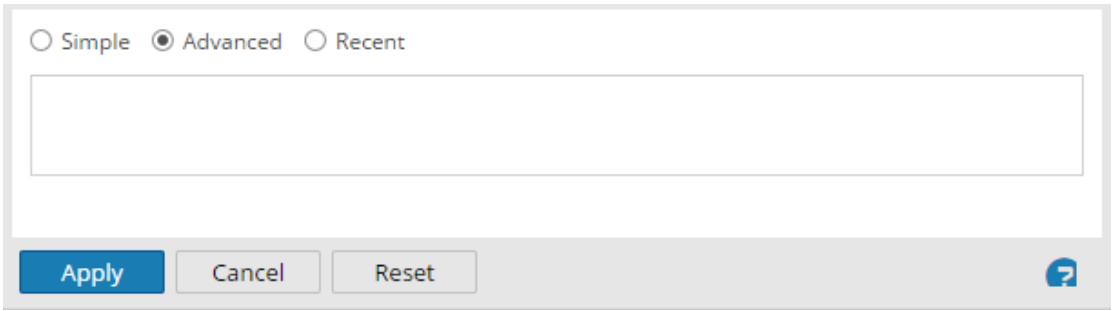
b. Cliquez sur **Annuler**.
La fenêtre est fermée et aucun changement n'est apporté à la vue ou à la requête en cours.

Créer une requête en utilisant la méthode avancée

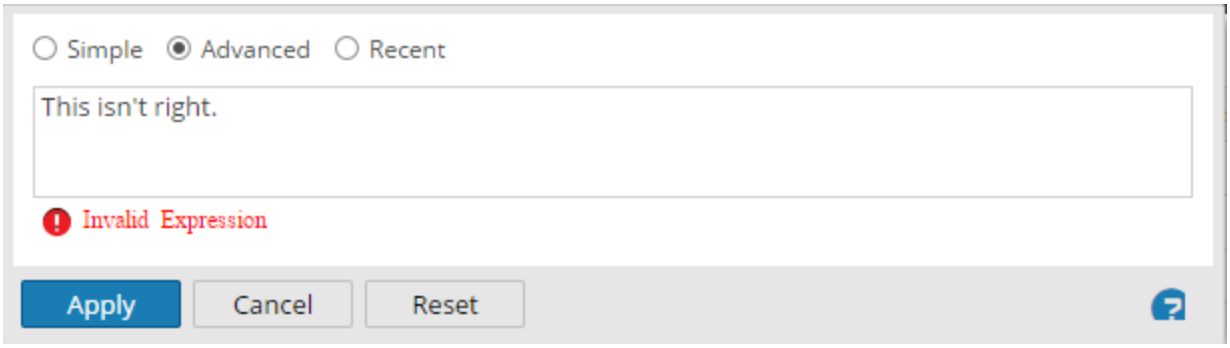
1. Dans la barre d'outils de la **vue Naviguer**, sélectionnez **Requête.**
La boîte de dialogue Requête s'affiche.



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.

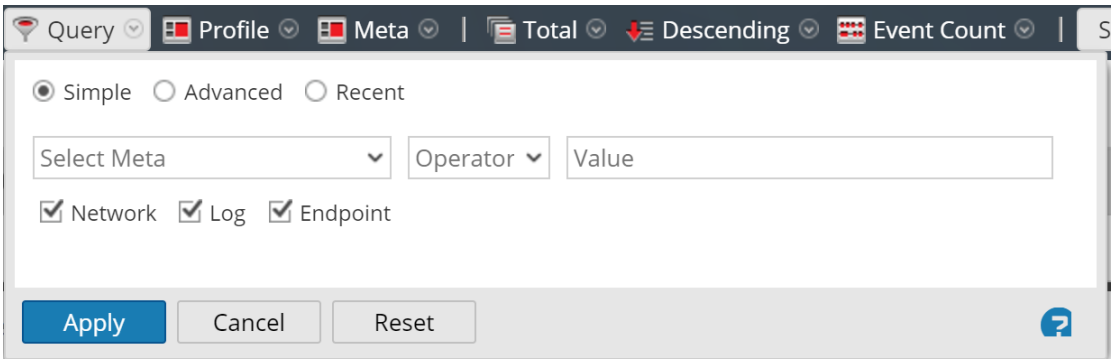


6. Exécutez l'une des opérations suivantes :
   - Cliquez sur **Apply**.
     La fenêtre est fermée et la vue est mise à jour avec les résultats de la nouvelle requête. La requête s'affiche dans le fil d'Ariane.
   - Cliquez sur **Annuler**.
     La fenêtre est fermée et aucun changement n'est apporté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

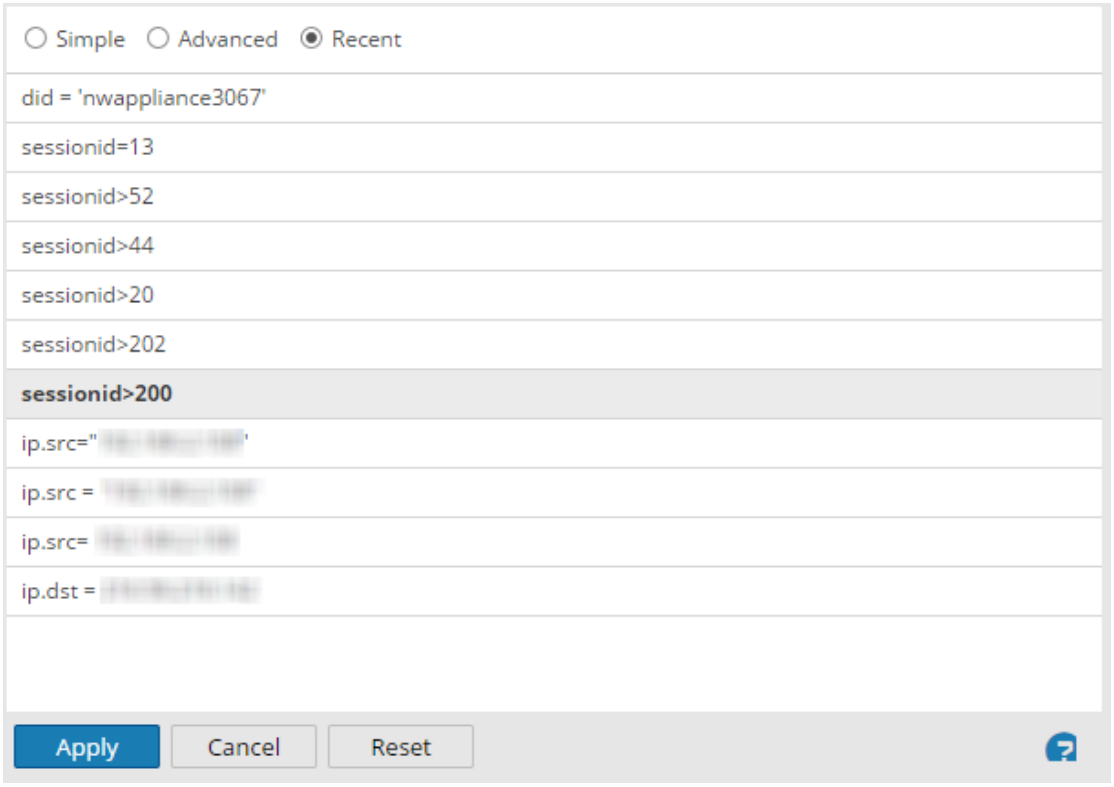
Appliquer une requête récente

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**, 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.



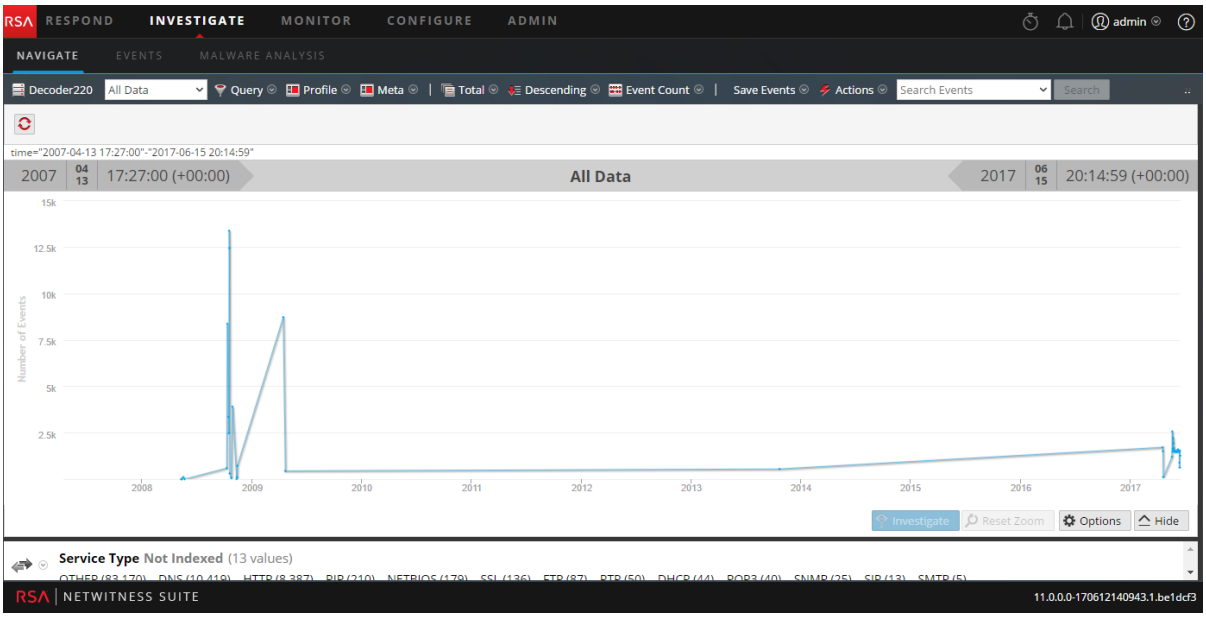
3. Dans la liste des requêtes récentes, cliquez sur une requête pour la sélectionner.
4. Exécutez l'une des opérations suivantes :
   - Double-cliquez sur une requête.
   - Sélectionnez une requête, puis cliquez sur **Appliquer**.
     La fenêtre est fermée et la vue est mise à jour avec les résultats 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.

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 > Parcourir**.
   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.

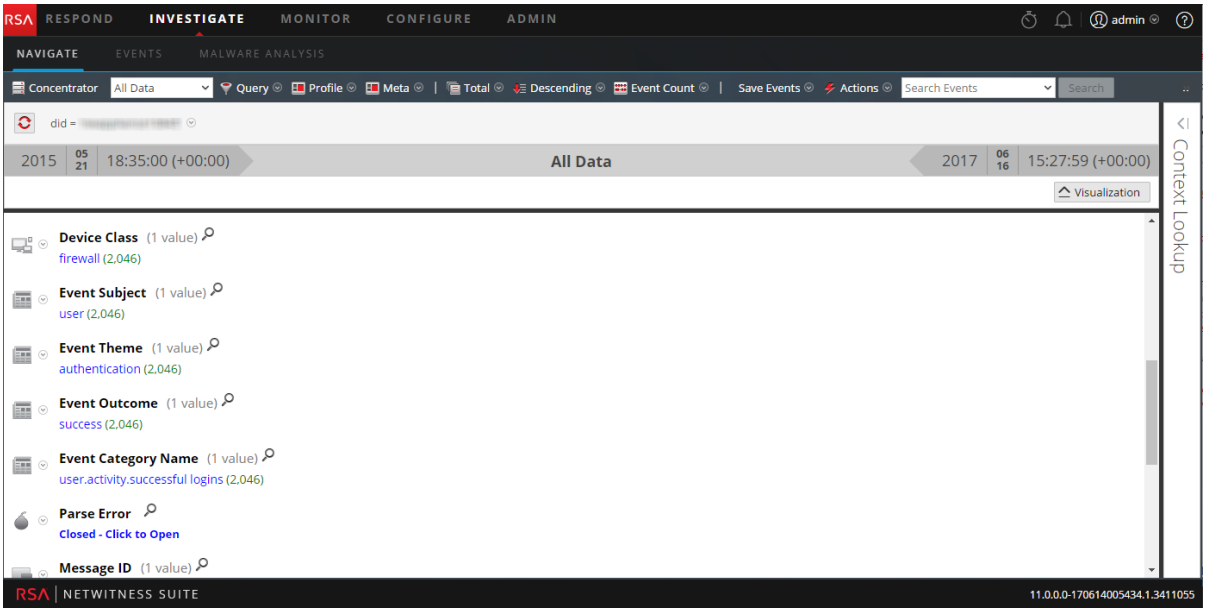
4. Pour réinitialiser le graphique chronologique à la période d'origine, cliquez sur **Réinitialiser le zoom**.
   L'URL est mise à jour pour refléter l'URL d'origine avant l'analyse des données et le panneau des options de procédure d'enquête est mis à jour pour refléter la période sélectionnée avant 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 Suite 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

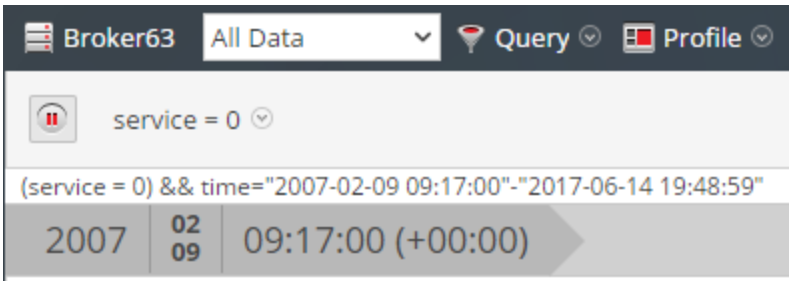
1. Lancez une procédure d'enquête pour afficher les métadonnées dans la vue Naviguer.



2. Pour effectuer une recherche verticale dans les métadonnées, effectuez une ou plusieurs des opérations suivantes :

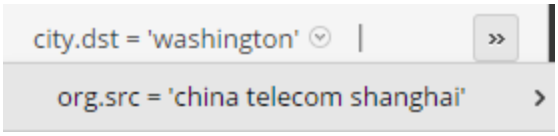
   a. Cliquez sur une **clé méta**, par exemple, Pays d'origine ou Pays de destination.

   b. Cliquez sur une **valeur méta**, le texte en bleu dans les résultats. Par exemple, Italie.
   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.

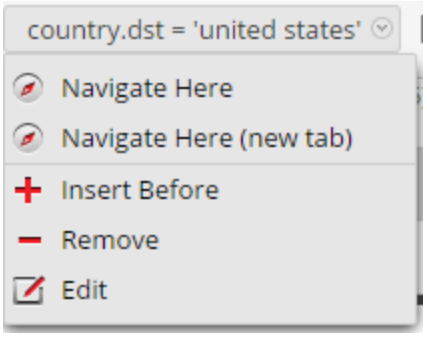


Ajouter une requête au fil d'Ariane

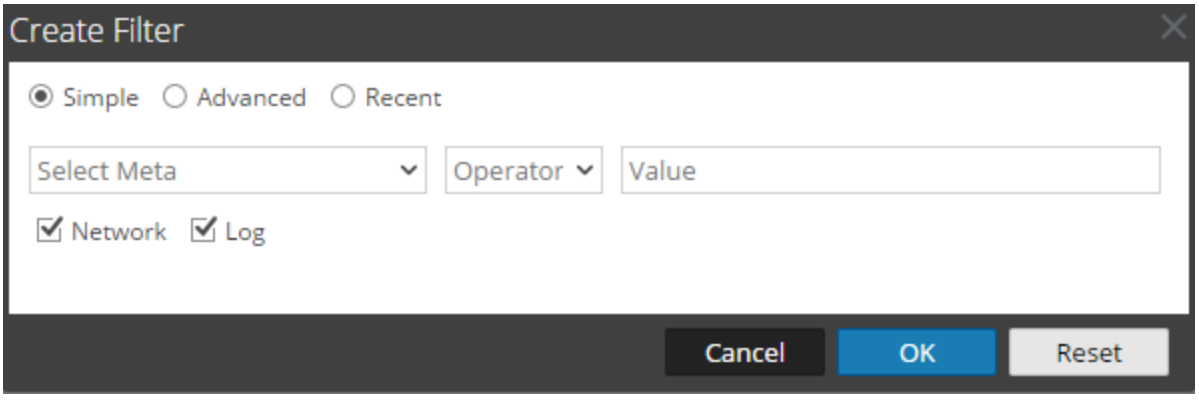
Dans le fil d'Ariane, vous pouvez cliquer sur l'un des fils pour afficher le menu Requête. Vous pouvez insérer une nouvelle requête avant un fil et en ajouter une nouvelle à la fin d'un fil. Après chaque modification dans le fil, NetWitness Suite actualise les résultats.

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.



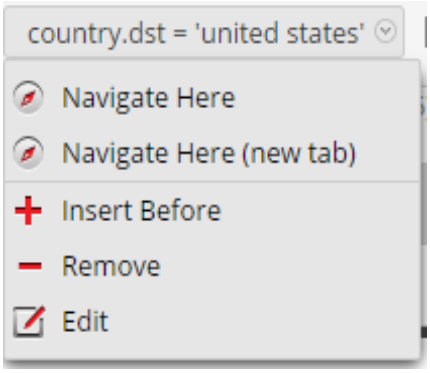
3. Créez la requête comme décrit dans la rubrique Créer une requête personnalisée.

Modifier une requête au fil d'Ariane

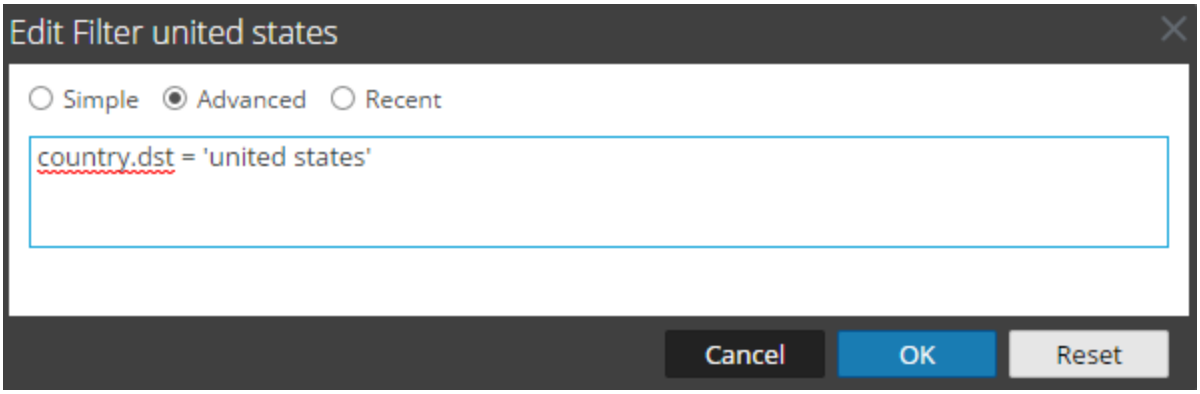
Dans le fil d'Ariane, vous pouvez cliquer sur l'un des fils pour afficher le menu Requête. Vous pouvez supprimer un fil et modifier une requête dans un fil. Après chaque modification dans le fil, NetWitness Suite actualise les résultats.

Pour utiliser les requêtes dans le fil d'Ariane :

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



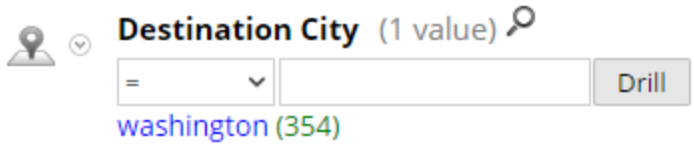
2. Pour modifier une requête dans le fil d'Ariane, sélectionnez **Modifier**.
   La boîte de dialogue Créer s'affiche avec la requête sélectionnée ouverte à des fins de modification.



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

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.

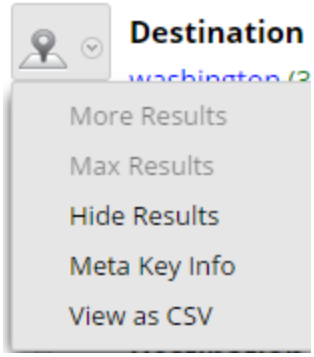


2. (Facultatif) Si vous souhaitez fermer le formulaire de recherche, cliquez de nouveau sur la loupe.
3. Sélectionnez l'opération dans la liste déroulante située à gauche, puis saisissez la valeur du texte à rechercher. Ensuite, cliquez sur **Recherche verticale** pour effectuer l'opération.
   Les métadonnées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

Afficher les informations relatives aux clés méta dans la vue Naviguer

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.



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

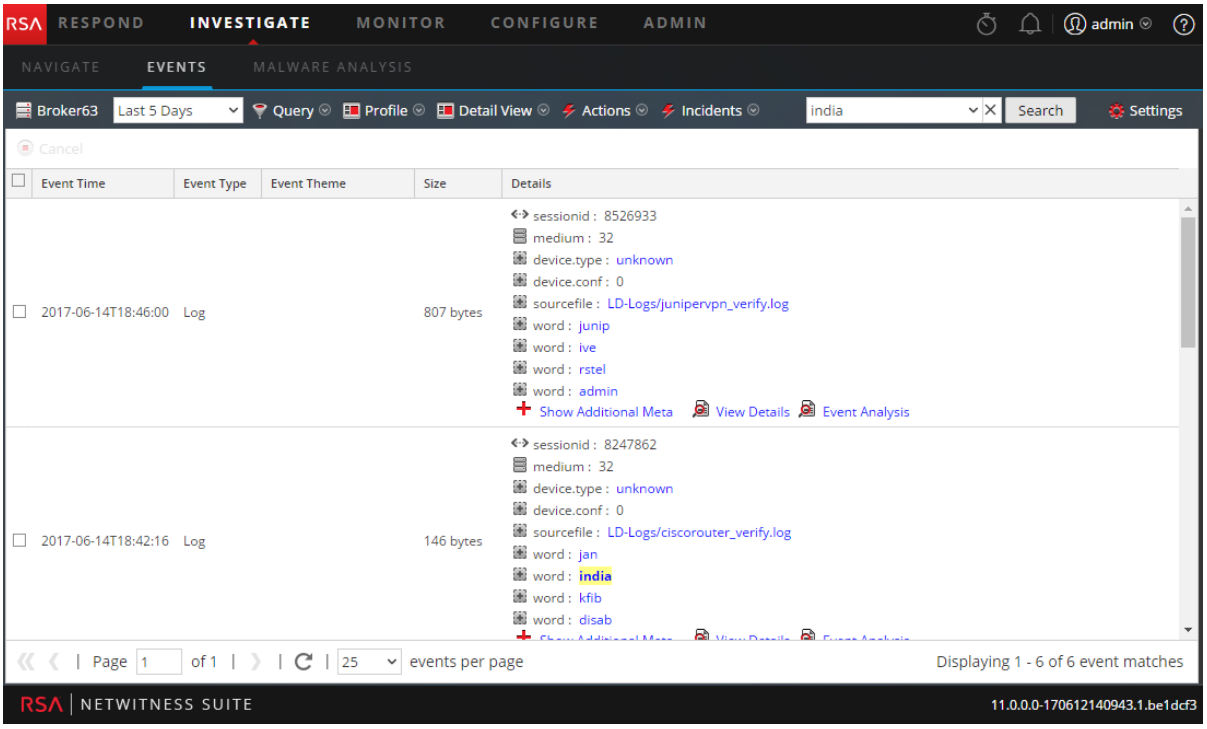
Affichage des événements associés à une valeur méta

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 des événements.

Recherche d'événements spécifiques associés à une valeur méta

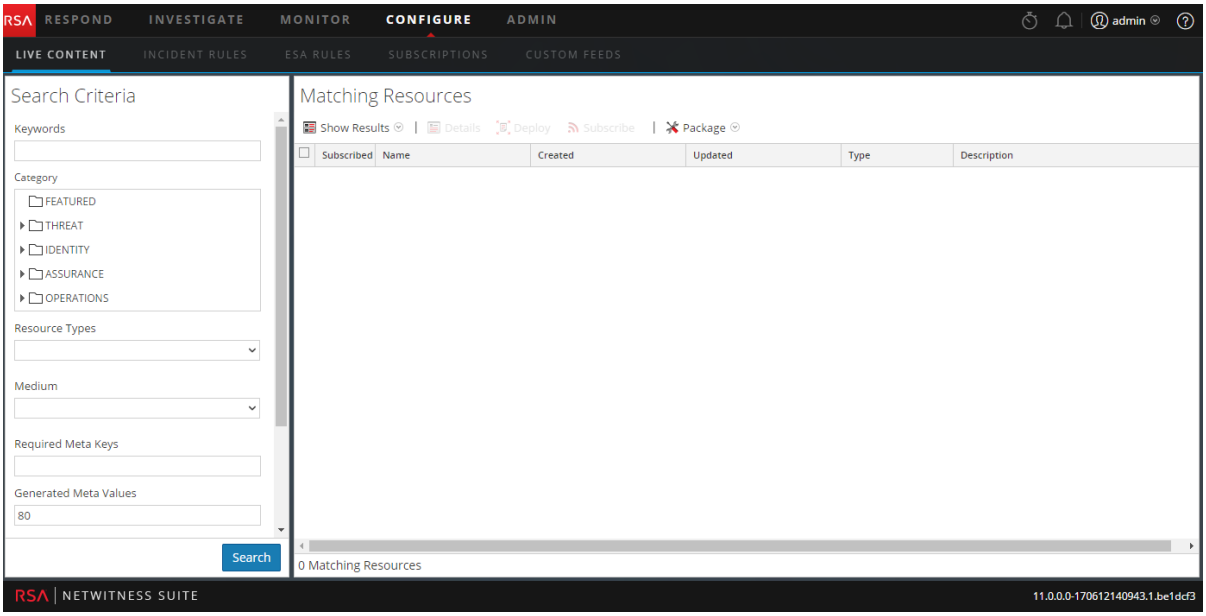
1. Dans la vue Naviguer, effectuez une recherche verticale dans les métadonnées qui font l'objet de votre investigation (cliquez sur une valeur méta ou ajoutez une requête).
2. Saisissez une chaîne de recherche dans le champ Rechercher et appuyez sur **Entrée** ou cliquez sur **Rechercher**.
   Vous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



Afficher une valeur méta sélectionnée dans Live

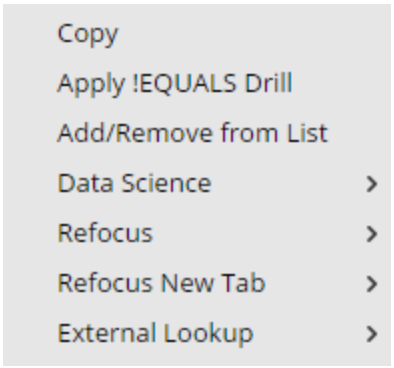
1. Dans la vue Naviguer, effectuez une recherche verticale dans les métadonnées sur lesquelles votre procédure d'enquête est axée.
2. Cliquez avec le bouton droit de la souris sur une valeur méta (le texte en bleu).
   Le menu déroulant Valeur méta s'affiche.
3. Pour rechercher la métavaleur dans NetWitness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



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.

Recherche d'un nombre spécifique dans un nouvel onglet

Pour afficher le nombre d'une valeur méta dans un nouvel onglet ou pour afficher un Geomap des emplacements de la valeur méta sélectionnée :

1. Cliquez avec le bouton droit sur un nombre correspondant à une valeur méta (le nombre en vert suivant la valeur méta en bleu).
   Le menu contextuel s'affiche.

2. (Facultatif) Pour ouvrir une procédure d'enquête distincte pour la valeur méta spécifique, sélectionnez **Ouvrir dans un nouvel onglet**.
3. (Facultatif) Pour ouvrir un Geomap affichant les emplacements d'origine de la valeur méta choisie, sélectionnez **Emplacements de géo-mappage dans un nouvel onglet**.

Afficher et modifier des requêtes avec l'intégration d'URL

Investigation 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 Suite. En utilisant une requête dans un URI, vous pouvez pivoter directement d'un produit qui autorise les liens personnalisés vers un point de recherche verticale spécifique dans la vue Procédure d'enquête de NetWitness Suite. 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 Suite. Si NetWitness Suite ne peut pas résoudre le service, l'analyste est redirigé vers la vue Navigation, qui contient la boîte de dialogue Sélection de service. Une fois que le service est sélectionné, la vue Navigation 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 Suite 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 Suite. Cette valeur change en fonction du service à analyser.
- `<encoded query>` est la requête NetWitness Suite 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 Suite que le service peut interroger. NetWitness Suite tente de résoudre l'hôte et le port en tant qu'ID de service défini dans NetWitness Suite.
- `<encoded query>` est la requête NetWitness Suite 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 SA 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.

Agir sur un point de recherche verticale dans la vue Parcourir

Cette section décrit les actions disponibles pour les analystes qui souhaitent envoyer un point d'extraction à une forme de sortie ou afficher le point d'extraction depuis une perspective différente dans la vue Naviguer.

Lors d'une procédure d'enquête dans NetWitness Suite, plusieurs actions sont disponibles une fois qu'un point d'extraction a été atteint dans la vue Naviguer. Les analystes peuvent :

- Exporter un point de recherche verticale (vue Naviguer et vue Événements)
- Imprimer le point de recherche verticale actuel (vue Naviguer)
- Ouvrir la liste d'événements d'une valeur méta (vue Naviguer)
- Lancer la recherche externe d'une clé méta (vue Naviguer)
- Lancer une analyse Malware Analysis à partir de la vue Naviguer
- Afficher un contexte supplémentaire pour un point de données (vue Naviguer et vue Événements)
- Gérer les listes et les valeurs de liste Context Hub dans Enquêter (vue Naviguer et vue Événements)
- Visualiser le point d'extraction verticale actuel dans Informer (vue Naviguer)

Exporter un point de recherche verticale

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

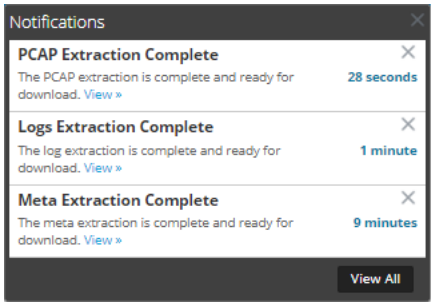
- Extraire des fichiers d'une session et choisir le type de fichier à extraire : archives, BitTorrent audio, documents, exécutable, images, autre, vidéo et web.
- Exporter le point d'extraction en tant que fichier de capture de paquet (PCAP), fichier log ou fichier de données méta.

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 Suite 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 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. Lorsque l'extraction du fichier planifié est terminée, un message s'affiche dans la barre d'état Notifications de tâche.



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

Lancer la recherche externe d'une clé méta

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

Les analystes peuvent utiliser des recherches externes NetWitness Suite 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 Suite :

- Google Malware : Ouvre une recherche Google Malware dans un nouvel onglet.
- McAfee SiteAdvisor : Ouvre une recherche McAfee SiteAdvisor 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

- Recherche Malwaredomainlist.com : Ouvre une recherche Malwaredomainlist.com dans un nouvel onglet
- Recherche Malwaredomains.com : Ouvre une recherche Malwaredomains.com dans un nouvel onglet
- Recherche d'adresses IP Robtex : Ouvre une recherche RobtexIP dans un nouvel onglet
- Recherche SamSpade : Ouvre une recherche SamSpade dans un nouvel onglet
- Recherche ThreatExpert : Ouvre une recherche ThreatExpert dans un nouvel onglet
- Recherche UrlVoid : 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.

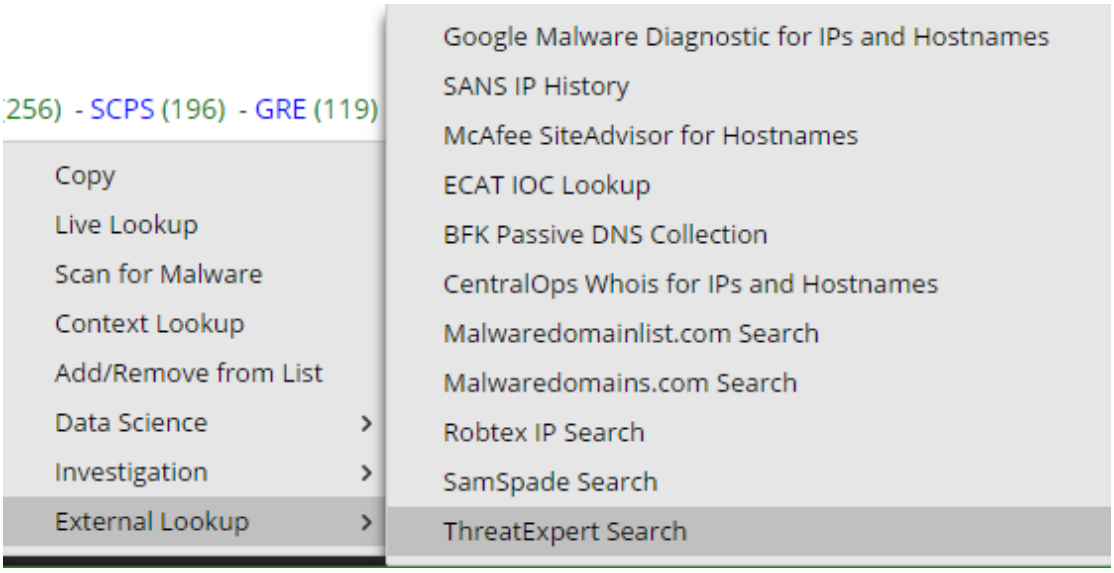
Pour la métaclé `client`, l'option ECAT Lookup ouvre un client ECAT dans un nouvel onglet si le client ECAT est installé sur le même système que celui sur lequel le navigateur est utilisé.

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*.

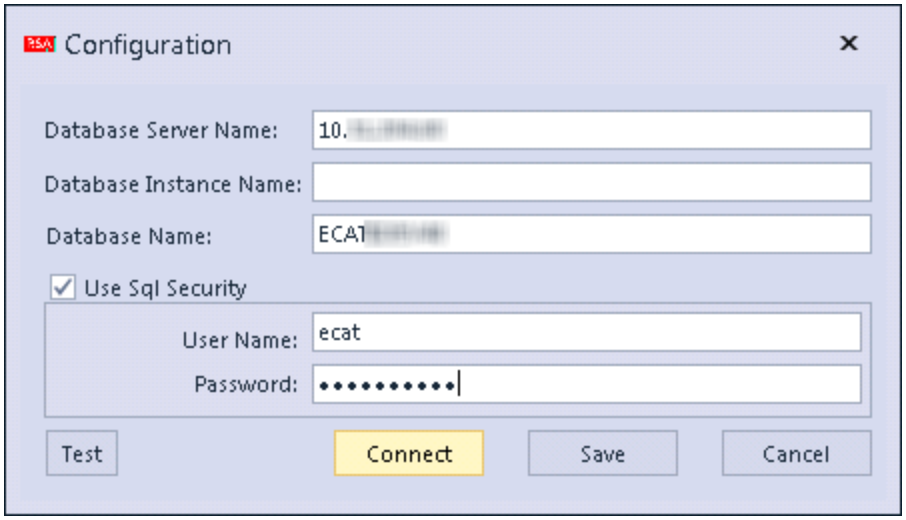
Lancer une recherche des IOC ECAT

Pour lancer une recherche de données ECAT à partir de la vue Procédure d'enquête > Parcourir :

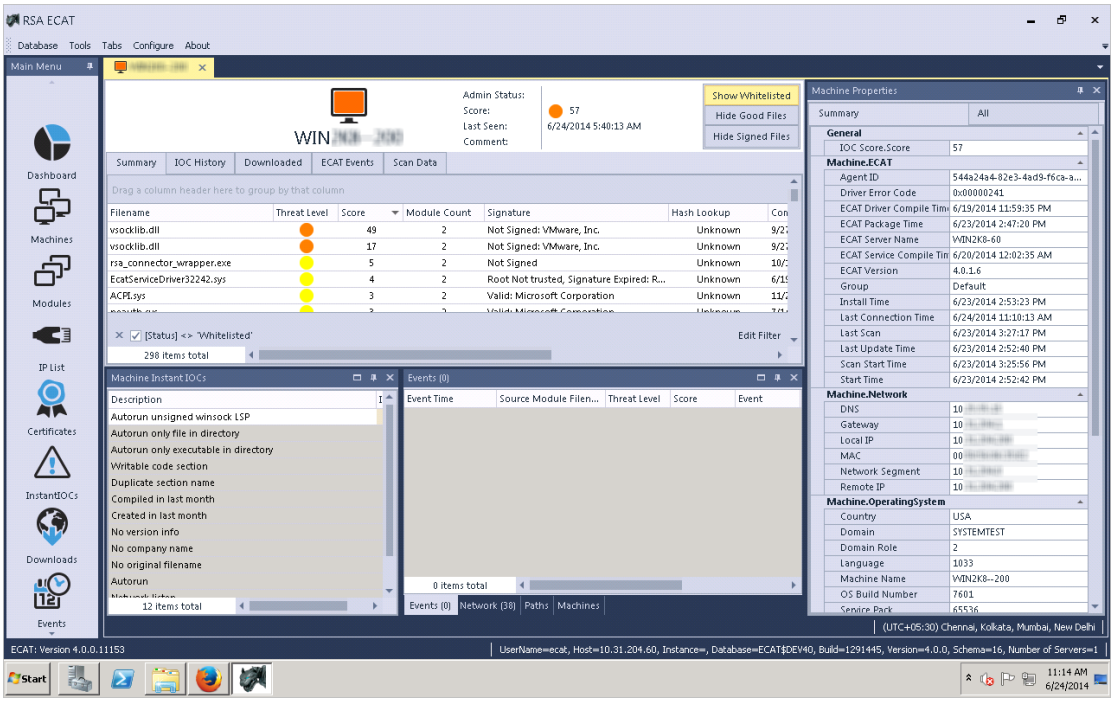
1. Cliquez avec le bouton droit de la souris sur une valeur méta pour l'une des clés méta suivantes : `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst`, `client`.
2. Sélectionnez **Recherche externe** dans le menu contextuel.
   Un sous-menu des options de recherche externes s'affiche.



3. Sélectionnez **Recherche des IOC ECAT**.
   Une boîte de dialogue vous demande de choisir une application.
4. Sélectionnez ECAT, puis cliquez sur **OK**.
   La boîte de dialogue Configuration RSA ECAT apparaît.



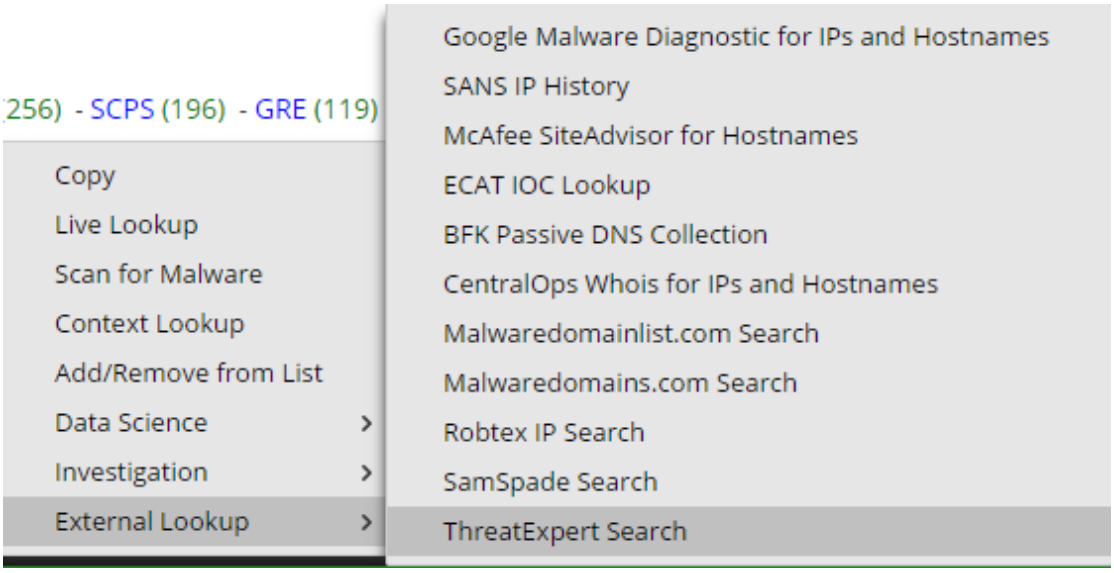
5. Saisissez le nom d'utilisateur et le mot de passe requis pour vous connecter au client ECAT, puis cliquez sur **Se connecter.**
   Le point de recherche verticale s'ouvre dans RSA ECAT.



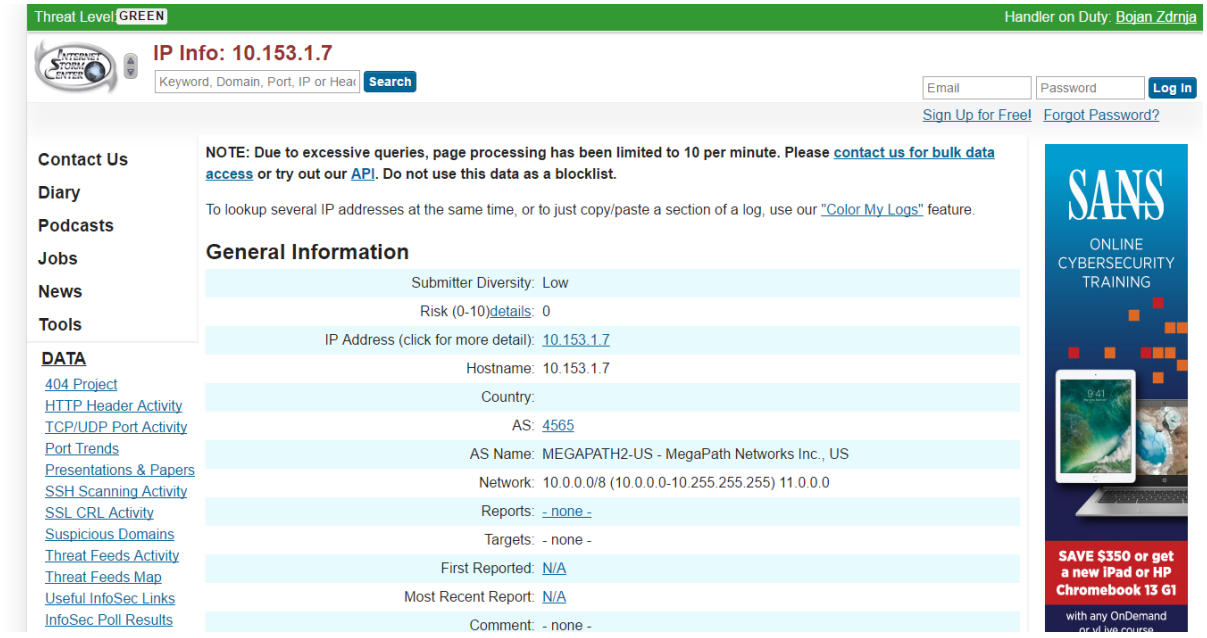
Lancer d'autres recherches externes

Pour lancer une recherche externe (autre qu'ECAT IOC) de données à partir de la vue Procédure d'enquête > Parcourir :

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.

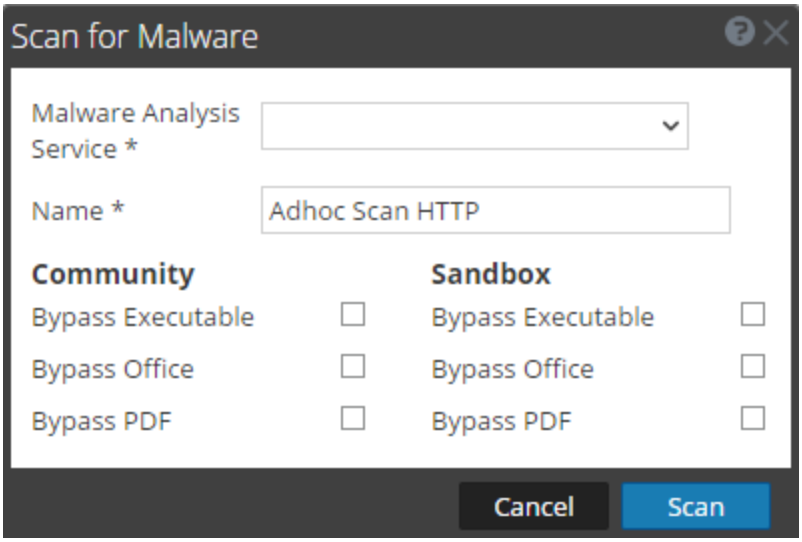


Lancer une analyse Malware Analysis à partir de la vue Naviguer

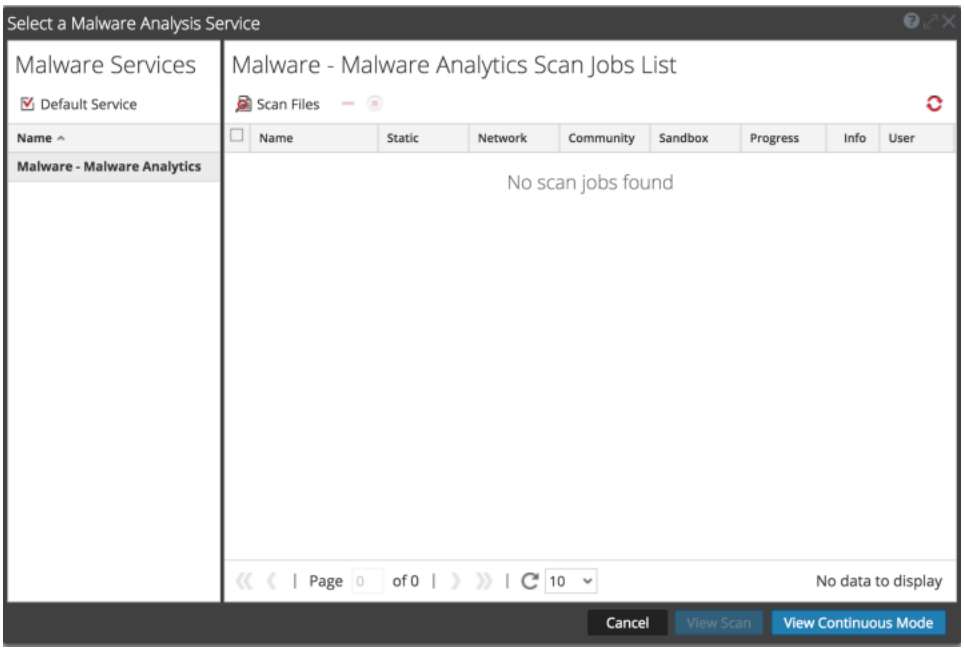
À partir d'Investigation, les analystes peuvent lancer une analyse Malware Analysis à la demande en sélectionnant un service et une valeur méta, puis en choisissant une option dans le menu contextuel. Lorsque l'interrogation est terminée, les données analysées sont disponibles pour l'analyse de malware.

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

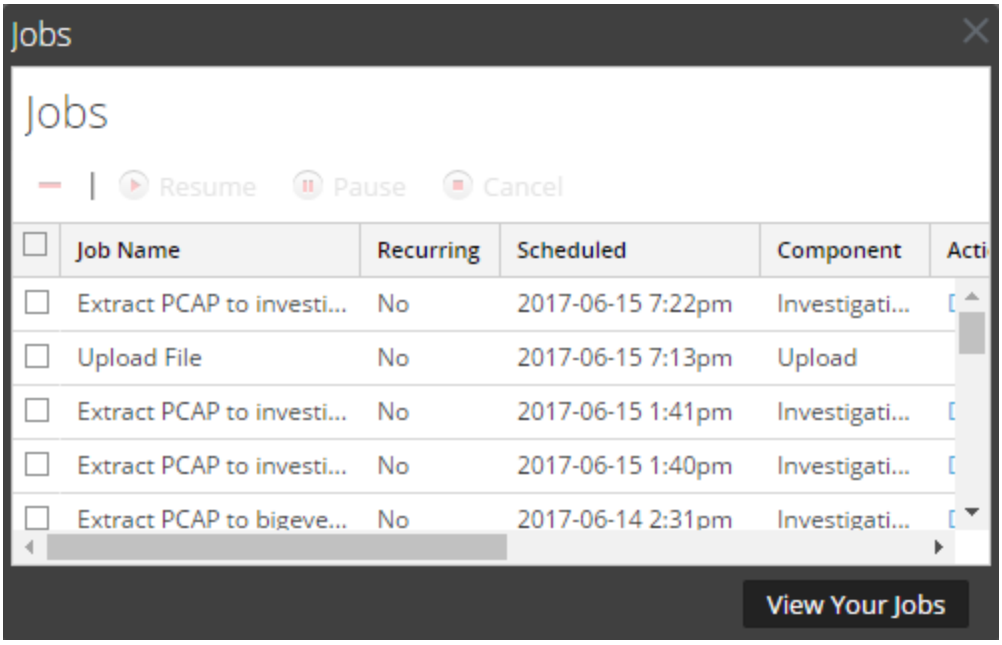
1. Cliquez avec le bouton droit de la souris sur une valeur méta (par exemple, OTHER, DNS ou FTP) et sélectionnez **Analyser les malwares** dans le menu contextuel.
   La boîte de dialogue Analyser les malwares s'affiche avec un nom suggéré pour l'analyse à la demande et aucun service sélectionné.
2.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

Gérer les listes et les valeurs de liste Context Hub dans Enquêter

Les analystes peuvent ajouter des listes et des valeurs de liste pour l'enrichissement de Context Hub dans les vues Naviguer et Événements. Lorsque le service Context Hub est activé et configuré, NetWitness Suite 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 Investigation. 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.

