



# Guide de configuration 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](http://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

---

<b>Comment fonctionne Malware Analysis</b> .....	<b>1</b>
Présentation fonctionnelle .....	1
Méthode d'analyse .....	3
Serveur NetWitnessAccédez au service Malware Analysis .....	3
Méthode de notation .....	4
Déploiement .....	4
<b>Modules de scores</b> .....	<b>5</b>
Réseau .....	5
Analyse statique .....	6
Communauté .....	6
Sandbox .....	6
<b>Rôles et autorisations pour les analystes</b> .....	<b>7</b>
Rôles et autorisations nécessaires .....	7
<b>Configuration de Malware Analysis</b> .....	<b>11</b>
Liste de contrôle de configuration de base .....	11
Configurer l'environnement d'exploitation de Malware Analysis .....	13
Connexions réseau .....	14
Ajouter un hôte et un service Malware Analysis .....	15
Condition préalable .....	16
Procédure .....	16
Configurer les paramètres généraux de Malware Analysis .....	20
Afficher les paramètres de base .....	21
Configurer le rappel continu .....	22
Configurer les paramètres de téléchargement manuel des fichiers .....	24
Configurer le référentiel d'entreprise .....	25
Calibrer les modules de score .....	25
Configurer le score d'analyse Static .....	26
Configurer le score d'analyse des pairs .....	27
Configurer le score d'analyse Sandbox .....	28
Configurer les Indicateurs de compromission .....	30

Filtrer les IOC affichés par module .....	32
Filtrer les modules affichés pour montrer uniquement les modules modifiés .....	33
Activer et désactiver les IOC d'un module de score .....	33
Modifier la pondération de score d'un IOC .....	34
Définir l'indicateur de forte probabilité d'un IOC .....	35
Réinitialiser les paramètres par défaut des IOC .....	36
Configurer les fournisseurs d'antivirus installés .....	36
Identifier le logiciel AV installé .....	37
Activer l'analyse de la communauté .....	38
(Facultatif) Configurer l'auditing sur l'hôte Malware Analysis .....	40
Configurer le seuil d'audit .....	41
Configurer Alerte de gestion des incidents .....	41
Configuration de l'audit SNMP .....	42
Configurer Paramètres d'audit des fichiers .....	42
Configurer Paramètres d'audit Syslog .....	43
(Facultatif) Configurer le filtre de hachage .....	44
Afficher la liste de hachage .....	44
Ajouter un hachage de fichier au filtre de hachage .....	45
Marquer un hachage comme fiable ou non fiable .....	45
Supprimer un hachage du filtre de hachage .....	45
Rechercher un hachage de fichier .....	45
Importer une liste de hachage à l'aide du dossier surveillé .....	46
(Facultatif) Configurer les paramètres proxy de Malware Analysis .....	49
Configurer le proxy Web .....	49
(Facultatif) Enregistrez-vous pour recevoir une clé API ThreatGrid .....	50

## Procédures supplémentaires pour la configuration de Malware

<b>Analysis .....</b>	<b>52</b>
Créer une alerte personnalisée au format CEF .....	52
Modèle CEF .....	52
Comprendre une entrée de fichier d'audit Syslog .....	53
Modifier le fichier de configuration .....	58
Exemple .....	58
Activer le contenu YARA personnalisé .....	72
Conditions préalables .....	72
Installer les bibliothèques et les applications nécessaires à la création YARA sur une .....	73

appliance basée CentOS .....	
Configurer Yara .....	74

**Références de Malware Analysis ..... 76**

Vue Configuration des services - Onglet Audit .....	77
Détails de la reconstruction de paquets .....	80
Détails de la reconstruction de texte .....	80
Détails de la reconstruction de fichier .....	81
Description détaillée .....	82
Vue Configuration des services - onglet AV .....	84
Vue Configuration des services - onglet Général .....	85
Section Configuration de l'analyse continue .....	85
Section Configuration du référentiel .....	91
Section Configuration diverse (10.3 SP2 et versions supérieures) .....	92
Section Configuration des modules .....	93
Paramètres de ThreatGrid Sandbox .....	96
Vue Configuration des services - Onglet Hachage .....	98
Vue Configuration des services - onglet Indicateurs de compromission .....	100
Vue Configuration des services - onglet Intégration .....	103
Vue Configuration des services - onglet Récapitulatif des indicateurs de compromission des services .....	105
Vue Configuration des services - onglet Proxy .....	107
Vue Configuration des services - onglet ThreatGRID .....	108