Conditions préalables

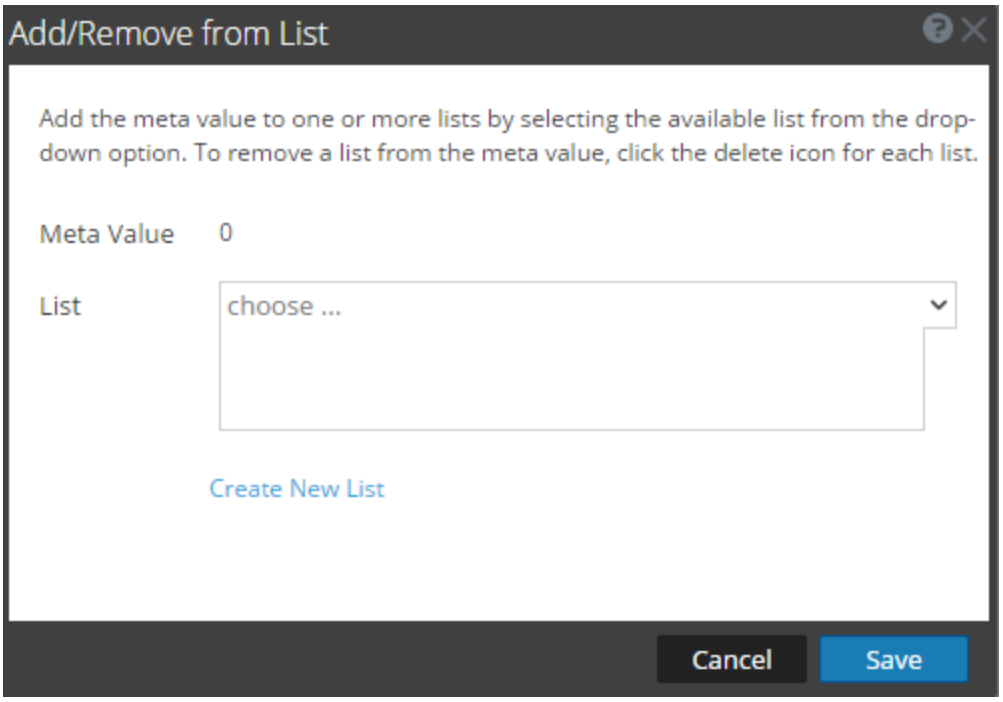
Pour permettre à un analyste de gérer des listes dans Investigation, l'administrateur doit :

- Activez 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 dans Investigation

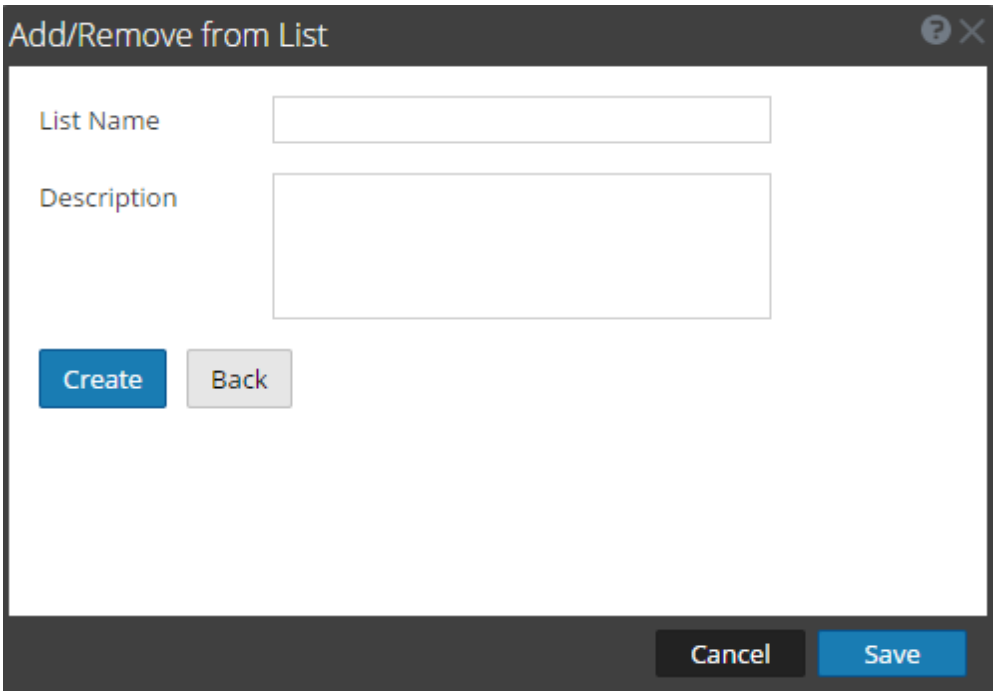
Pour supprimer une valeur méta d'une liste :

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 dans Investigation

Pour créer une liste Context Hub dans Investigation :

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.

Ouvrir la liste d'événements

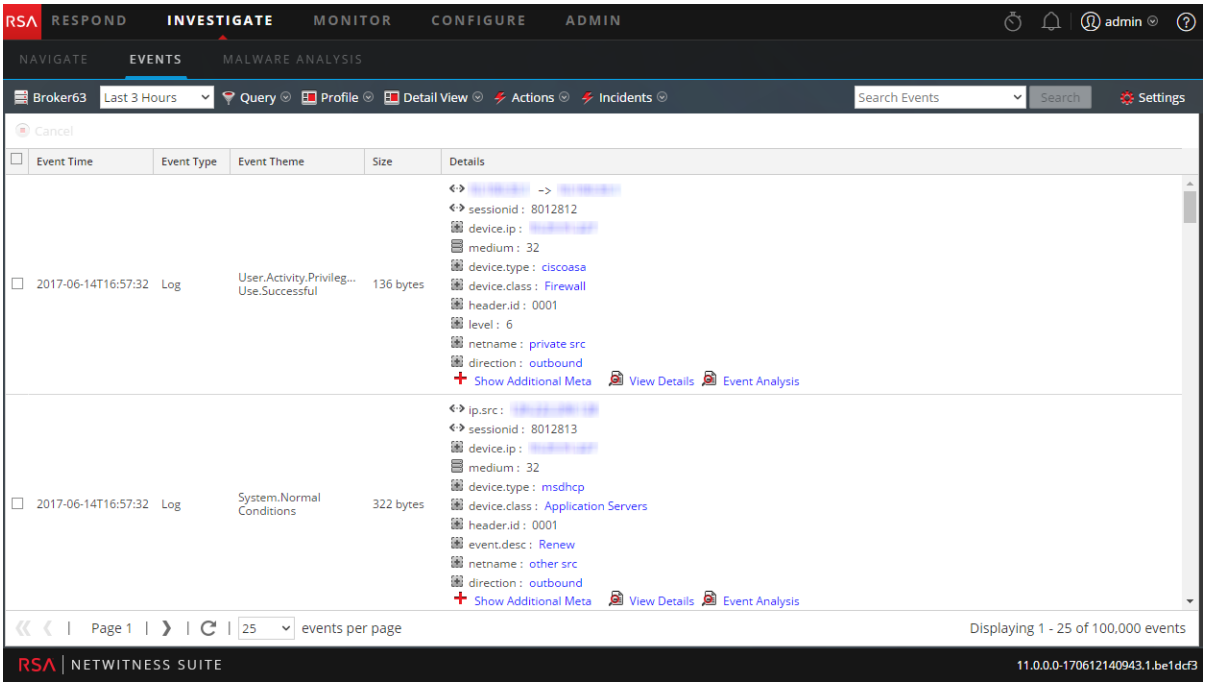
Une liste d'événements associée à une session est disponible dans Enquêter > vue Événements.

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 Suite 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 une métavaleur (en bleu) sous une clé méta.
   La vue Événements affiche les événements correspondant à la métavaleur sélectionnée.

Voici un exemple de la vue Détails.



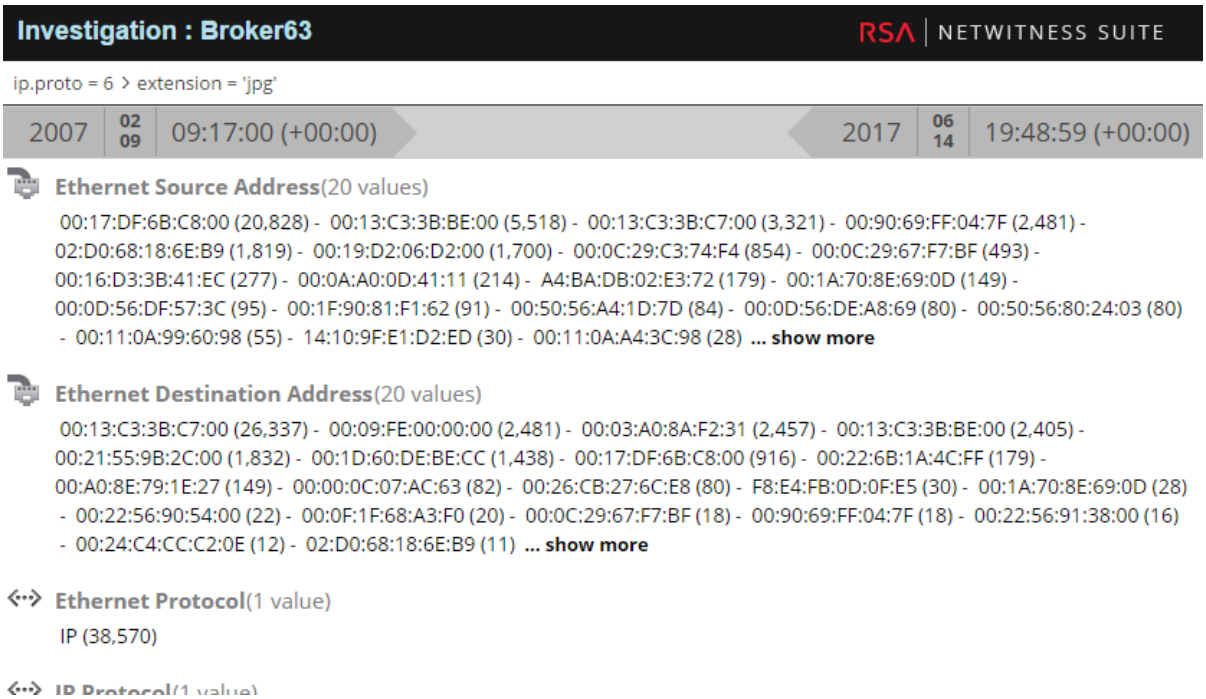
Vous pouvez utiliser des requêtes, le paramètre de plage temporelle et les profils pour filtrer les événements répertoriés dans la vue Événements. Depuis tous les types de vue dans la vue Événements, vous pouvez extraire des fichiers, exporter des événements, exporter des logs et ouvrir le panneau Reconstruction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

Imprimer le point de recherche verticale actuel

Dans la vue Enquêter > 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 **Enquêter > 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.

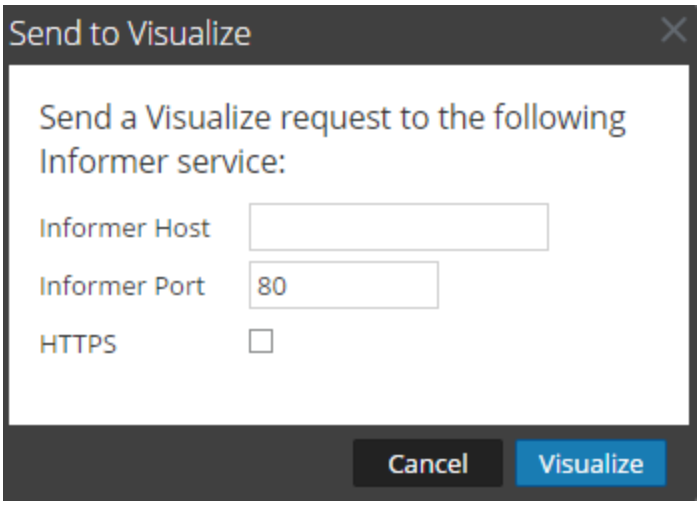
Visualiser le point d'extraction verticale actuel dans Informer

Cette rubrique fournit des instructions pour l'envoi d'un point d'extraction verticale dans la vue Enquêter> 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 Suite.

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 Suite 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.

Afficher un contexte supplémentaire pour un point de données

À partir d'une reconstruction d'événement ou du panneau Valeurs dans la vue Procédure d'enquête, vous pouvez consulter des détails et des renseignements sur les éléments associés à un événement dans le service Context Hub. Les données issues de sources configurées, comme RSA NetWitness Endpoint, peuvent vous aider à comprendre ce qui se passe.

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. Pour rechercher des informations externes sur une entité donnée, NetWitness Suite utilise le service Context Hub. 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 immédiates 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.

Lorsque vous cliquez avec le bouton droit de la souris sur l'entité dans Enquêter, le service Context Hub interroge les sources de données configurées pour obtenir des informations pertinentes. Le panneau Contexte s'ouvre depuis le côté droit de la fenêtre du navigateur. Le panneau Contexte 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 Contexte est mis à jour avec les informations de cette entité.

Pour fermer le panneau Contexte, cliquez sur ✕.

Dans le panneau Recherche contextuelle, vous pouvez visualiser et explorer des sources de données pour approfondir la procédure d'enquête. Par exemple, lorsque vous cliquez sur une valeur particulière Incident, le détail de l'incident est affiché dans la vue Répondre à un incident.

Pour une description détaillée des informations affichées dans chaque source de données du panneau Recherche contextuelle, consultez Panneau Recherche contextuelle.

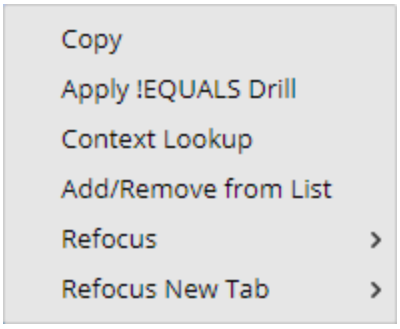
Avant qu'un analyste ne puisse afficher des informations contextuelles, l'administrateur doit :

- Assurez-vous que l'analyste dispose d'un rôle disposant de l'autorisation `Context Lookup`, comme décrit dans « Autorisations de rôle » et « Gérer les utilisateurs avec les rôles et autorisations » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.
- Ajoutez le service Context Hub dans RSA NetWitness Suite.
- configurer les sources de données du service Context Hub, comme indiqué dans le *Guide de configuration de Context Hub*.

Remarque : Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Pour afficher des informations dans le panneau Résumé du contexte :

1. Dans la vue Naviguer ou Événements, identifiez une valeur méta pour laquelle vous souhaitez afficher un contexte supplémentaire et survolez la valeur méta.
   Le panneau **Points forts du contexte** s'affiche avec un rapide résumé du type de données contextuelles disponible pour la source de données : 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** pour ouvrir le panneau Recherche contextuelle.



   Le panneau Récapitulatif du contexte s'ouvre depuis le côté droit de la fenêtre du navigateur. Le panneau Récapitulatif du contexte est renseigné avec les informations du service Context

Hub dès que possible.

3. Pour effectuer des actions à partir du panneau Contexte, cliquez sur une entité, comme l’adresse IP, et effectuez un clic droit.
   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.

Examiner des 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 Suite 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 Investigation > 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 :

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

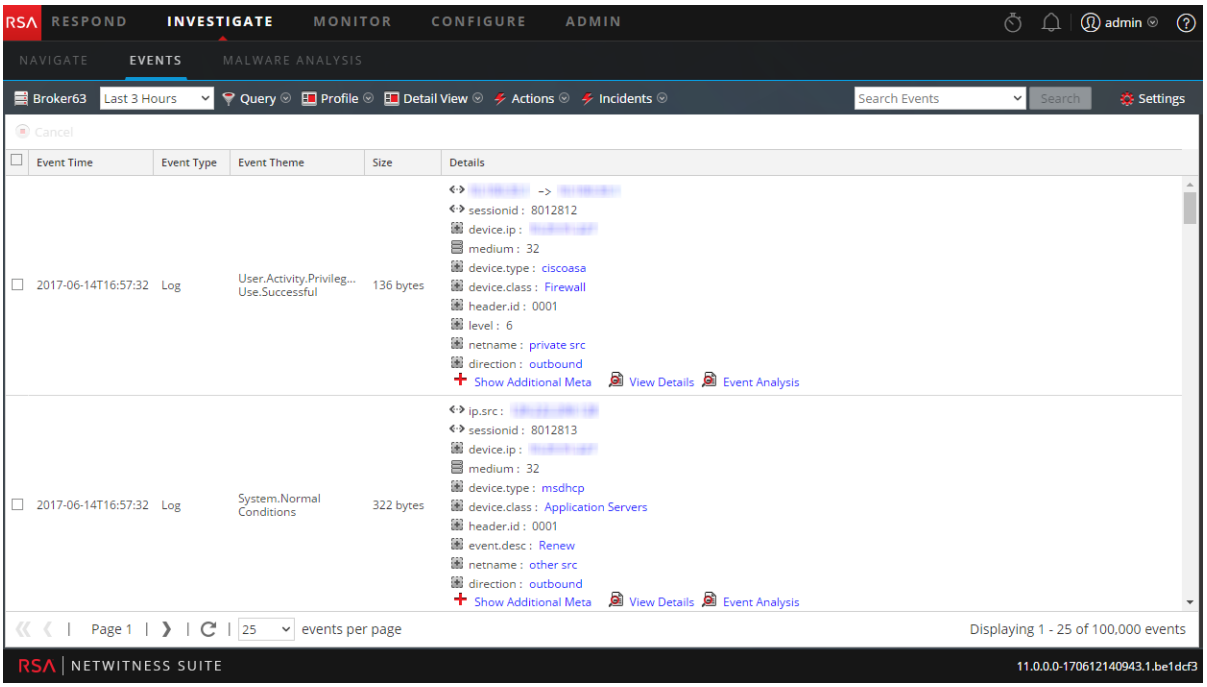
Si vous avez ouvert la vue Événements à partir d'un point de recherche verticale de la vue Naviguer, la vue détaillée des événements s'ouvre par défaut. Les analystes qui ne disposent pas des autorisations pour utiliser la vue Naviguer peuvent interroger les services directement à partir de la vue Événements.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

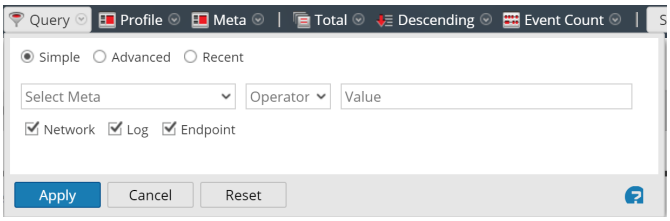
Filtrer les événements affichés dans la vue Événements

Pour filtrer les données affichées dans la vue Événements :

1. Dans la vue **Enquêter**, sélectionnez la vue **Événements**.
   La vue Événements s'affiche.



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 des métadonnées**, puis sélectionnez une clé méta dans la liste déroulante.

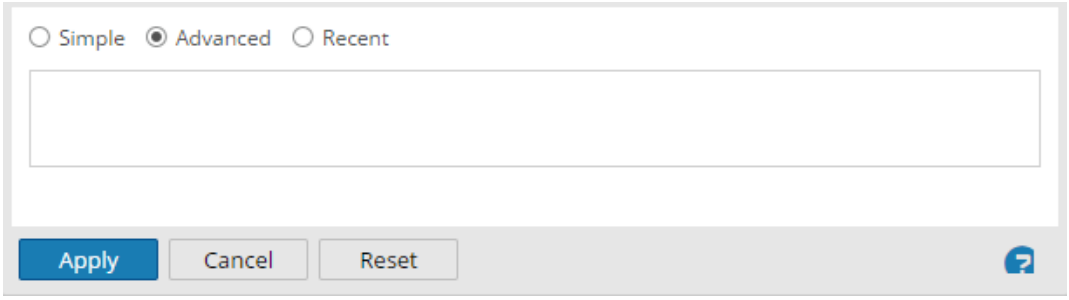
   b. Sélectionnez un opérateur dans la liste déroulante sous le champ **Opérateur**.

   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 :

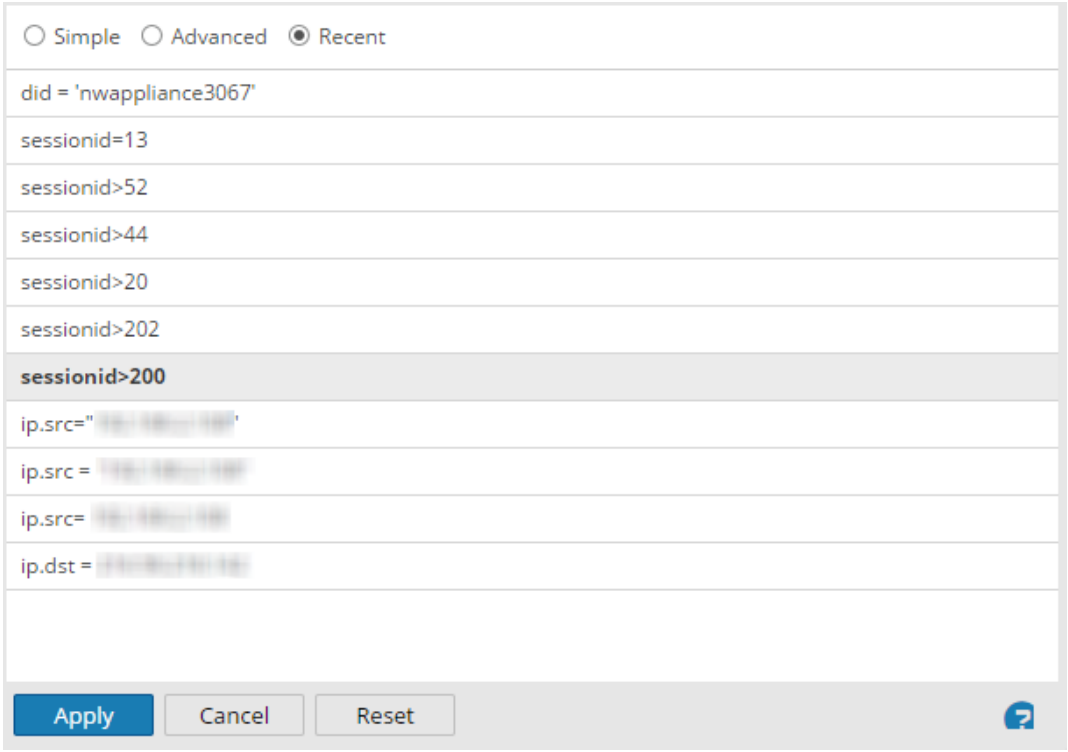
   a. Cliquez sur **Avancée**.
   La boîte de dialogue Requête avancée s'affiche.



   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 Suite actualise les résultats.

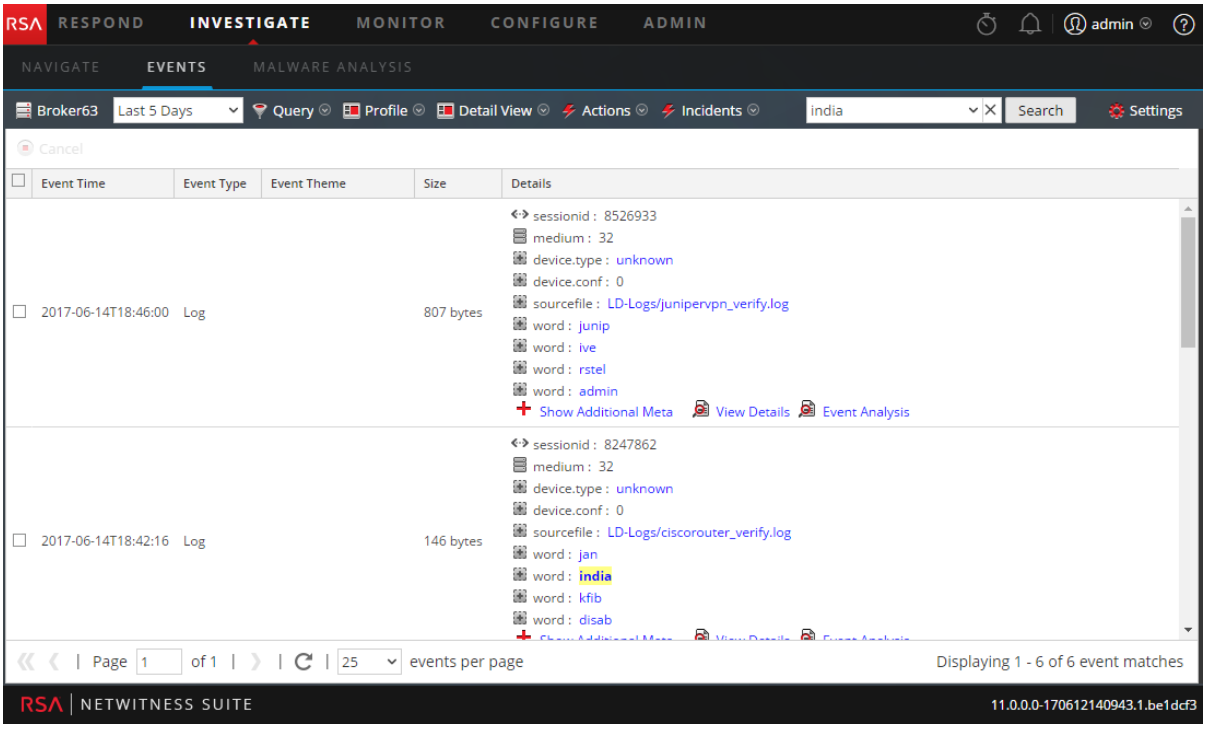
Rechercher des événements dans la vue Événements

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 le **X** dans la zone de recherche.

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 Suite 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

Dans NetWitness Suite version 10.5 et ultérieure, 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.

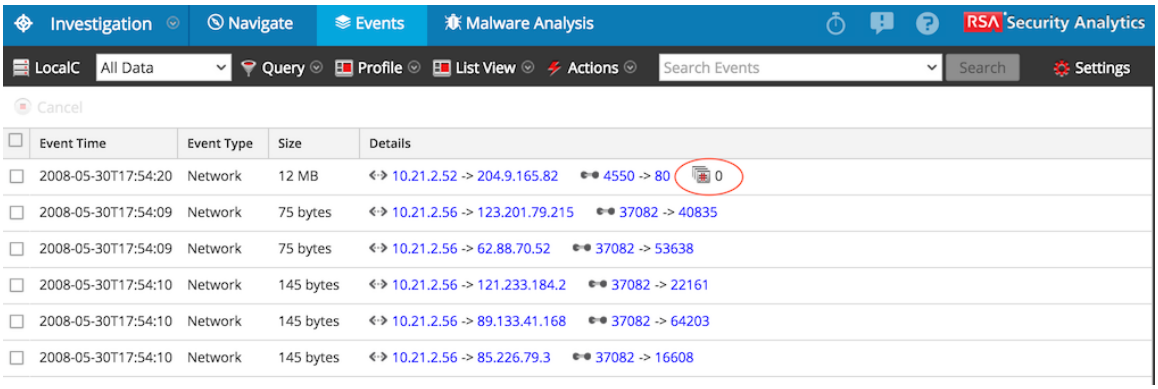
Mise en évidence des fragments de session

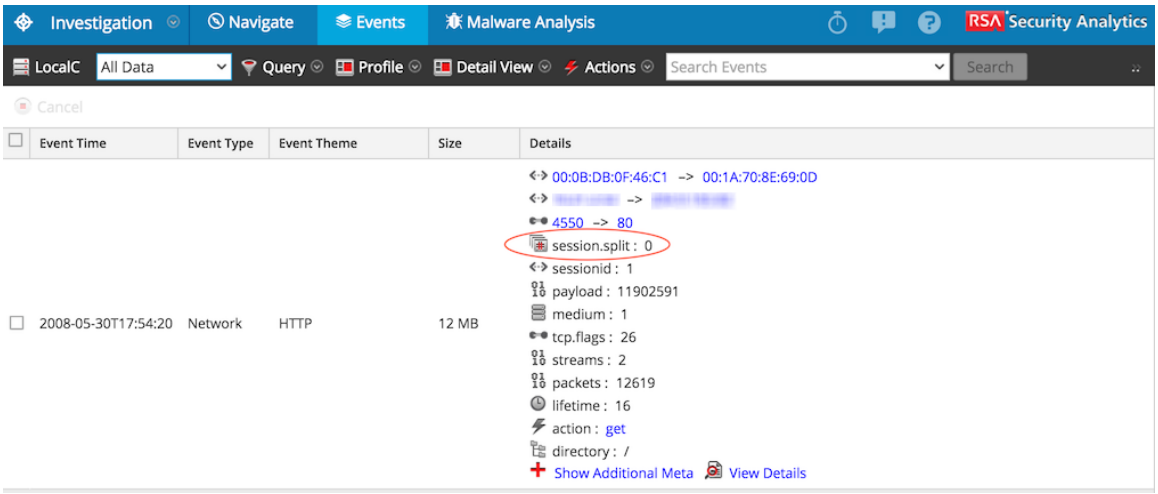
Chaque fragment de session dispose d'un méta supplémentaire, `session.split`. La valeur du méta `session.split` pour un fragment de session donné indique le nombre de fragments qui précèdent ce fragment. Lors de l'affichage des sessions dans la vue Événements, le méta `session.split` identifie clairement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

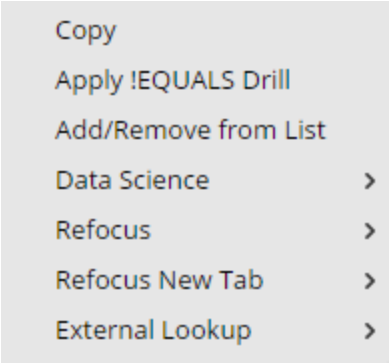
1. Identifier les sessions qui sont des fragments de sessions réseau.
2. Afficher tous les fragments de session d'une session réseau avec un fragment de session unique.
3. Exporter les paquets de toute la session réseau sous forme de fichier PCAP unique.

Rechercher et associer des fragments

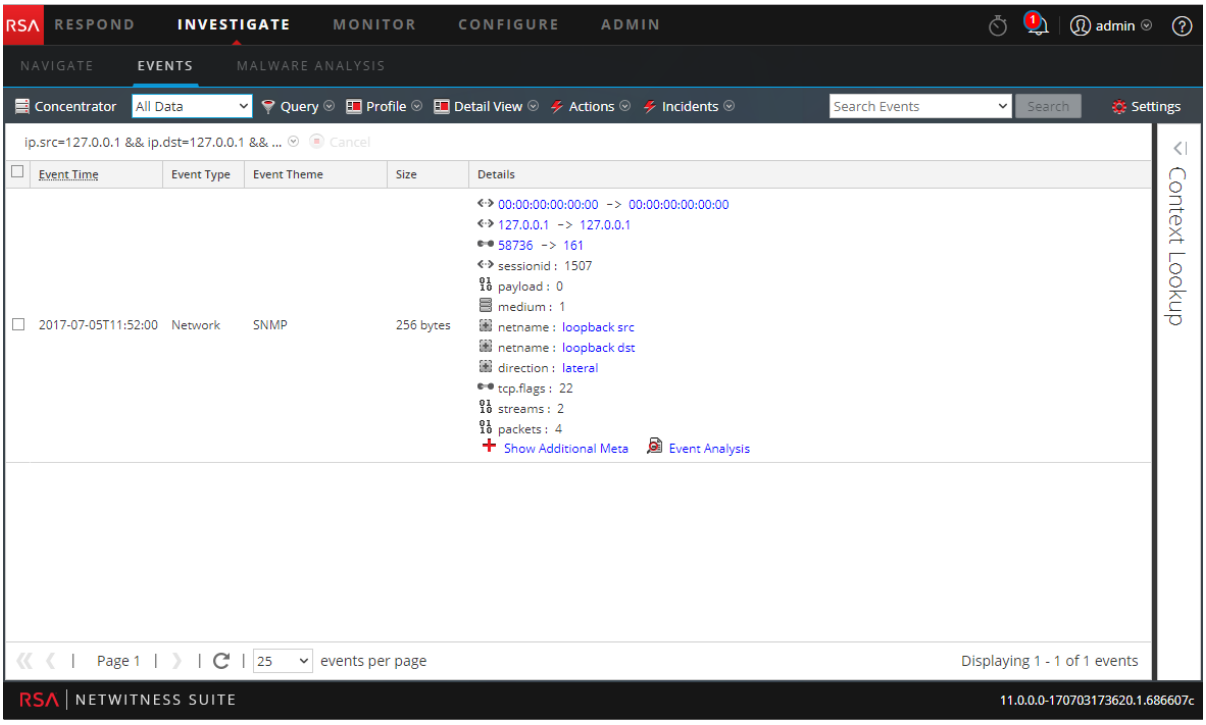
Depuis la vue Événements, vous pouvez trouver les fragments d'une session en utilisant l'option du menu contextuel Recentrer > Rechercher des fragments de session. NetWitness Suite crée une requête en utilisant les ports et les adresses source et de destination de la session sélectionnée, et affiche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

Pour rechercher des fragments de session :

1. Dans la vue **Investigation > 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 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 Suite 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.

Gérer des groupes de colonnes dans la vue Événements

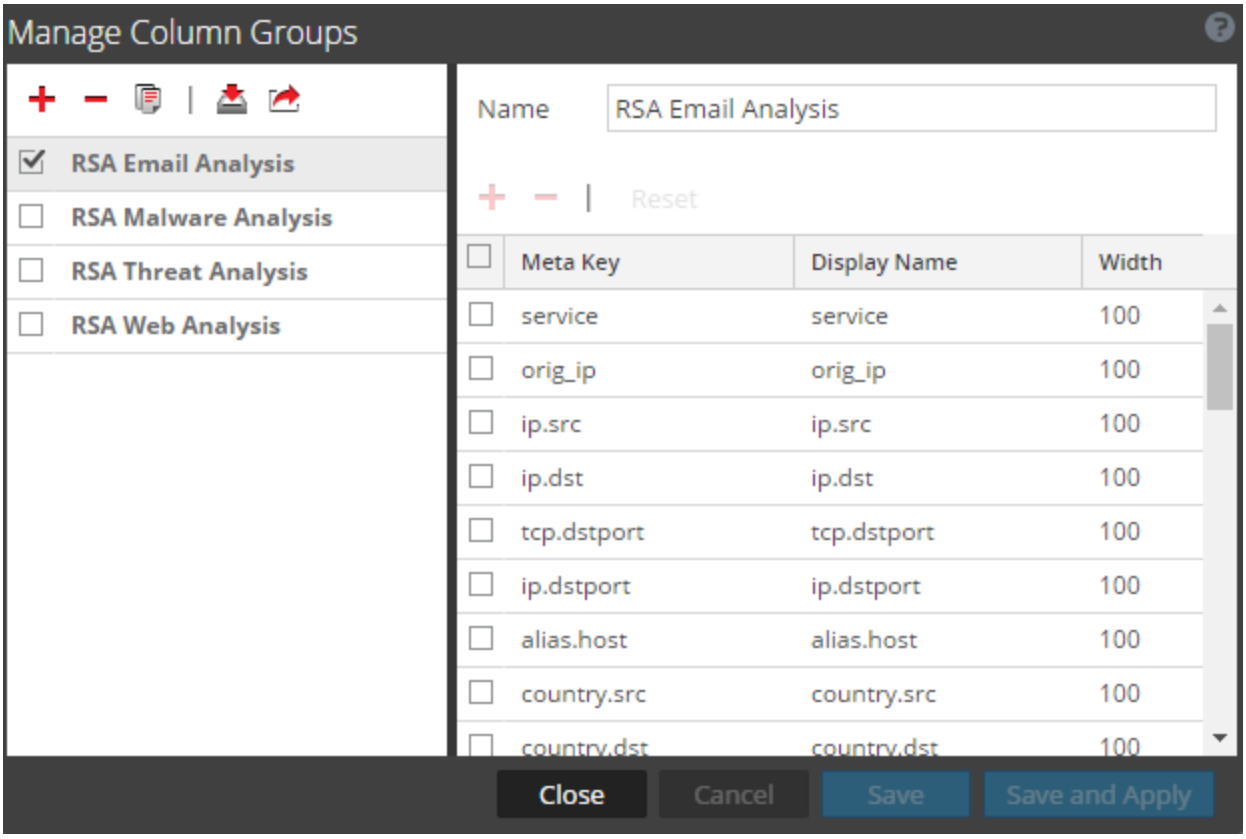
Cette rubrique fournit des instructions pour permettre à un analyste de créer et de gérer des groupes de colonnes personnalisés pour afficher des données dans la vue Événements.

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 métadonnées dans une colonne, la position de la colonne dans la grille et la largeur par défaut de la colonne.

Remarque : 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. Dans le mode **Rechercher**, sélectionnez la vue **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.

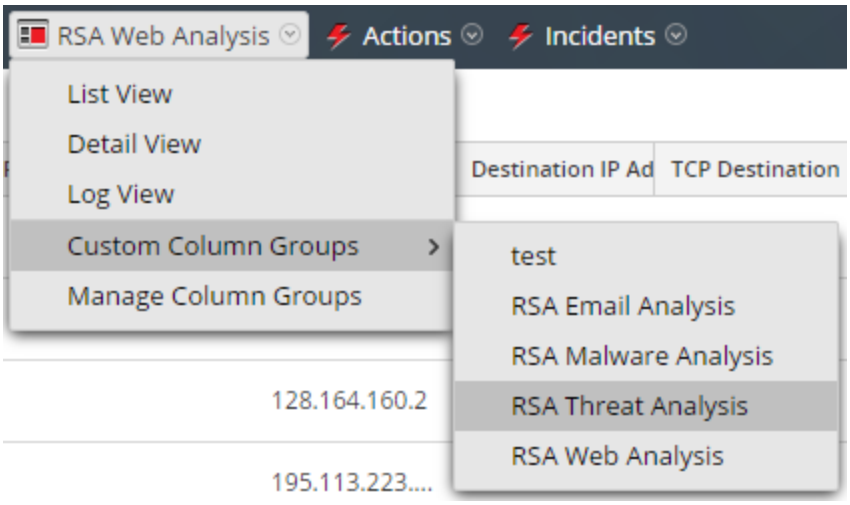


3. Pour ajouter un nouveau groupe de colonnes dans le panneau Groupe de colonnes, cliquez sur + et saisissez le nom du nouveau groupe dans le champ qui en résulte.
4. Le panneau de définition de colonne s'ouvre sur la droite avec le nom de groupe rempli. Vous pouvez modifier ce dernier.
5. Pour ajouter une colonne au groupe, cliquez sur + et cliquez dans le champ **Clé méta** vide pour afficher la liste déroulante **Clé méta**.
6. Sélectionnez un champ de clé méta dans la liste et répétez cette étape jusqu'à ce que l'ensemble de colonnes soit terminé.
7. (Facultatif) Pour supprimer une clé méta du groupe de colonnes, cliquez sur −.
8. (Facultatif) Pour réorganiser l'ordre dans lequel les colonnes apparaissent dans la liste Événements, faites glisser les clés méta à l'emplacement souhaité.
9. (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.

10. (Facultatif) Pour rétablir les paramètres précédents pour le groupe de colonnes et annuler toutes vos modifications, cliquez sur **Réinitialiser**.
11. 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 personnalisé

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 Détail ou valeur actuelle).



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

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.

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.

  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.

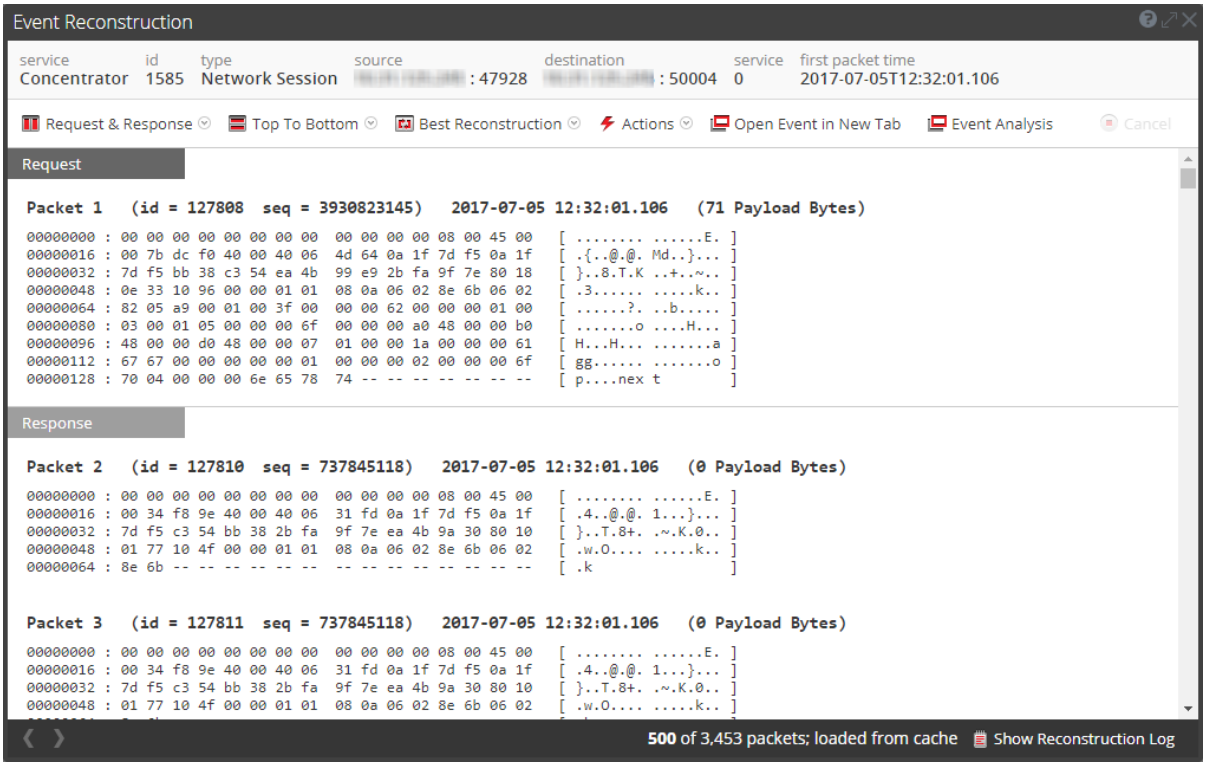
Remarque : Les paramètres de reconstruction et les paramètres du cache de reconstruction permettent à un administrateur de gérer les performances de l'application dans le cadre d'une procédure d'enquête. Lorsque les analystes reconstruisent les sessions qu'ils inspectent, deux situations peuvent affecter 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 Suite 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 Serveur NetWitness actif.

Reconstruire un événement

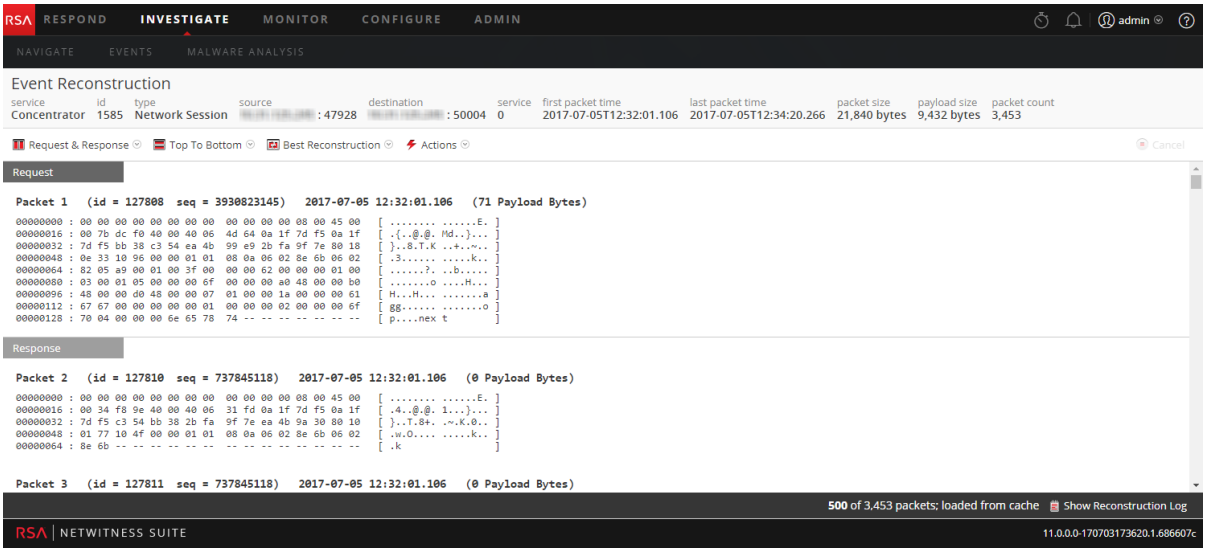
1. Ouvrez un point de recherche verticale dans la vue **Événements**.
2. Pour afficher toutes les métadonnées, cliquez sur 

.
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 de l'événement s'ouvre dans une fenêtre contextuelle dans la même vue.

Par défaut, NetWitness Suite affiche la meilleure reconstruction pour l'événement déterminée par son contenu ou la reconstruction que vous avez sélectionnée dans le paramètre Visualisation des sessions par défaut de Procédure d'enquête. 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 **Événements**, 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'ouvre 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**.

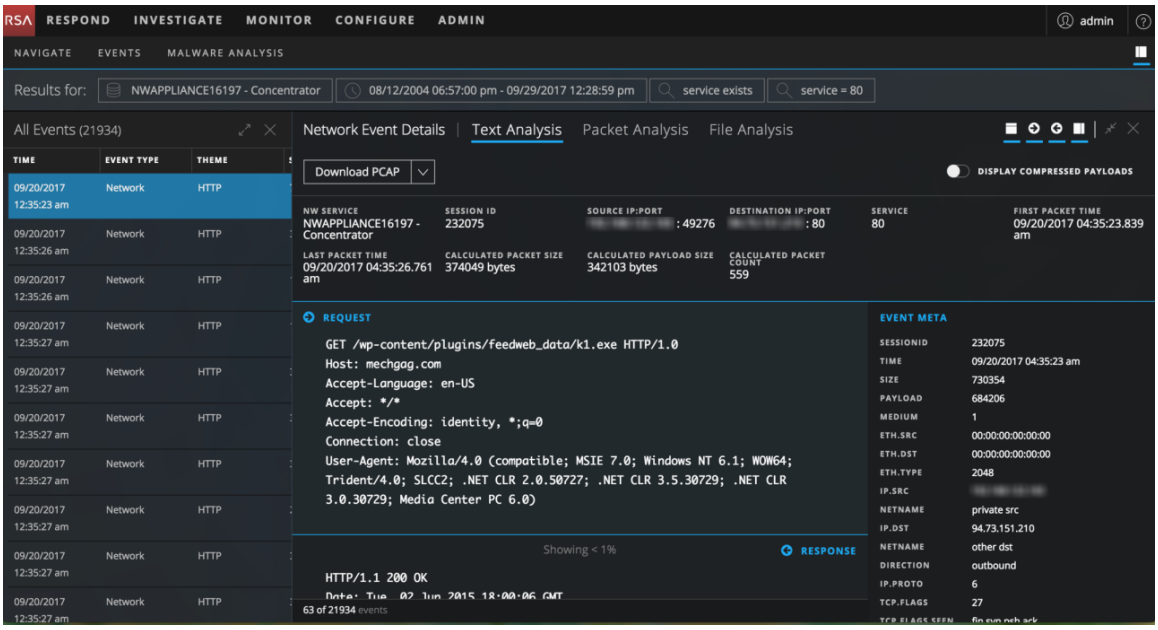
4. La tâche est planifiée et une fois l'opération terminée, les types de fichiers sélectionnés sont téléchargés sur le système de fichiers local. Sous Profil > onglet Tâches, vous pouvez télécharger les fichiers.

Analyser les événements dans la vue Analyse d'événements

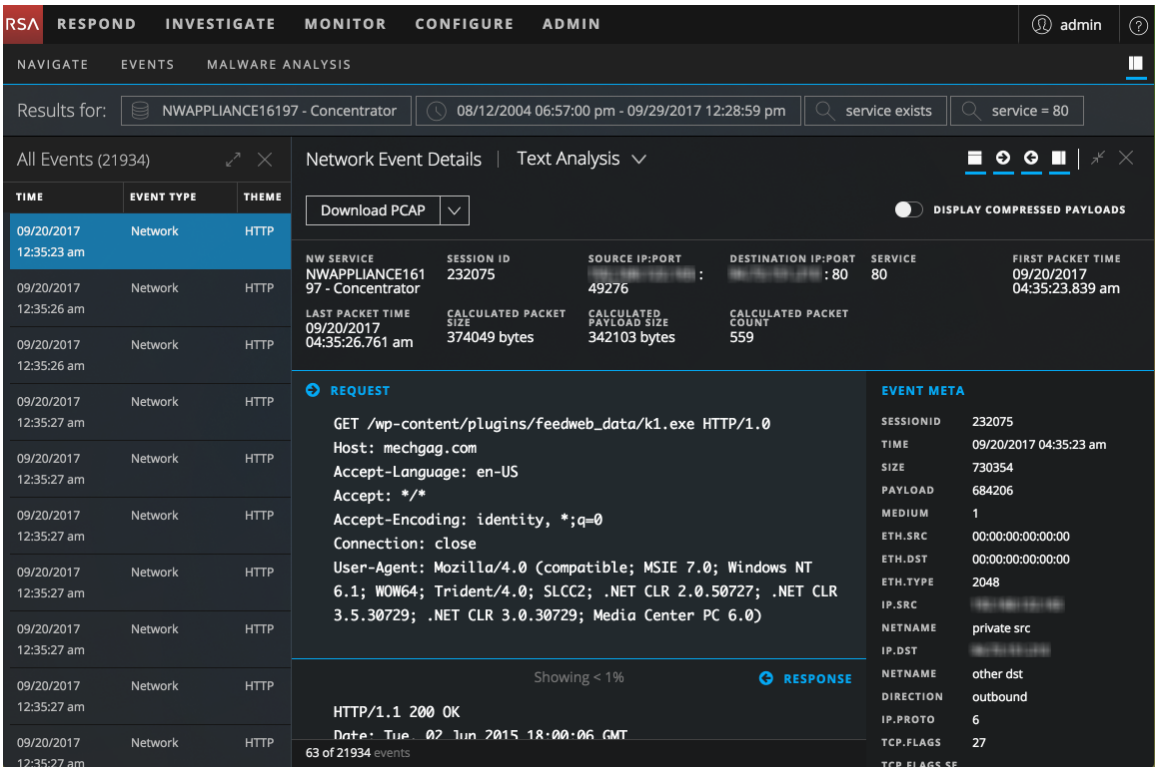
Lors de la chasse aux menaces possibles dans les données de réseau capturées, vous pouvez accéder à différents points d'intérêt dans les données. Si une session donnée contient des événements suspects, vous pouvez examiner la liste des événements pour la session et afficher également en toute sécurité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

Dans la vue Analyse d'événements, vous pouvez sélectionner le format de la reconstruction : Analyse de paquets, Analyse de fichiers ou Analyse de texte. Lorsque la clé méta `medium` étiquette un événement en tant qu'un événement de log ou de point de terminaison (requête en tant que `medium=32`), seul le 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.

La figure suivante est un exemple de détails d'événement de réseau : un panneau Analyse de paquets 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.



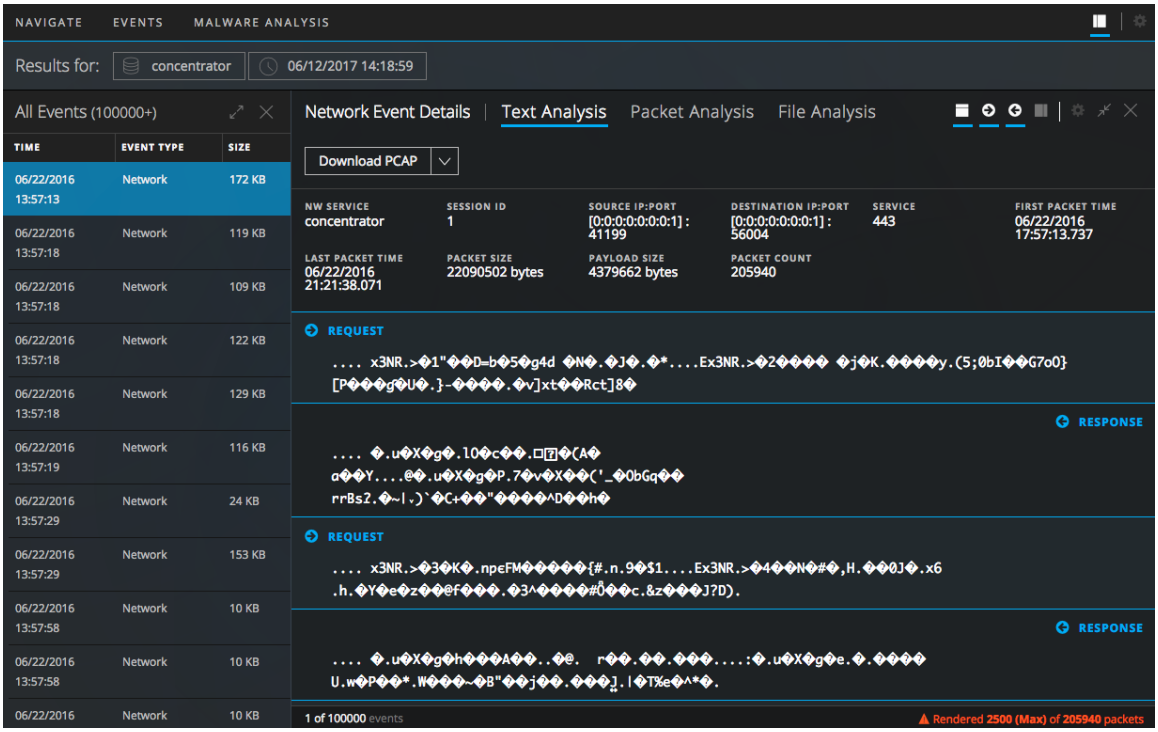
Au sein de chaque type d'analyse, de nombreux paramètres sont disponibles afin d'améliorer votre analyse. Si vous modifiez un paramètre, ce dernier est conservé entre les actualisations de navigateur et les connexions au sein du même navigateur. Les paramètres conservés sont les suivants :

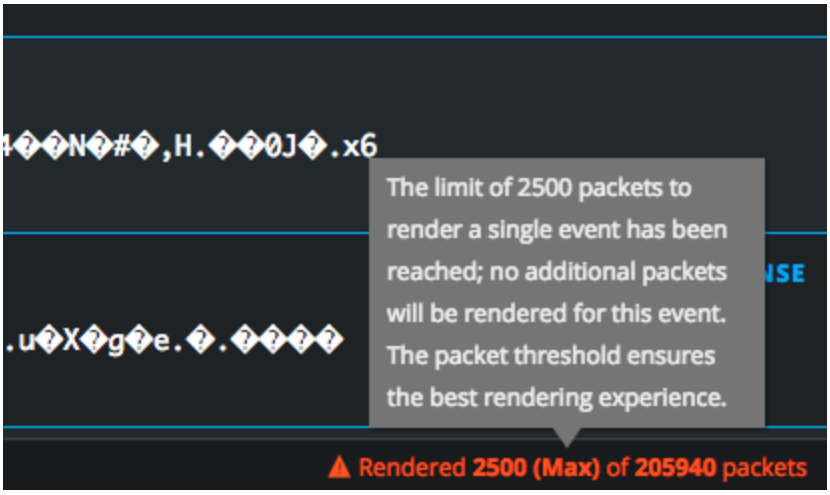
- La reconstruction sélectionnée actuelle : Analyse de texte, Analyse de paquets ou Analyse de fichiers.
- Si le Panneau des métadonnées d'événement est ouvert ou fermé.
- Si l'en-tête d'événement est ouvert ou fermé.
- Si la demande ou réponse ou les deux sont affichés.
- Si les charges utiles des paquets sont affichées dans le panneau Analyse de paquets.
- Si les octets ombrés 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.
- 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.

Le panneau Analyse de texte pour certains événements de réseau peut être très volumineux. Pour garantir le meilleur rendu, le nombre de paquets pouvant être rendus dans un seul événement est limité à 2500. Si le panneau Analyse de texte n'affiche pas tous les paquets, le pied de page indique que la limite de 2 500 paquets a été atteinte ; aucun paquet supplémentaire ne sera restitué pour cet événement. La figure suivante illustre une reconstruction qui comporte 205 940 paquets avec uniquement 2 500 paquets rendus ; aucun autre paquet ne sera rendu pour cette reconstruction.





Remarque : Certains événements de réseau possèdent un grand nombre de paquets mais la charge utile est très petite. Dans ce cas, si la charge utile entière est contenue dans les 2 500 premiers paquets, cela est conforme à la définition de l'affichage de tous les paquets. Aucun message indiquant que vous n'affichez pas tous ces paquets ne s'affiche.

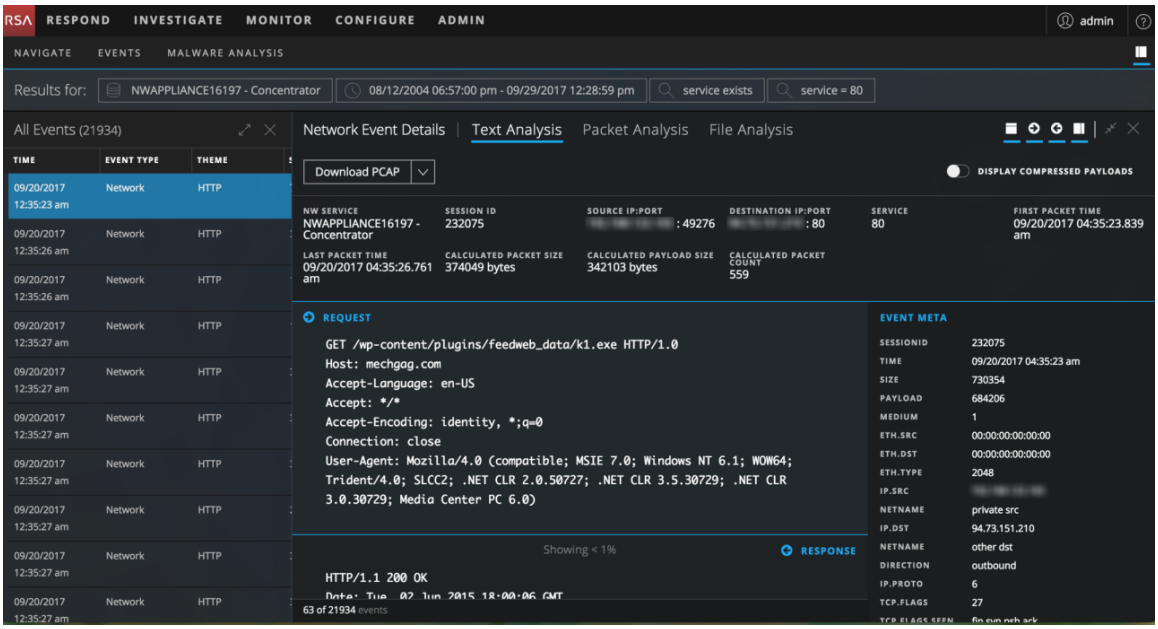
Dans le panneau Analyse de texte, les événements de réseau, les événements de log et les événements de point de terminaison sont présentés différemment.

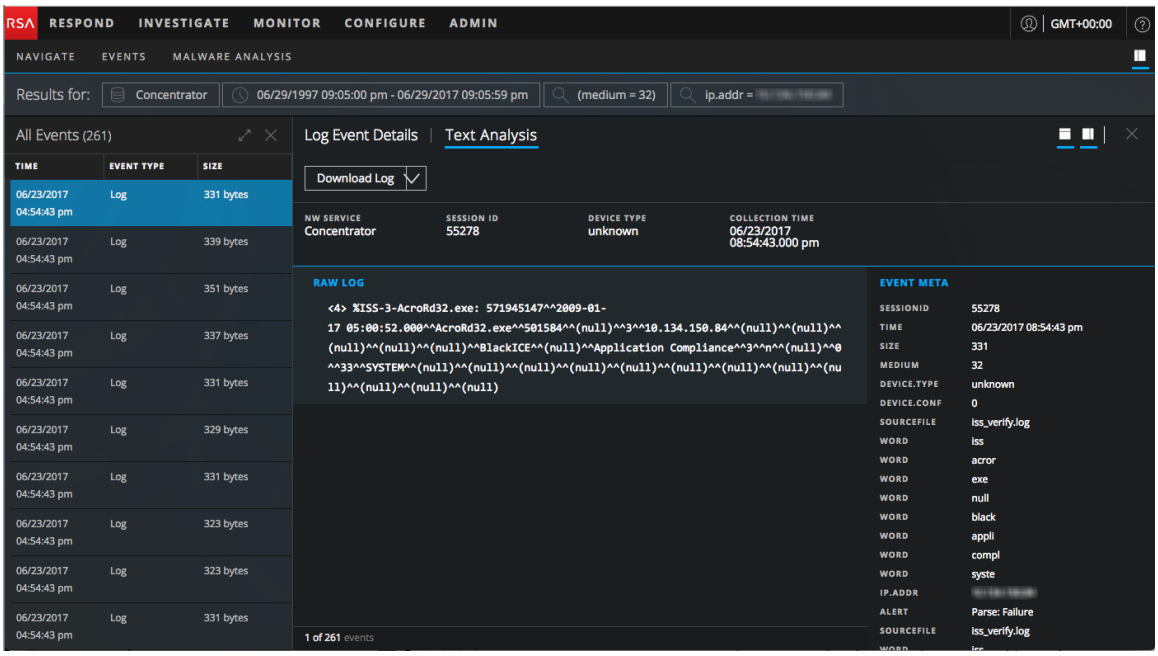
- Pour les événements de réseau, la vue Enquêter affiche l'orientation du paquet (demande ou réponse) et le contenu de chaque paquet au format texte. Si vous reconstruisez un événement de réseau, le panneau Analyse de texte est déroulant. Lorsque vous faites défiler la liste, les informations relatives 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 (filtrer sur `medium = 32` et `nwe.callback_id does not exist`) et les événements de point de terminaison (filtrer sur `medium = 32` et `nwe.callback_id exists`) n'ont aucune demande ou réponse ; seul l'événement brut s'affiche dans le panneau Analyse de texte.

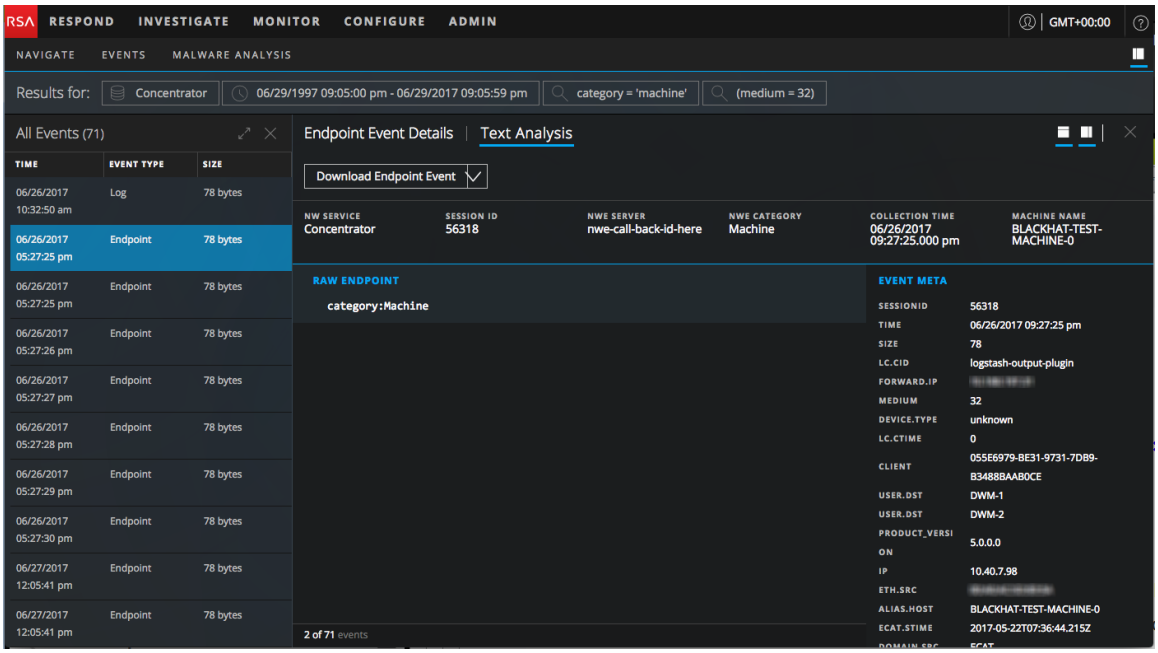
Pour chaque type d'événement (réseau, log ou point de terminaison), il existe plusieurs différences :

- 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.



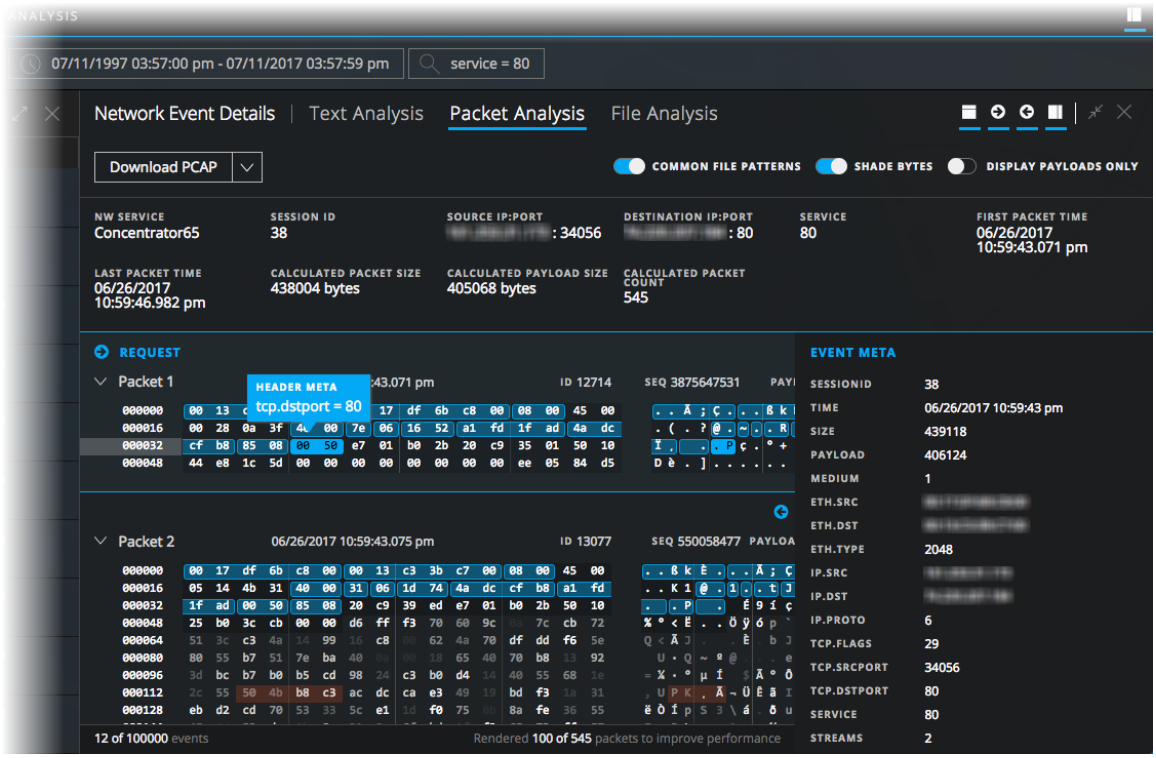




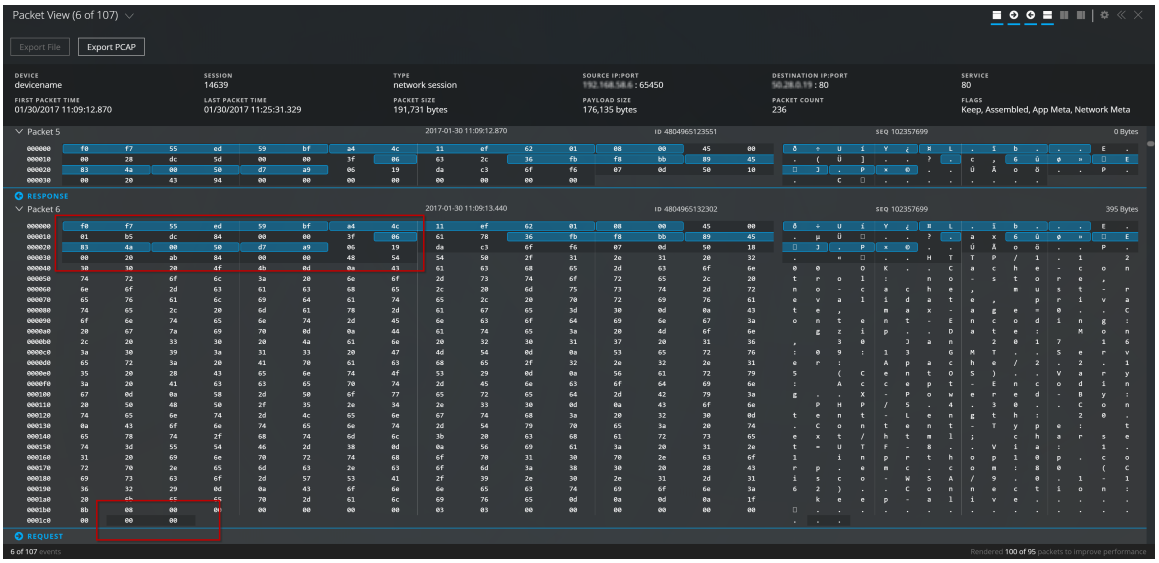
Remarque : Le nombre de paquets calculé, la taille de paquets calculée et la taille de charge utile calculée dans l'en-tête Événement peut être différente des mêmes statistiques dans le Panneau des métadonnées d'événement car les métadonnées sont parfois écrites avant la fin de l'analyse des événements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

Le panneau d'analyse des paquets

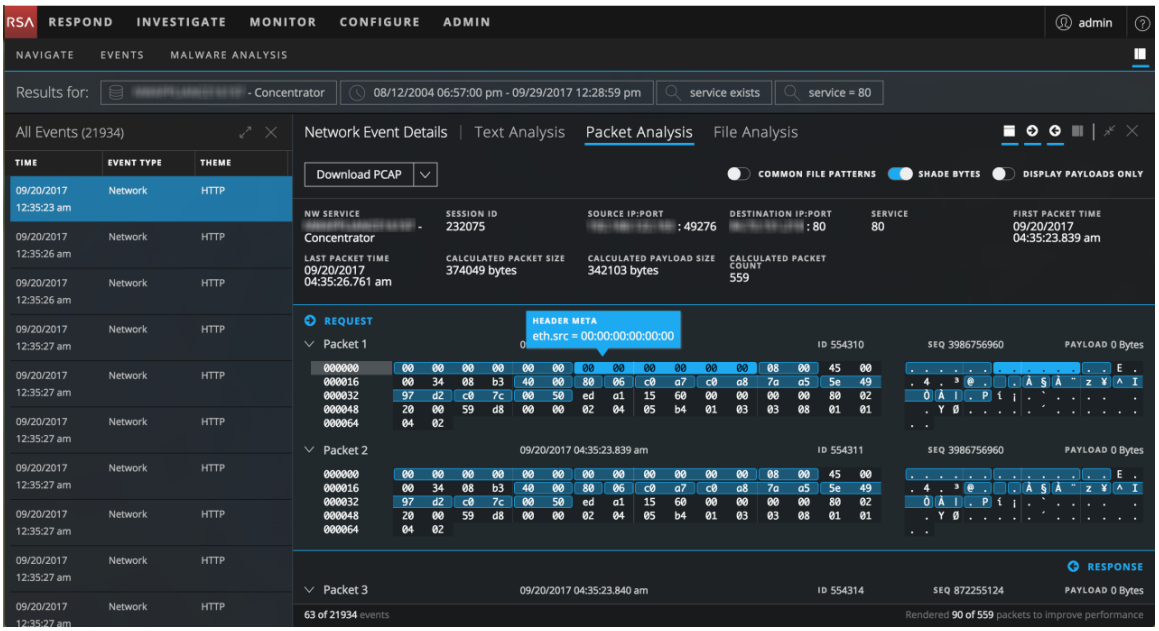
Le panneau Analyse de paquets concerne uniquement les événements de réseau. Le panneau Analyse de paquets peut défiler et les informations d'identification du paquet, ainsi que les libellés de requête et de réponse, restent visibles, au lieu de quitter l'affichage.



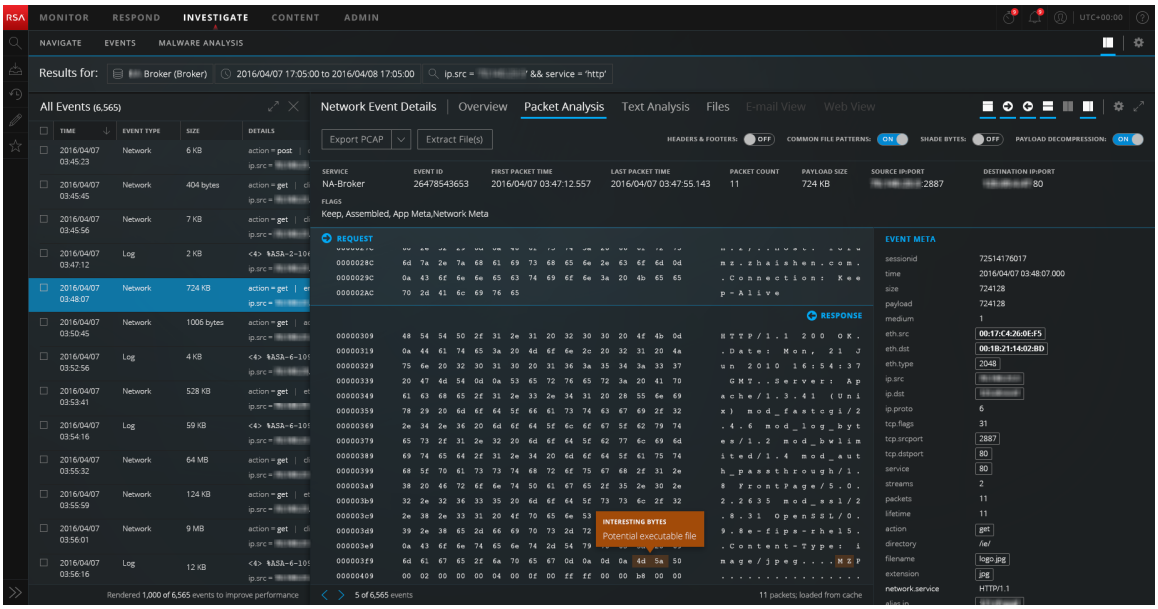
Dans le panneau Analyse de paquets, les en-têtes fournissent la direction du paquet (demande ou réponse), le nombre de paquets, l'heure de début du paquet, l'ID de paquet et la séquence, ainsi que la taille de la charge utile. Tous les paquets commencent par un en-tête, et certains paquets ont un pied de page. Certains paquets ont une charge utile. Dans la Analyse de paquets, l'en-tête et le pied de page affichent un arrière-plan plus sombre qui vous permettent de les distinguer de la charge utile du paquet. L'arrière-plan plus sombre de l'en-tête et le pied de page s'affiche au format hexadécimal et ASCII.



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.

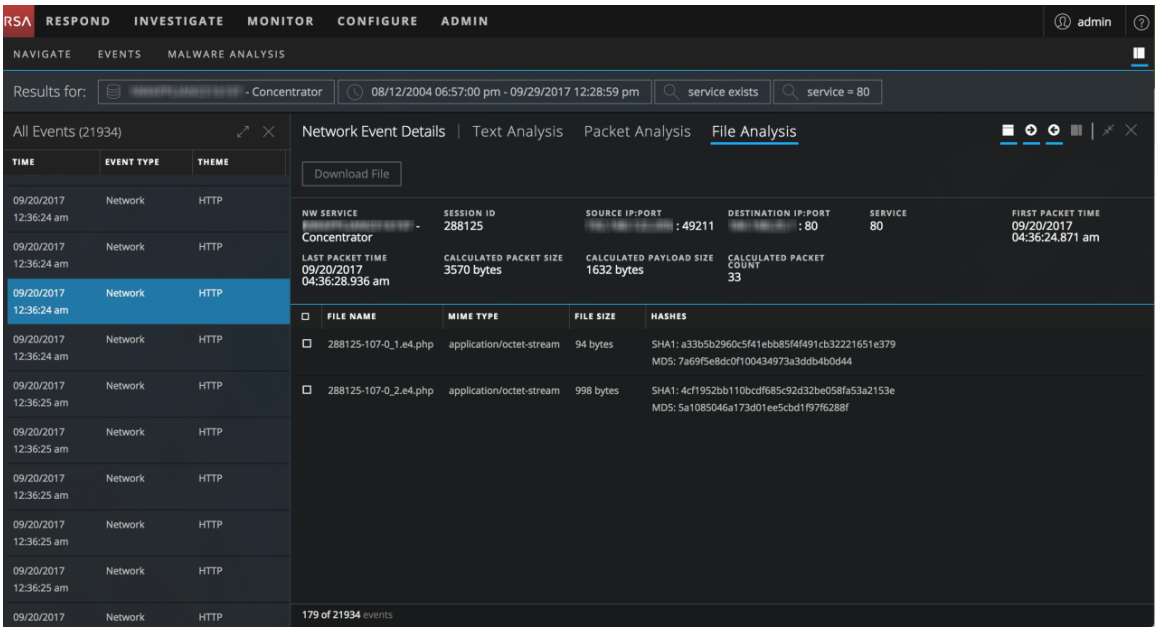


Les signatures de fichier courant sont mises en surbrillance avec un arrière-plan orange. Lorsque vous placez le curseur sur le texte en surbrillance, la description du type de fichier s'affiche dans une zone de survol.

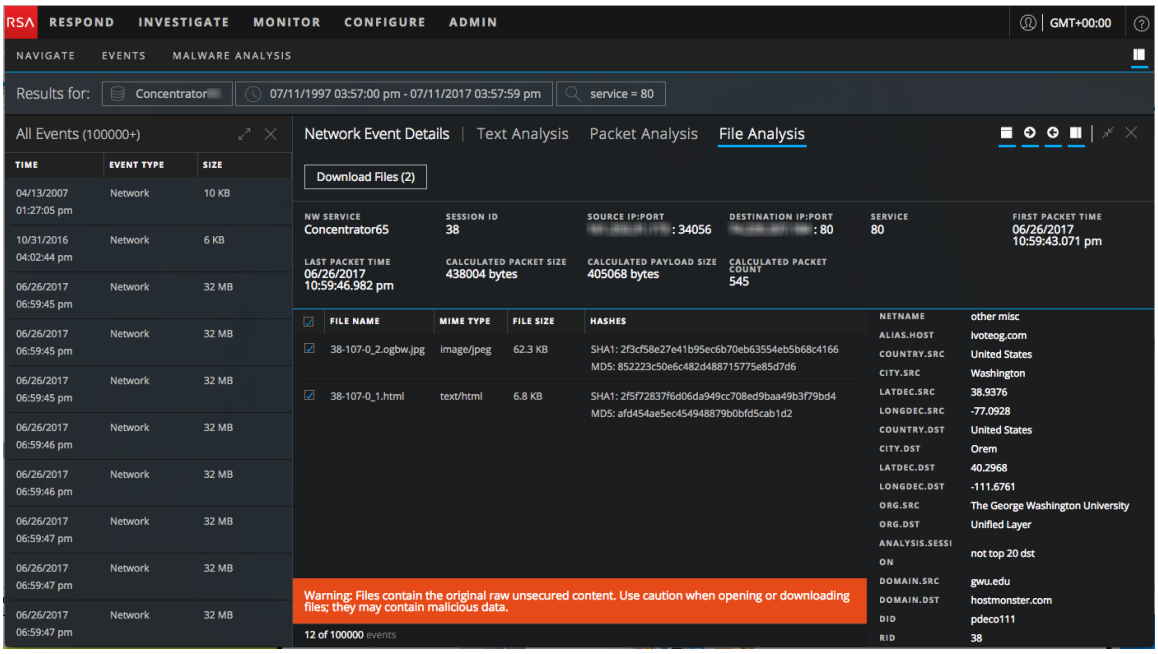


Le panneau Analyse de fichiers

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	√		

Action	Événement réseau	Consignation d'événements	Événement de point de terminaison
Ouvrir, fermer et ajuster la taille des panneaux	√	√	√
Régler l'affichage des demandes et réponses	√		
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	√		

Action	Événement réseau	Consignation d'événements	Événement de point de terminaison
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 en cours dans le panneau de point de terminaison NetWitness			√

Sélectionner le type Analyse d'événements

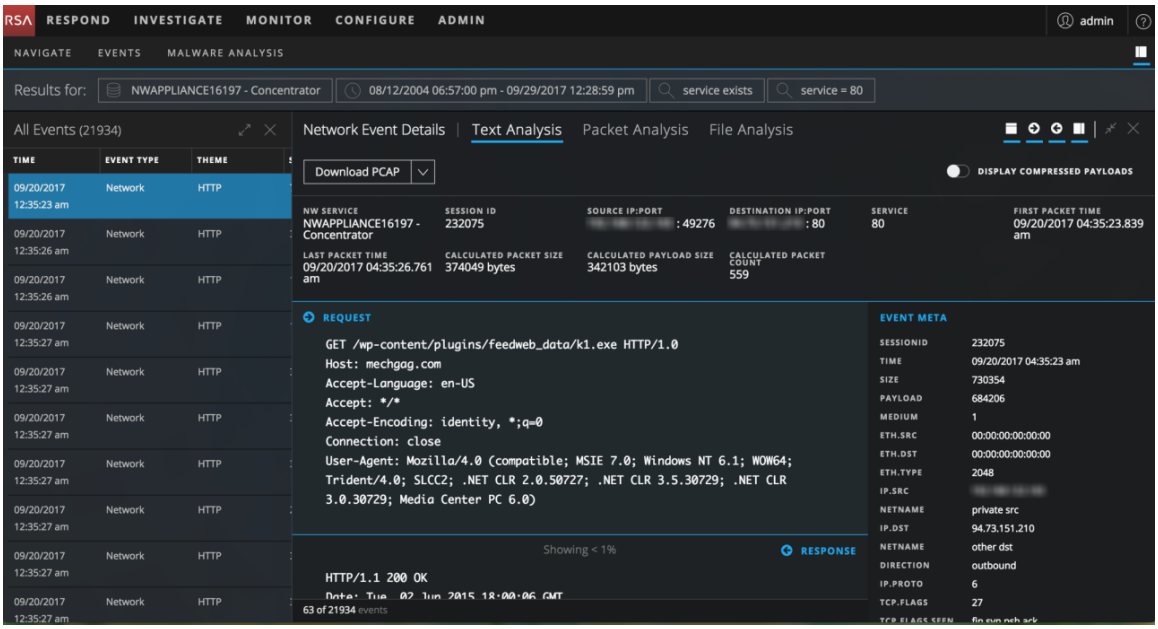
Pour sélectionner le type d'analyse d'événement d'un événement, effectuez l'une des opérations suivantes :

1. Dans la barre d'outils de la **vue Analyse d'événements**, cliquez sur le menu de type d'analyse dans le coin supérieur gauche.
2. Dans le menu contextuel, sélectionnez le type d'analyse : **Analyse de paquets, Analyse de fichiers** ou **Analyse de texte**.
   La vue est actualisée avec le panneau Analyse de paquets, le panneau Analyse de fichiers ou le panneau Analyse de texte ouvert.

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 des événements s'ouvre avec la liste des événements sur la gauche et le panneau Détails de réseau, Détails de log ou Détails de point de terminaison s'ouvre sur la droite. Vous pouvez cliquer sur un événement dans la liste des événements pour afficher une reconstruction différente. Au départ, le panneau Détails de réseau, Détails de log ou Détails de point de terminaison occupe 75 % de la largeur de la fenêtre par défaut.



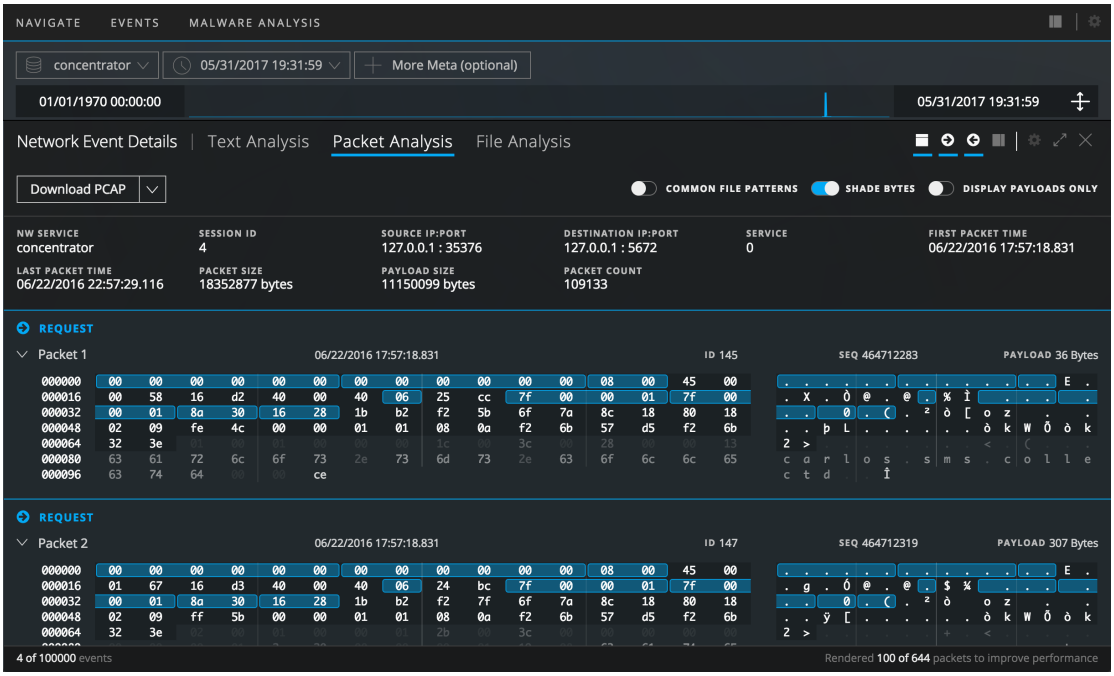
Vous pouvez modifier le rapport de dimensionnement entre les deux panneaux pour améliorer la lisibilité en développant un des panneaux, en en réduisant un ou en fermant un. Vous pouvez rouvrir le panneau après sa fermeture. Le rapport que vous sélectionnez persiste jusqu'à ce que vous modifiiez ou actualisiez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

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.

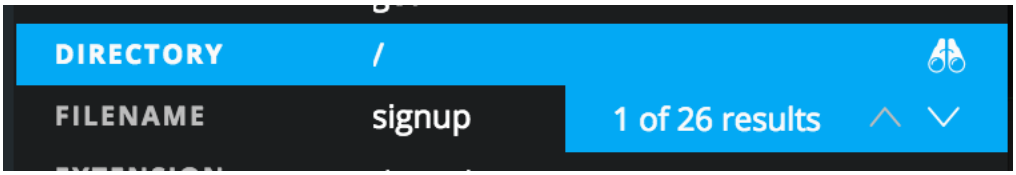
Pour sélectionner le côté de la conversation à afficher (Demande, Réponse ou les deux), cliquez sur l'une ou l'autre des icônes de direction.  . La reconstruction est actualisée avec les informations sélectionnées.

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/.



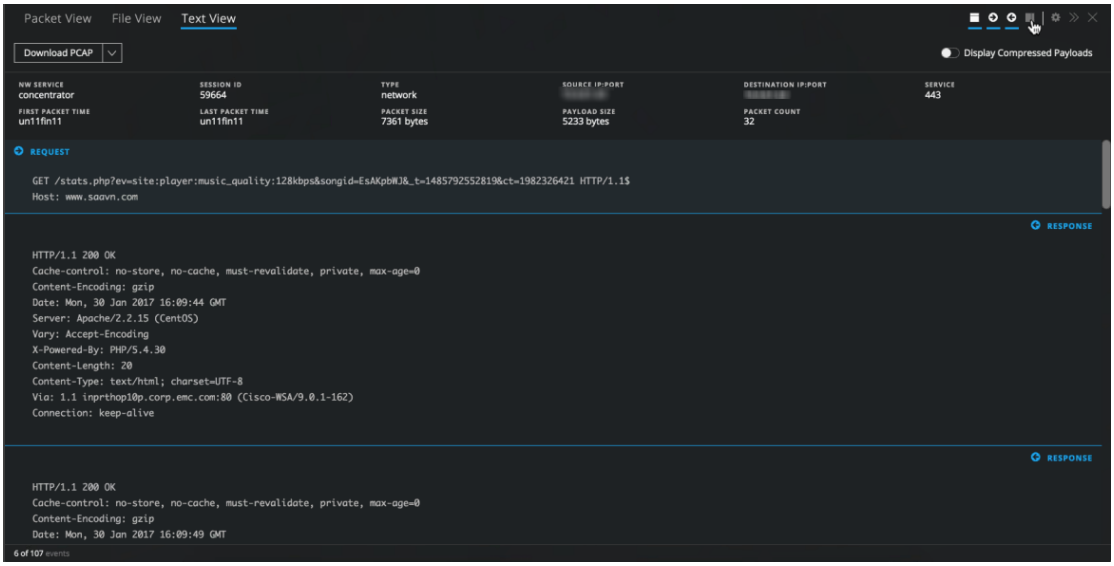
Cliquer sur l’icône déclenche une recherche pour la paire clé méta/valeur méta (non sensible à la casse) dans le panneau Analyse de texte et chaque instance est mise en surbrillance. Dans le Panneau des métadonnées d’événement, la ligne en surbrillance dispose d’un nombre de résultats et d’une barre 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 des métadonnées d’événement supprime la mise en surbrillance du texte brut. La mise en surbrillance est également supprimée si vous fermez le Panneau des métadonnées d’événement.

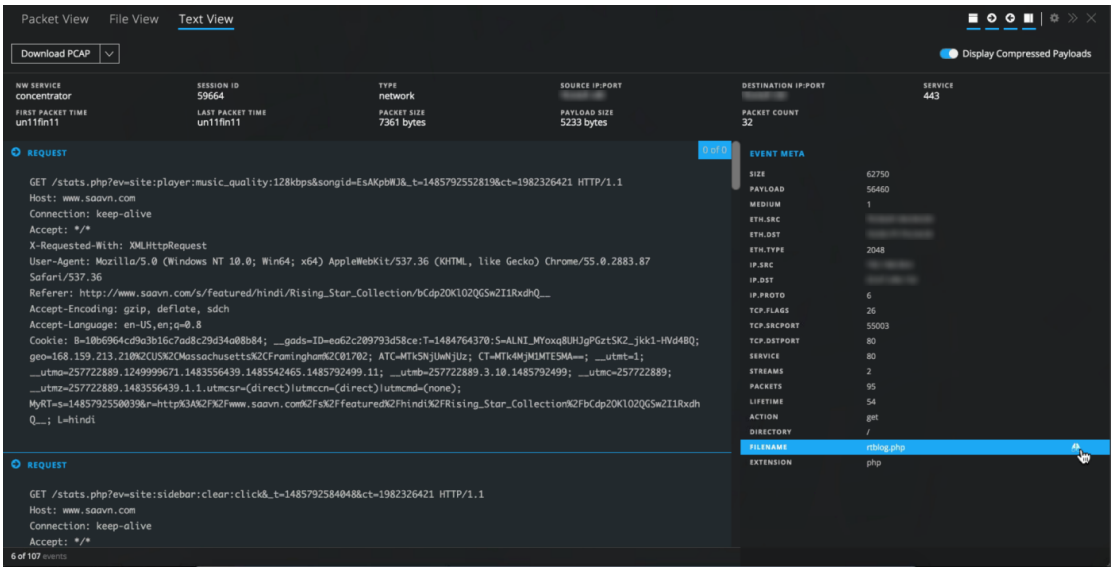
Pour rechercher le texte brut des valeurs méta qui ont déclenché une clé méta :

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



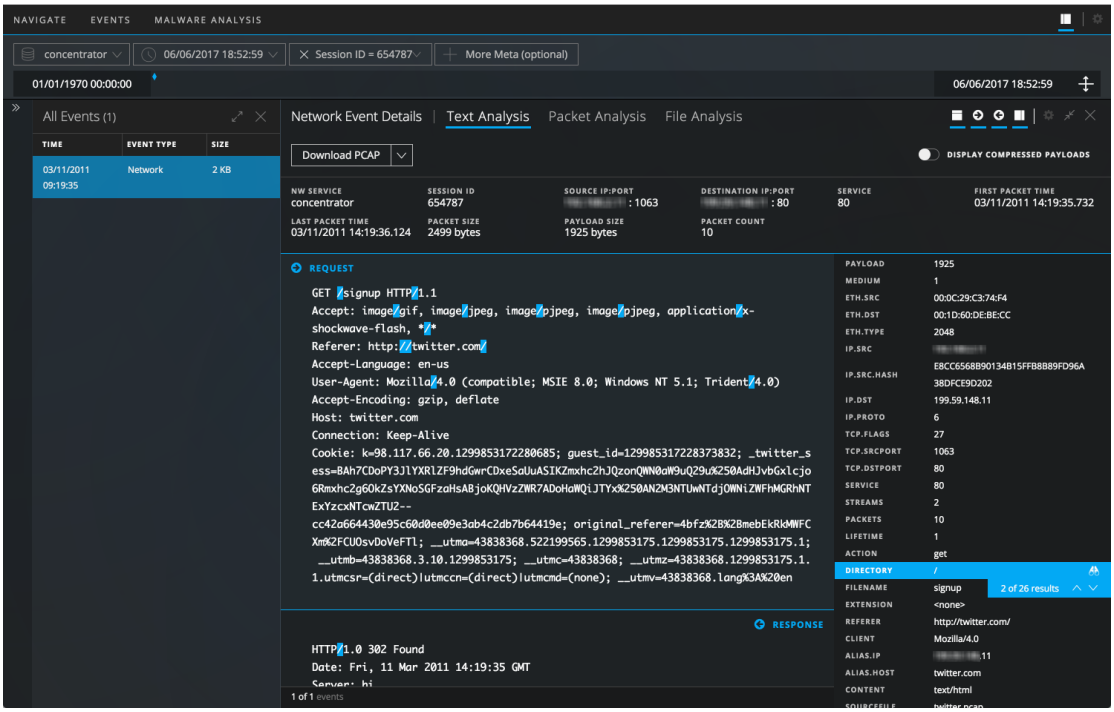
2. Dans la barre d'outils, cliquez sur pour ouvrir le Panneau des métadonnées d'événement.
   Lorsque vous survolez les paires clé méta - valeur méta dans la liste, une icône de jumelles identifie les valeurs qui peuvent être recherchées dans le panneau Analyse de texte.

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 des métadonnées d'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 des métadonnées d'événement et la barre de défilement est visible.



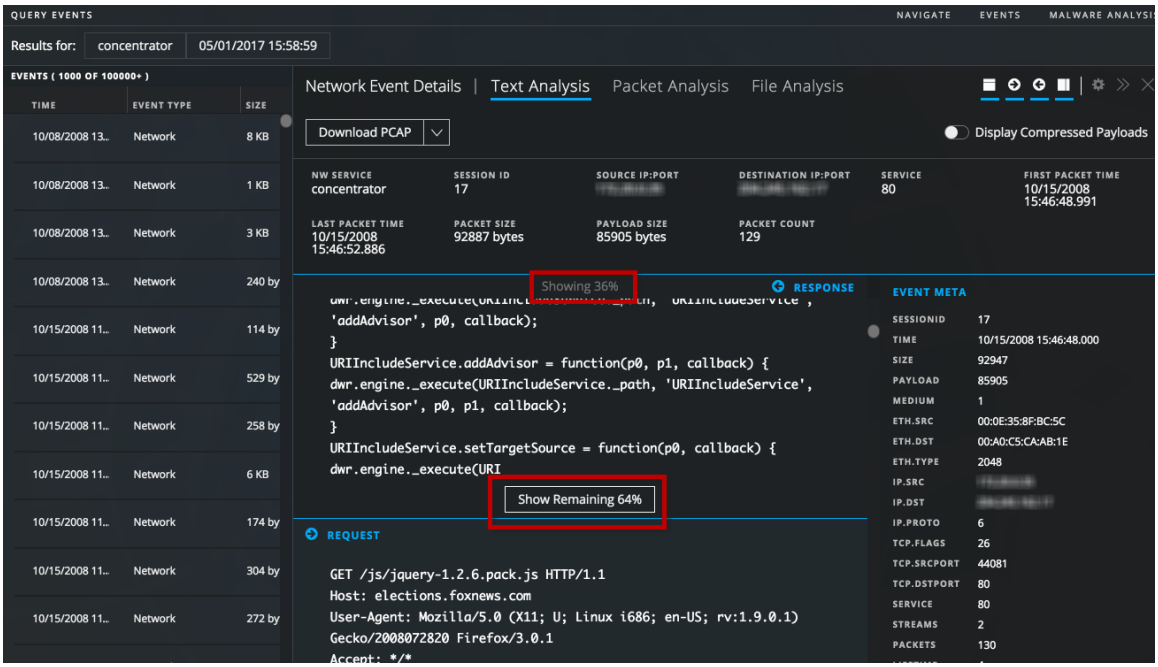
4. Pour supprimer la mise en évidence, fermez le Panneau des métadonnées d'événement, cliquez sur la même paire clé méta/valeur méta dans le Panneau des métadonnées d'événement ou cliquez sur une paire clé méta/valeur méta différente dans le Panneau des métadonnées d'événement.
   La mise en surbrillance 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  .

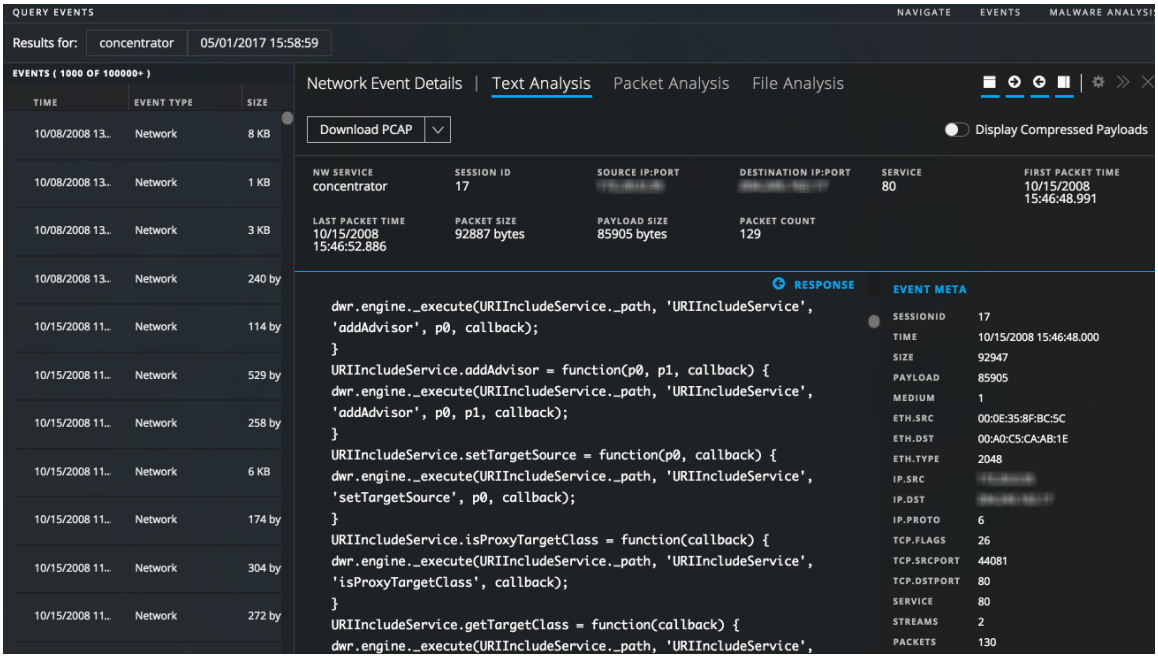
Développer les entrées de texte tronquées dans le panneau Analyse de texte

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 36 % des caractères (les 2 000 premiers) s'affichent. Cliquez sur **Afficher les 64 % restants** pour afficher le reste de l'entrée.