## Comment fonctionne 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)

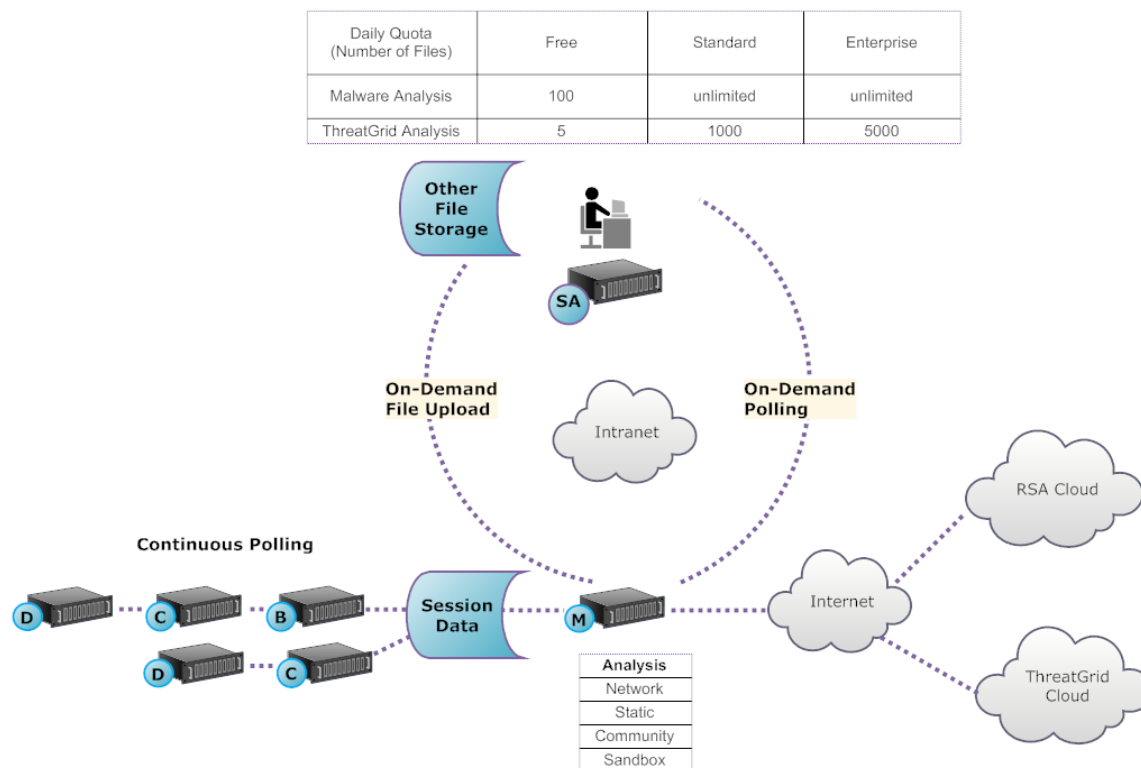
Chacune des quatre méthodologies distinctes d'analyse est conçue pour compenser toutes faiblesses inhérentes aux autres. Par exemple, Analyse de fichier dynamique peut compenser des attaques de type Zero-Day qui ne sont pas détectées pendant la phase Analyse de communauté de sécurité. En évitant l'analyse 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.



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 entraînent 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 scores

---

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

---

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.

The screenshot displays the RSA NetWitness Suite Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN (selected). Below this, a secondary navigation bar shows HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM (selected), and SECURITY. The main content area is divided into a left sidebar and a main panel. The sidebar, under the 'Info' section, lists various settings: Updates, Licensing, Email, Global Notifications, Legacy Notifications, System Logging, Global Auditing, Jobs, Live Services, URL Integration, Context Menu Actions, Investigation, ESA, ESA Analytics, Whois, HTTP Proxy Settings, and NTP Settings. The main panel displays 'Version Information' with the following details:

Current Version	11.0.0.0-170709005430.1.9127d8d
Current Build	170709005430
License Server ID	000C29A985E5
License Status	Enabled <input type="button" value="Disable"/>

The bottom of the console features the RSA | NETWITNESS SUITE logo.

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.