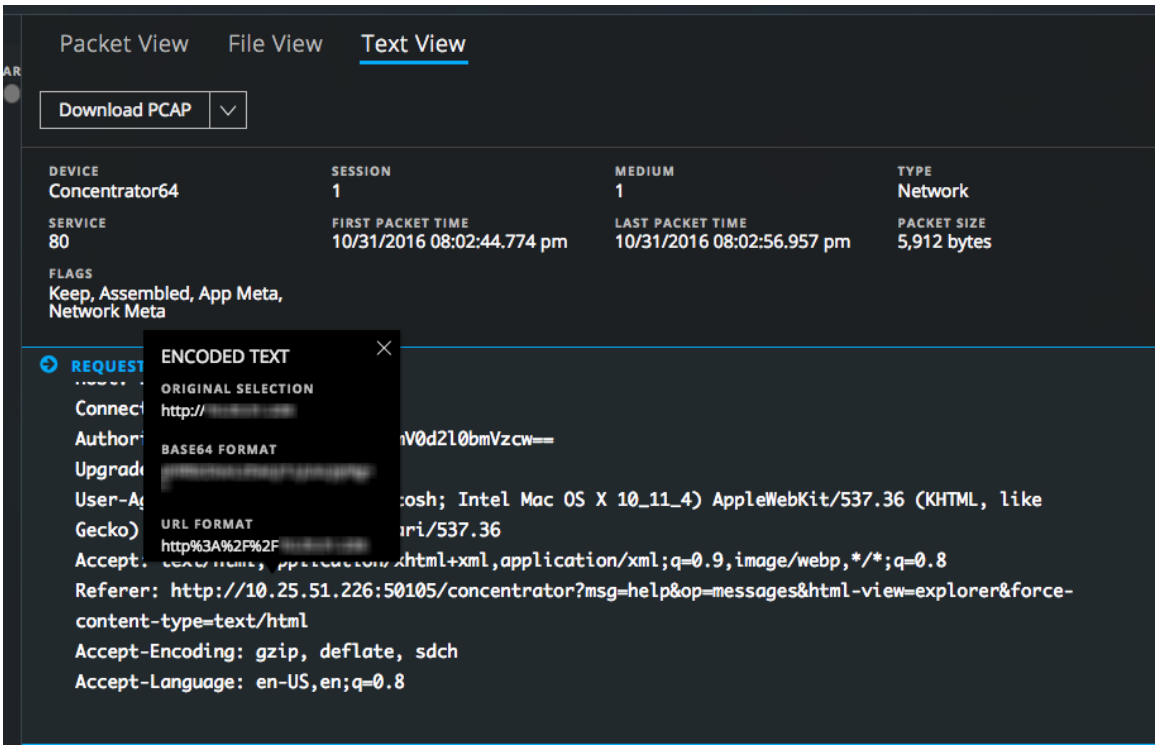
Si vous recherchez des données méta visibles dans le Panneau des métadonnées d'événement alors que le texte est tronqué dans le panneau Analyse de texte, le texte tronqué est recherché. Si les données méta se trouvent dans du texte masqué, l'entrée de texte se développe pour afficher le texte avec les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

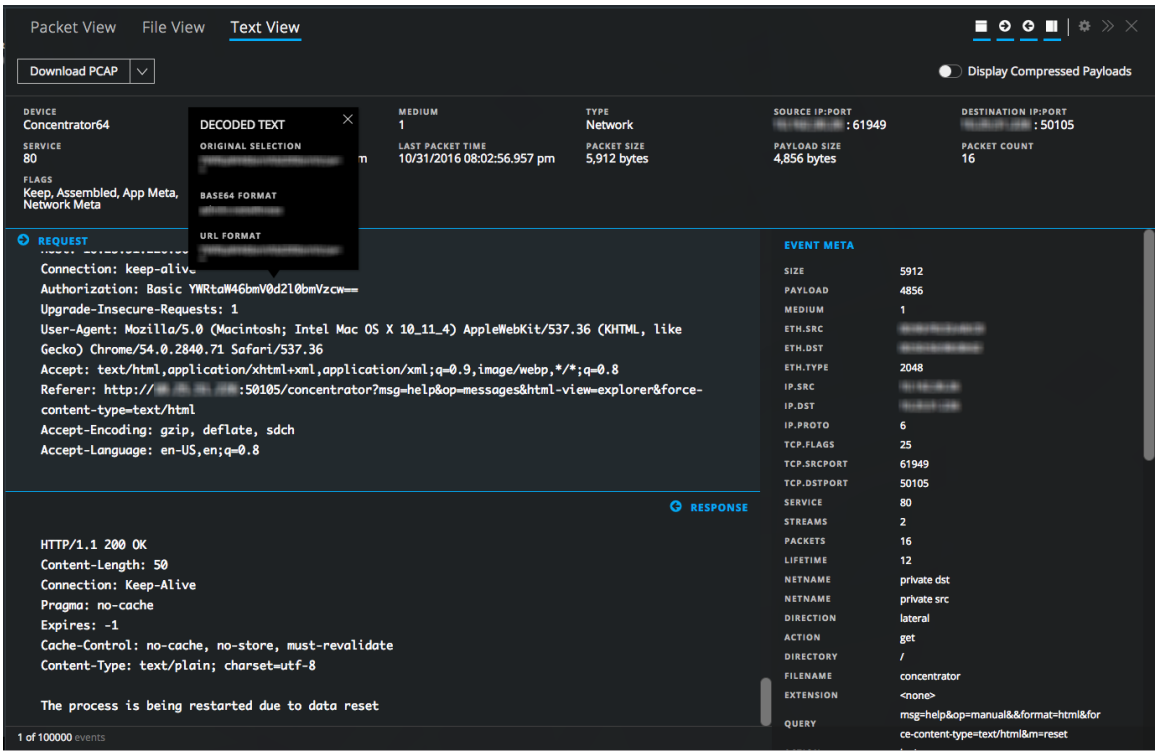
Effectuer un codage et un décodage URL et Base64 dans le panneau Analyse de texte

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.

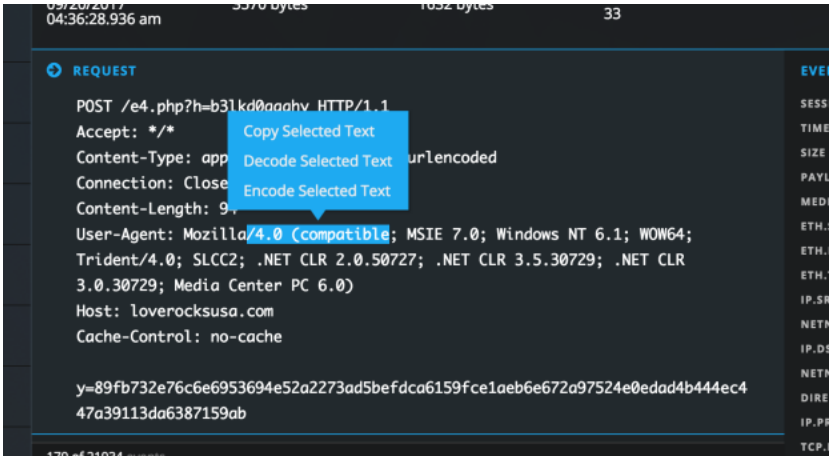
Vous trouverez ci-dessous des exemples d'une zone de survol qui affiche le codage URL et le texte codé Base 64.





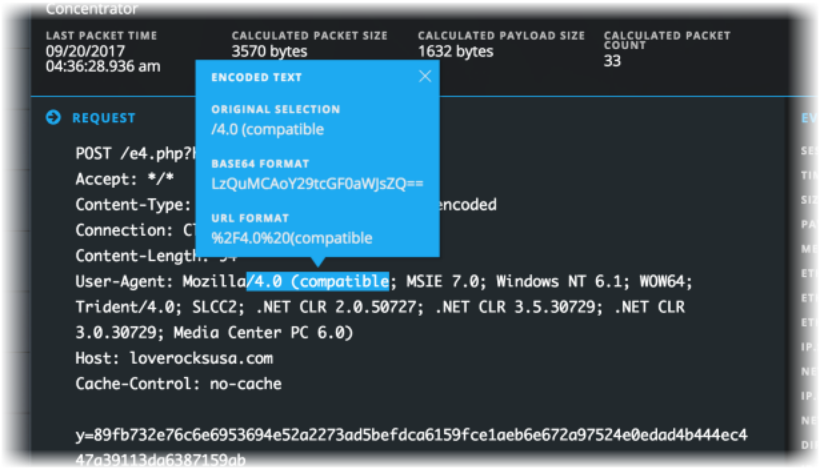
Pour effectuer l'encodage et le décodage dans le panneau Analyse de texte :

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.



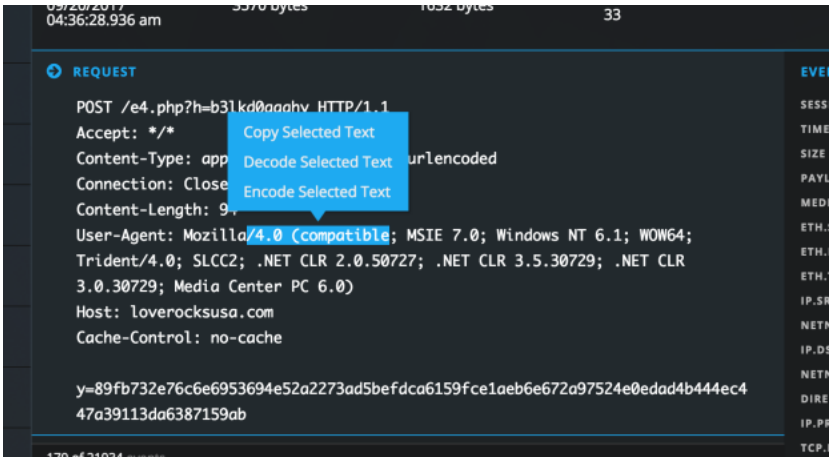
3. Cliquez sur **Encoder le texte sélectionné.**
   Le texte encodé s'affiche dans une zone de survol, qui reste en place jusqu'à ce que vous cliquiez sur le ■, sélectionnez un autre texte dans le panneau Analyse de texte, fermiez le

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 contextuel.



b. Faites glisser pour sélectionner du texte, puis sélectionnez **Décoder le texte sélectionné** ou **Coder le texte sélectionné**. Dans le menu contextuel, 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.

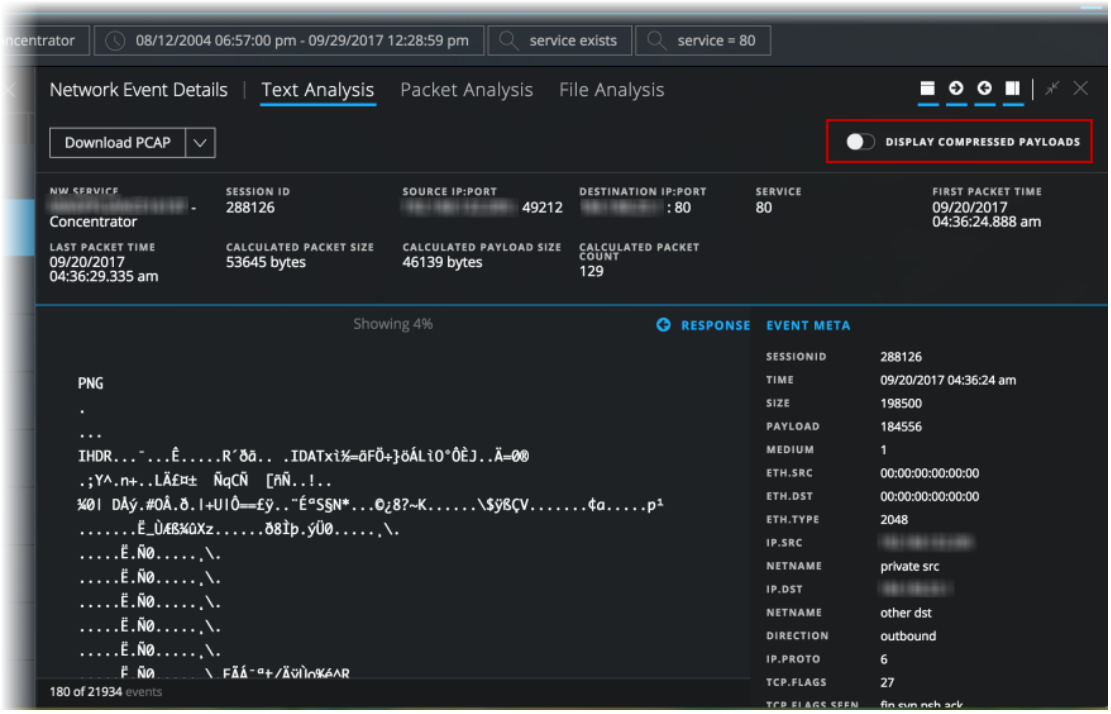
Afficher le texte décompressé pour une session de réseau HTTP dans le panneau Analyse de texte

Lorsque le contenu d'une session de réseau HTTP est compressé et que vous affichez le panneau Analyse de texte, NetWitness Suite 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.

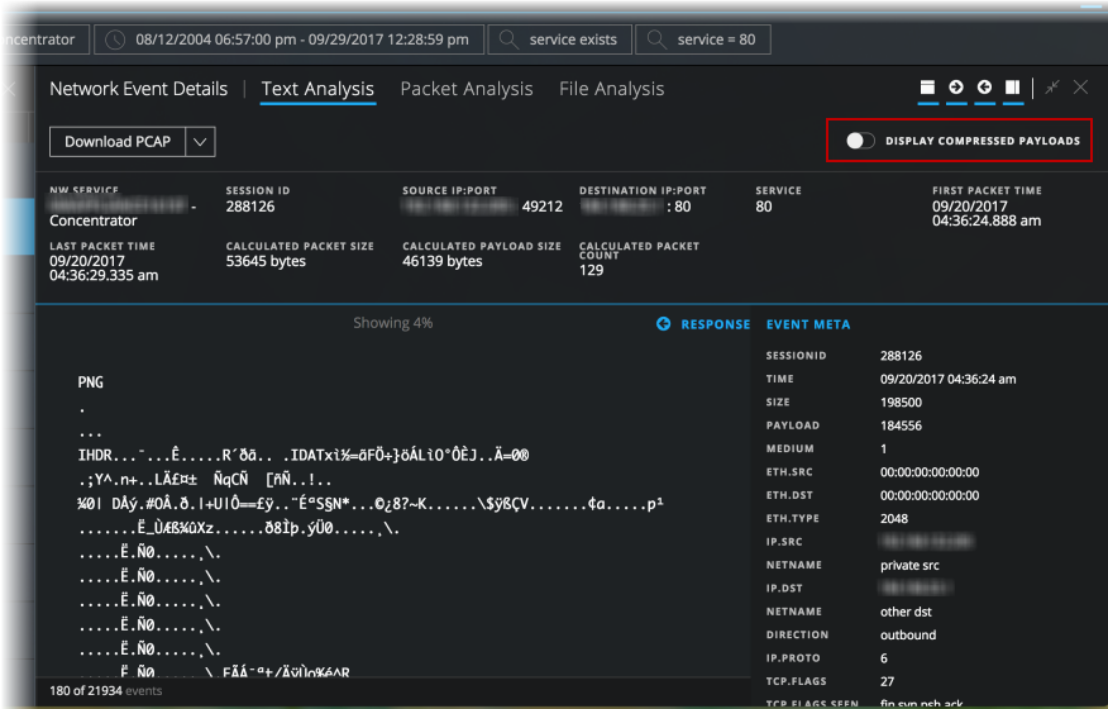
Remarque : Le texte décompressé n'est pas disponible pour le panneau Analyse de paquets, le panneau Analyse de fichiers, les sessions de réseau non-HTTP et les données des fichiers log.

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.

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.

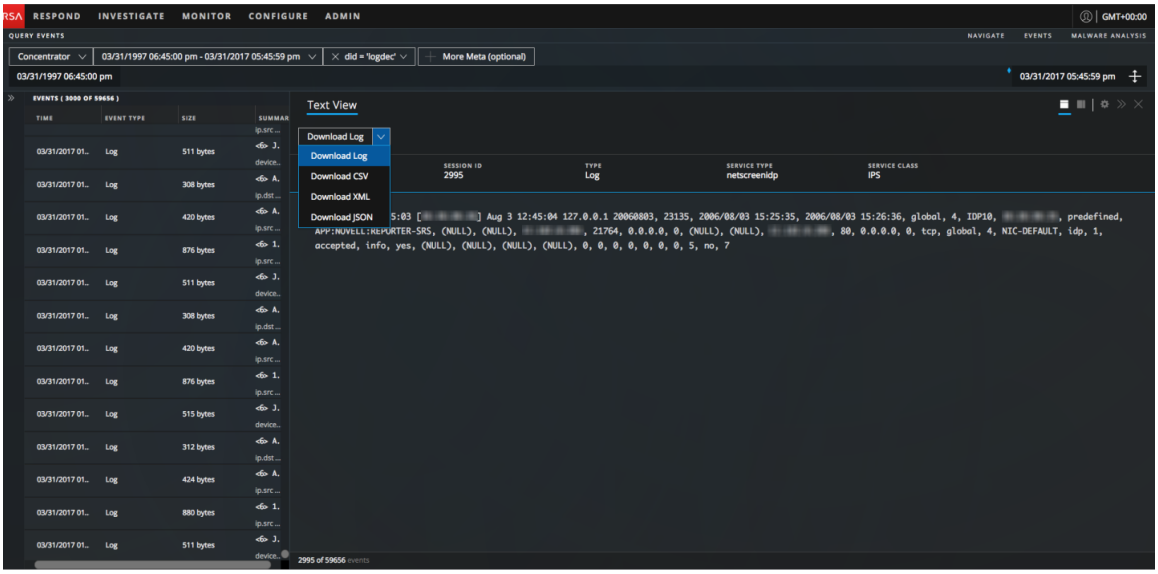
Télécharger un log dans le panneau Analyse de texte

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 Télécharger le log :

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

Remarque : 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.

Il s'agit d'un exemple de reconstruction de log avec les options de menu Télécharger le log.



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.

Remarque : Les fichiers exécutée depuis longtemps ou téléchargés historiquement ne sont pas téléchargeables.

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>
```

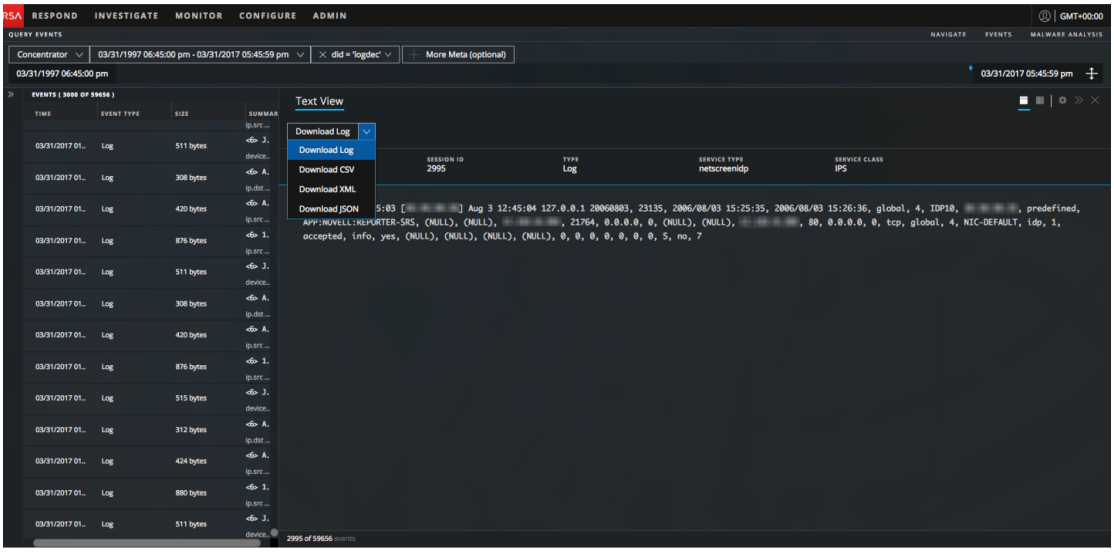
où :

- `<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="10.4.30.65"`.

Pour télécharger le log d'une session :

1. 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 **Télécharger le log** 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.

Télécharger les fichiers de données de réseau dans le panneau d'analyse de texte ou le panneau d'analyse de paquet

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 requête**.
- La charge utile de réponse en tant que fichier `*.payload2` à l'aide de l'option **Télécharger la charge utile de 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 :

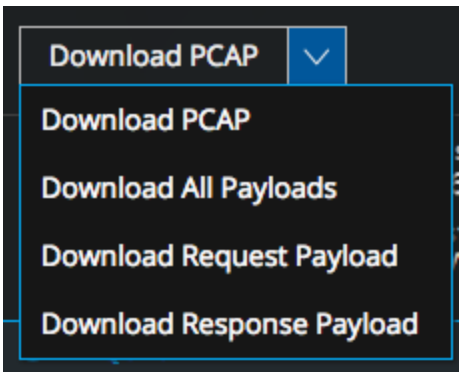
- `<service-ID or host name>` est le nom du service (par exemple, Concentrator ou Broker) où la session a été enregistrée.
- `SID<n>` est le numéro d'ID de la session.
- `<filetype>` est pcap, payload, payload1 ou payload2.

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 Tâches. 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 :

1. 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.



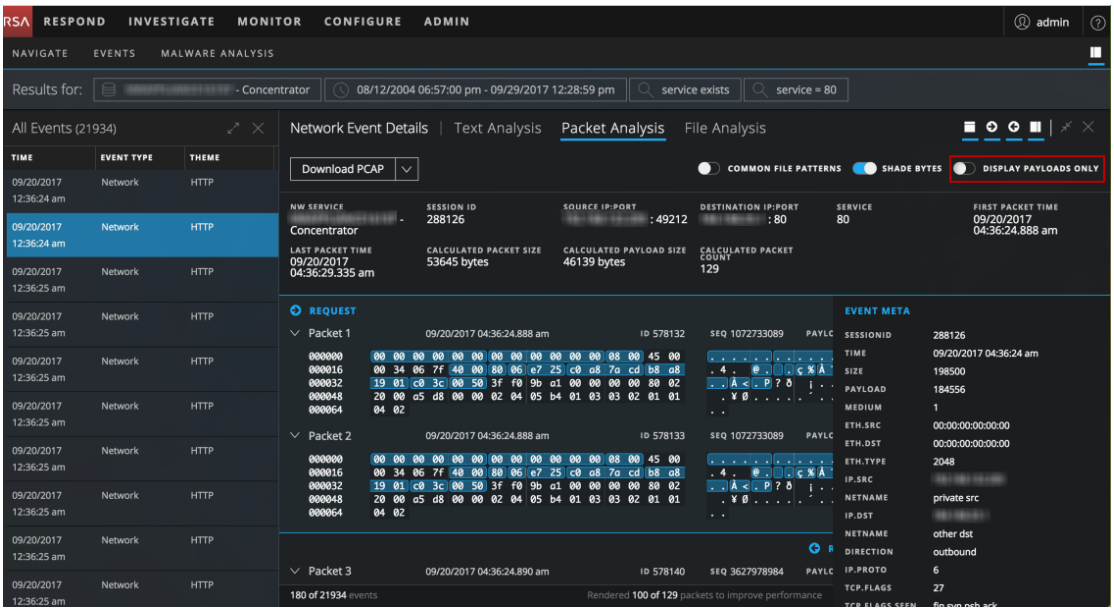
   Le fichier de données réseau est téléchargé sur votre système de fichiers local dans le format spécifié.

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

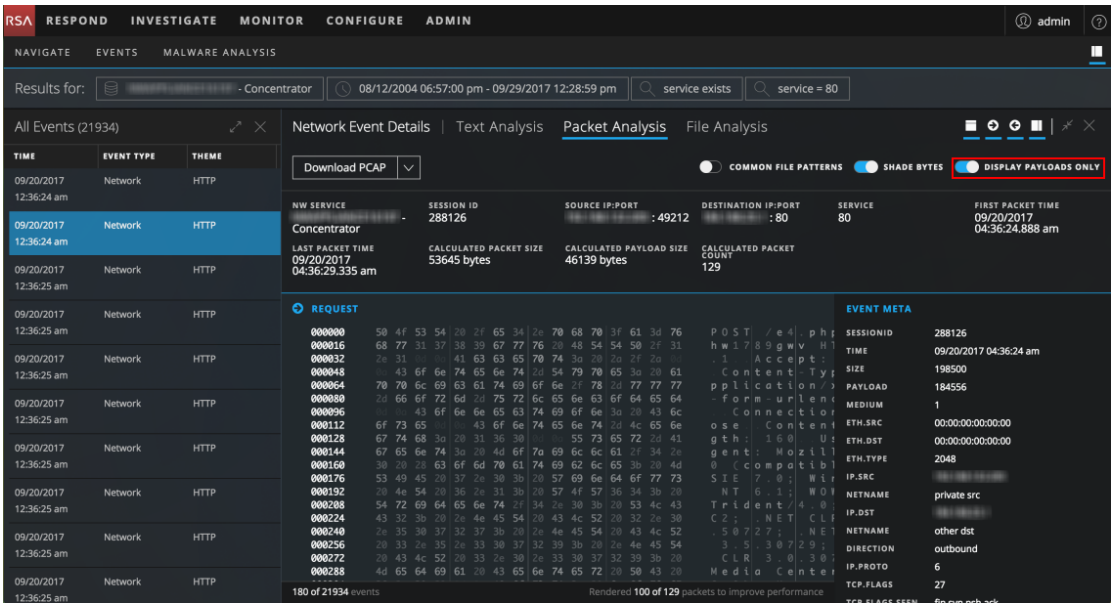
Lors de l'affichage d'une reconstruction d'une session réseau dans le panneau Analyse de paquets, vous pouvez choisir d'afficher uniquement la charge utile principale de chaque paquet. Par défaut, l'en-tête de paquet et les octets de pied de page s'affichent pour chaque paquet. Vous pouvez les masquer en cliquant sur le bouton Afficher des 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.

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.

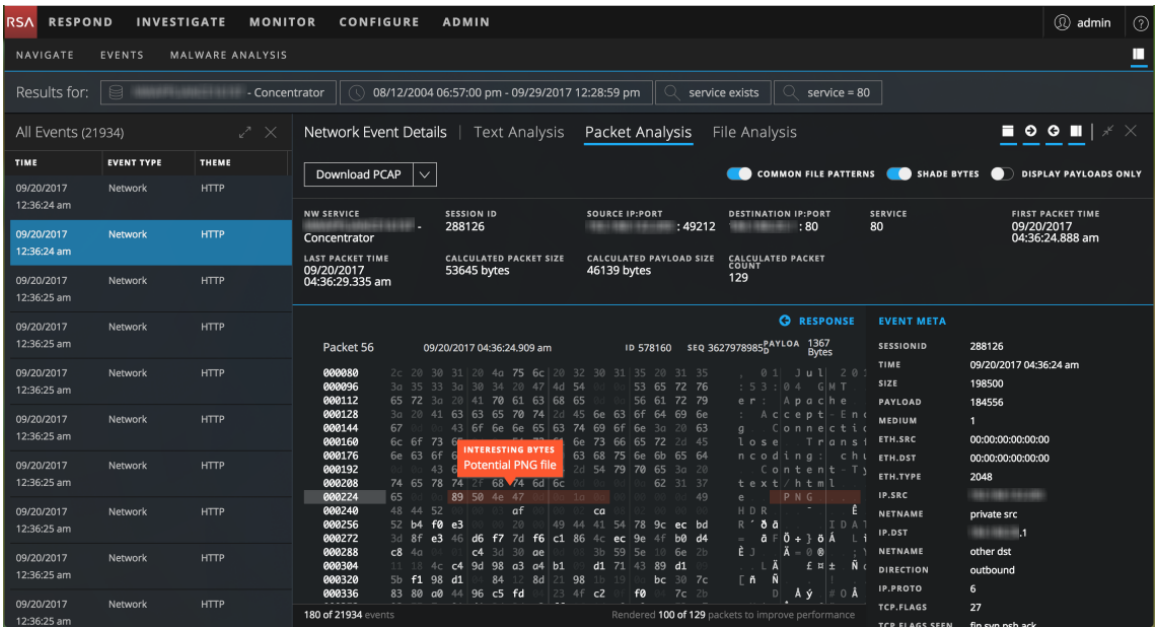


2. Pour modifier la vue afin d'afficher uniquement la charge utile pour chaque paquet, cliquez sur le commutateur **Afficher les charges utiles uniquement**.
   La vue change pour que seule la charge utile soit visible. Les paquets contigus du même côté sont concaténés pour rendre la charge utile plus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

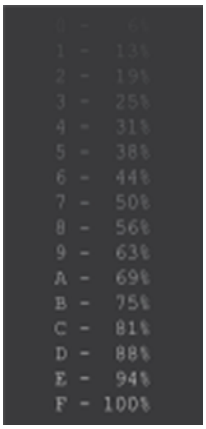


Afficher les octets mis en surbrillance dans le panneau Analyse des paquets

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.



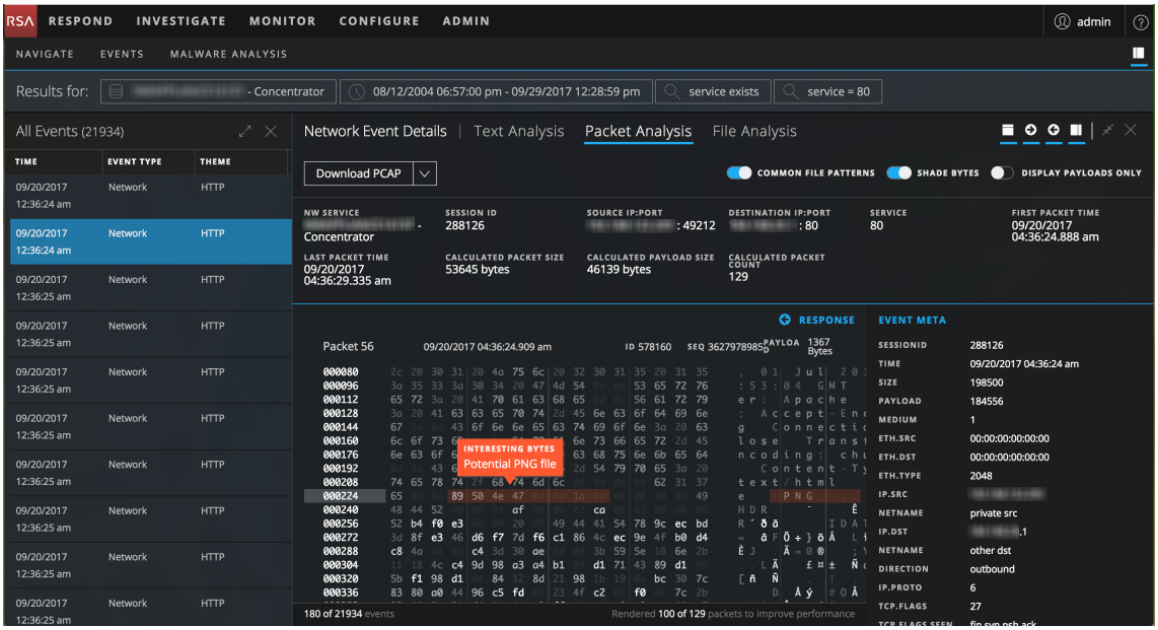
L'option Octets d'ombrage ajoute un ombrage pour identifier les différents octets hexadécimaux (00 à FF) à l'aide des degrés de mise en surbrillance. Les octets près de la plage inférieure sont plus transparents et les octets proches de 255 sont plus opaques. Les octets hexadécimaux et ASCII sont grisés.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



Le commutateur Octets ombrés contrôle l'ombrage d'octets. Lorsque vous activez ou désactiver Octets ombrés, 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 courants 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
JPEG/Exif	45 78 69 66	Exif

Type de fichier	Signature hexadécimale	Codage ASCII
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 :

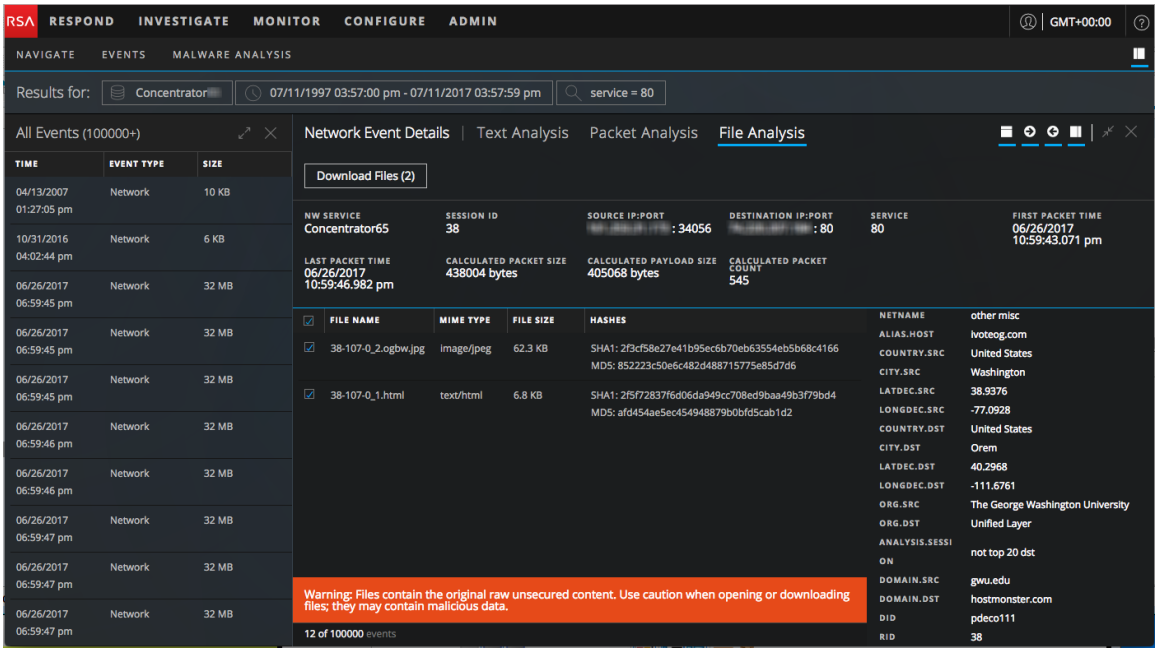
1. Accédez au panneau Analyse de paquets et activez l'option **Modèles de fichier communs**. S'il existe plus d'un élément mis en surbrillance dans la vue, tous sont affichés.
2. Pour afficher la boîte de survol, placez le curseur sur la mise en surbrillance.

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 sous cette forme 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`

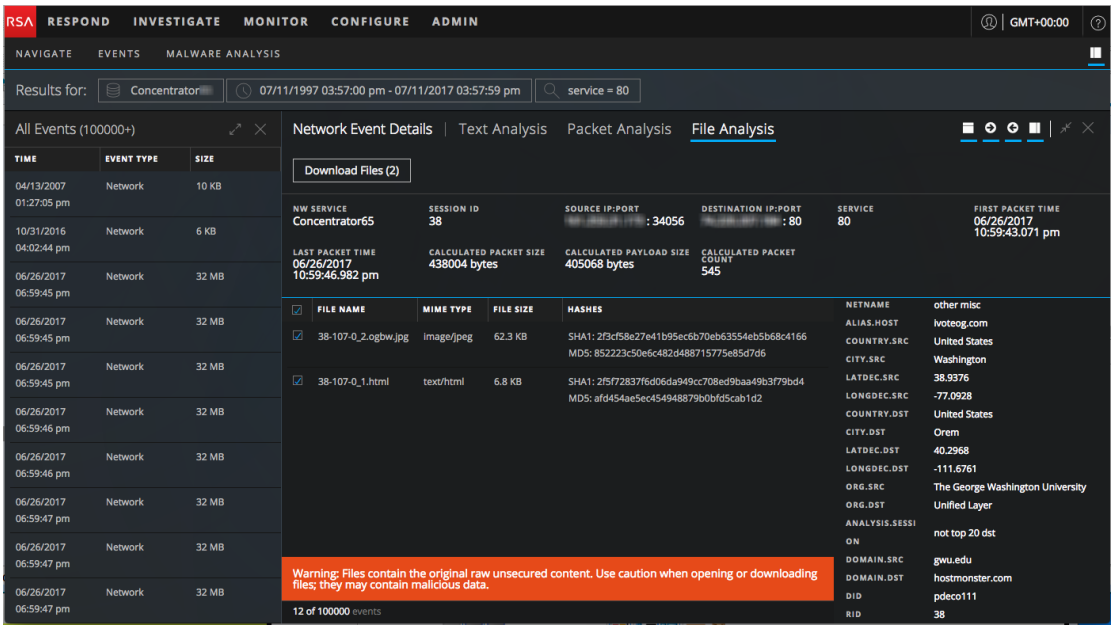
où :

- `<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`.

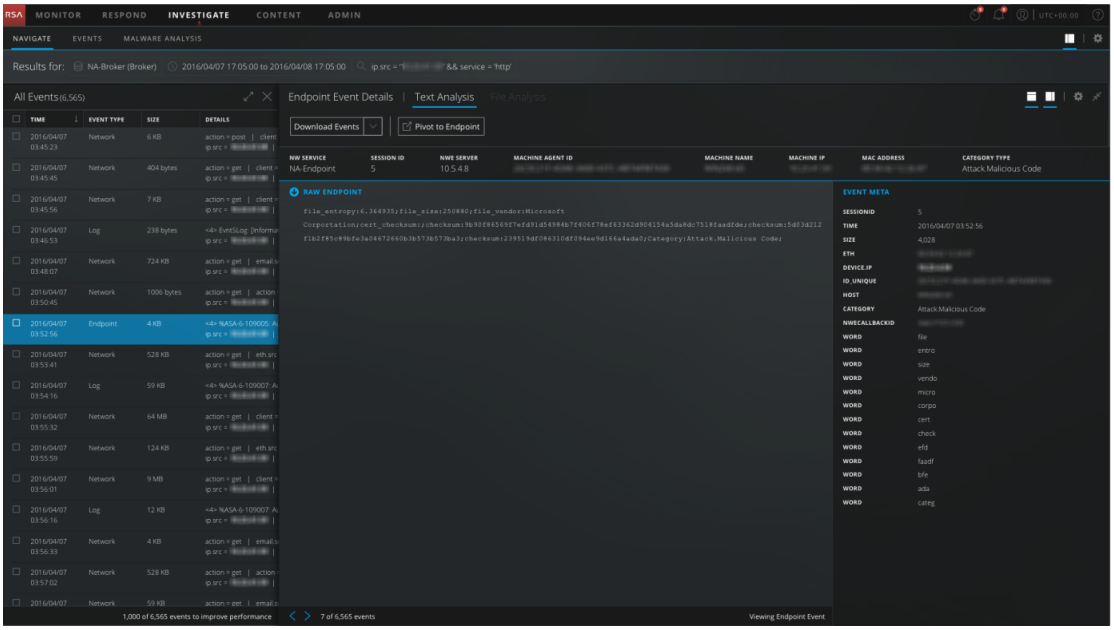
Ouvrir un événement de point de terminaison dans l'application de point de terminaison NetWitness

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.

Remarque : 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.

Pour ouvrir un événement dans NetWitness Endpoint :

1. Pour rechercher des événements de point de terminaison, sélectionnez **Requête** dans la barre d'outils de la vue Naviguer.
2. Dans la boîte de dialogue **Requête**, sélectionnez **Avancé** et saisissez l'une des requêtes suivantes : les données de point de terminaison `nwe.callback_id exists` ou `device.type='nwendpoint'`
   s'affichent dans le panneau Valeurs.
3. Cliquez sur un événement avec le bouton droit de la souris, puis sélectionnez **Analyse d'événements** dans le menu contextuel.
   L'Analyse d'événements s'ouvre avec l'événement sélectionné affiché dans l'Analyse de texte.



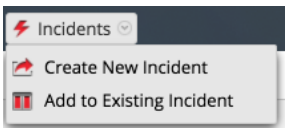
4. Dans l'en-tête d'événement, cliquez sur **Pivoter vers le point de terminaison.**
   Un nouvel onglet de navigateur avec l'URL `ecatui://<id>` s'ouvre et le client Thick NWE se lance.

Ajouter des événements à un incident pour obtenir une réponse

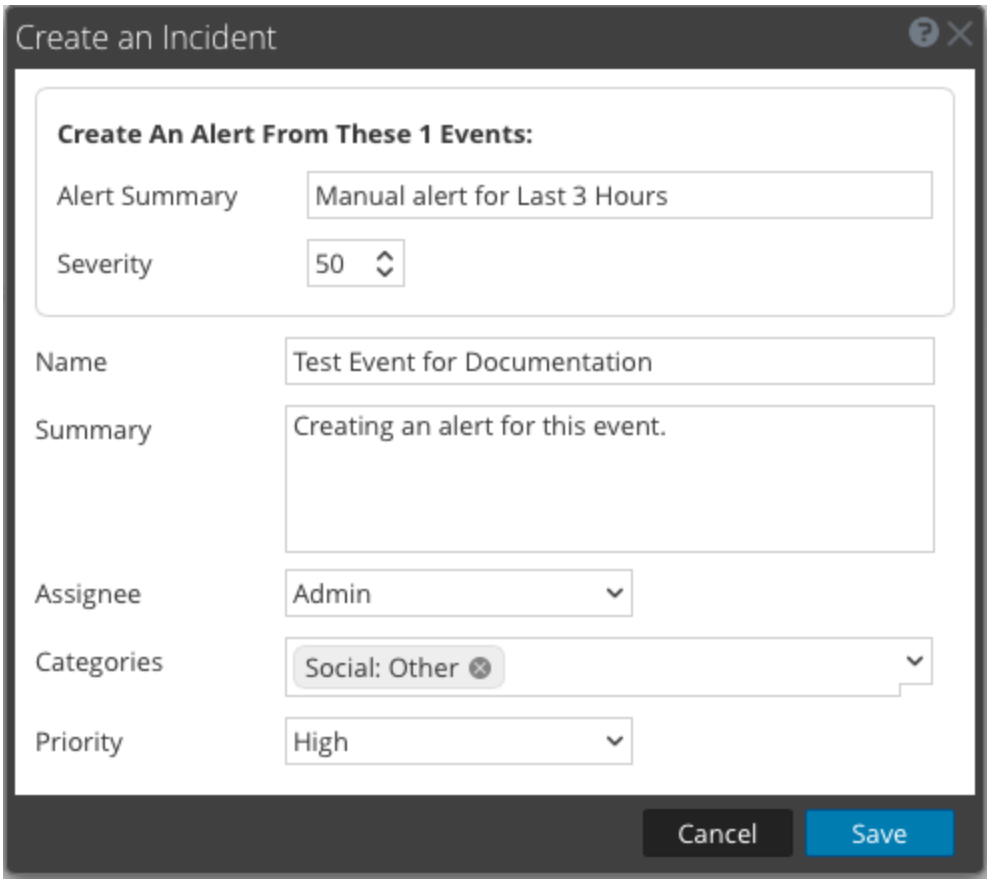
Lors d'une procédure d'enquête dans Vue Événements, vous pouvez sélectionner un ou plusieurs événements et créer un incident qui est disponible pour les responsables de la réponse aux incidents dans Répondre. Vous pouvez également ajouter des événements à un incident existant dans Répondre, auquel vous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

Exporter des 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.

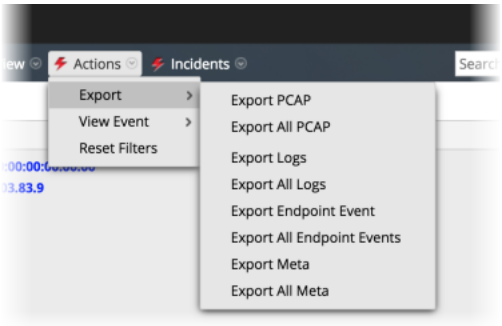
La fonction d'exportation recherche dans le service toutes les sessions comprises dans la période et le point d'extraction sélectionnés afin d'extraire le contenu de chaque session. Les détails exportés sont affectés par la plage temporelle et le point d'extraction au moment de l'exportation. Dans la 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 Suite 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.

   Un message vous informe que le PCAP est en cours de téléchargement.

Mener une analyse Malware Analysis

Les analystes peuvent utiliser le service RSA NetWitness Suite Malware Analysis pour détecter les malware dans certains fichiers et données.

Les analystes qui mènent une analyse avec NetWitness Suite Malware Analysis doivent disposer des rôles et autorisations du système appropriés pour leur compte utilisateur. Voir Rôles et autorisations pour les analystes Malware.

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.

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 Suite 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 Suite 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. Enquêter 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.

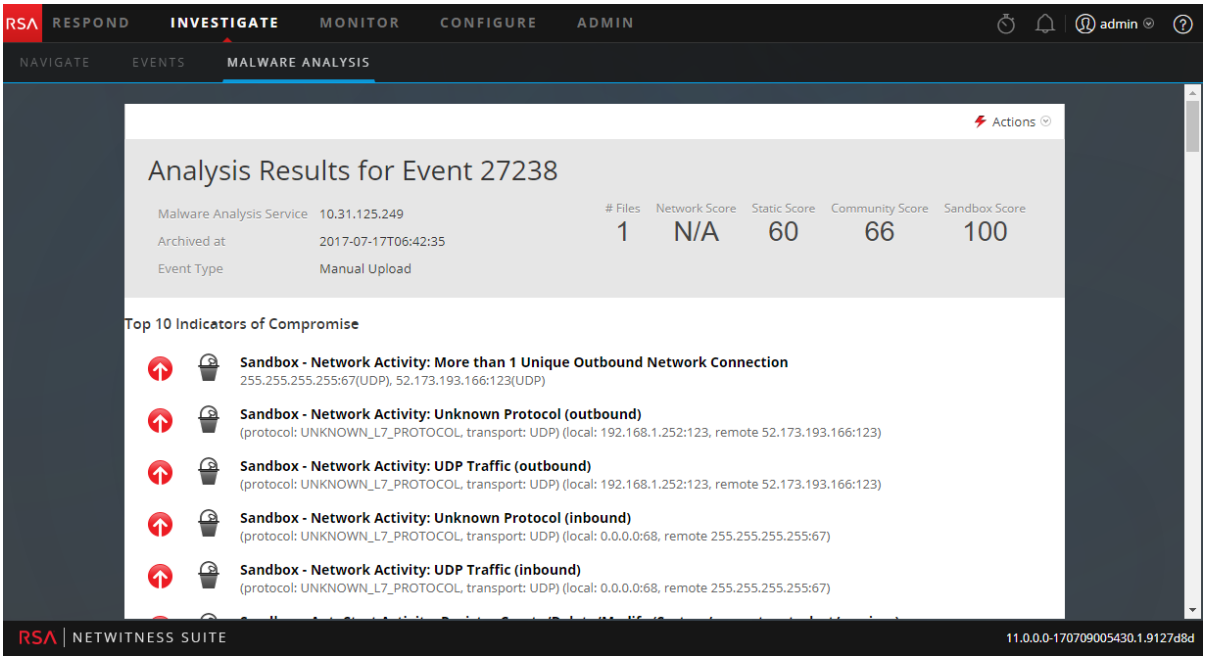
Lancer une procédure d'enquête sur les malware à partir d'un dashlet Malware Analysis

Il existe une condition préalable à respecter pour cette procédure : l'un des dashlets suivants doit être visible dans le tableau de bord NetWitness Suite 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 Suite 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 Suite*.

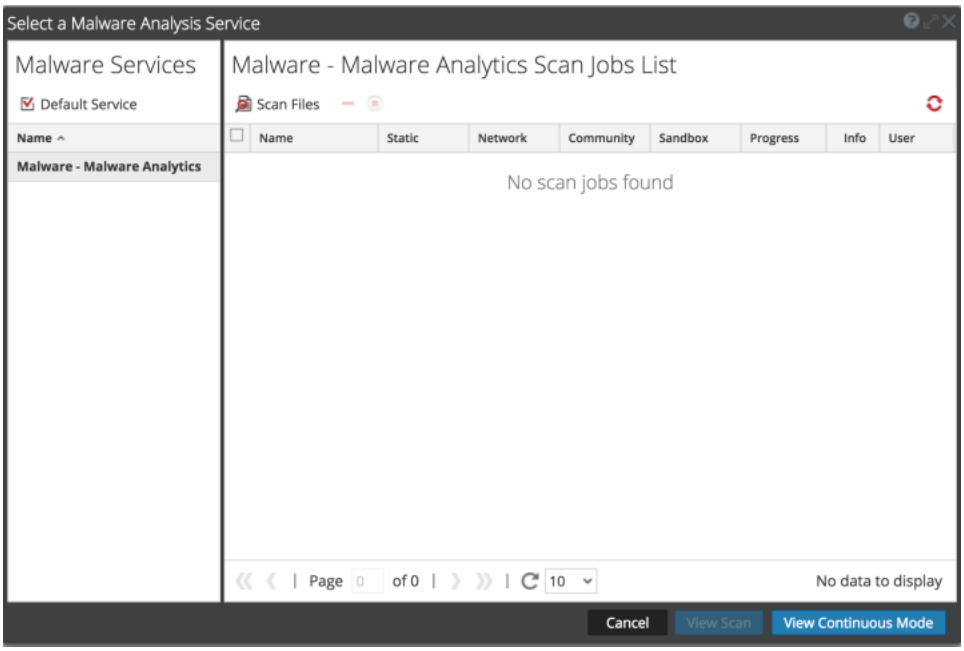
Pour en savoir plus sur les façons dont vous pouvez configurer et filtrer les informations dans les dashlets de la vue Malware Analysis, reportez-vous à la section Filtrer les données de dashlet dans la vue Récapitulatif des événements.

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.

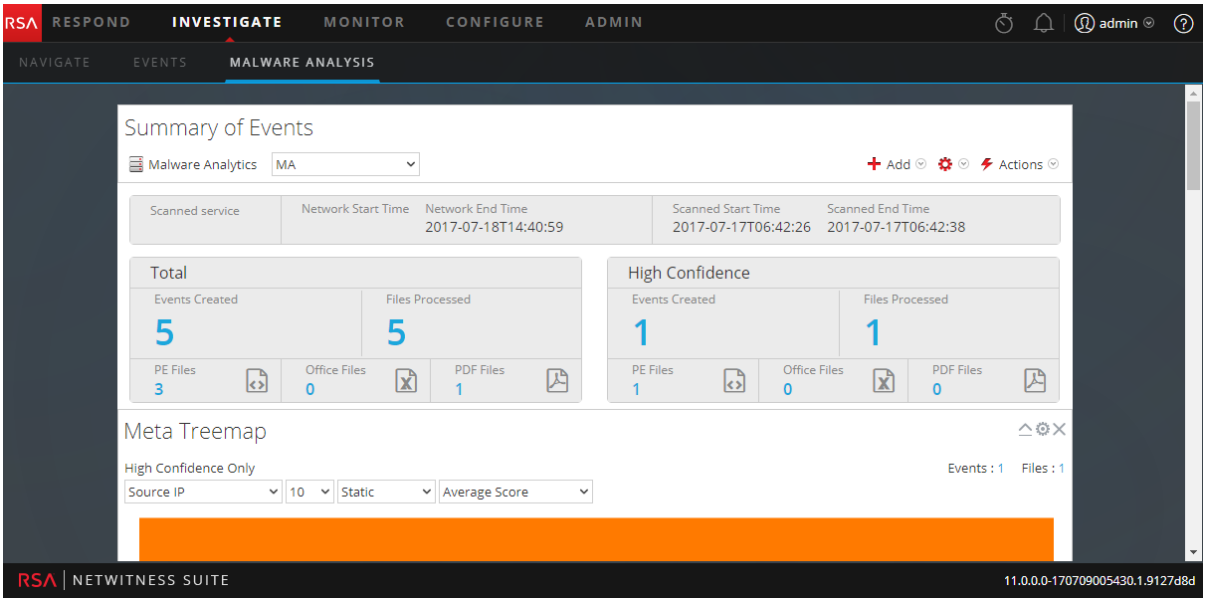
Lancer une procédure d'enquête Malware Analysis (aucun service par défaut)

Pour commencer une procédure d'enquête sans service par défaut :

1. Sélectionnez **Investigation > 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.

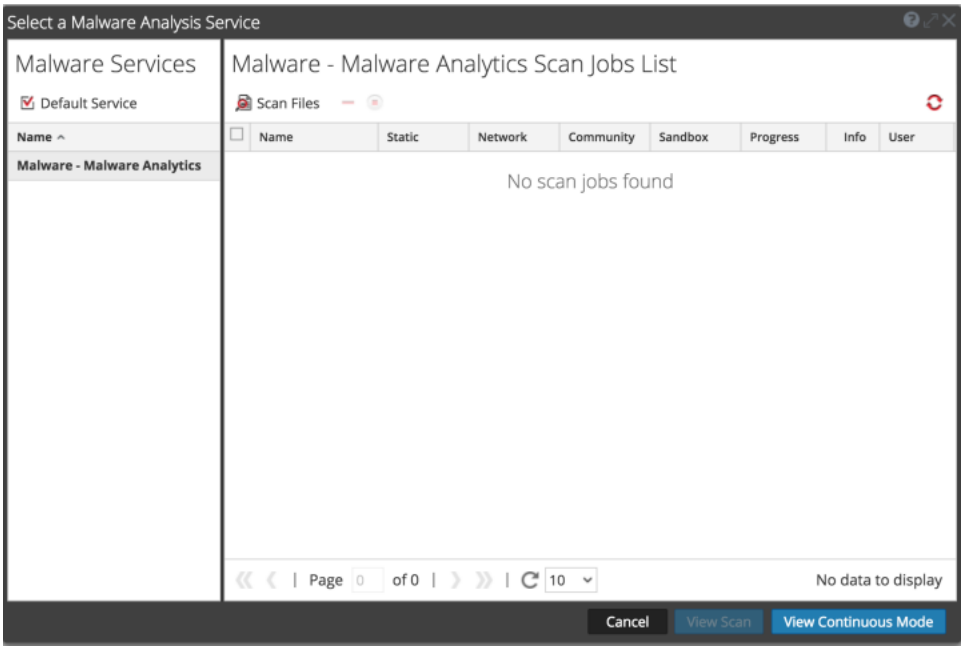


Définir ou effacer le service par défaut

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

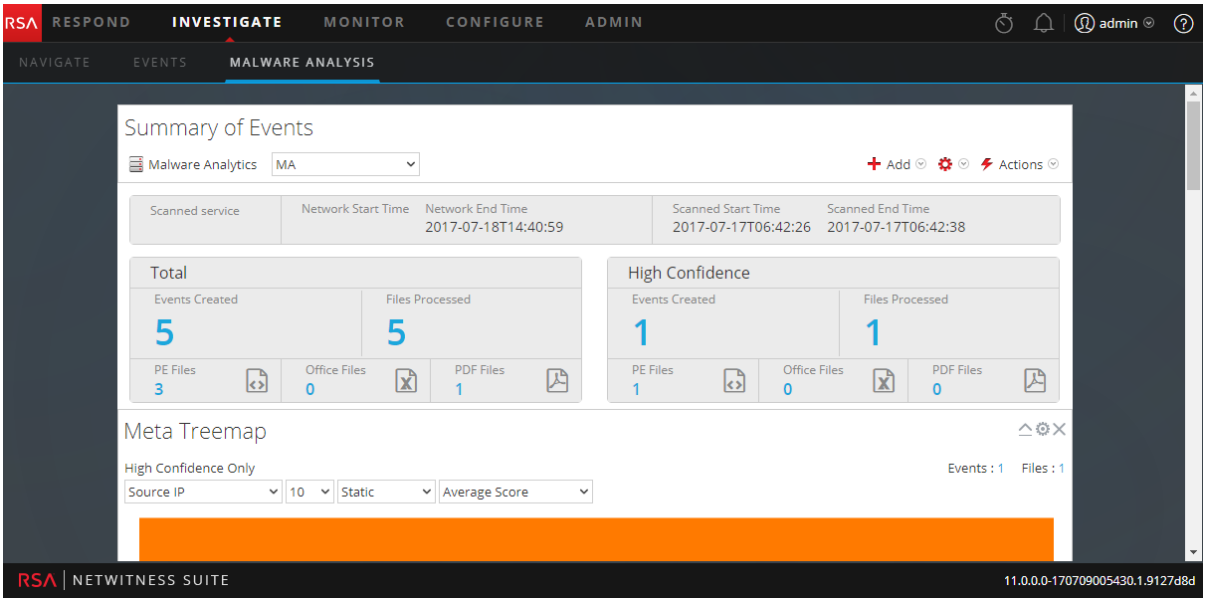
Un analyste de malware possédant l'autorisation `Initiate Malware Analysis Scan` peut télécharger des fichiers à analyser à l'aide de l'option Analyser des fichiers dans la boîte de dialogue Sélectionner un service Malware Analysis (voir Télécharger des fichiers pour l'analyse Malware Analysis. Un administrateur 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. Sélectionnez **Investigation > Malware Analysis**.

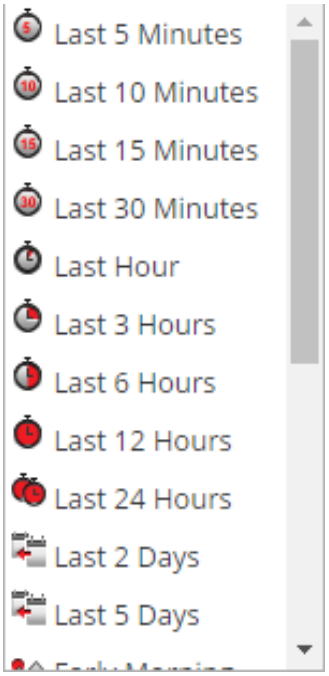
   La vue Récapitulatif des événements correspondant à l'analyse continue du service sélectionné s'affiche avec les dashlets par défaut ouverts. Chaque utilisateur peut ajouter, modifier et supprimer des dashlets par défaut, qui persistent à travers différentes procédures d'enquête. Les utilisateurs peuvent 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 .

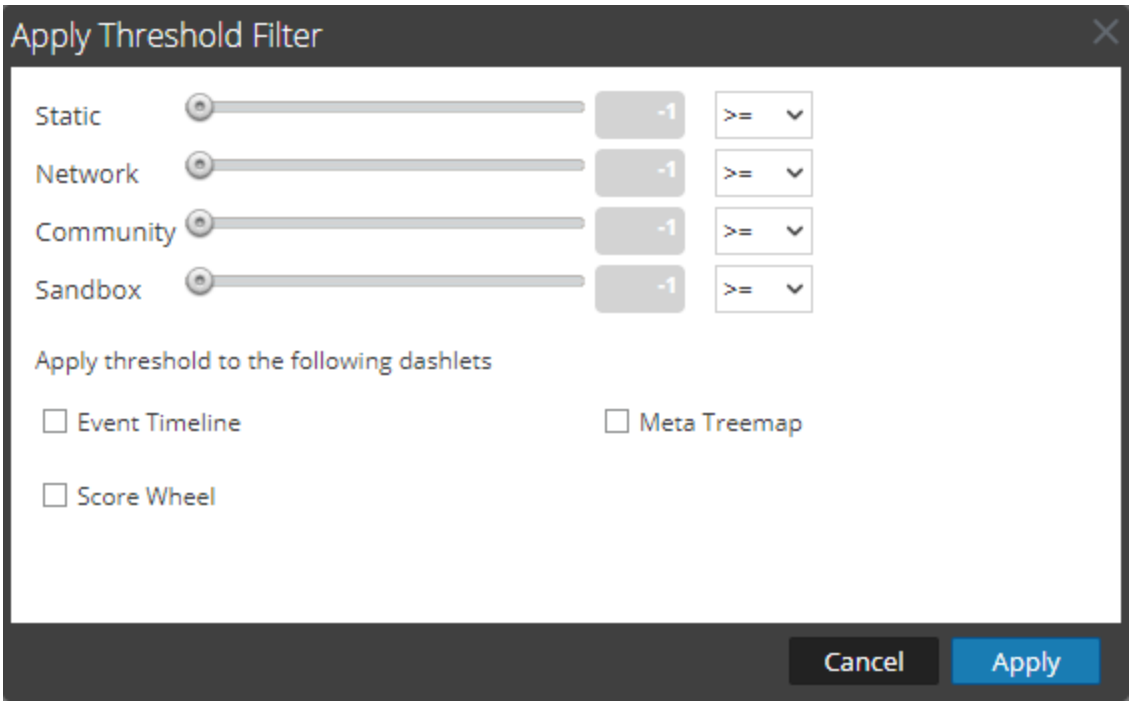
Appliquer un filtre de seuil aux résultats d'analyse en mode continu

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 **Apply**.

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 :

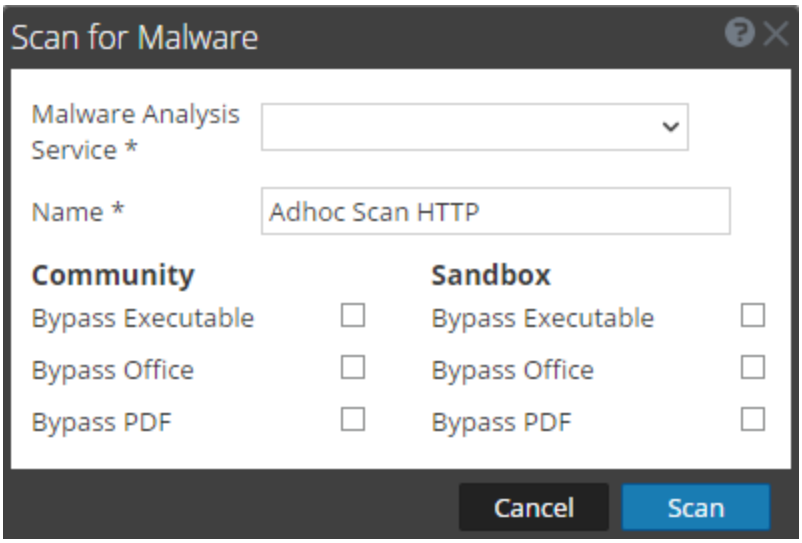
1. Sélectionnez **Actions > Supprimer l'analyse**.

   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.



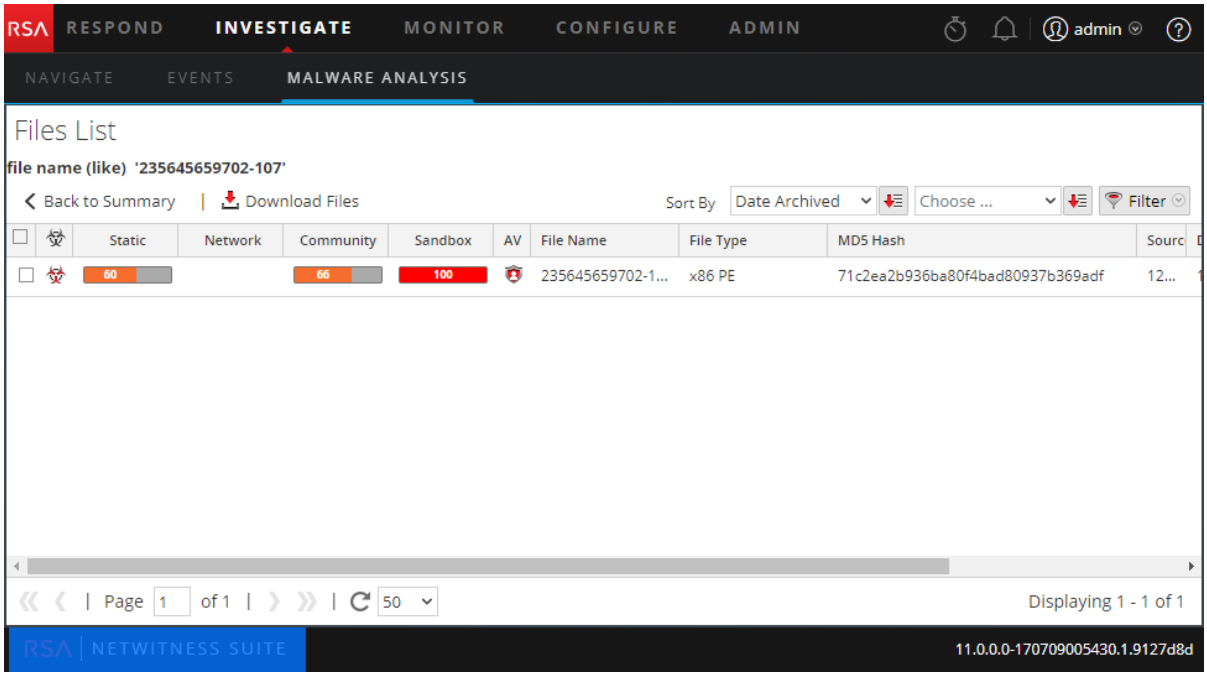
2. Sélectionnez les paramètres de contournement à utiliser pour la nouvelle analyse, puis cliquez sur **Analyser**.
   Malware Analysis réinitialise le cache et resoumet le fichier pour une nouvelle analyse. Les tâches d'analyse sont ajoutées à la file d'attente des tâches.
3. Une fois la tâche terminée, 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.

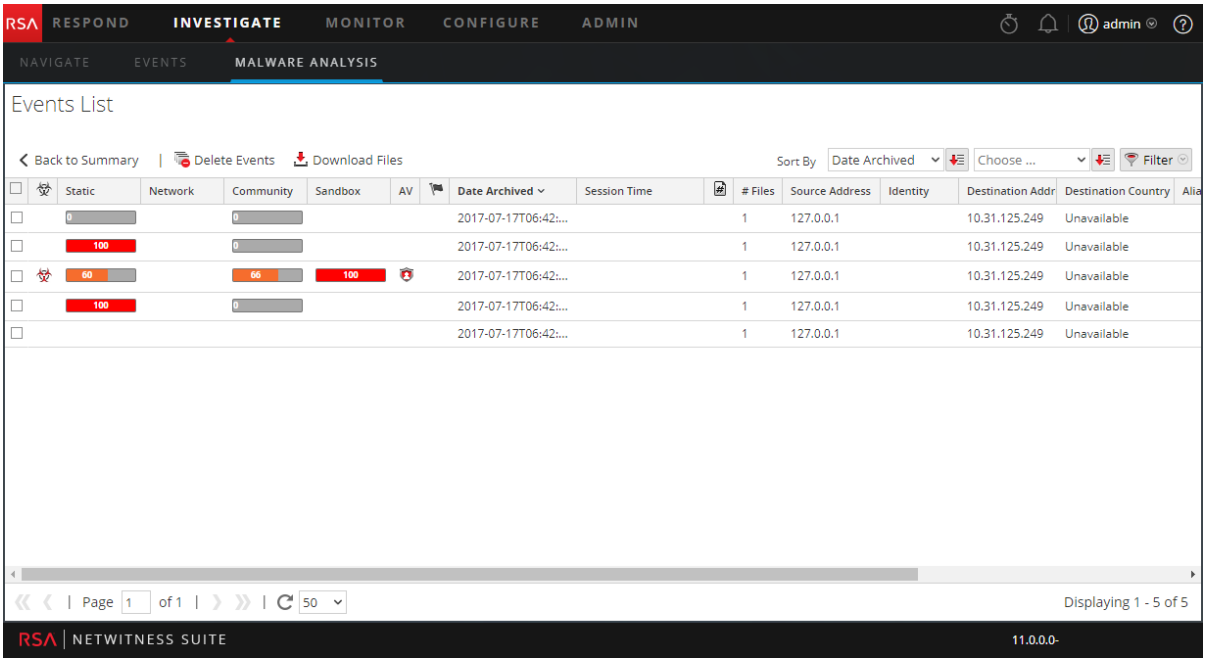
Pour revenir à la vue Récapitulatif des événements, cliquez sur **Retour au récapitulatif**.

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.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
NAVIGATE
EVENTS
MALWARE ANALYSIS
Events List
Back to Summary
Delete Events
Download Files
Sort By
Date Archived
Choose ...
Filter
Static
Network
Community
Sandbox
AV
Date Archived
Session Time
Files
Source Address
Identity
Destination Addr
Destination Country
2017-07-17T06:42:...
1
127.0.0.1
10.31.125.249
Unavailable
Page 1 of 1
50
Displaying 1 - 5 of 5
RSA | NETWITNESS SUITE
11.0.0.0-

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 1.7 (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 1.7 (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.

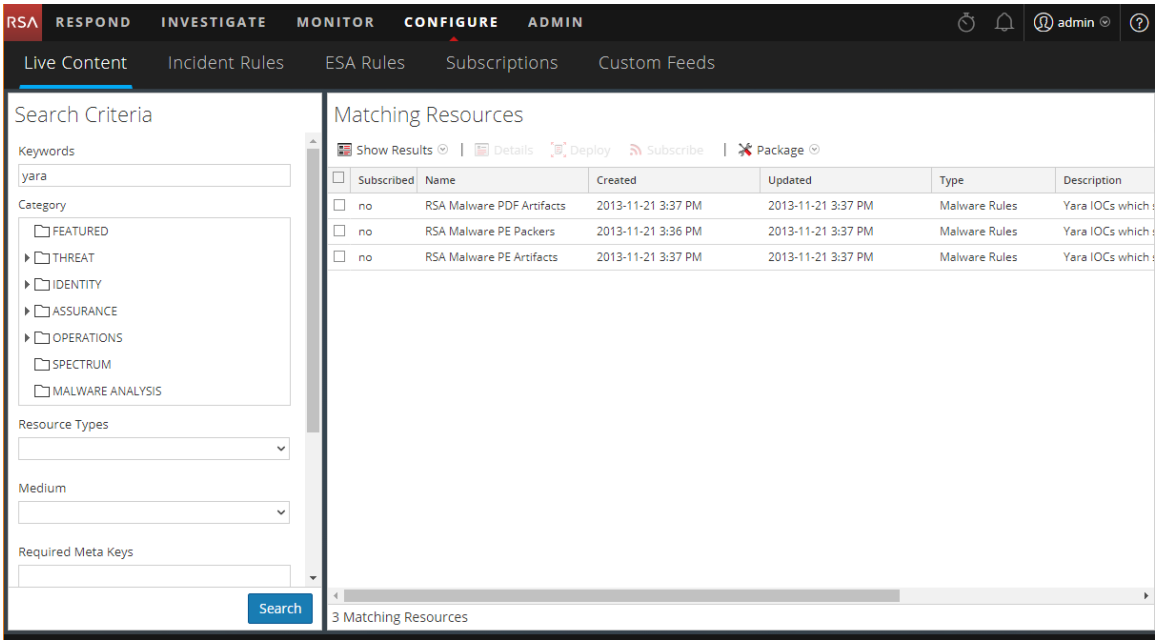
Remarque : Reportez-vous à l'URL suivante pour les ressources YARA : https://code.google.com/p/yara-project/downloads/list. NetWitness Suite utilise YARA 1.7 et non pas YARA 2.0.

Contenu YARA

RSA Live contient 3 ensembles de règles Yara :

- Packers PE
- Artefacts PDF
- Artefacts PE

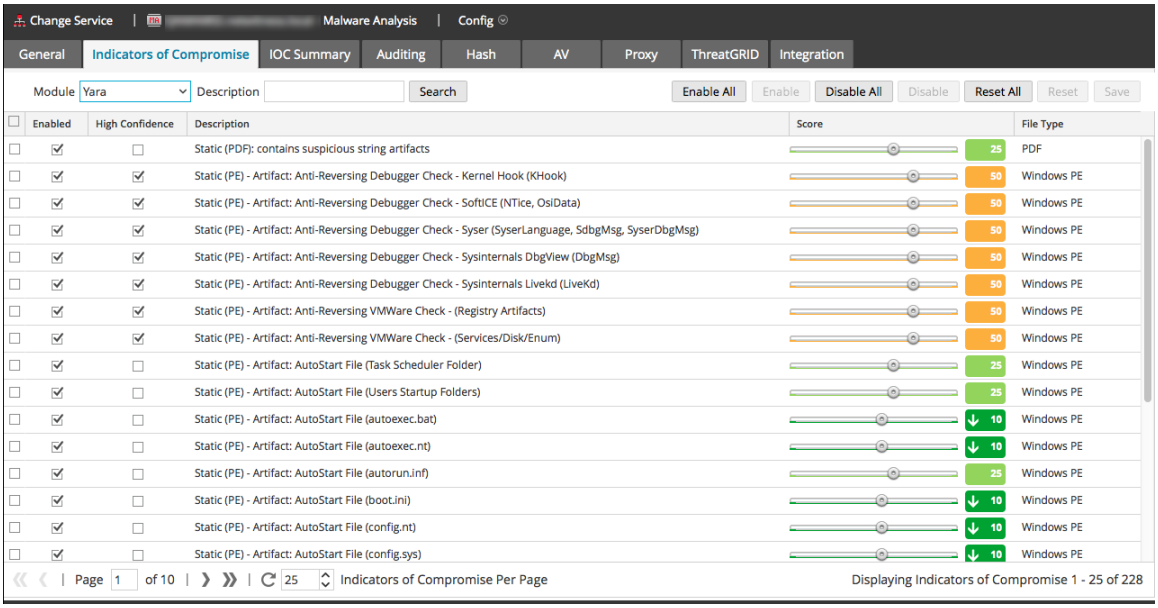
La figure suivante illustre le contenu YARA disponible en tant que règles YARA dans NetWitness Suite Live.



Sur l'hôte Malware Analysis, les règles YARA résident dans `/var/lib/rsamalware/spectrum/yara`, comme illustré dans l'exemple ci-dessous.

```
[root@TESTHOST yara]# pwd
 /var/lib/rsamalware/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/rsamalware/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/rsamalware/spectrum/yara/watch`

   Le fichier est utilisé en une minute.

   Ensuite, NetWitness Suite 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 Suite fournit les informations suivantes :

- Indiqué en tant qu'événement Forte probabilité, qui est considéré comme contenant probablement des Indicateurs de compromis.
- 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 Suite fournit les informations suivantes :

- Indiqué en tant qu'événement Forte probabilité, qui est considéré comme contenant probablement des Indicateurs de compromis.
- 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 :

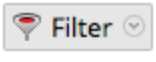
1. Dans la première liste déroulante **Trier par**, choisissez un nom de colonne et le sens du tri :  par ordre décroissant ou  par ordre croissant.
2. (Facultatif) Dans la deuxième liste déroulante **Trier par**, choisissez un nom de colonne, le sens du tri,  par ordre décroissant ou  par ordre croissant.

   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

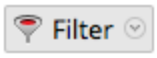
Vous pouvez filtrer la liste des fichiers et la liste des événements par nom de fichier ou hachage de fichier. Avec cette fonctionnalité, vous pouvez spécifier un sous-ensemble limité des données d'origine sur la base des critères de recherche.

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 du fichier** ou **Hachage MD5**, puis cliquez sur **Filtrer**. Les champs Nom du 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 

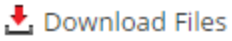
. Lorsque la boîte de dialogue Filtrer s'affiche, cliquez sur **Réinitialiser**.

Télécharger les fichiers à partir de la liste des fichiers

NetWitness Suite 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 Suite 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).

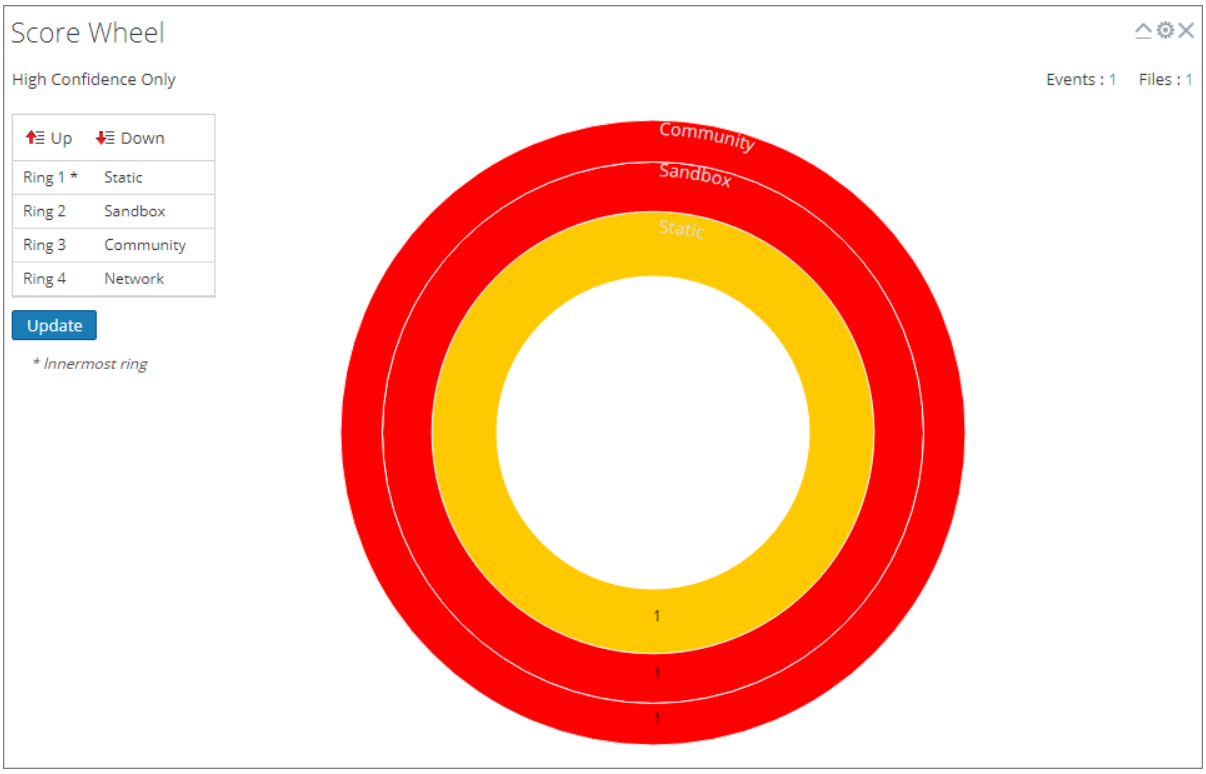
Filtrer les données de dashlet dans la vue Récapitulatif des événements

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.

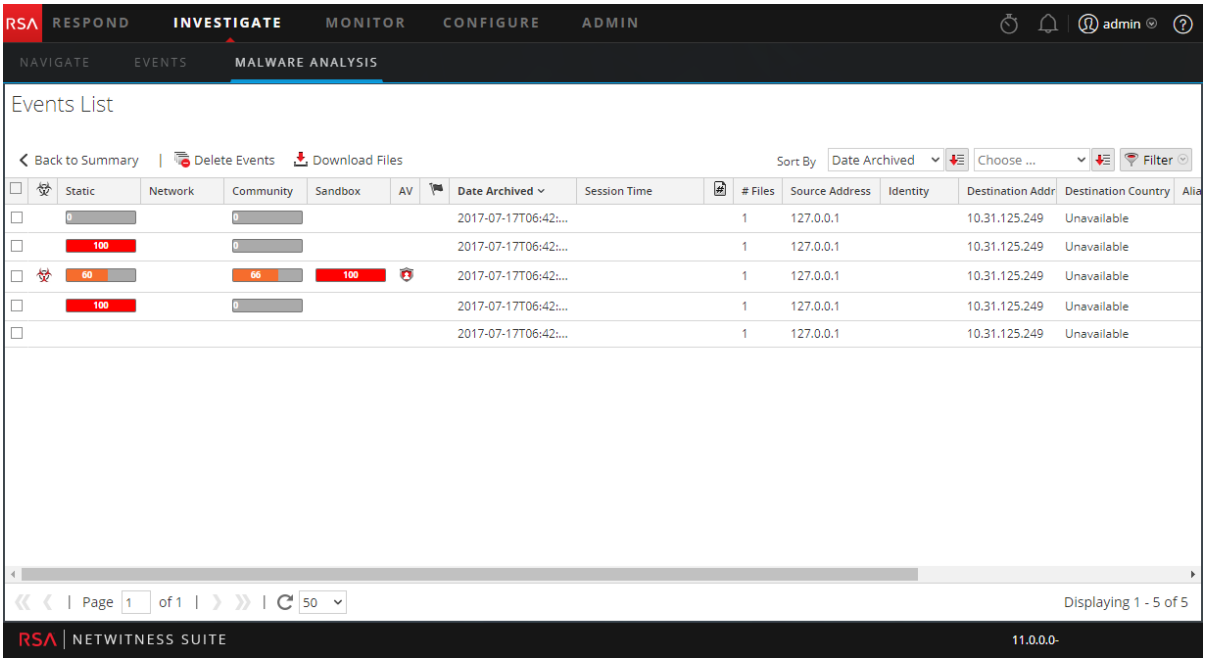


Vous pouvez modifier l'ordre des anneaux pour mettre en évidence des indicateurs de compromission qui ont été marqués dans une catégorie, mais pas dans une autre. La comparaison des mêmes résultats dans un ordre d'anneaux différent offre une visibilité sur les vulnérabilités supplémentaires dans une 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

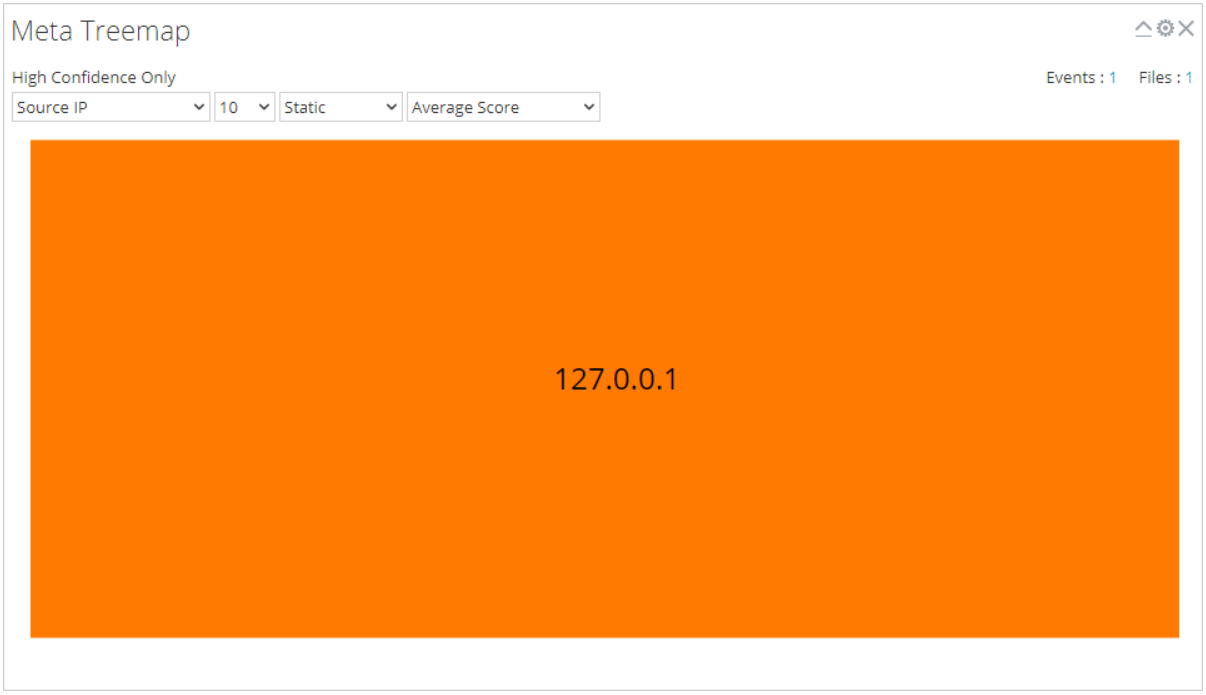
Dans la roue des scores, vous pouvez réorganiser la séquence d'anneaux par module de notation. Dans un premier temps, la séquence d'anneaux de l'intérieur vers l'extérieur est statique, réseau, communauté et Sandbox.

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.

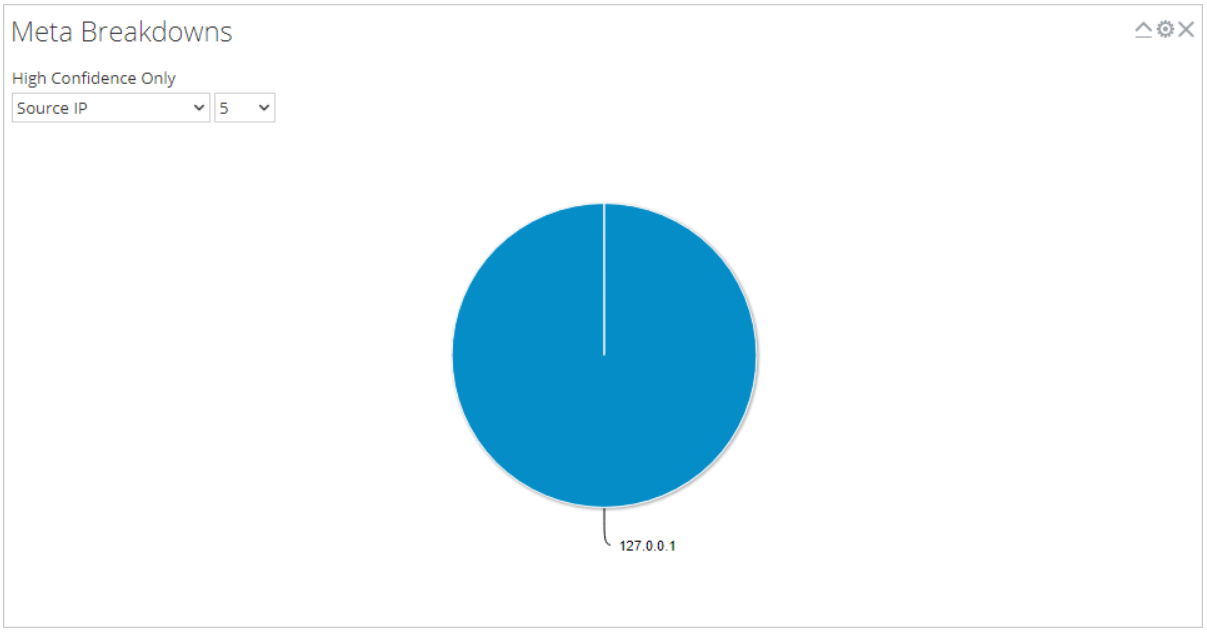
Configurer le dashlet de Compartimentage des méta

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.



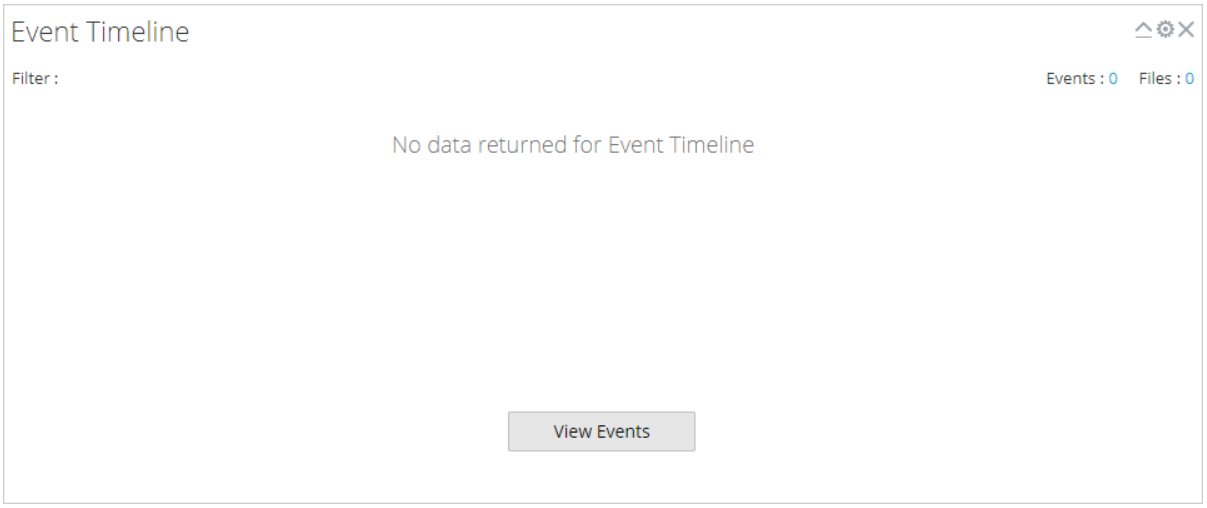
Configurer le dashlet de Répartition des méta

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 du Calendrier des 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.

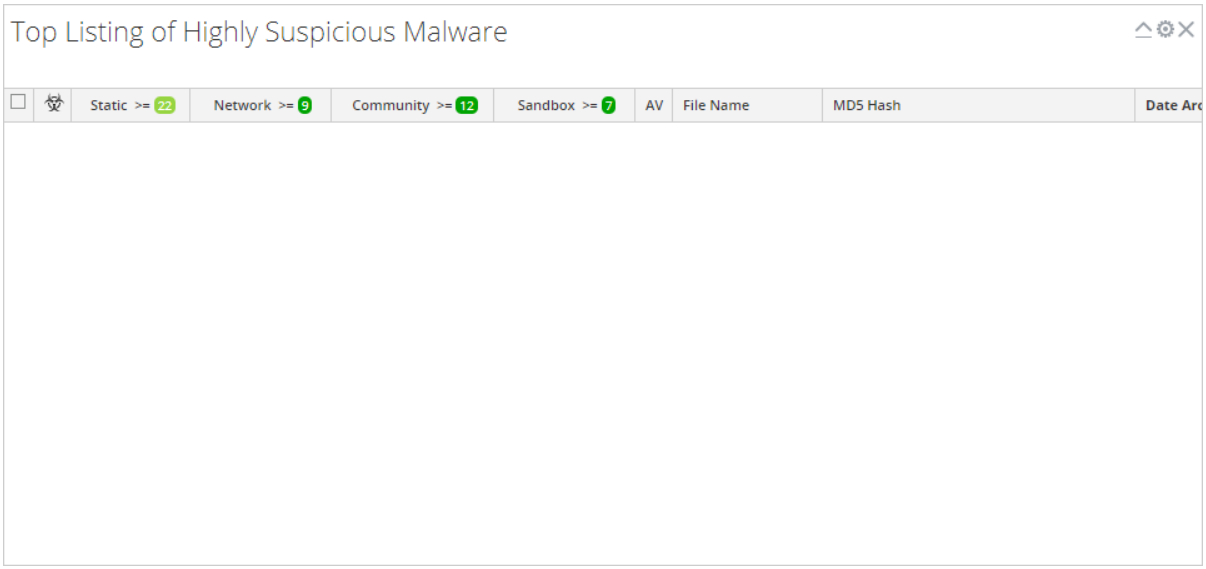


Ouvrir Tous les événements dans la liste des événements

À partir de la chronologie des événements, vous pouvez ouvrir la liste complète des événements dans la liste des événements. Pour cela, cliquez sur View Events. 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.

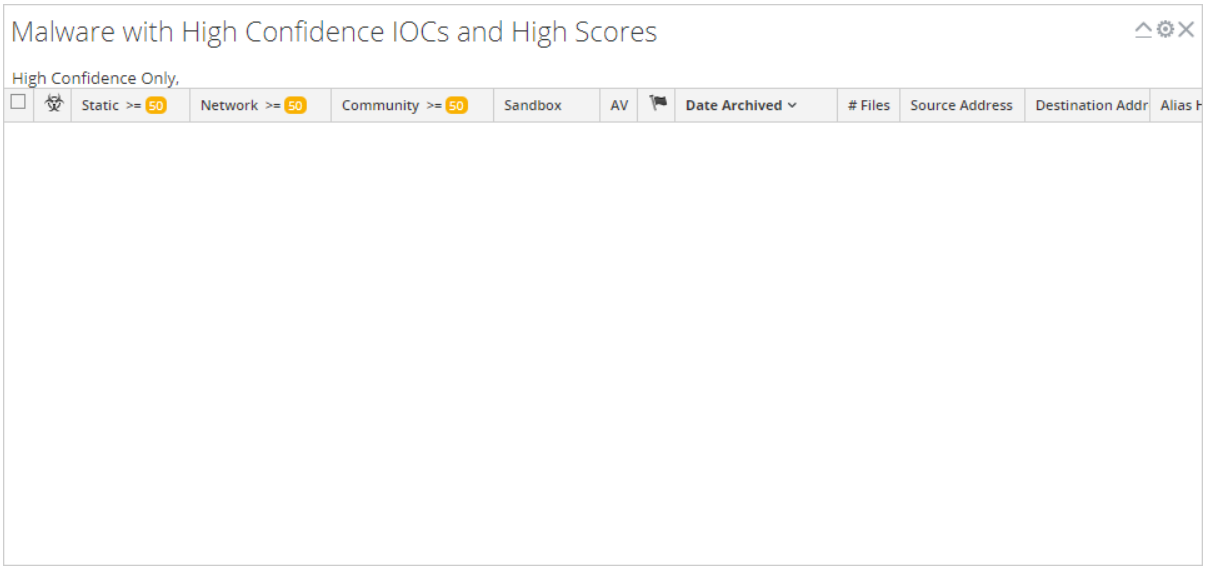
Configurer le dashlet Liste des principaux malwares fortement suspects

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.



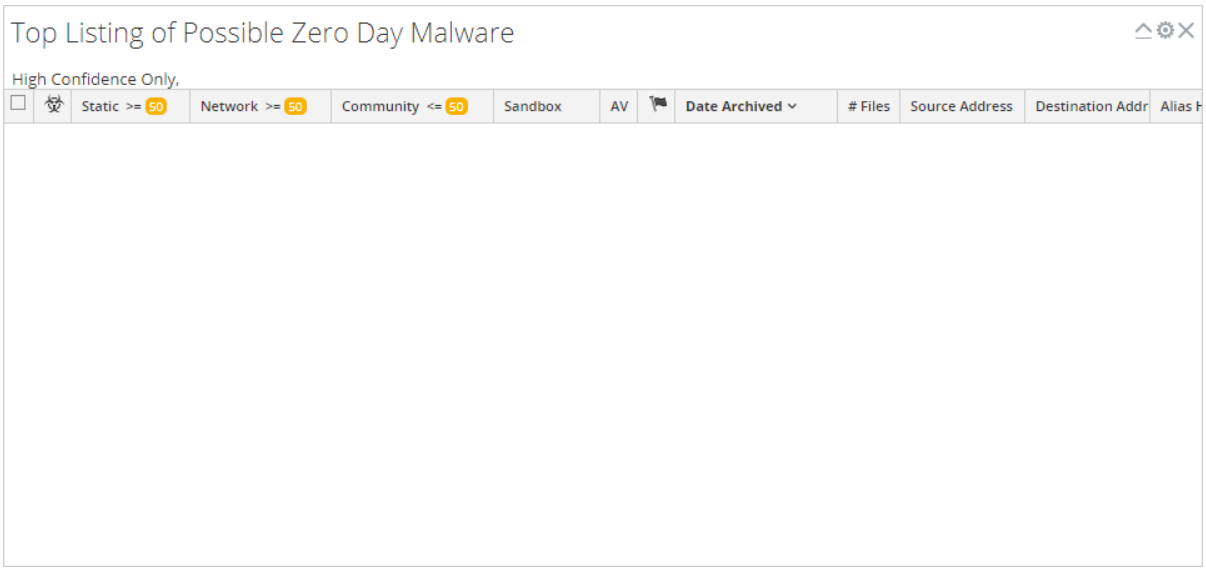
Configure le Dashlet Malware à forte probabilité d'indicateur de compromission et scores élevés

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.


Top Listing of Possible Zero Day Malware
High Confidence Only,
Static >= 50
Network >= 50
Community <= 50
Sandbox
AV
Date Archived
Files
Source Address
Destination Addr
Alias H

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.

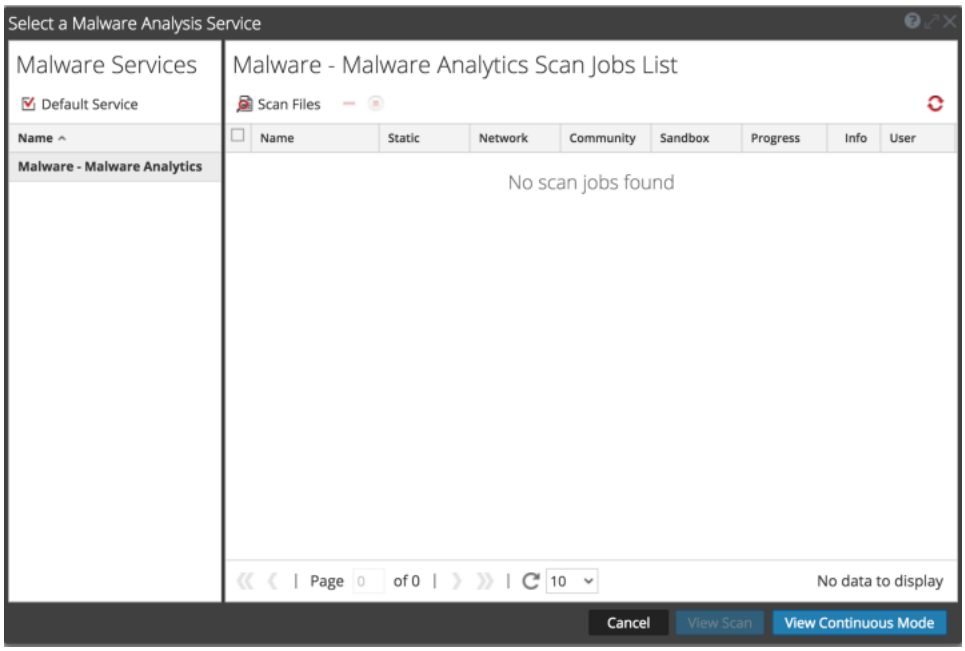
Il est également possible de télécharger un fichier à analyser à l'aide d'un partage de fichiers observé.

Télécharger des fichiers manuellement

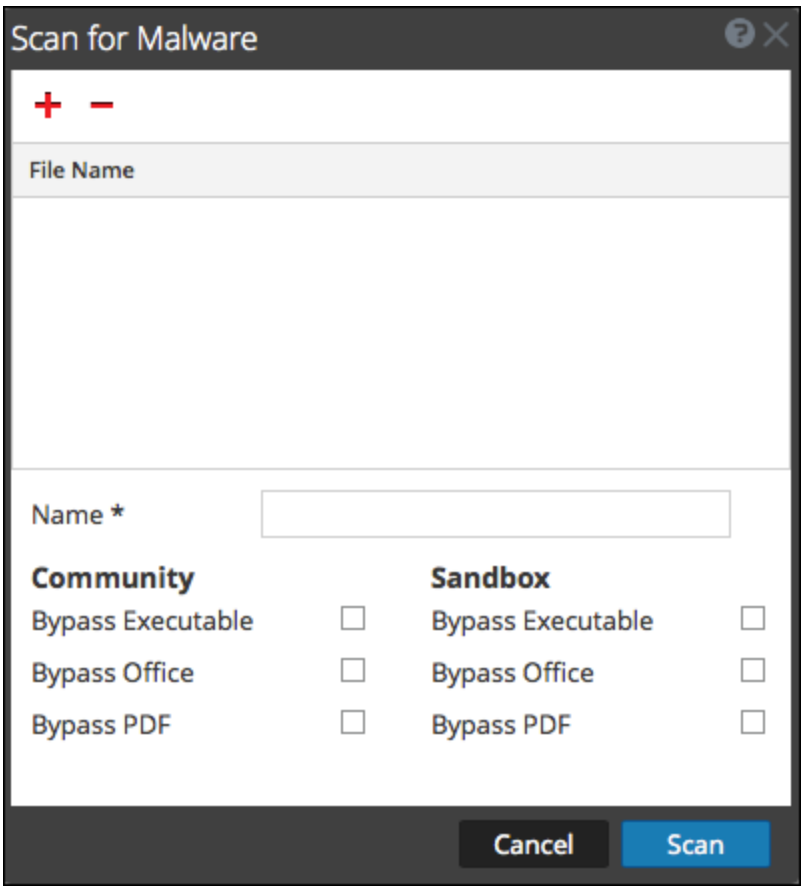
Cette rubrique fournit les instructions permettant de lancer l'analyse à la demande d'un fichier téléchargé. Lorsque vous téléchargez un fichier en vue d'une analyse, NetWitness Suite lance la tâche de téléchargement, puis l'ajoute à la file d'attente. Une fois la tâche terminée, vous pouvez consulter 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 Suite.
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 Suite 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.
   La vue Récapitulatif des événements de Malware Analysis 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/rsamalware/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*.

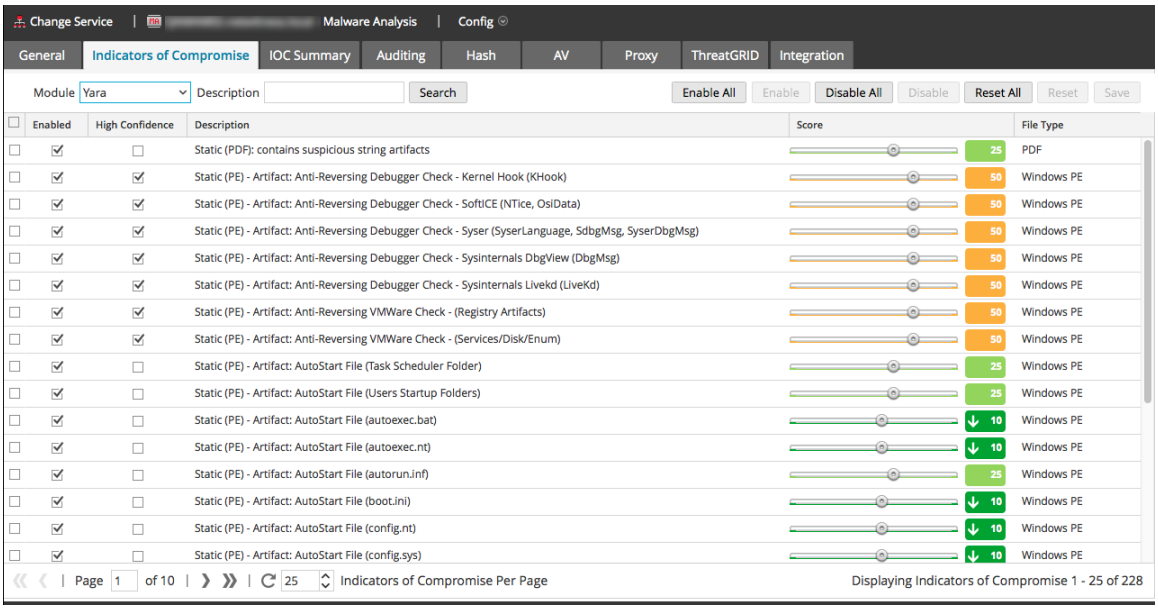
Pour importer une liste de hachage à l'aide de la méthode du dossier surveillé :

1. Dans le répertoire **`/var/lib/rsamalware/spectrum/hashWatch`** , copiez les listes de hachage que vous souhaitez importer.
   NetWitness Suite 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/rsamalware/spectrum/yara/watch`
Le fichier est utilisé en une minute.
Ensuite, NetWitness Suite 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.