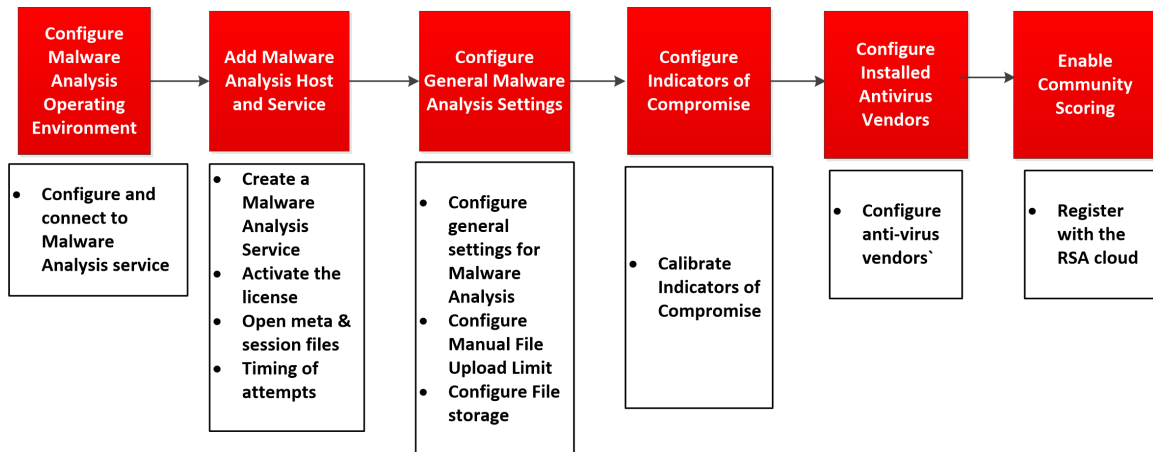




## Configuration de Malware Analysis

Malware Analysis peut fonctionner en tant que service sur un Decoder ou en tant que service sur une appliance dédiée. Ce guide explique comment configurer l'environnement d'exploitation, puis le service Malware Analysis. Une fois la configuration terminée, les analystes peuvent procéder à des analyses de malware.

Il s'agit des étapes de configuration requises pour Malware Analysis, de même que pour modifier la configuration. Suivez les étapes de la section dans l'ordre où elles sont indiquées.



### Liste de contrôle de configuration de base

La liste de contrôle suivante précise l'ordre des tâches requises pour configurer Malware Analysis qui a été ajouté à NetWitness Suite conformément au *Guide des hôtes et services*.

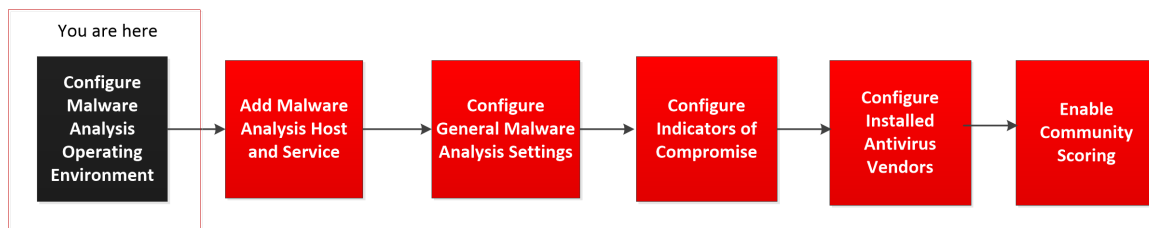
Étape	Tâche générale
Étape 1 - Configurer l'environnement d'exploitation de Malware Analysis	<p><a href="#">Configurer l'environnement d'exploitation de Malware Analysis</a></p> <p>Cette rubrique décrit les procédures de configuration de l'environnement d'exploitation de Security Analytics pour une connexion à un service Malware Analysis.</p>