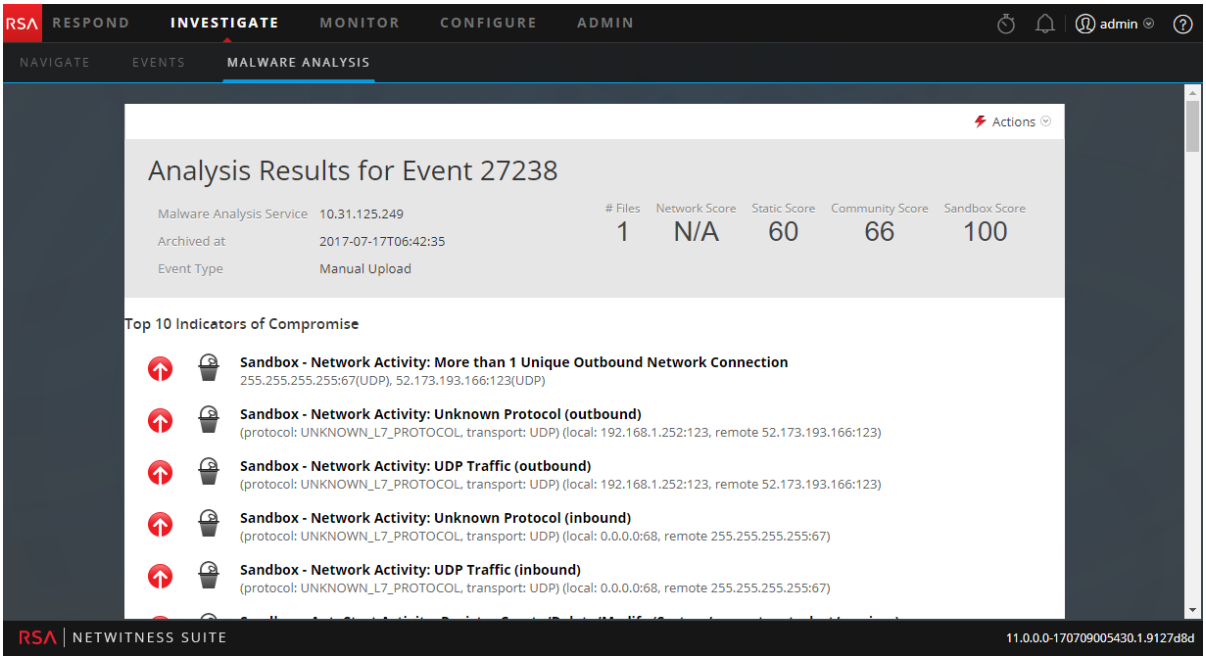
1. En étant connecté en tant qu'administrateur, compressez les fichiers à traiter avec le mot de passe `infected` et placez le fichier zip dans `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   En une ou deux minutes, Malware Analysis utilise l'archive et crée une tâche à la demande dans la liste 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.

Afficher 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.

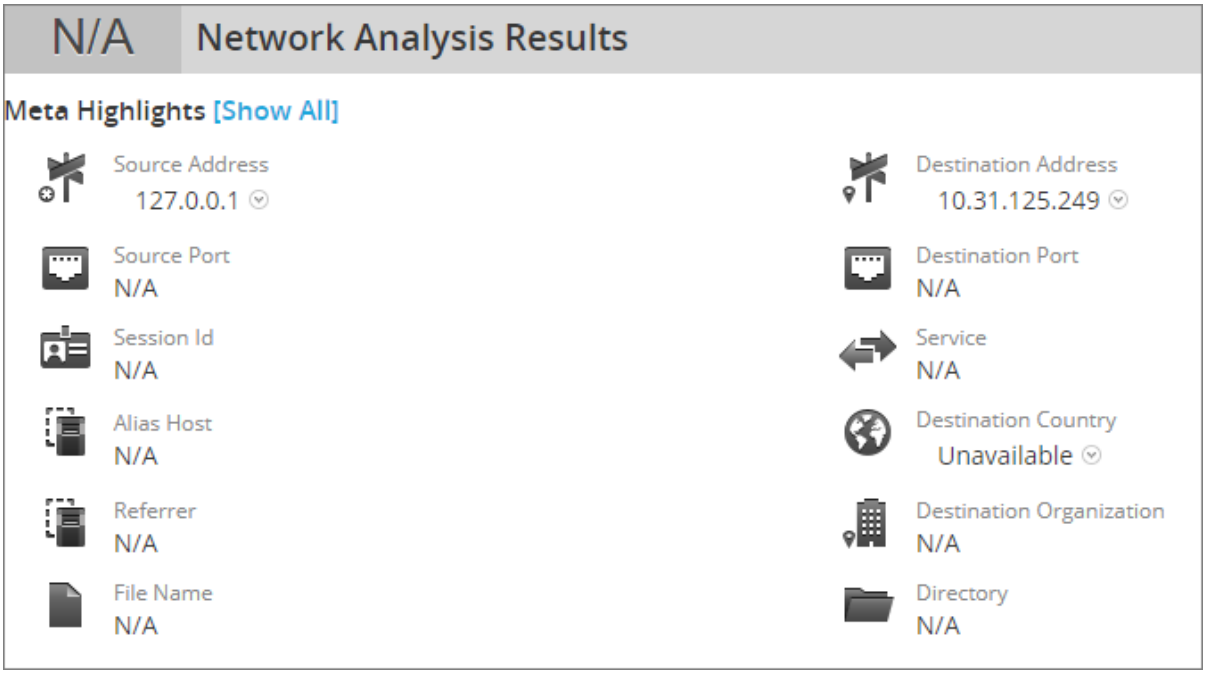


4. (Facultatif) Si vous souhaitez supprimer un événement, sélectionnez **Actions > Supprimer un événement**.
5. Pour afficher une reconstruction de la session réseau, sélectionnez **Actions > Afficher la session réseau**.
   La session s'ouvre dans la vue Naviguer > Reconstruction d'événement.

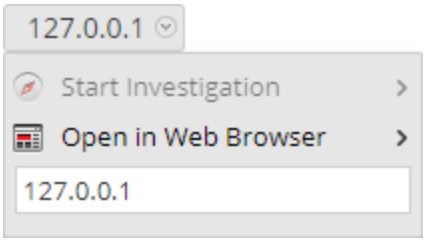
Pivotage des résultats de l'analyse réseau

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.

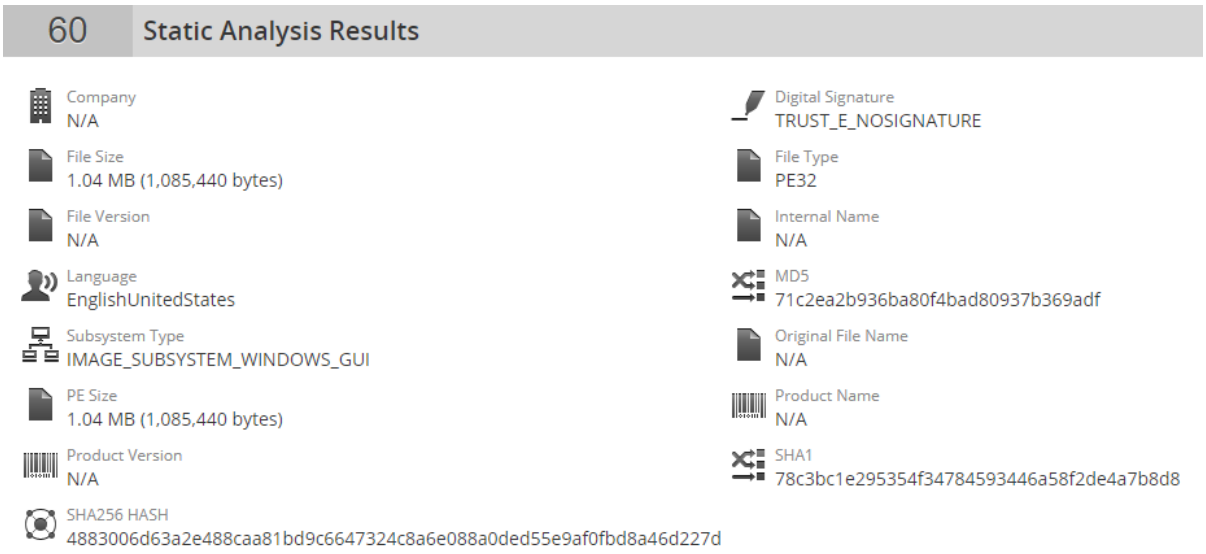


3. Pour afficher la valeur méta sélectionnée dans la vue **Naviguer**, sélectionnez **Démarrer Investigation** et une option d'heure.

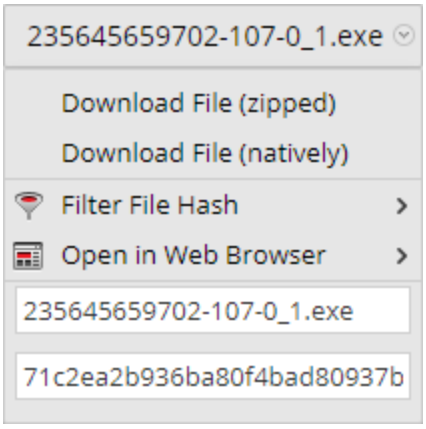
4. Pour afficher la métavaleur sélectionnée dans un navigateur, sélectionnez **Ouvrir dans un navigateur Web > Ouvrir dans Google**.

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**.

Afficher les détails des résultats de l'analyse des pairs

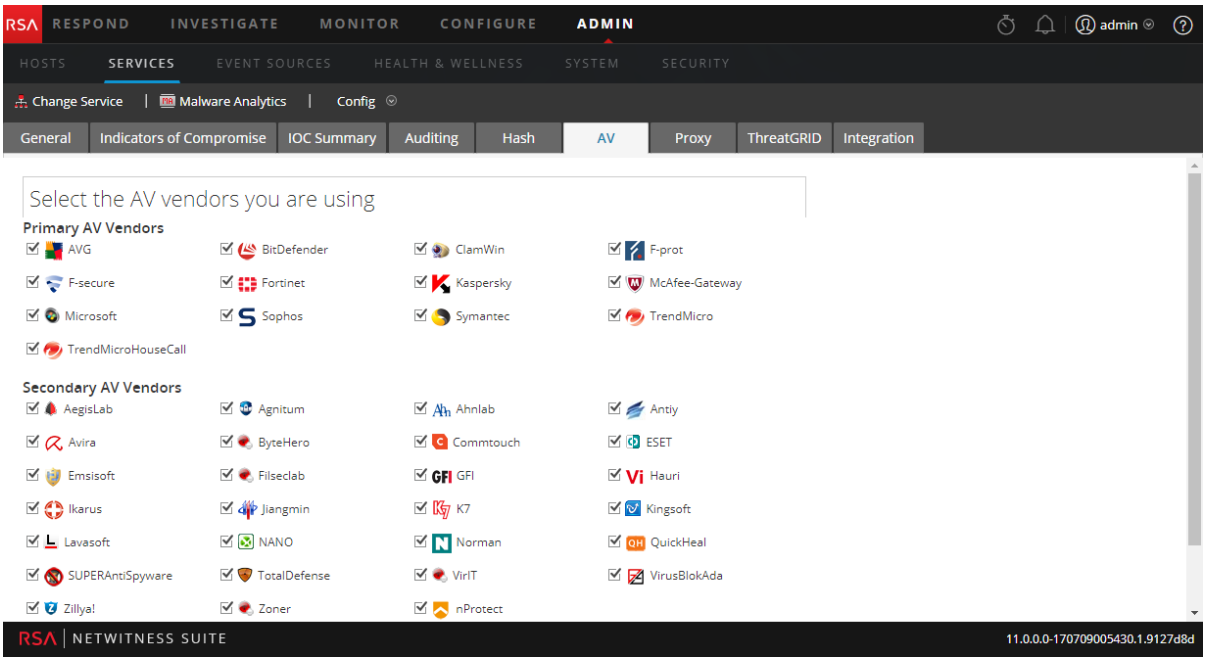
Résultats de l'analyse de la communauté résume les résultats de la communauté, identifiant les indicateurs de compromis qui ont été marqués comme risqués ou identifiés comme corrects.

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.

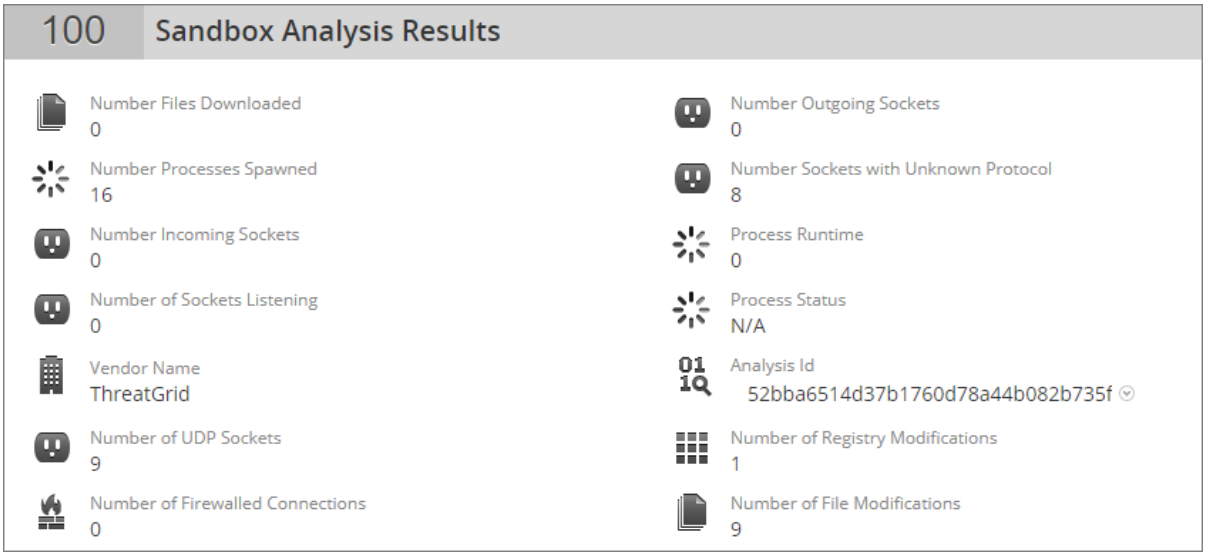
Si aucun fournisseur AV installé n'a été configuré pour le service Malware Analysis actuel, le message suivant s'affiche : Aucun fournisseur d'antivirus n'est signalé comme étant installé. Accédez à la page de configuration du service Malware Analysis pour identifier les fournisseurs AV installés.



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.

Matériaux de référence de procédure d'enquête

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.

- Vue Naviguer
- Vue Événements
- Vue Malware Analysis
- Boîte de dialogue Ajouter à la liste/Supprimer de la liste
- Boîte de dialogue Ajouter des événements à un incident
- 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
- Boîte de dialogue Analyser
- Onglet Procédure d'enquête - Panneau Préférences utilisateur
- Boîte de dialogue Gérer les clés méta par défaut
- Liste d'événements Malware Analysis et liste Fichiers
- Boîte de dialogue Gérer les groupes de colonnes
- Boîte de dialogue Gérer les profils
- Vue Naviguer
- Boîte de dialogue Requête
- Boîte de dialogue Analyser les malware

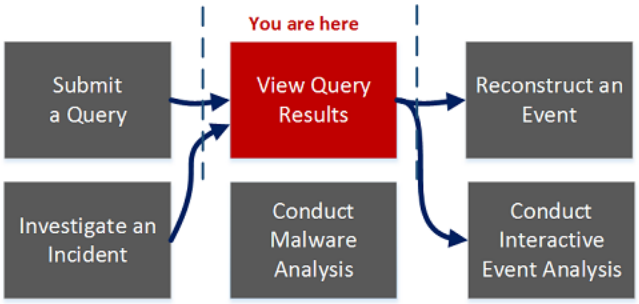
- Boîte de dialogue Sélectionner un service Malware Analysis
- Boîte de dialogue Paramètres pour les vues Naviguer et Événements

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 Procédure d'enquête > Événements, sélectionnez **Incidents > Ajouter à un incident existant** dans la barre d'outils.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	ajouter un ou plusieurs événements à un incident existant ou à un nouvel incident*	Ajouter des événements à un incident pour obtenir une réponse
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	effectuer une analyse interactive des événements	Analyser les événements dans la vue Analyse d’événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d’utilisation de NetWitness Respond*
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis

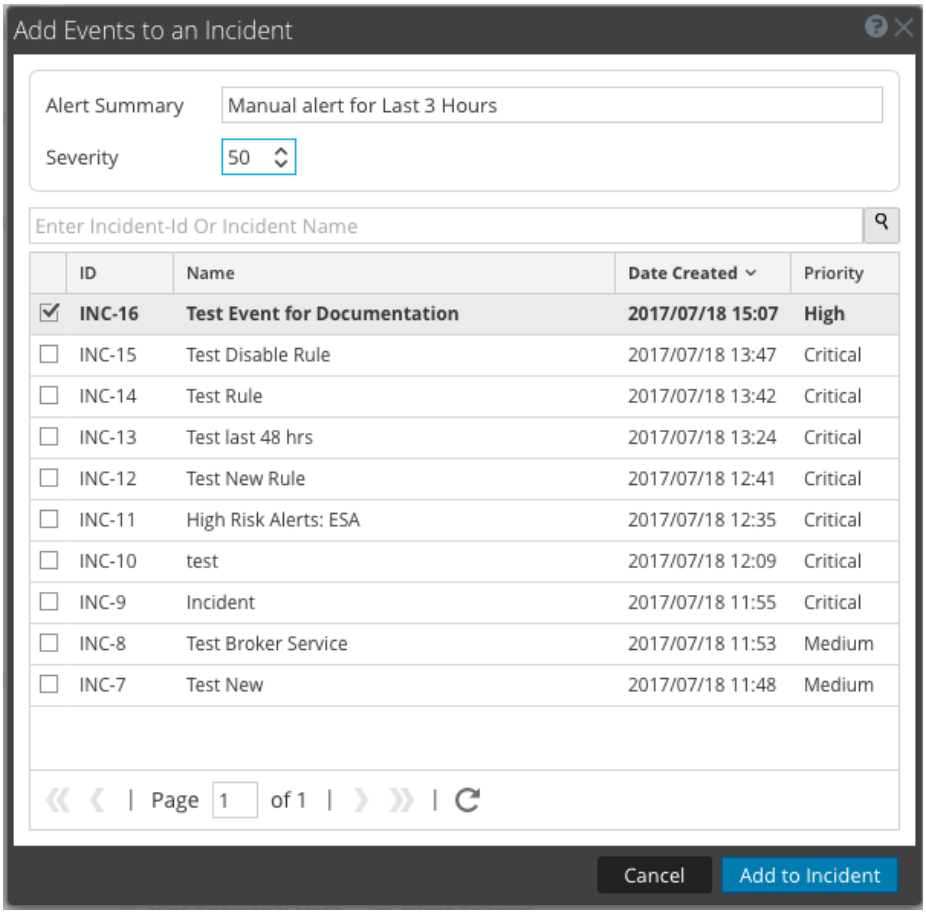
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Examiner des événements
- 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.



Fonction	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.

Fonction	Description
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.
Ajouter à l'incident	Ajoute les alertes à l'incident. Une boîte de dialogue confirme que les alertes ont été ajoutées avec succès.

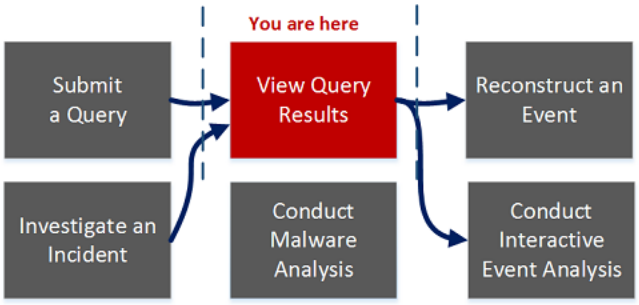
Boîte de dialogue Ajouter à la liste/Supprimer de la liste

Lorsque vous travaillez dans Enquêter, vous pouvez trouver une adresse IP ou un nom d'utilisateur que vous souhaitez surveiller dans la vue Naviguer et la vue Événements. Dans la boîte de dialogue Ajouter à la liste/Supprimer de la liste, vous pouvez ajouter des métavaleurs pour les clés méta `Source IP`, `Destination IP`, ou `Username` à une liste Context Hub existante. Vous pouvez aussi créer une nouvelle liste contenant les métavaleurs. Lorsque vous ajoutez des métavaleurs à une liste, vous pouvez rechercher un contexte supplémentaire sur ces métavaleurs.

Pour afficher la boîte de dialogue. 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.

Workflow

Le diagramme de flux de travail suivant illustre le workflow de haut niveau pour Enquêter avec l'emplacement de l'activité en cours mis en surbrillance.



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	ajouter des métavaleurs à une liste Context Hub*	Gérer les listes et les valeurs de liste Context Hub dans Enquêter
Responsable de la recherche des menaces	créer une liste Context Hub*	Gérer les listes et les valeurs de liste Context Hub dans Enquêter

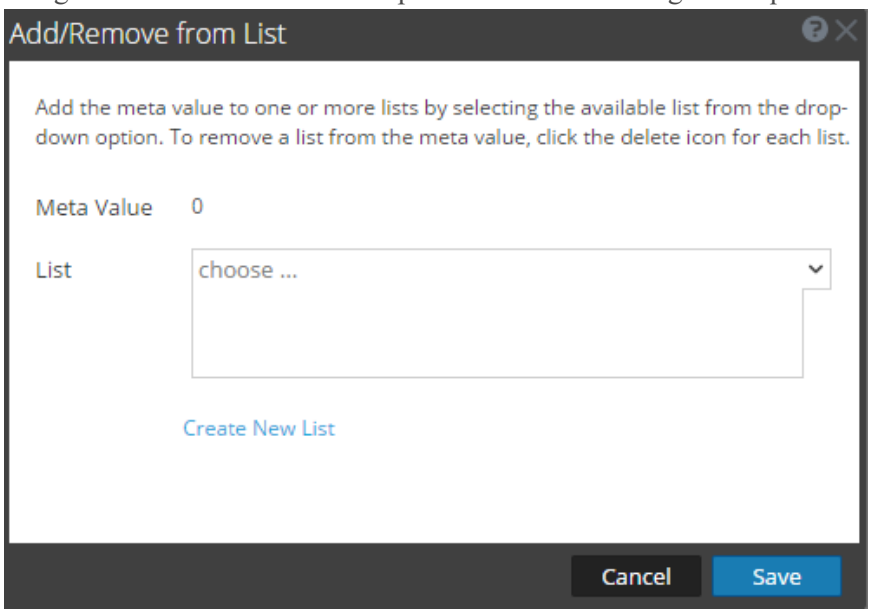
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement*	Analyser les événements dans la vue Analyse d'événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

Rubriques connexes

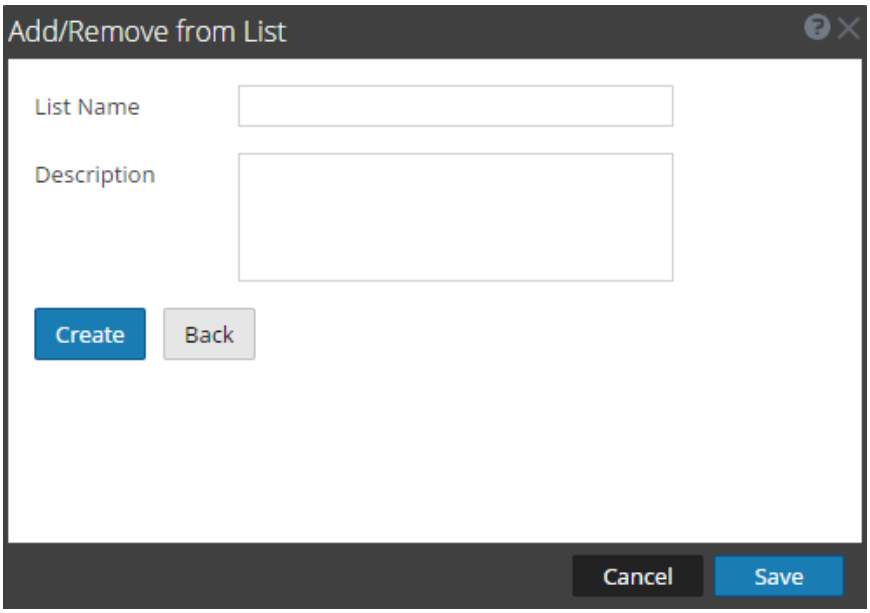
- Afficher un contexte supplémentaire pour un point de données
- Examiner des événements
- Vue Événements

Aperçu rapide

La figure suivante donne un exemple de la boîte de dialogue 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.

Fonction	Description
Valeur méta	Valeur méta à ajouter à la liste existante ou à la nouvelle liste.

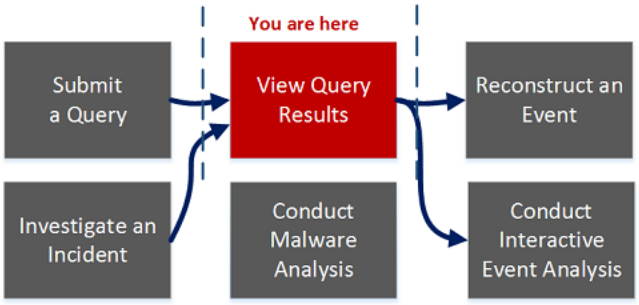
Fonction	Description
Répertorier	Liste à laquelle la métavaleur sélectionnée doit être ajoutée. Un menu déroulant contient les listes disponibles auxquelles vous pouvez ajouter la métavaleur.
Créer une nouvelle liste	Ouvre une nouvelle boîte de dialogue dans laquelle vous pouvez créer une nouvelle liste 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.

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 et la vue Événements d'Enquêter. Le service Context Hub est pré-configuré avec un mappage du type de méta et de la clé méta par défaut. Pour plus d'informations sur le mappage de la métavaleur du service Context Hub avec une clé méta de procédure d'enquête, consultez la rubrique « Gérer le mappage du type de méta » 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 du module Investigation. Les métavaleurs qui ont été ajoutées à une liste Context Hub sont mises en surbrillance en gris dans le panneau Valeurs de la vue Naviguer. 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.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	mener une enquête sur les valeurs de métadonnées*	Afficher un contexte supplémentaire pour un point de données
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	effectuer une analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

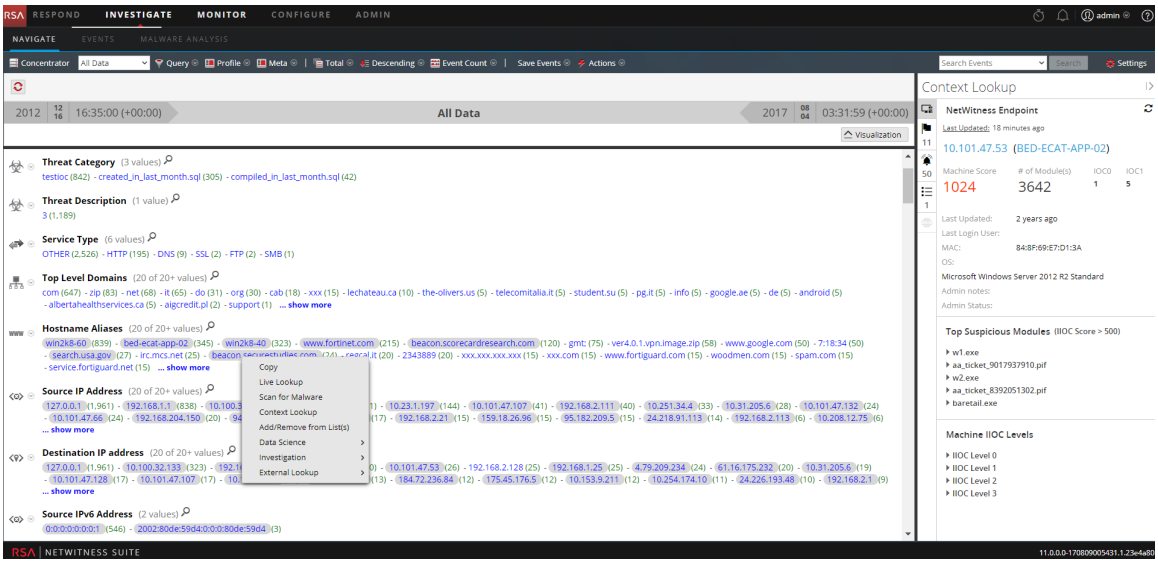
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Vue Événements
- Vue Naviguer
- « Commentaires et partage de données NetWitness » dans le *Guide de gestion des services Live*
- Afficher un contexte supplémentaire pour un point de données

Aperçu rapide

La figure suivante donne un exemple du panneau Recherche contextuelle, et les commandes et les fonctionnalités sont décrites dans le tableau.



Fonction	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
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 éléments (n premiers résultats)	Le pied de page indique le nombre total de résultats et le nombre de résultats actuellement affichés. Par exemple, 50 alertes (50 premières alertes).

Résultats de la recherche

Le panneau Recherche contextuelle affiche les informations suivantes lors de la récupération des données contextuelles à partir des sources configurées.

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 score de risque des incidents
- 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

Point de terminaison

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

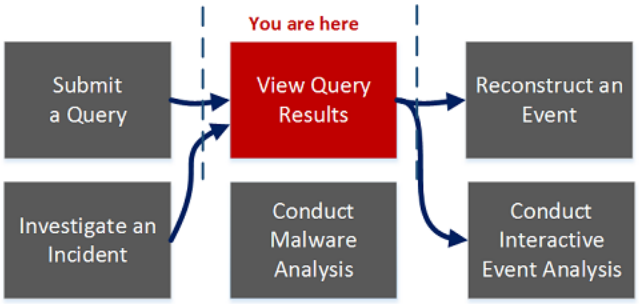
- Notes Admin (le cas échéant)
- État Admin (le cas échéant)
- Modules les plus suspects (modules dont le score IIOC est supérieur à 500). Cet élément se base sur la valeur définie dans le champ « Valeur IIOC minimale » de la fenêtre Configurer le point de terminaison. La valeur par défaut pour la « Valeur IIOC minimale » est de 500.
- Niveaux IIOC de la machine

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...	Documentation
Responsable de la recherche des menaces	créer un incident ou ajouter des événements à un incident*	Ajouter des événements à un incident pour obtenir une réponse
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

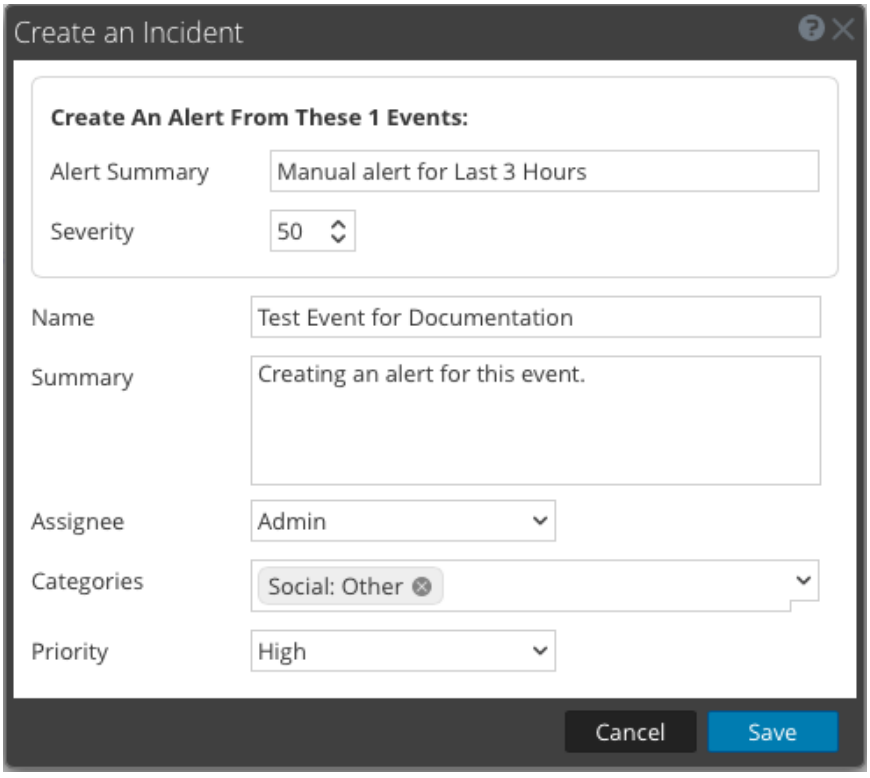
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	effectuer une analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- 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.



Fonction	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.
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

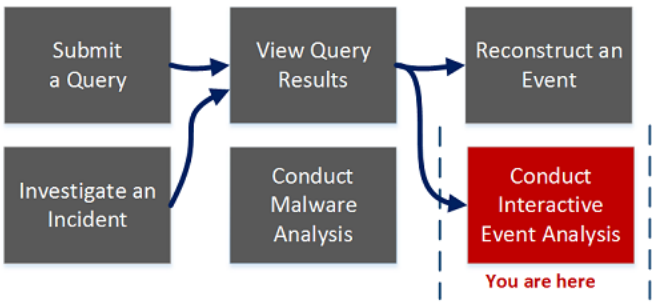
Dans la vue Analyse d’événements, les fonctions interactives améliorent votre capacité à déceler des schémas significatifs dans les données. Il s’agit d’une solution alternative à la vue statique Reconstruction d'événement. Les analystes à qui un rôle d’utilisateur est attribué avec un accès à la vue Analyse d’événements peuvent examiner des événements de réseau, de log et de point de terminaison dans la vue Analyse d’événements. Vous pouvez choisir entre cette vue ou la vue Reconstruction d’événement.

La vue Analyse d’événements répertorie les événements associés au point d’extraction actuel dans Vue Naviguer dans l’ordre chronologique. 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.

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

- Dans la vue Événements avec la vue Détails sélectionnée, cliquez sur **Analyse d’événements** à la fin de l’événement,
- Dans la barre d'outils Reconstruction d'événement, cliquez sur **Analyse d’événements**.

Workflow



Que voulez-vous faire ?

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement*	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

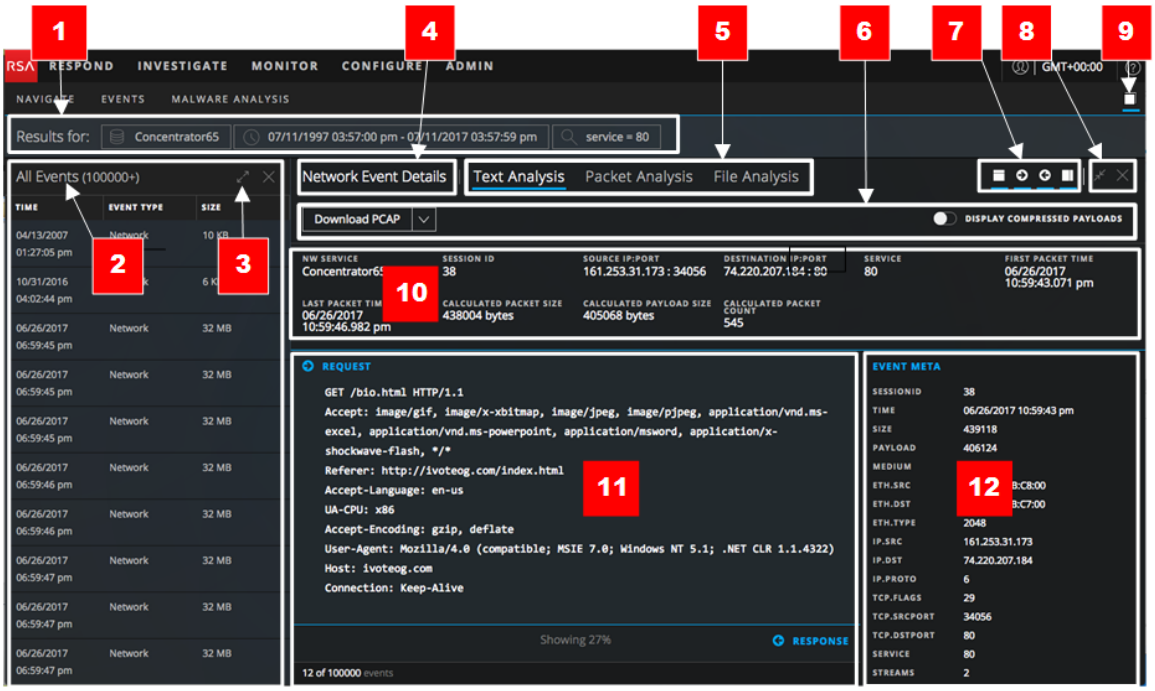
- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements - Panneau Analyse de paquets
- Vue Analyse d'événements - Panneau Analyse de texte
- Vue Analyse d'événements - Panneau Analyse de fichiers

Aperçu rapide

Lorsque vous ouvrez 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 1 000 premiers événements, paquets, logs et événements de point de terminaison sont chargés dans le panneau Liste d'événements. Les colonnes du panneau Liste d'événements indiquent l'heure de l'événement, le type de l'événement (réseau, log ou point de terminaison), la taille de l'événement et le récapitulatif. Vous pouvez :

- Faire défiler la liste, puis cliquer sur **Charger davantage** pour consulter les 100 000 événements suivants.
- Faire glisser les colonnes pour les réorganiser.

- Rendre les colonnes plus larges ou plus étroites.
- Afficher l’analyse d’un événement.



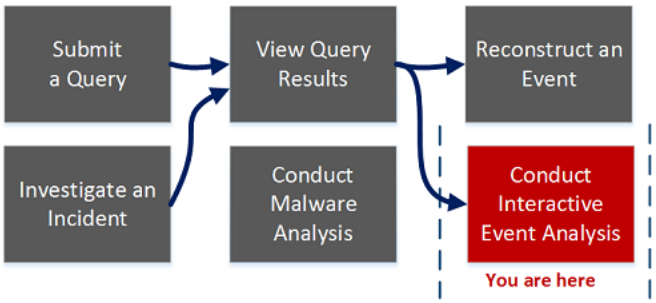
1	Le fil d’Ariane en lecture seule affiche la requête utilisée pour générer ce jeu de données. Toutes les requêtes sont effectuées dans la vue Naviguer ou la vue Événements.
2	Il s’agit d’une liste en lecture seule des événements en fonction de la requête effectuée dans la vue Naviguer ou la vue Événements. La liste d’événements indique le nombre des 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 Analyser les événements dans la vue Analyse d’événements).
3 et 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 Analyser 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 Analyser 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 Analyser les événements dans la vue Analyse d'événements.  Cliquez sur cette icône pour masquer l'en-tête d'événement ou l'afficher. Le fait de masquer l'en-tête offre plus d'espace pour la liste des paquets, en réduisant le défilement requis pour afficher plus de paquets.  Cliquez sur cet élément pour afficher Panneau des métadonnées d'événement pour l'événement dans un autre panneau.
9	Ouvrez à nouveau le panneau Liste d'événements ou le Panneau des métadonnées d'événement si vous l'avez fermé.
10	En-tête d'événement, qui fournit 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 des métadonnées d'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 Analyser les événements dans la vue Analyse d'événements.

Vue Analyse d’événements - Panneau Analyse de fichiers

Dans le panneau Analyse de fichiers (**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 que vous avez trouvé dans la vue Naviguer ou la vue Événements.

Workflow



Que voulez-vous faire ?

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement*	Analyser les événements dans la vue Analyse d’événements
Responsable de la recherche des menaces	exporter des fichiers à partir d’un événement*	Analyser les événements dans la vue Analyse d’événements

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

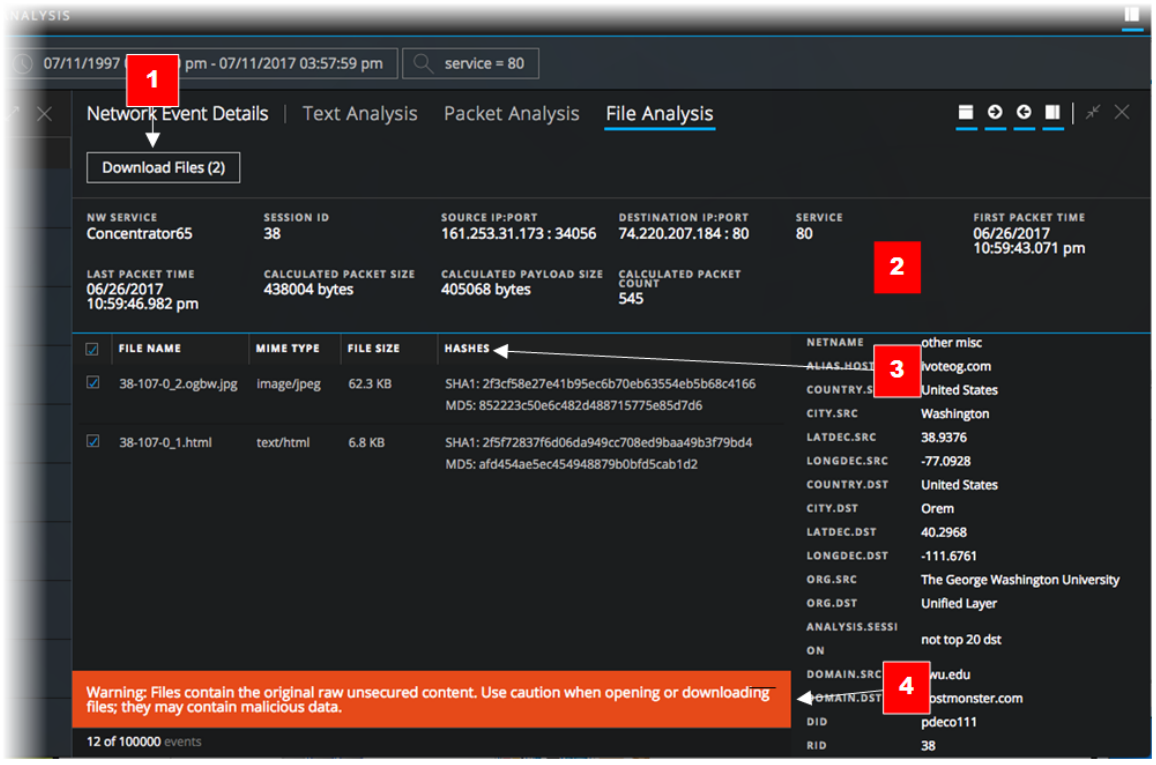
Rubriques connexes

- 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.

Vous trouverez ci-dessous un exemple d'analyse de fichiers.

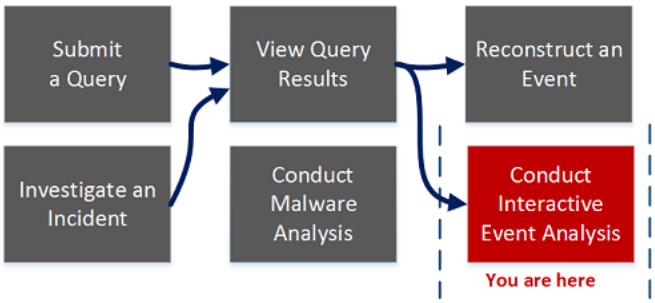


1. Cliquez pour télécharger un ou plusieurs fichiers sélectionnés.
2. L’en-tête d’événement affiche les informations récapitulatives de l’événement réseau qui contient les fichiers.
3. Liste déroulante des fichiers associés que vous pouvez sélectionner et télécharger.
4. Rappel qu’il est nécessaire de 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 trouvé dans la vue Naviguer ou la vue Événements.

Workflow



Que voulez-vous faire ?

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement*	Analyser les événements dans la vue Analyse d’événements
Responsable de la recherche des menaces	exporter des fichiers à partir d’un événement*	Analyser les événements dans la vue Analyse d’événements

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d’utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

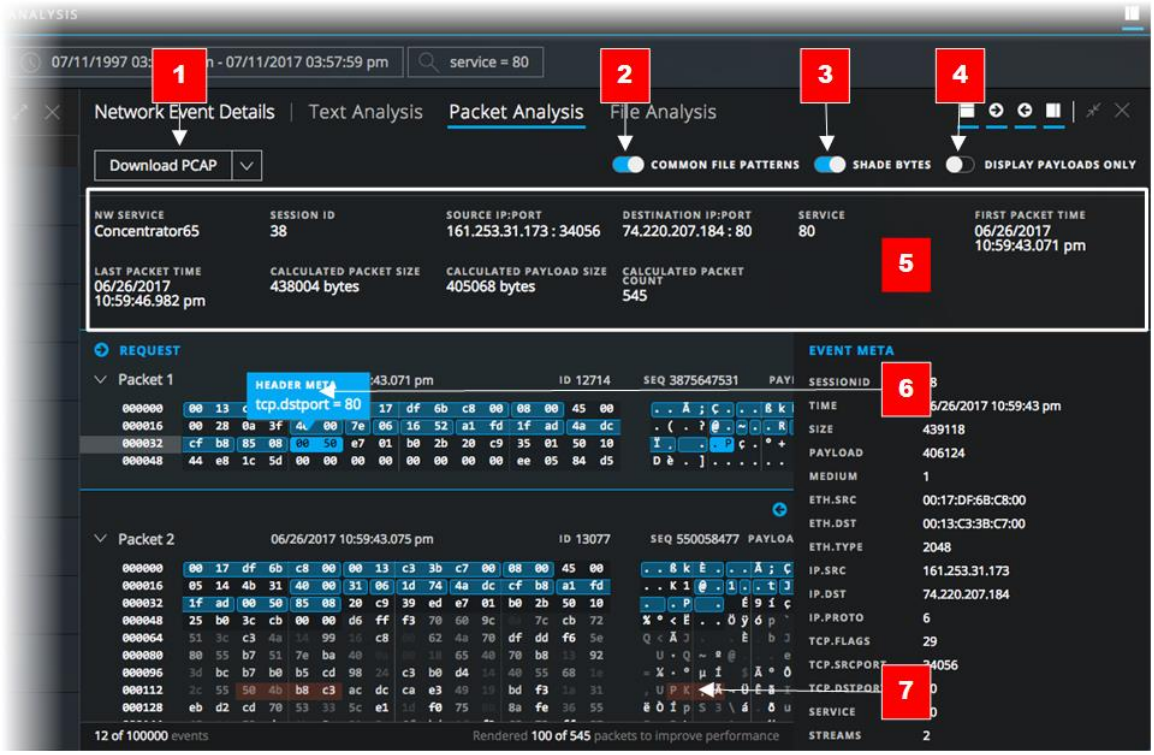
- Fonctionnement de NetWitness Investigate
- Vue Analyse d’événements
- Vue Analyse d’événements - Panneau Analyse de texte
- Vue Analyse d’événements - Panneau Analyse de fichiers

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. Pour chaque paquet, vous pouvez voir le numéro du paquet, l’orientation (demande ou réponse) et le contenu du paquet au format ascii sur la gauche, dans un format hexadécimal au milieu et dans un format texte sur la droite. 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.

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.

Vous trouverez ci-dessous un exemple du panneau Analyse de paquets.

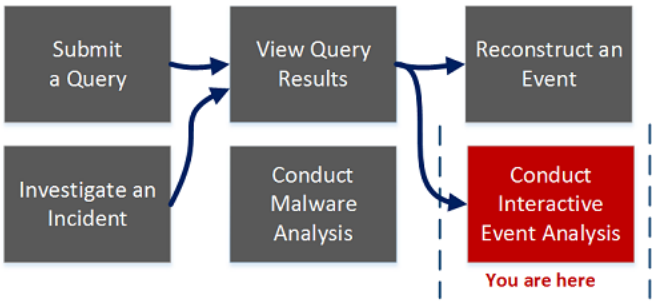


1	Options permettant d'exporter un événement réseau. Vous pouvez exporter un PCAP, toutes les charges utiles, charges utiles de demande ou charges utiles de réponse pour une analyse plus approfondie et partager avec d'autres utilisateurs.
2	L'option permettant d'identifier les signatures de fichiers courants est activée par défaut. Les signatures des fichiers courants sont mises en surbrillance en orange (7) ; 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. Par exemple, **Méta d'en-tête ip.proto=6** est une info-bulle pour les métadonnées en surbrillance dans la représentation hexadécimale et binaire de l'en-tête du paquet.
7	La mise en surbrillance en orange identifie une signature de fichiers courants. Déplacer la souris sur la zone permet d'afficher le type de fichier possible dans une zone de survol.

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 que vous avez trouvé dans la vue Parcourir ou la vue Événements. 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...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Examiner des événements
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement*	Analyser les événements dans la vue Analyse d’événements

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	exporter des fichiers à partir d'un événement*	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

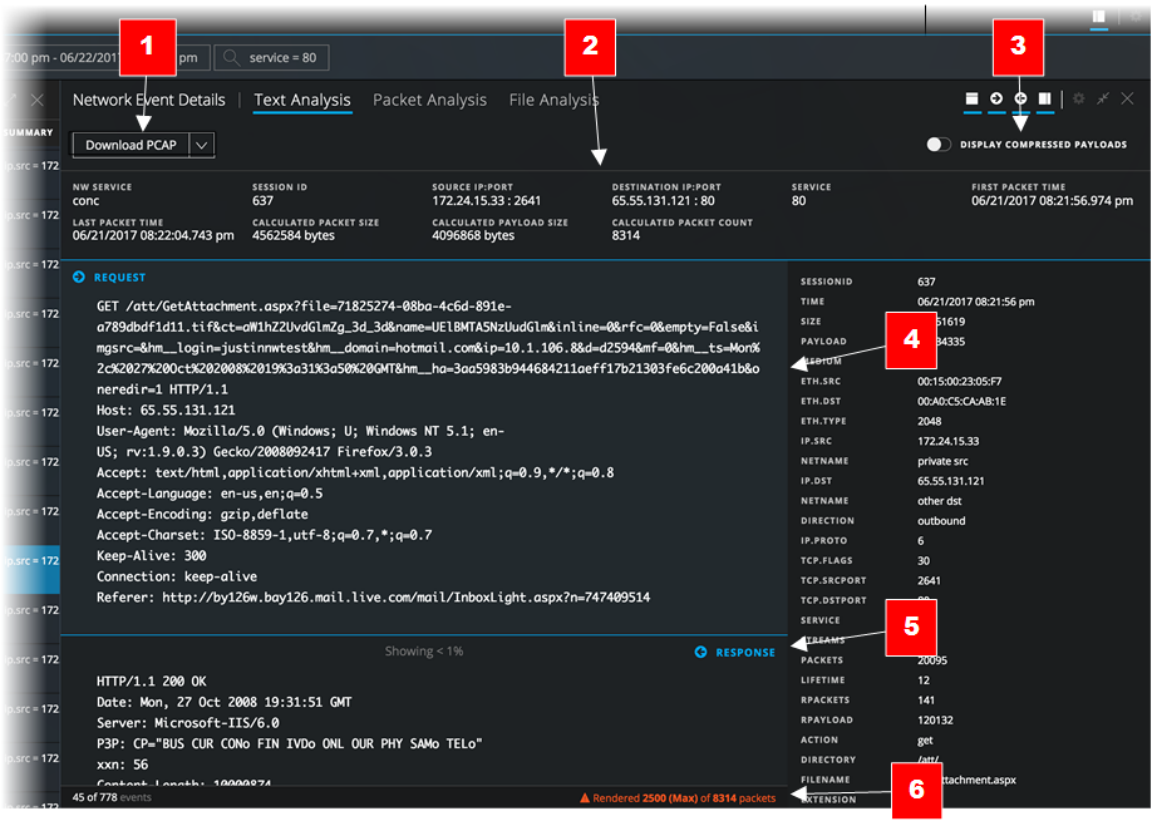
*Vous pouvez effectuer cette tâche dans la vue actuelle.

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.



1	Options permettant d'exporter un log, un 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	Cliquez sur cette option pour afficher la charge utile du réseau sous une forme compressée ou décompressée.
4	La charge utile d'un événement réseau inclut les demandes et les réponses. Il s'agit de la partie de la demande du paquet.
5	Il s'agit de la partie de la réponse du paquet. Seul 1 % de la réponse s'affiche, car elle a été tronquée pour permettre l'affichage de plus de paquets. Lorsque vous faites défiler vers le bas, vous pouvez cliquer sur une option pour afficher le reste de la charge utile.
6	Ce message s'affiche lorsque le seuil de paquets de 2 500 est atteint, une mesure permettant d'optimiser les performances. Les paquets supplémentaires ne s'affichent pas. Vous pouvez télécharger l'événement pour afficher tous les paquets.

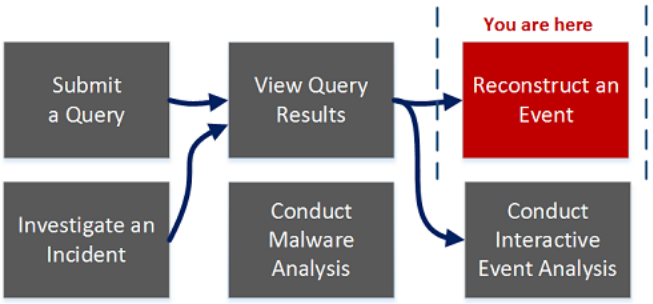
Vue Reconstruction d'événement

La vue Reconstruction d'événement fournit une reconstruction d'un événement sélectionné à partir de la Vue Événements. Par défaut, NetWitness Suite 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**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	afficher la reconstruction d'un événement*	Reconstruire un événement
Responsable de la recherche des menaces	afficher l'analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter des fichiers à partir d'un événement*	Reconstruire un événement
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

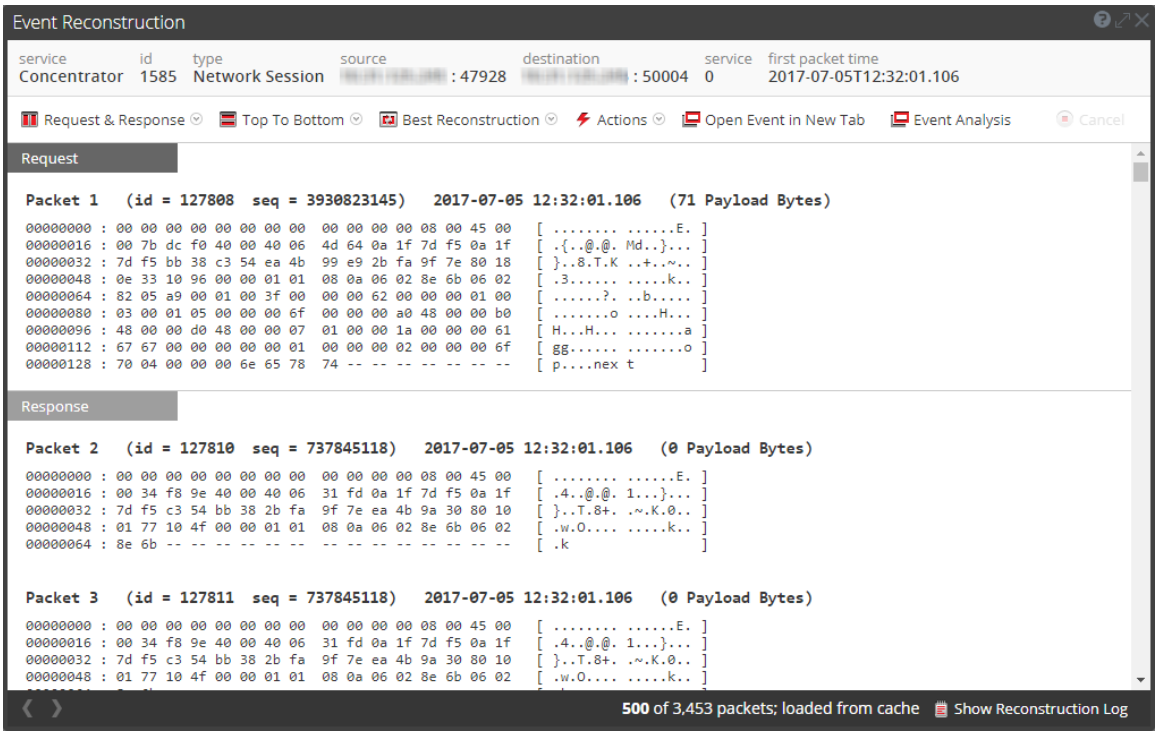
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Vue Analyse d'événements

Aperçu rapide

Cette figure est un exemple de la vue Reconstruction d'événement. Le tableau suivant décrit les options de la barre d'outils.



Fonction	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.

Fonction	Description
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
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.

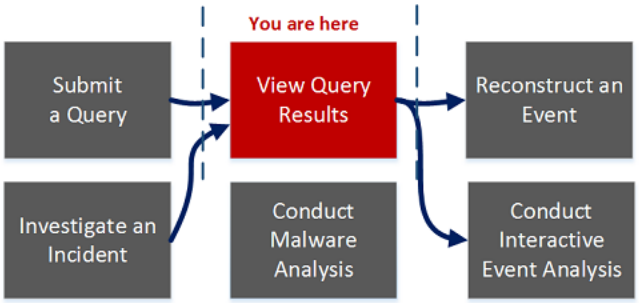
Fonction	Description
	Affiche l'événement précédent.
	Affiche l'événement suivant.
Afficher le log de reconstruction	Affiche le log de reconstruction au bas de la vue. Si vous cliquez sur ce bouton, son intitulé devient Masquer le log de reconstruction.

Vue Événements

Une liste d'événements associée à une session est disponible dans la **Vue Événements**. Il existe deux façons d'afficher la vue Événements :

- Sélectionnez **Enquêter > Événements.** NetWitness Suite 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...	Documentation
Responsable de la recherche des menaces	envoyer une requête*	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	définir les préférences utilisateur pour la vue Événements*	Configurer la vue Parcourir et la vue Événements
Responsable de la recherche des menaces	résultats du filtrage et de la recherche dans la vue Événements*	Examiner des événements

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	associer des événements à partir de sessions partagées*	Associer des événements à partir de sessions partagées
Responsable de la recherche des menaces	ajouter des événements à un incident pour obtenir une réponse*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement*	Reconstruire un événement
Responsable de la recherche des menaces	afficher l'analyse interactive des événements*	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	exporter des fichiers à partir d'un événement*	Exporter des événements
Responsable de la recherche des menaces	gérer les groupes de colonnes*	Gérer des groupes de colonnes dans la vue Événements
Responsable de la recherche des menaces	rechercher le contexte supplémentaire d'une métavaleur*	Afficher un contexte supplémentaire pour un point de données
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Examiner des événements
- Vue Naviguer

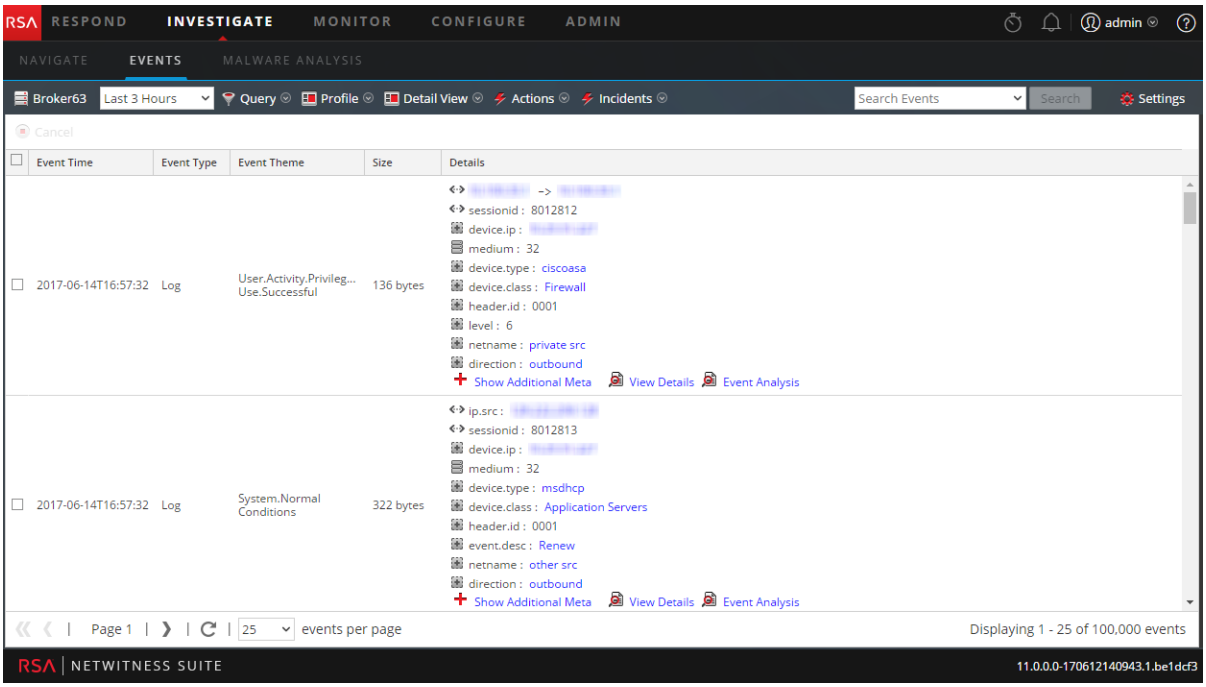
Aperçu rapide

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.

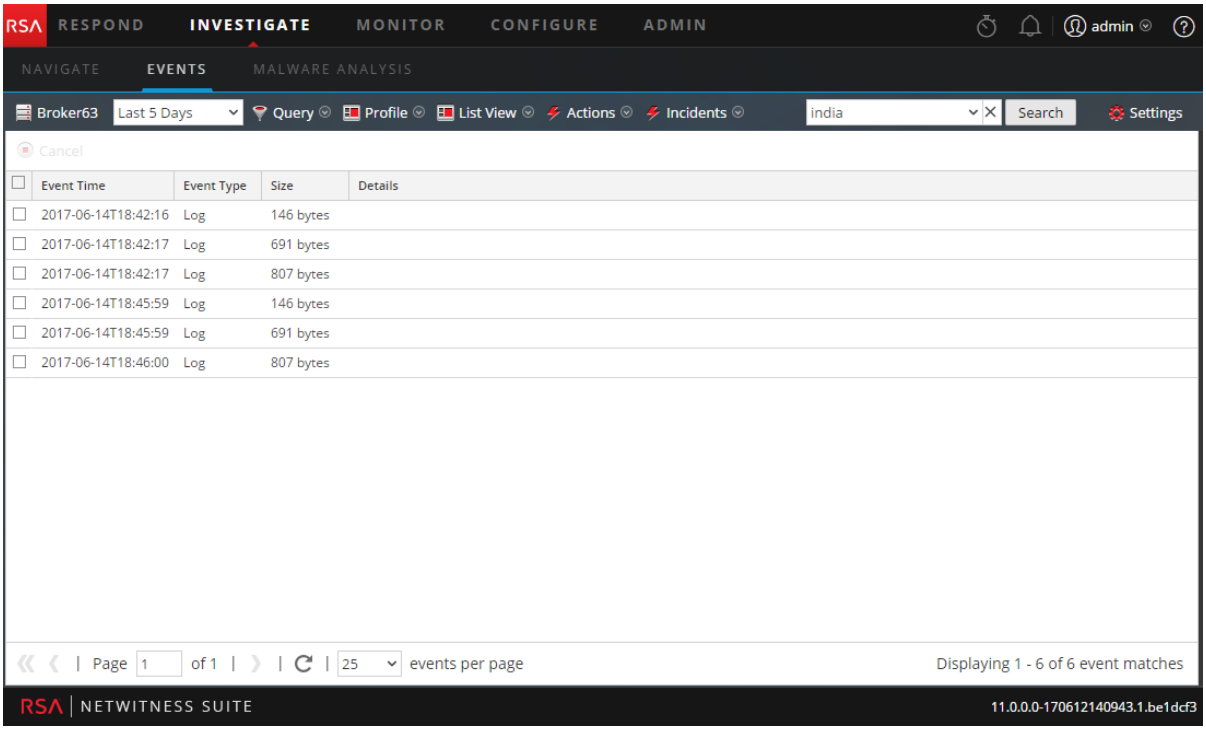
- La vue Liste affiche les informations relatives à l'adresse et au port source et de destination pour les événements sous forme de résumé dans une grille.
- La vue Détails affiche toutes les métadonnées collectées pour l'événement dans une vue de page.
- La vue Log est optimisée pour l'affichage des 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.

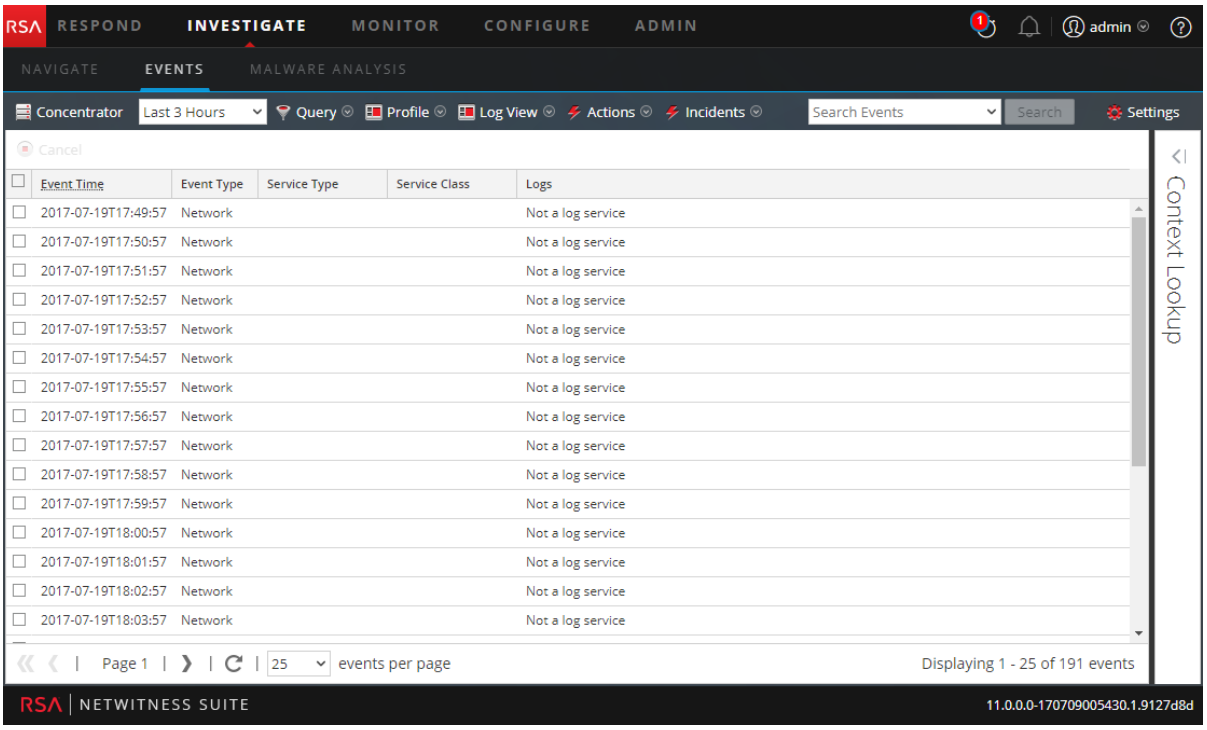
La figure suivante est un exemple d'événements de la vue Détails. Le panneau Recherche contextuelle est visible uniquement si le service Context Hub est configuré.



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.

Fonction	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).

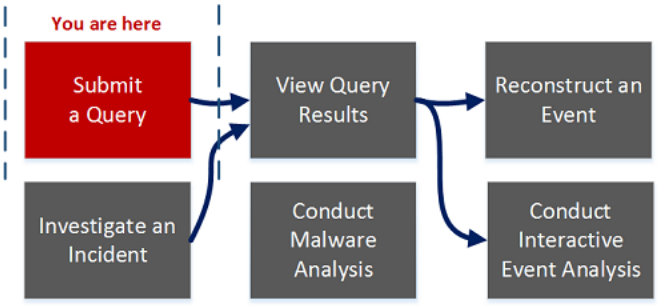
Fonction	Description
Profil	Affiche le menu Profil d'utilisation ; le profil actuellement sélectionné s'affiche dans la barre d'outils. Un profil vous permet de gérer et d'utiliser des profils qui peuvent inclure des groupes méta personnalisés, un groupe de colonne par défaut et une requête de début. 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.

Fonction	Description
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.
Rechercher	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 dans la vue Enquêter
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 Parcourir et la vue Événements).

Boîte de dialogue Analyser

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...	Documentation
Responsable de la recherche des menaces	définir ou modifier un service par défaut*	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	enquêter sur un service ou une collection*	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête

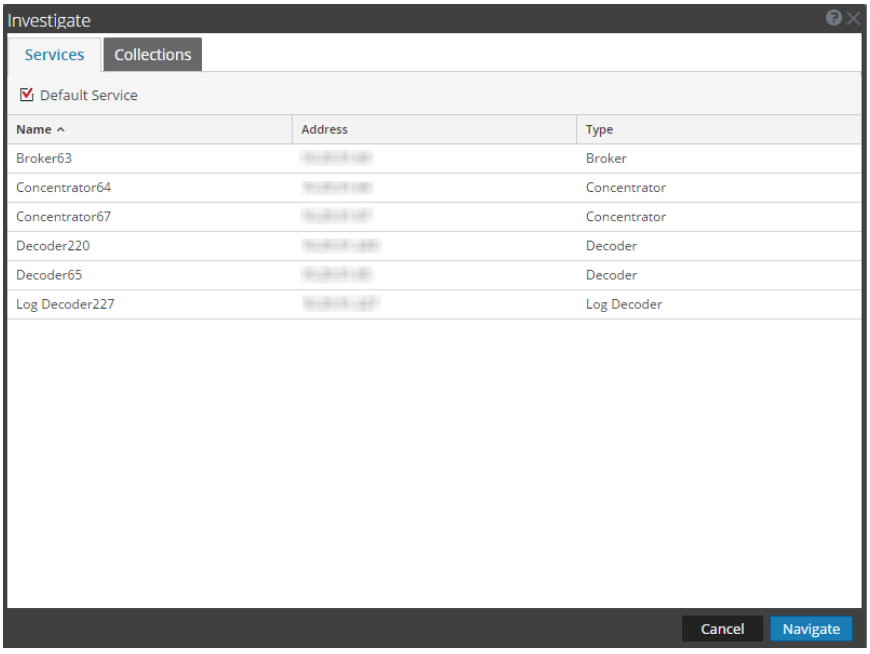
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	effectuer une analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate

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.

Fonction	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.

Fonction	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 Suite lors de l'analyse de données, de l'affichage des événements et de la reconstruction d'événements dans Procédure d'enquête. Pour accéder à cet onglet, sélectionnez  > 

. Lorsque la vue Profil s'affiche, sélectionnez Préférences >onglet Procédure d'enquête. Vous pouvez modifier les préférences utilisateur à tout moment lorsque vous travaillez dans NetWitness Suite.

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher et modifier les préférences utilisateur pour Enquêter*	Configurer la vue Parcourir et la vue Événements
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	effectuer une analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis

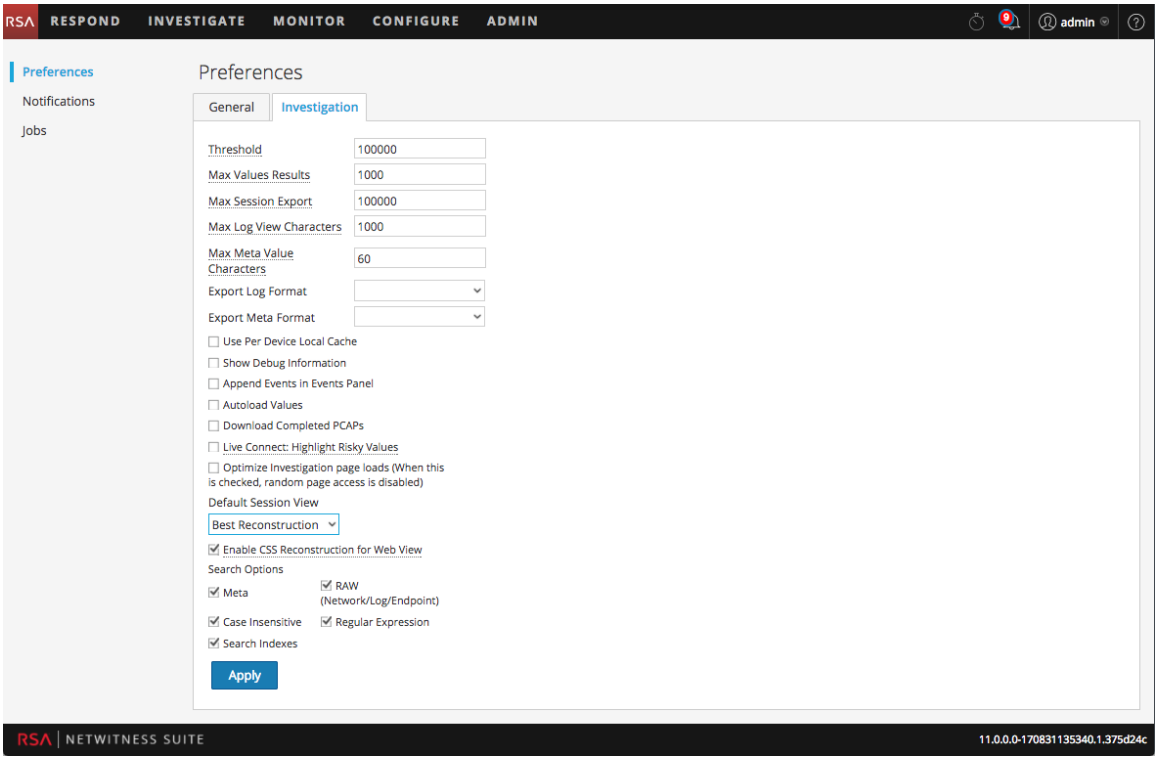
*Vous pouvez effectuer cette tâche dans la vue actuelle.

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.



Fonction	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 Suite 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 max 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**.
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 Suite 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.

Fonction	Description
Format d’exportation de méta	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 Suite 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 Format d’exportation de méta 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 Suite 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.

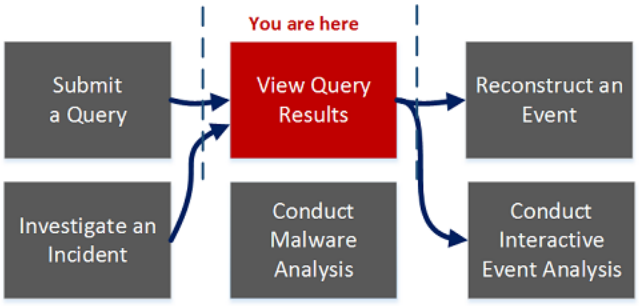
Fonction	Description
Charger automatiquement les valeurs	Lorsque cette option est sélectionnée, les valeurs du service sont automatiquement chargées dans la vue Naviguer. Lorsqu'elle n'est pas sélectionnée, NetWitness Suite affiche un bouton **Charger les valeurs**, ce qui donne à l'utilisateur l'opportunité 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 surbrillance les valeurs risquées	
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.

Fonction	Description
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 dans la vue Enquêter fournit des informations détaillées.
Appliquer	Enregistre vos préférences et les applique immédiatement.

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...	Documentation
Responsable de la recherche des menaces	configurer les clés méta par défaut pour un service*	Gérer et appliquer des clés méta par défaut dans une procédure d'enquête.
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d’événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d’utilisation de NetWitness Respond*

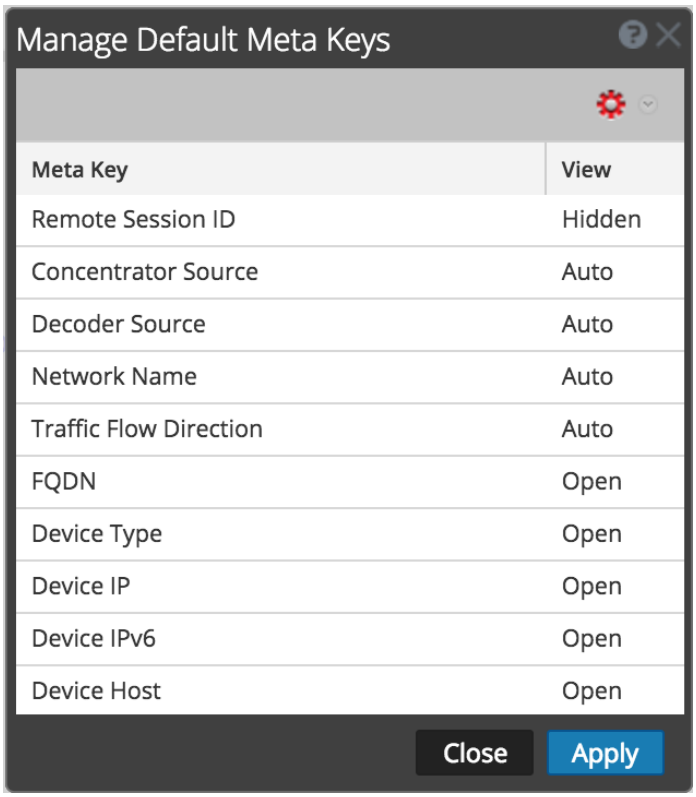
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Gérer les groupes méta
- Fonctionnement de NetWitness Investigate

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.

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.

Fonction	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.

Fonction	Description
Fermer	Ferme la boîte de dialogue. Toutes les modifications non sauvegardées sont perdues.
Appliquer	Applique les modifications, qui prennent effet immédiatement.

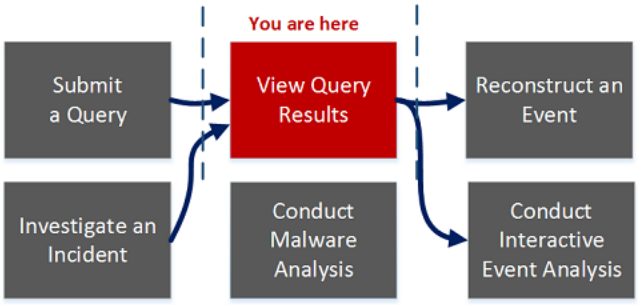
Liste d'événements Malware Analysis et liste Fichiers

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...	Documentation
Responsable de la recherche des menaces	afficher les données d'analyse de malware détaillées des fichiers ou des événements*	Examiner les fichiers et événements d'analyse dans le formulaire de liste
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware*	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

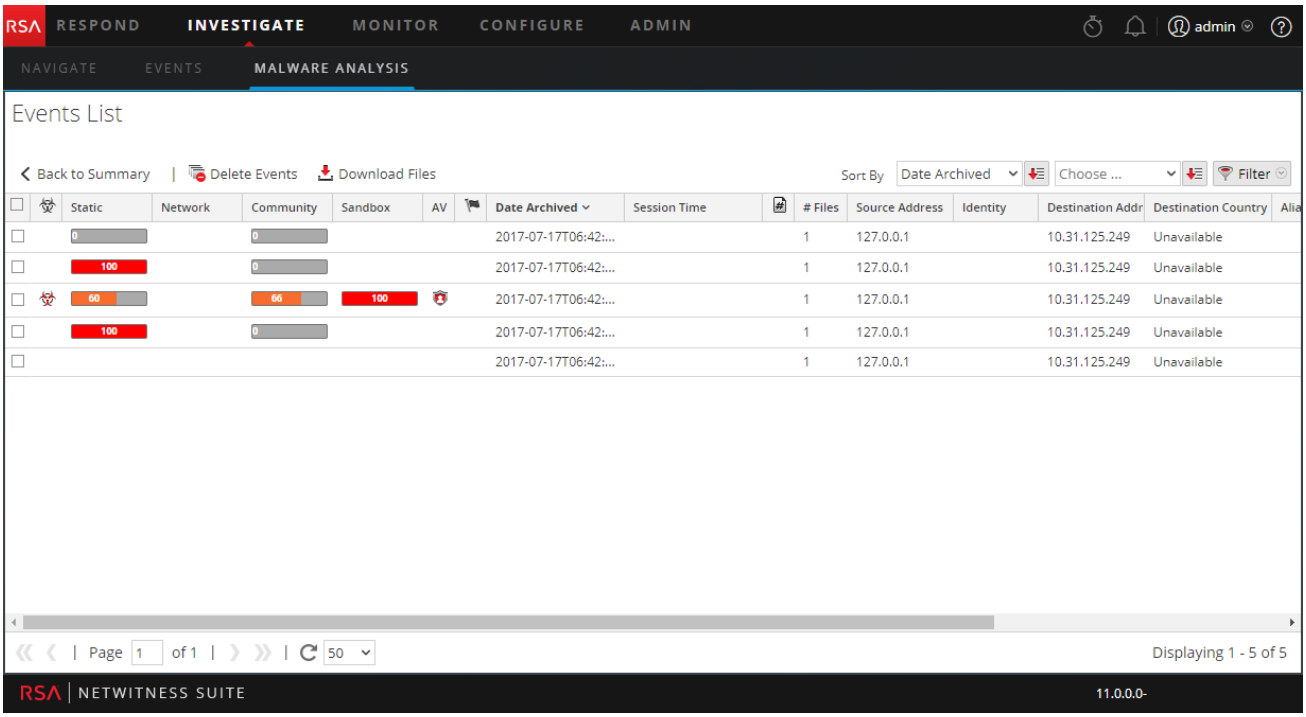
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

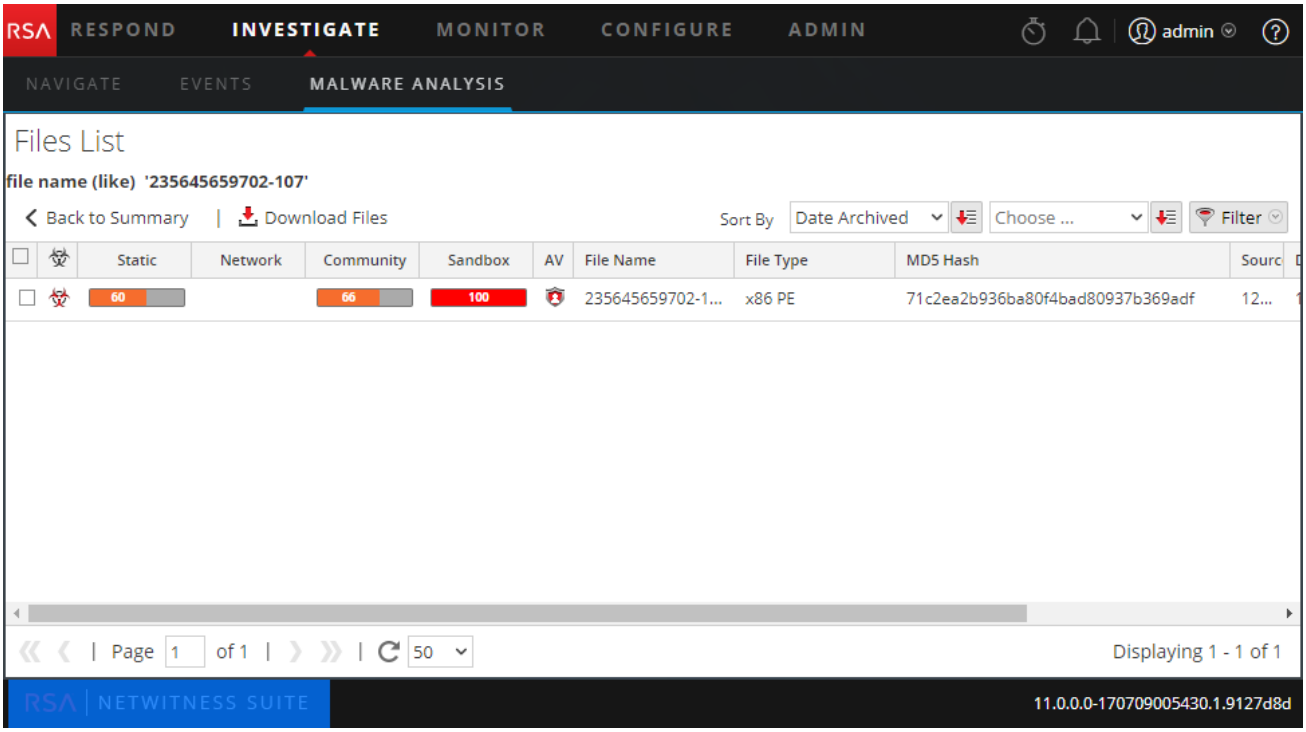
- Fonctionnement de NetWitness Investigate

Aperçu rapide

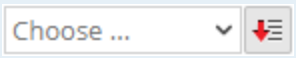
Il s'agit d'un exemple de la vue Liste des événements.

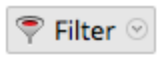


Il s'agit d'un exemple de la vue Liste de fichiers.



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.

Fonction	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.

Fonction	Description
	Affiche un menu déroulant à partir duquel vous pouvez sélectionner un ordre de tri secondaire. Ce menu comprend une option pour NetWitness Suite**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 MD5 Hash.

Voici les fonctions de la liste d'événements.

Fonction	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.
	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.

Fonction	Description
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.

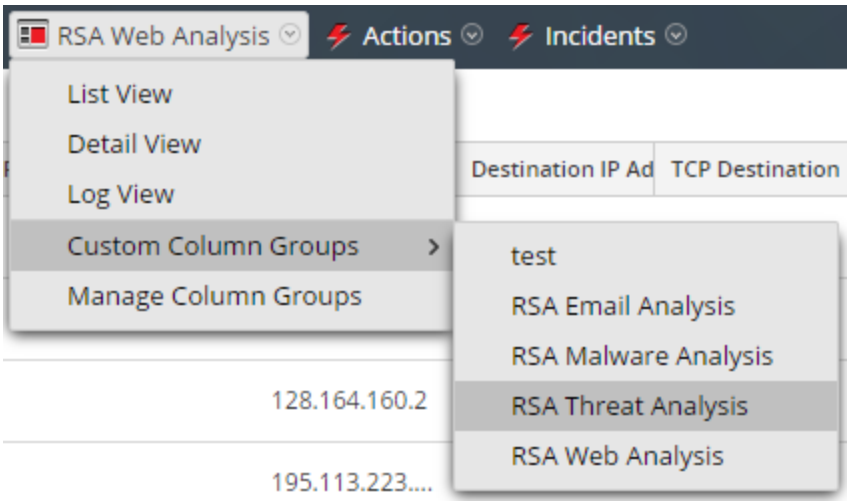
Voici les fonctions de la grille de la liste Fichiers.

Fonction	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.

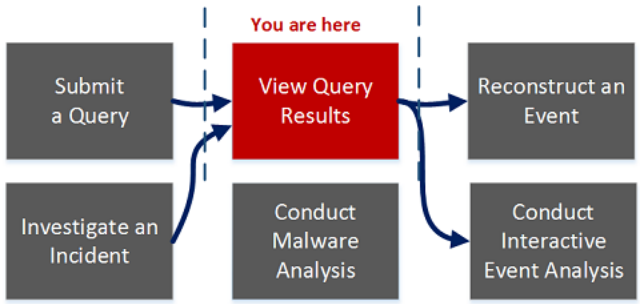
Boîte de dialogue Gérer les groupes de colonnes

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 > vue 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.



Workflow



Que voulez-vous faire ?

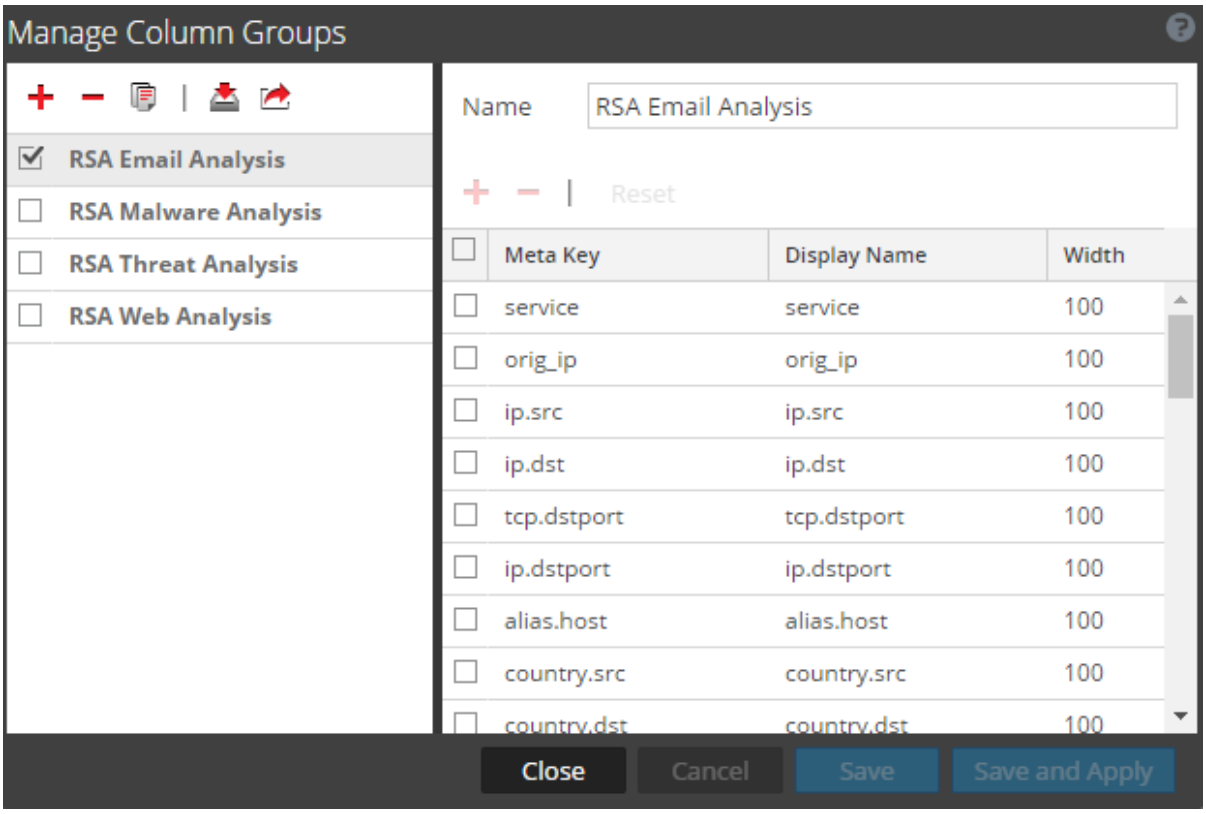
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	groupes de colonnes*	Gérer des groupes de colonnes dans la vue Événements.
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate

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.

Fonction	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.

Fonction	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.

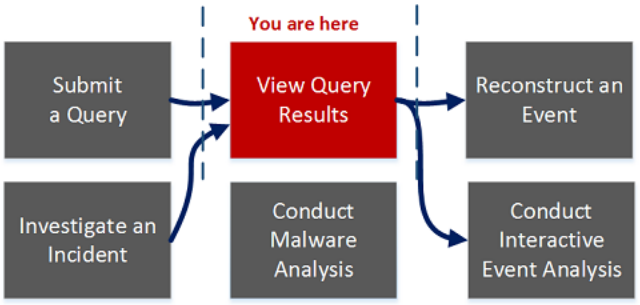
Fonction	Description
Largeur	Spécifie la largeur de chaque colonne de métaclés. La largeur peut être définie entre **10** et **1000**. La largeur par défaut est **100**.

Boîte de dialogue Gérer les 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...	Documentation
Responsable de la recherche des menaces	ajouter, modifier et supprimer des groupes de méta*	Gérer les groupes méta
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

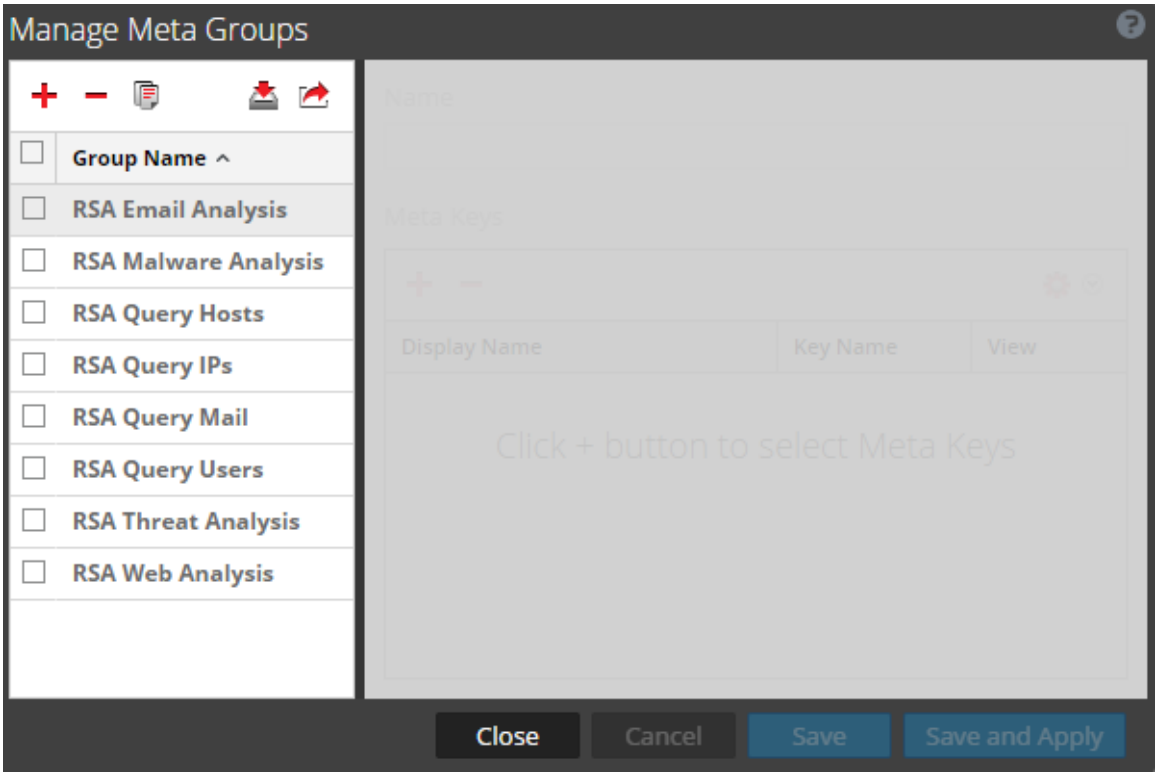
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Gérer et appliquer des clés méta par défaut dans une procédure d'enquête
- Fonctionnement de NetWitness Investigate

Aperçu rapide



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.

Fonction	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.

Fonction	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.

Fonction	Description

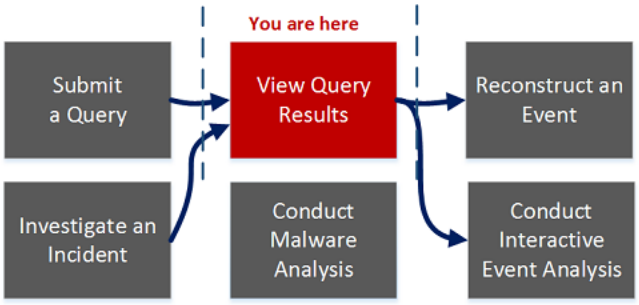
Fonction	Description
Nom	Affiche le nom du métagroupe sélectionné.
	Affiche la boîte de dialogue Clés méta disponibles dans laquelle vous pouvez sélectionner les clés méta à ajouter au groupe.
	Supprime les clés méta sélectionnées.
	Affiche un menu déroulant qui vous permet de sélectionner la vue de 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.
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.

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**.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	configurer des profils*	Utiliser des profils d'investigation pour encapsuler les vues personnalisées.
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

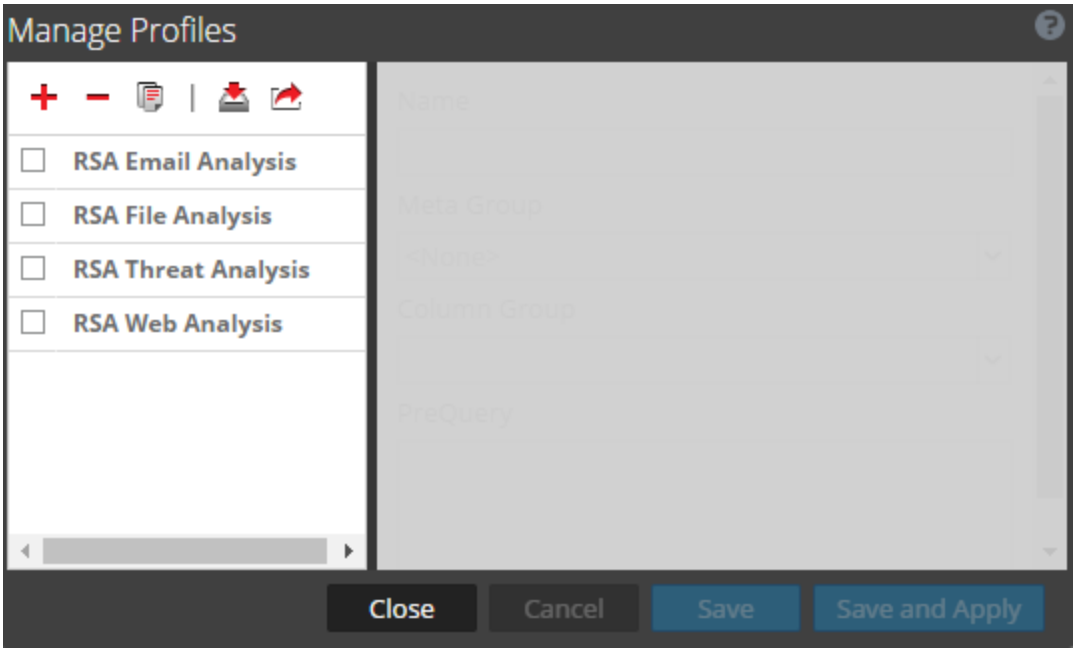
*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Gérer les groupes méta
- Fonctionnement de NetWitness Investigate

Aperçu rapide

Il s'agit d'un exemple de la boîte de dialogue Gérer les 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.
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.

Fonction	Description
Nom	Affiche le nom du profil.
Groupe méta	Affiche un menu déroulant répertoriant les groupes méta disponibles.

Fonction	Description
Groupe de colonnes	Affiche un menu déroulant répertoriant les groupes de colonnes disponibles. Par défaut, trois groupes sont disponibles : • Vue Liste • Vue Détail • 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'`.

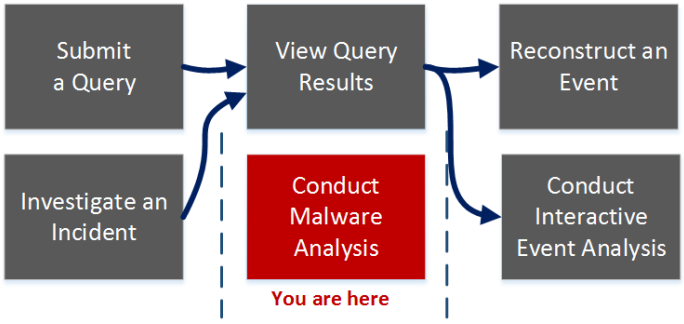
Vue Malware Analysis

Dans NetWitness Suite Enquêter, 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.**

Dans NetWitness, sélectionnez**Procédure d'enquête > 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...	Documentation
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware*	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

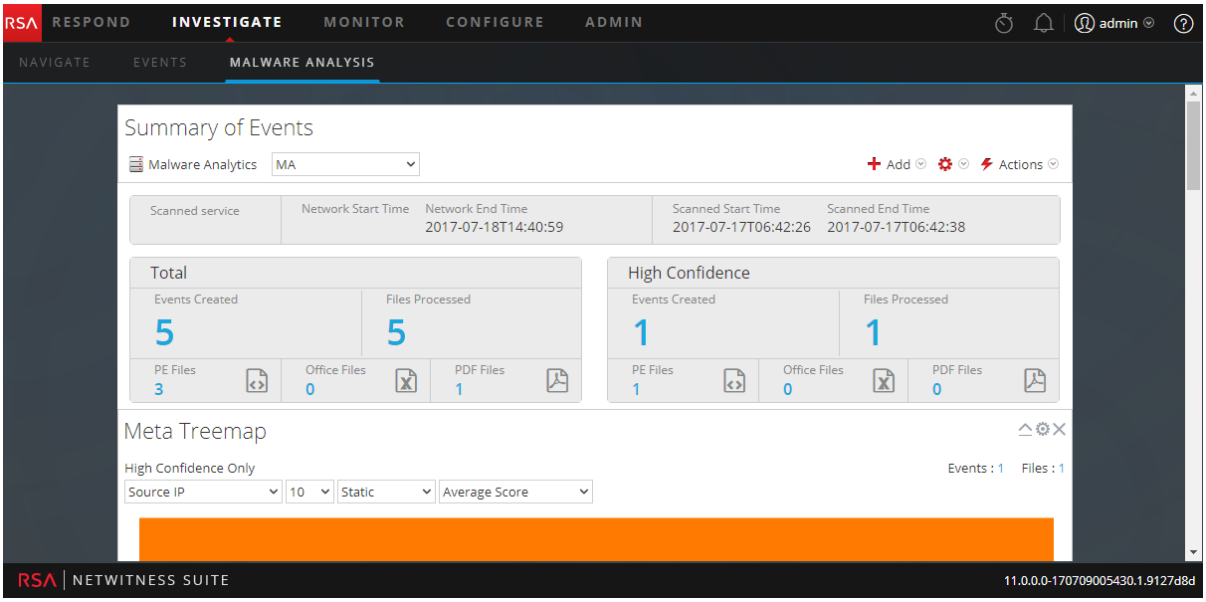
*Vous pouvez effectuer cette tâche dans la vue actuelle.

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 NetWitness Suite sont également disponibles et sont décrites dans la rubrique Dashlets. Voir la rubrique Dashlets dans l'espace Contenu RSA de RSA NetWitness® Suite.

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.

Fonction	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.
	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.

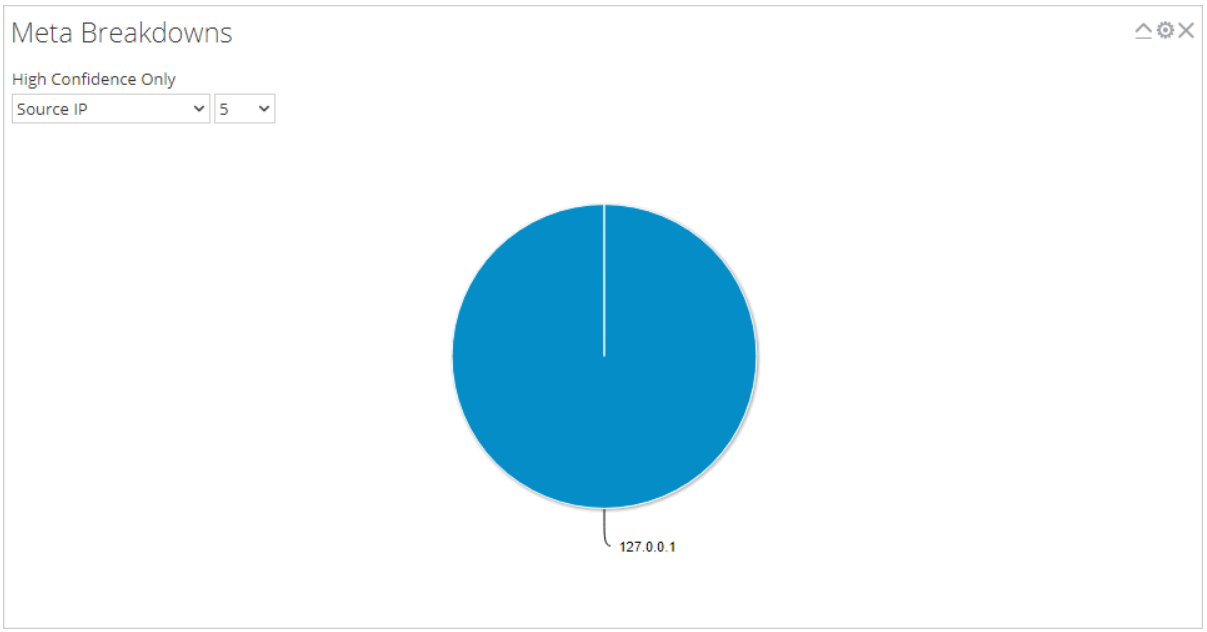
Boîte de dialogue Options

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.

Fonction	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.

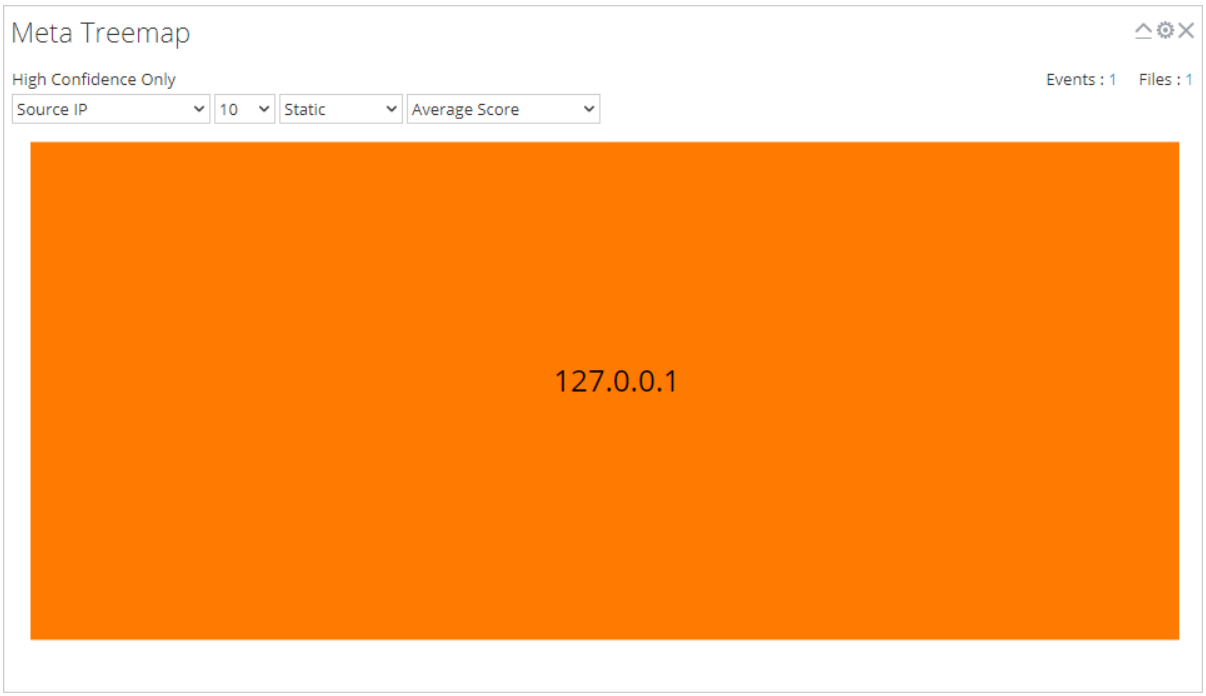


Le tableau suivant décrit les options du dashlet Répartition des méta.

Fonction	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.

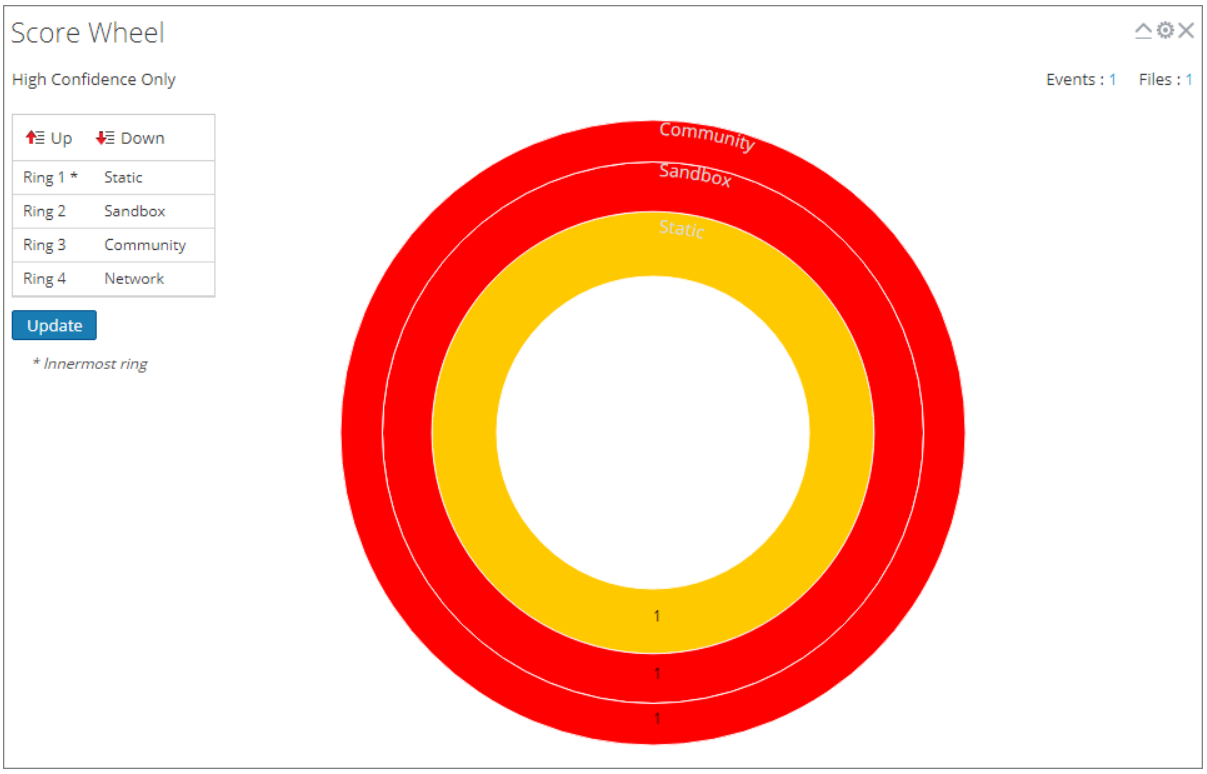


Le tableau suivant décrit les options du dashlet Compartimentage des méta.

Fonction	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.

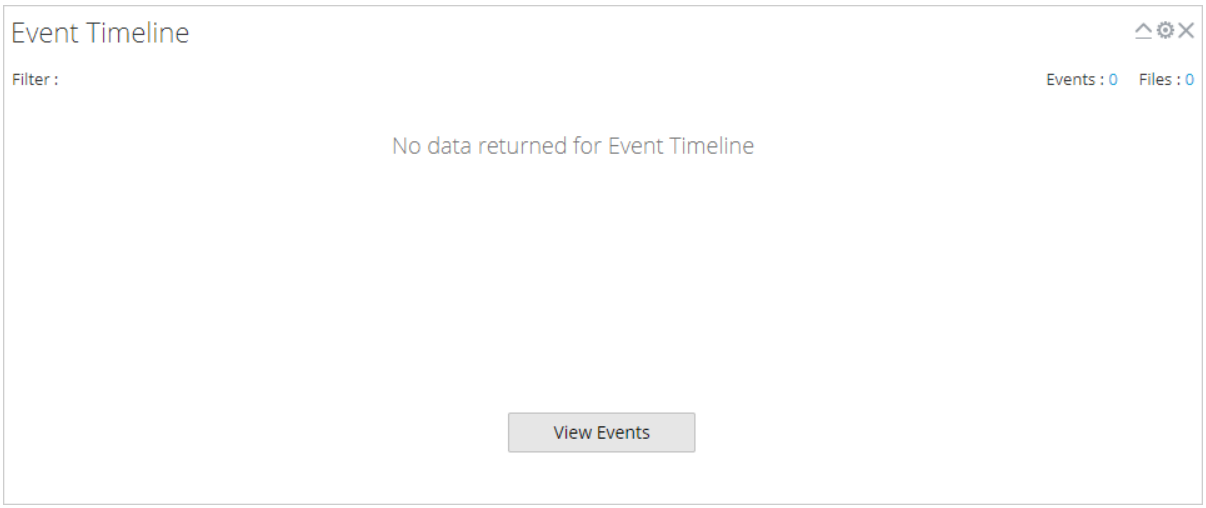


Le tableau suivant décrit les fonctionnalités du dashlet Roue des scores.

Fonction	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 notes, 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.

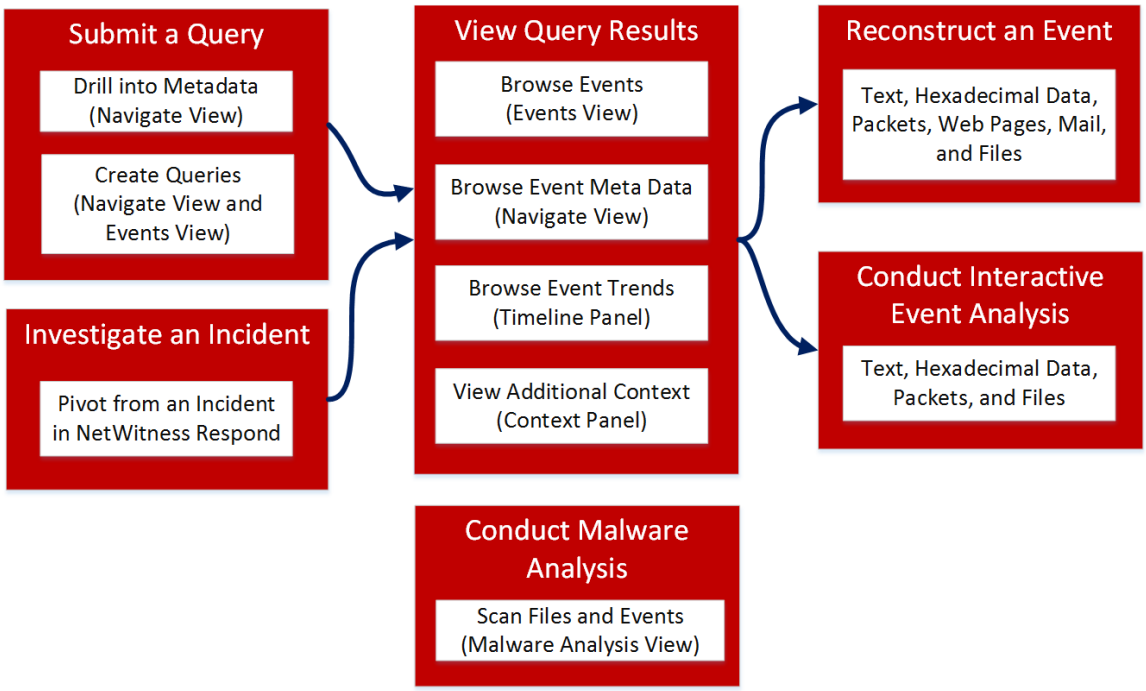
Fonction	Description
Forte probabilité uniquement	Indique si les résultats sont limités aux événements indiqués en tant que confiance élevée ou non. Si les résultats ne sont pas restreints, cette ligne ne s'affiche pas.
Affichage des événements	Affiche la vue Procédure d'enquête > Événements.

Vue Naviguer

Vue Naviguer (**ENQUÊTER** > Parcourir) est le point d'entrée principal pour NetWitness Investigate. La vue Naviguer affiche l'activité et les valeurs du service sélectionné en conformité avec les options de Procédure d'enquête : profil, période, groupe méta et requête. Au fur et à mesure que les analystes recherchent des événements pertinents, les clés méta et les valeurs méta s'affichent.

Workflow

Le workflow ci-dessous décrit les étapes générales et les sous-tâches d'enquête portant sur les événements.



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 des 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, 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...	Documentation
Responsable de la recherche des menaces	envoyer une requête ou effectuer une recherche verticale dans le jeu de données*	Interroger les données dans la vue Parcourir
Responsable de la recherche des menaces	définir les préférences utilisateur pour la procédure d'enquête*	Configurer les vues et préférences de procédure d'enquête
Responsable de la recherche des menaces	affiner les résultats de la requête*	Affiner les résultats affichés dans la vue Naviguer
Responsable de la recherche des menaces	ouvrir un point de recherche verticale dans la vue Événements*	Ouvrir la liste d'événements
Responsable de la recherche des menaces	visualiser un événement*	Effectuer une recherche verticale dans les données au sein du graphique chronologique de la vue Naviguer
Responsable de la recherche des menaces	exporter ou imprimer un point d'extraction, lancer une recherche externe ou une analyse de malware*	Agir sur un point de recherche verticale dans la vue Parcourir
Responsable de la recherche des menaces	rechercher un contexte supplémentaire sur un événement*	Afficher un contexte supplémentaire pour un point de données

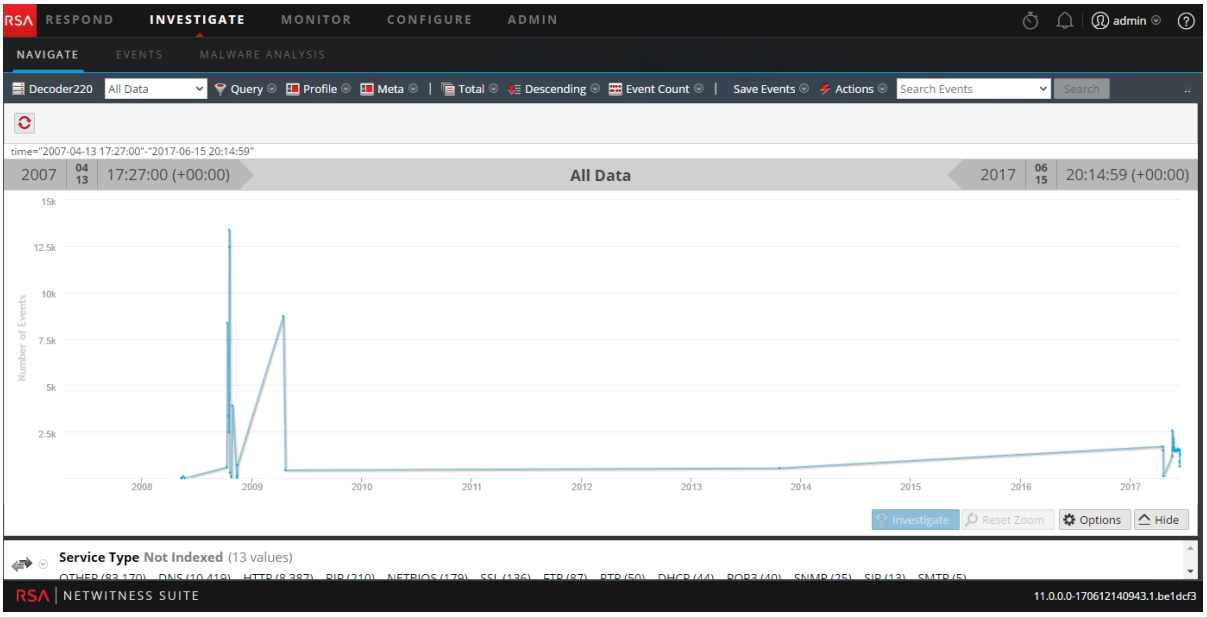
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	afficher la reconstruction d'un événement	Reconstruire un événement
Responsable de la recherche des menaces	afficher l'analyse interactive des événements	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	Mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle

Rubriques connexes

- Fonctionnement de NetWitness Investigate
- Mener une procédure d'enquête
- Vue Événements
- Vue Malware Analysis

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, 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 d'un service ou d'une collection). 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 Définir la période d'investigation). 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 > Naviguer.
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.

Option	Description
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 d'investigation pour encapsuler les vues personnalisées.
Meta	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).
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 la rubrique Définir la méthode de quantification et trier la séquence des résultats de clé méta).
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 la rubrique Définir la méthode de quantification et trier la séquence des résultats de clé méta).

Option	Description
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 la rubrique Définir la méthode de quantification et trier la séquence des résultats de clé méta)). 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).

Option	Description
Actions	Le menu Actions contient plusieurs actions (Visualiser, Accéder à l'événement et Imprimer) que vous pouvez effectuer dans la vue Naviguer (voir la rubrique Agir sur un point de recherche verticale dans la vue Parcourir).
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 dans la vue Enquêter).
Paramètres	Affiche les paramètres Investigation de la vue Naviguer (qui sont également modifiables dans la vue Profil) pour que vous puissiez modifier les paramètres Investigation 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 Parcourir 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.

Fonction	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).
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 Suite 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

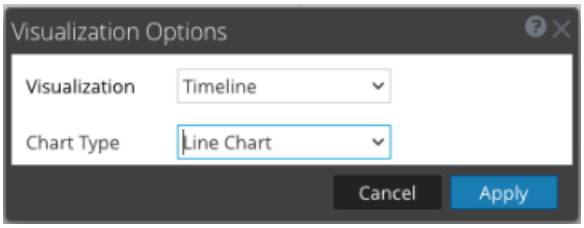
Juste en dessous du fil d'Ariane et des informations de débogage, (si disponibles), la bannière Temps affiche la période utilisée pour créer le graphique.

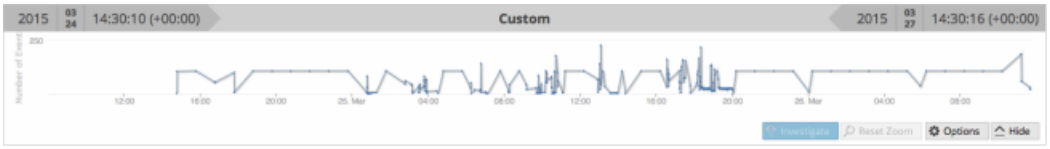
Visualisation

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 la rubrique Effectuer une recherche verticale dans les données au sein du graphique chronologique de 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.



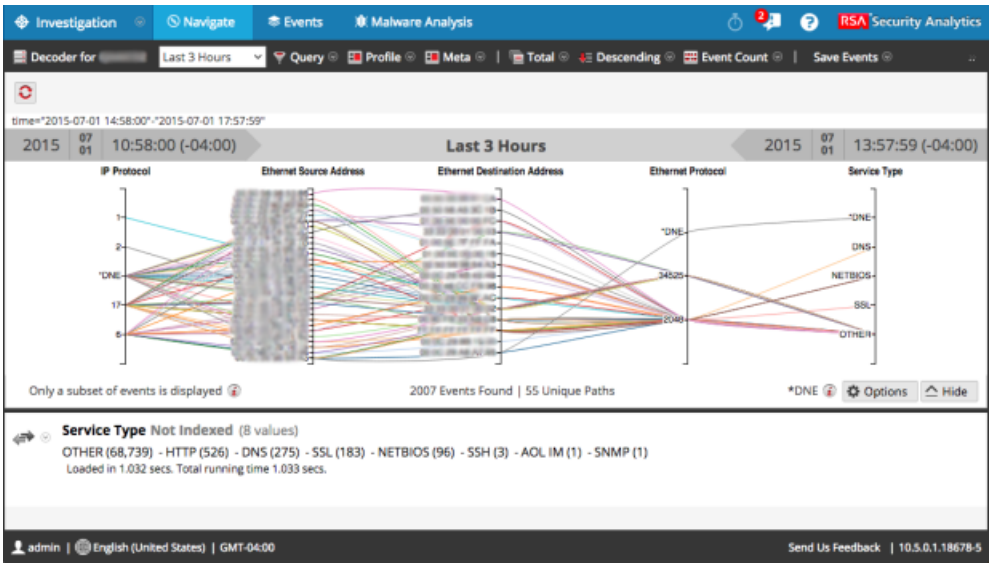


La chronologie affiche une activité pour le service et la période spécifiés, comme un graphique linéaire ou un graphique à barres en fonction de votre choix dans le menu Options.

Fonction	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).



Fonction	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.

Fonction	Description
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.

Fonction	Description
Sélection de visualisations	Affiche une liste déroulante des types de visualisation : Chronologie et coordonnées
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.

Fonction	Description
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.

Fonction	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 la rubrique Effectuer une recherche verticale dans les données dans le panneau Valeurs).

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 Suite interroge les clés. Au fur et à mesure que le chargement des données s'effectue dans le panneau Valeurs, NetWitness Suite 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 Suite cesse de compter le nombre de métavaleurs dans une session (Seuil de session). Si un seuil est défini pour une session, la vue Navigation 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 Suite cesse de compter le nombre de métavaleurs dans une session (Seuil de session). Si un seuil est défini pour une session, la vue Navigation 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 Suite 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 Suite affiche les résultats dans le panneau Valeurs.

1. NetWitness Suite 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 Suite reçoit et affiche les messages de progression.

ii. **Résultats partiels** : NetWitness Suite 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 Suite 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 Suite 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 Suite 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 Suite. Par exemple, lorsque vous interrogez un service Broker 10.4 extrayant ses données de plusieurs services Concentrator, NetWitness Suite 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. 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.

Fonction	Description
Clé méta	Nom de la clé méta qui est affiché. Par exemple, **Service Type** 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 **Service Type** et 20 of 20+ values correspond aux valeurs actuellement affichées. Vous pouvez afficher d'autres valeurs en cliquant sur **...show more**.

Fonction	Description
🔍	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.
Métavaleur, 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.

Fonction	Description
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.

Menus contextuels des clés méta

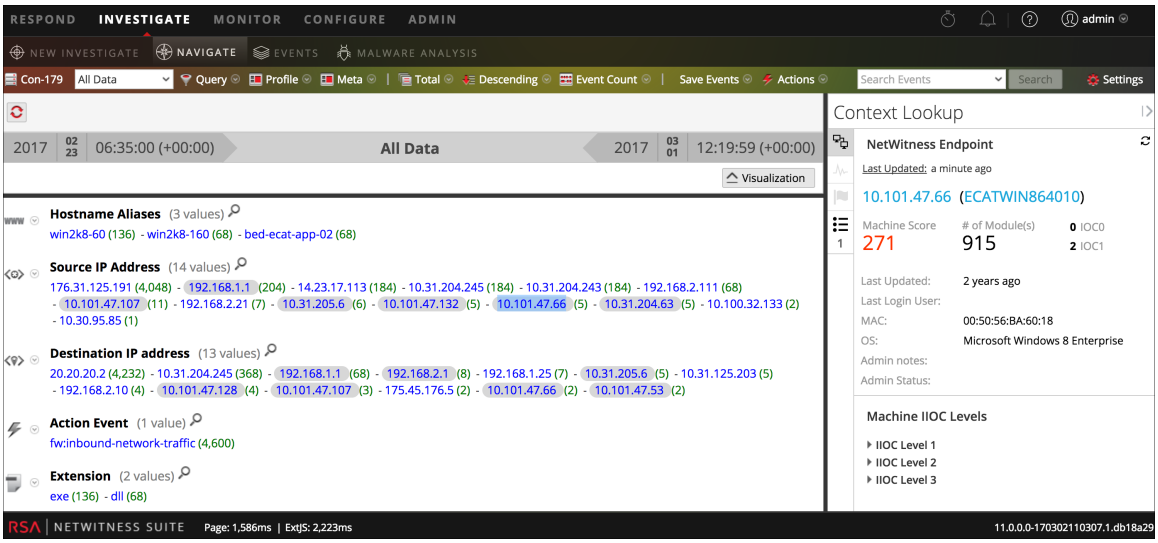
Les clés méta contenues dans le panneau Valeurs fournissent des menus contextuels. En regard de chaque libellé de méta, une flèche déroulante affiche les options qui peuvent être appliquées à cet élément. Vous pouvez les utiliser pour modifier le mode d'affichage des résultats de la clé méta dans la vue actuelle. Les modifications apportées aux clés méta s'affichent dans la vue active lors d'une recherche verticale, sauf si vous actualisez la page ou sélectionnez un nouveau service dans la barre d'outils de la vue Naviguer. Une actualisation Gérer et appliquer des clés méta par défaut dans une procédure d'enquête 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 dans une procédure d'enquête). Si vous n'avez effectué aucune modification dans la boîte de dialogue Gérer les clés méta par défaut, NetWitness Suite restaure les clés méta par défaut à partir du service de base.

- Autres résultats
- Résultats maximum
- Masquer les résultats
- Info sur la clé méta

Panneau Recherche contextuelle

La vue Naviguer et la vue Événements ont un panneau sur le côté droit appelé le panneau Recherche contextuelle. 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.

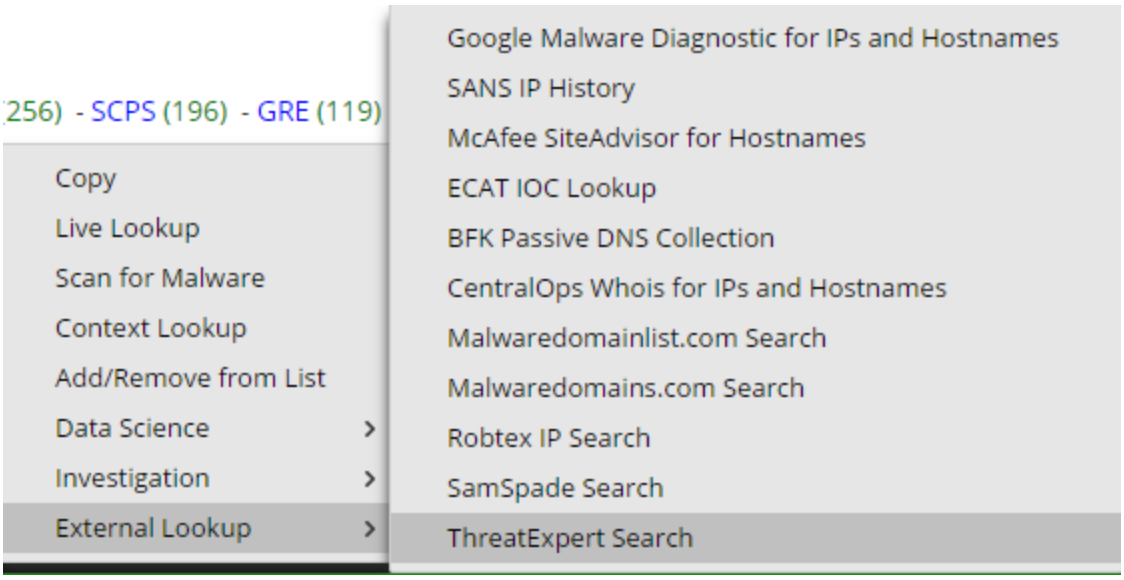


Une fois que l'administrateur a configuré le service Context Hub, vous pouvez afficher les informations contextuelles des métavaleurs dans la vue Naviguer et la vue Événements. Pour plus d'informations sur la configuration du service Context Hub, reportez-vous au *Guide de configuration du service Context Hub*. Pour plus d'informations sur l'exécution de la recherche contextuelle des valeurs méta, consultez la rubrique Afficher un contexte supplémentaire pour un point de données.

Le service Context Hub est pré-configuré avec un mappage du type de méta et de la clé méta par défaut. Pour plus d'informations sur le mappage de la métavaleur du service Context Hub avec une clé méta de procédure d'enquête, consultez la rubrique « Gérer le mappage 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.

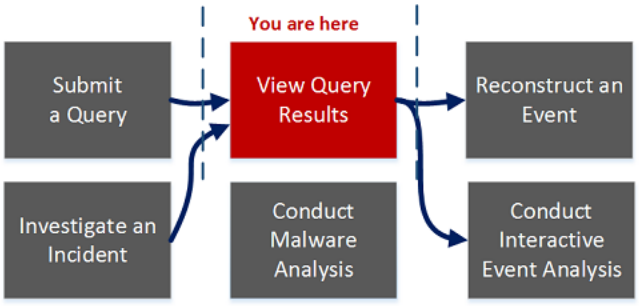
Les données sont affichées dans le panneau Contexte, uniquement si des données sont disponibles.

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...	Documentation
Responsable de la recherche des menaces	créer une requête personnalisée*	Créer une requête personnalisée
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements

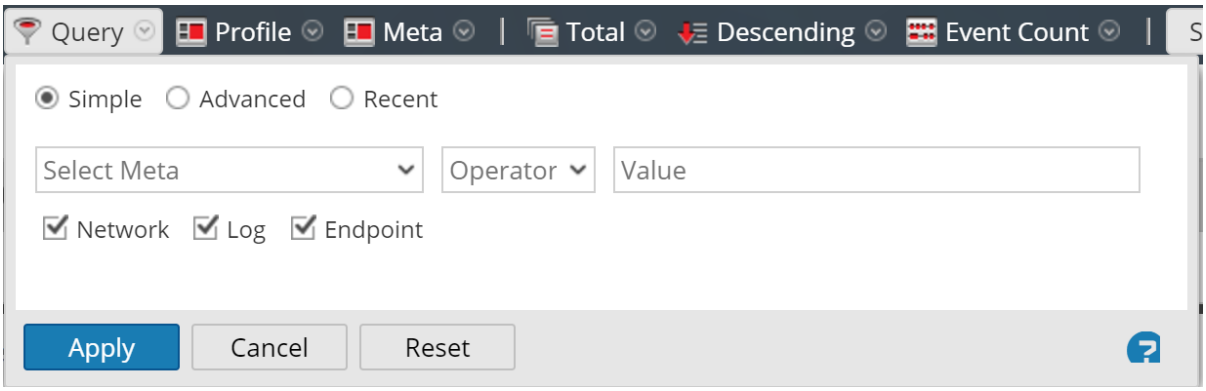
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Rubriques connexes

- Fonctionnement de NetWitness Investigate

Aperçu rapide

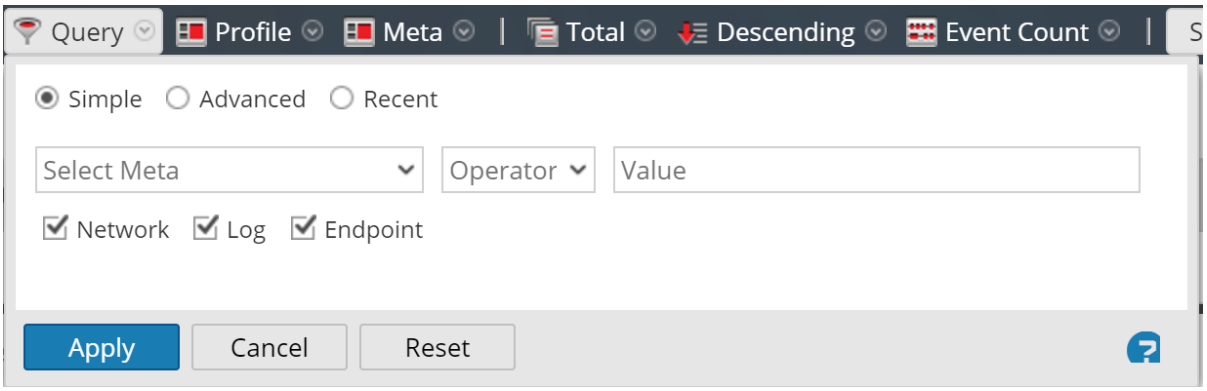


La boîte de dialogue Requête propose trois vues :

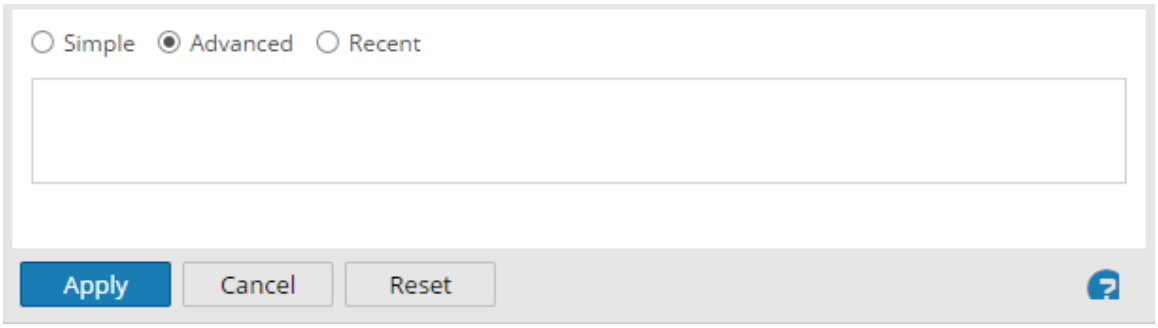
- Simple
- Avancé
- Récente

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.

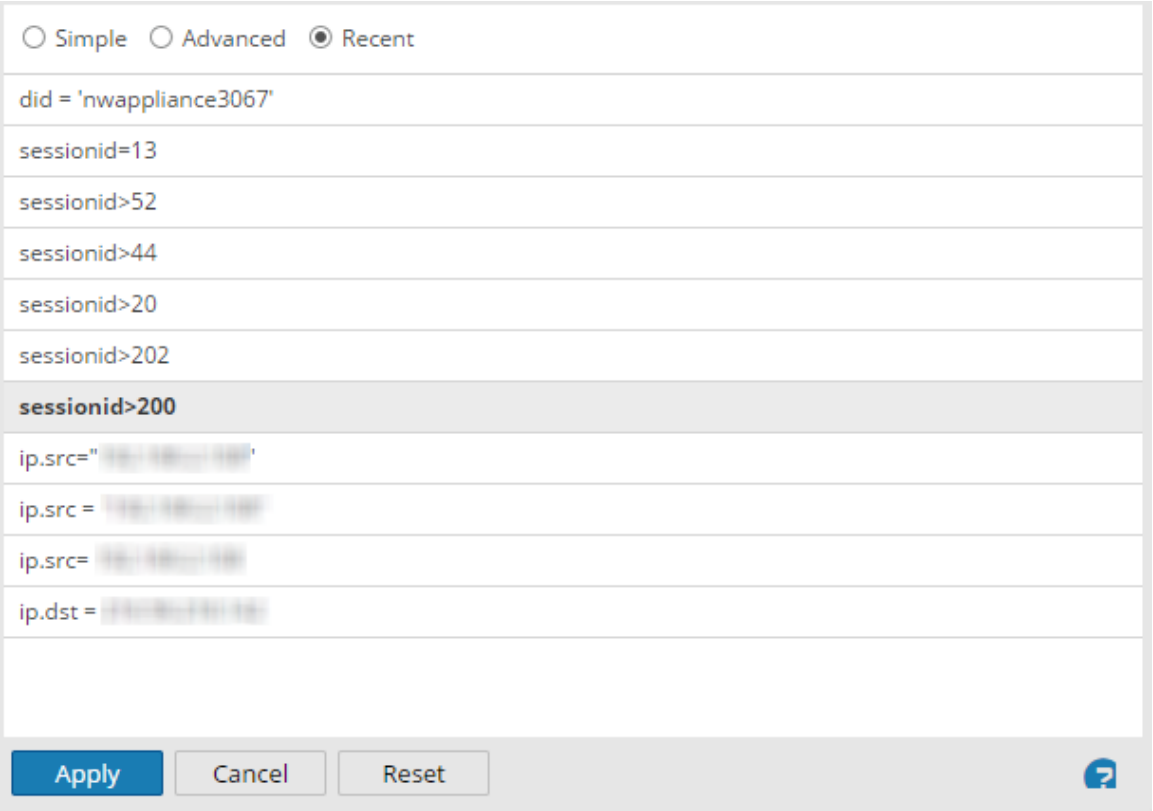
Vue Simple



Vue Avancé



Vue Récente



Le tableau suivant décrit les fonctions de la boîte de dialogue Requête.

Fonction	Description
Sélectionner les méta	Affiche une liste déroulante de métagroupes.
Opérateur	Affiche une liste déroulante d'opérateurs (=,NetWitness Suite!=,NetWitness Suiteexists,NetWitness Suite!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.

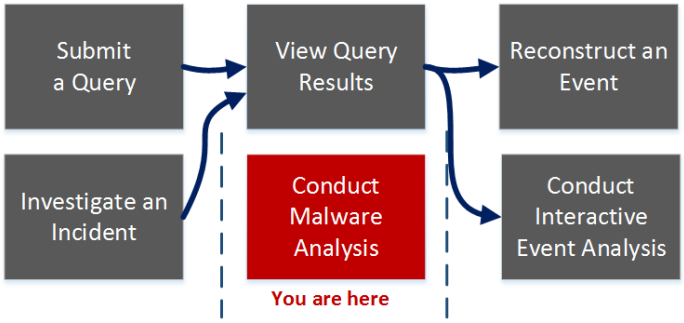
Fonction	Description
Zone de requête	Permet de saisir une requête dans la vue Avancé. Au début de la saisie, une liste déroulante répertoriant les clés méta disponibles pour le service s'affiche, suivie d'une liste d'opérateurs. Si l'expression saisie dans la zone de recherche n'est pas valide, un message d'avertissement s'affiche à côté. Lorsque la requête est valide, cet avertissement disparaît.
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 malware

Dans la boîte de dialogue Analyser les malware, 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...	Documentation
Responsable de la recherche des menaces	envoyer un fichier à l'analyse des malware *	Télécharger des fichiers pour l'analyse Malware Analysis
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware*	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d'utilisation de NetWitness Respond*

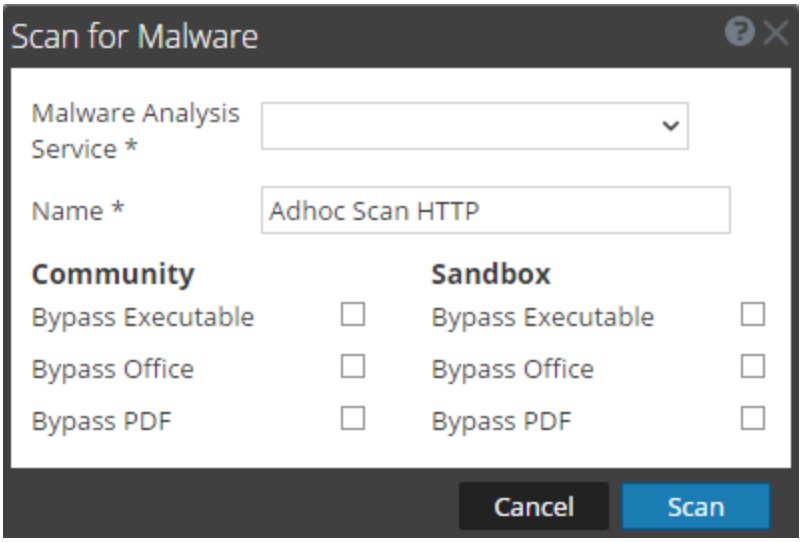
*Vous pouvez effectuer cette tâche dans la vue actuelle.

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 malware et le tableau suivant décrit les fonctions disponibles dans la boîte de dialogue Analyser les malware.

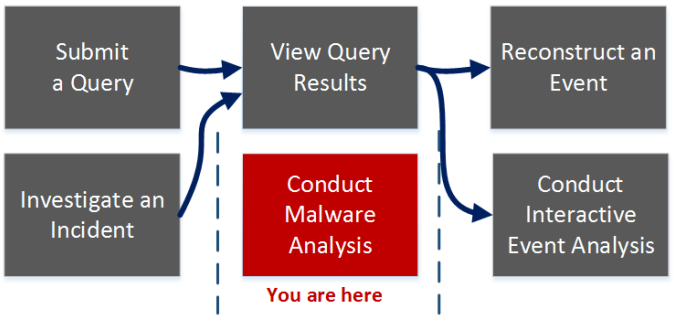


Fonction	Description
	Télécharge un fichier depuis votre ordinateur.
	Supprime un fichier de la liste.
Nom de fichier	Affiche les noms des fichiers ajoutés à la liste.
Nom	Vous permet de nommer la tâche d'analyse.
Communauté	Affiche des options pour la communauté pour contourner ou ignorer certains types 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...	Documentation
Responsable de la recherche des menaces	envoyer un fichier à l'analyse des malware * Source for Warehouse	Télécharger des fichiers pour l'analyse Malware Analysis
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

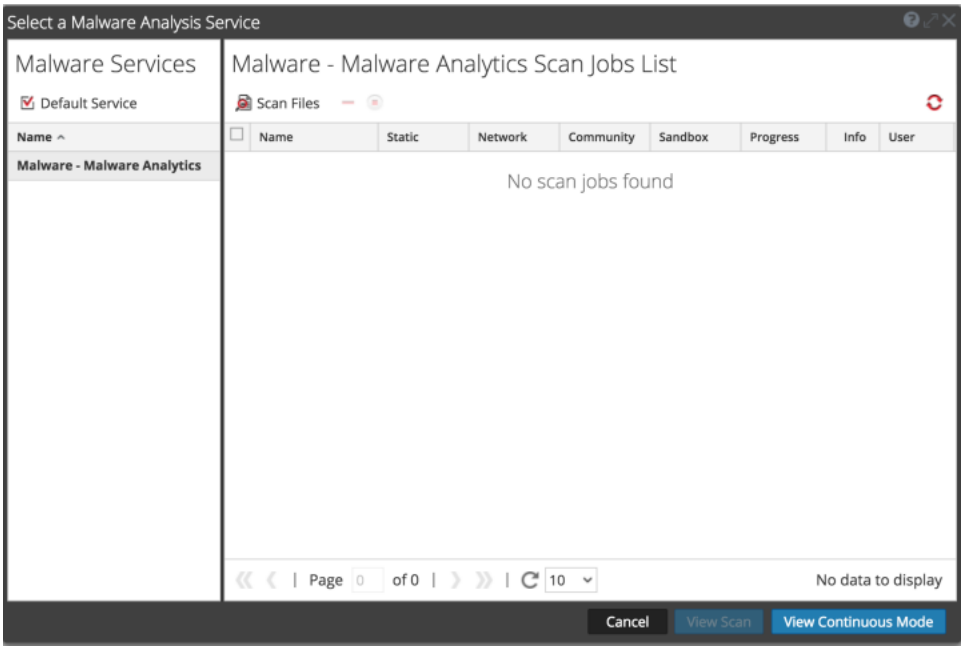
Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d'événements
Responsable de la recherche des menaces	mener une analyse de malware*	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*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.

Fonction	Description
Scan Files	Affiche la boîte de dialogue Analyser les malware, 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 Suite 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.

Fonction	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 :

Fonction	Description
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.
Planifiée	Affiche la date et l'heure auxquelles la tâche a été exécutée.

Les actions disponibles dans la boîte de dialogue sont les suivantes.

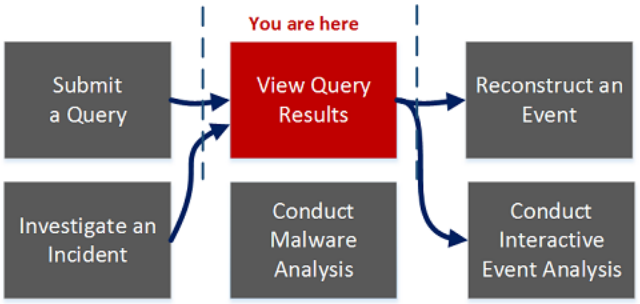
Fonction	Description
Bouton Annuler	Annule la tâche d'analyse sélectionnée.
Bouton Afficher l'analyse	Affiche le Récapitulatif des événements pour l'analyse sélectionnée avec les dashlets par défaut affichés.
Bouton Afficher le mode continu	Affiche le Récapitulatif des événements pour l'analyse sélectionnée avec les dashlets par défaut affichés.

Boîte de dialogue Paramètres pour les vues Naviguer et Événements

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 Suite 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, allez à la vue **Naviguer** ou **Événements** et sélectionnez l'option **Paramètres** dans la barre d'outils.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	configurer les préférences pour Enquêter*	Configurer la vue Parcourir et la vue Événements
Responsable de la recherche des menaces	envoyer une requête	Commencer une procédure d'enquête d'un service ou d'une collection
Responsable de la recherche des menaces	afficher les résultats de la requête*	Mener une procédure d'enquête
Responsable de la recherche des menaces	reconstruire un événement	Reconstruire un événement

Rôle d’utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	analyser un événement	Analyser les événements dans la vue Analyse d’événements
Responsable de la recherche des menaces	mener une analyse de malware	Mener une analyse Malware Analysis
Responsable de la réponse aux incidents	enquêter sur un incident	*Guide d’utilisation de NetWitness Respond*

*Vous pouvez effectuer cette tâche dans la vue actuelle.

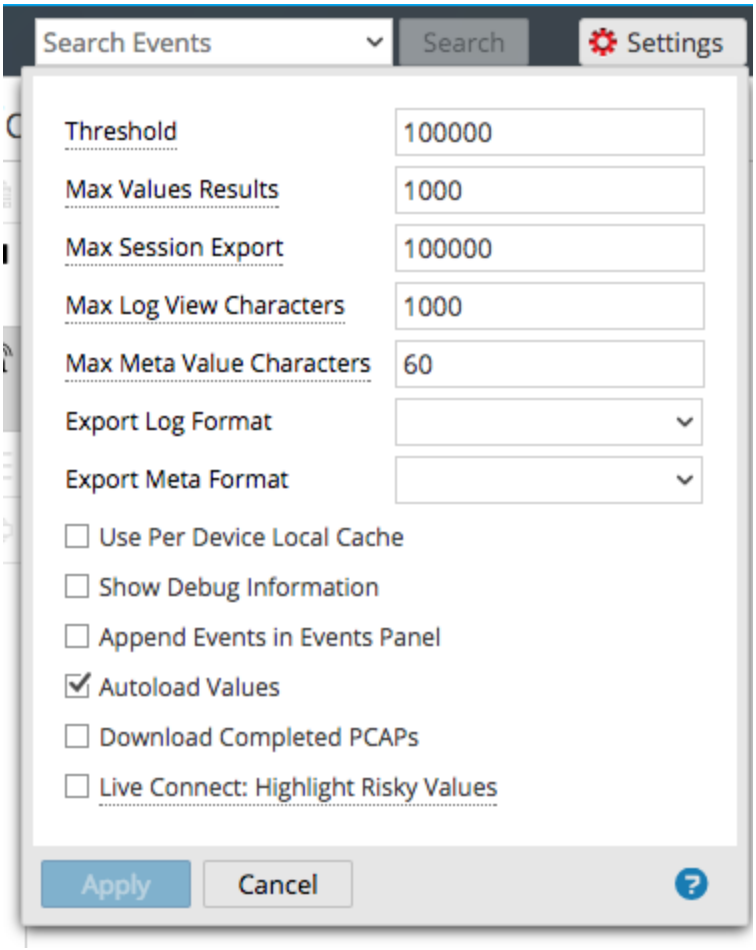
Rubriques connexes

- 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.



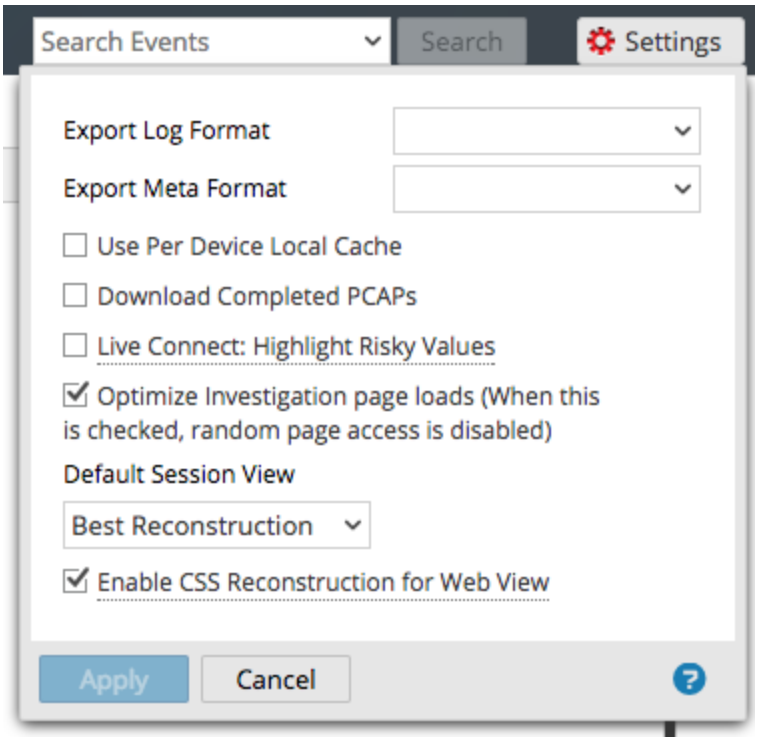
Fonction	Description
Seuil	Définit le seuil du nombre maximum de sessions chargées pour une valeur de clé meta dans le panneau Valeurs. Un seuil supérieur offre des décomptes précis pour une valeur, et cause également des temps de charge plus longs. La valeur par défaut est **100000**.
Nb max résultats 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**.

Fonction	Description
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
Format d'exportation de méta	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)

Fonction	Description
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**.
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.



Fonction	Description
Format du log d'exportation	Définit le format des logs exportés. Quatre formats sont disponibles : • Text • SML • CSV • JSON
Format d'exportation de méta	Définit le format de fichier des métavaleurs exportées. Quatre formats sont disponibles : • Text • SML • CSV • JSON

Fonction	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	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 Suite 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**.
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.

Fonction	Description
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.
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.