Étape	Tâche générale
<p>Étape 2 - Ajouter un hôte et un service Malware Analysis</p>	<p><a href="#">Ajouter un hôte et un service Malware Analysis</a></p> <div style="border: 1px solid green; padding: 5px; margin: 5px 0;"> <p><b>Remarque :</b> Pour effectuer cette étape, le serveur de licences NetWitness Suite doit être configuré comme décrit dans le Guide d'octroi des licences.</p> </div> <p>Dans NetWitness Suite, créez un service Malware Analysis et activez la licence. Le port REST par défaut est 60007. Les sites qui utilisent la version gratuite de Malware Analysis doivent configurer l'adresse IP du service en tant qu'hôte local ou boucle de rappel.</p>
<p>Étape 3 - Configurer les paramètres généraux de Malware Analysis</p>	<p><a href="#">Configurer les paramètres généraux de Malware Analysis</a></p> <ul style="list-style-type: none"> <li>• Activez le rappel continu.</li> <li>• Configurez la limite de téléchargement manuel des fichiers</li> <li>• Configurez le référentiel de stockage de fichiers et la base de données.</li> <li>• Calibrez les modules d'évaluation Statique, Réseau, Communauté et Sandbox.</li> </ul>
<p>Étape 4 - Configurer les Indicateurs de compromission</p>	<p><a href="#">Configurer les Indicateurs de compromission</a></p> <p>Calibrez les indicateurs de compromission (IOC) qui sont appliqués à ce module d'évaluation (Statique, Réseau, Communauté et Sandbox) et aux IOC YARA.</p>
<p>Étape 5 - Configurer les fournisseurs d'antivirus installés</p>	<p><a href="#">Configurer les fournisseurs d'antivirus installés</a></p>
<p>Étape 6 - Activer l'évaluation du score de la Communauté</p>	<p><a href="#">Activer l'analyse de la communauté</a></p> <p>S'enregistrer au RSA Cloud et tester les connexions pour activer l'évaluation du score de la communauté.</p>

Étape	Tâche générale
Étape 7 - Configurer l'auditing sur l'hôte Malware Analysis	<p><a href="#">(Facultatif) Configurer l'auditing sur l'hôte Malware Analysis</a></p> <p>Configurez le seuil d'audit et activez syslog, SNMP et l'audit des fichiers.</p>
Étape 8 - Configurer le filtre de hachage	<p><a href="#">(Facultatif) Configurer le filtre de hachage</a></p> <p>Configurez le filtrage de hachage pour perfectionner l'analyse des événements Malware Analysis d'après des hachages de fichiers connus, bons ou mauvais.</p>
Étape 9 - Configurer les paramètres proxy de Malware Analysis	<p><a href="#">(Facultatif) Configurer les paramètres proxy de Malware Analysis</a></p> <p>(Facultatif) Configurez Malware Analysis pour communiquer avec RSA Cloud via un proxy Web et non directement.</p>
Étape 10 - Inscrivez-vous pour recevoir une clé API ThreatGrid	<p><a href="#">(Facultatif) Enregistrez-vous pour recevoir une clé API ThreatGrid</a></p>

## Configurer l'environnement d'exploitation de Malware Analysis

Vous pouvez configurer l'environnement d'exploitation NetWitness Suite pour vous connecter à un service NetWitness Suite Malware Analysis.



Malware Analysis fonctionne en tant que service sur une appliance Malware Analysis dédiée. Si votre site utilise une appliance dédiée, effectuez l'une des actions suivantes :

- Si votre site ajoute une nouvelle appliance NetWitness Suite Malware Analysis dédiée, installez l'apppliance physique sur votre réseau et configurez l'environnement d'exploitation.

- Si votre site met à niveau une appliance Spectrum dédiée vers une appliance NetWitness Suite Malware Analysis dédiée, créez une nouvelle image de l'appliance Spectrum en tant qu'appliance Malware Analysis.

Le fonctionnement de Malware Analysis dépend de l'infrastructure Core. Les étapes suivantes sont nécessaires avant que Malware Analysis ne puisse analyser les données correctement.

1. Configurez le Broker intégré sur l'appliance Malware Analysis pour connecter un autre Broker ou Concentrator dans l'infrastructure Core existante.

**Remarque :** En l'absence d'une infrastructure Core, seuls les fichiers téléchargés manuellement peuvent être analysés.

2. Utilisez NetWitness Suite Live pour rechercher toutes les ressources Live avec la balise `malware analysis` et déployez ces ressources vers chaque service Decoder qui capturera le trafic à analyser par Malware Analysis. NetWitness Suite utilise cet ensemble propriétaire d'analyseurs et de feeds pour rechercher des événements qui sont susceptibles d'être un malware.
3. Configurez les ports de communication. Malware Analysis requiert l'ouverture d'un nombre de ports de communication différents, notamment le port TCP/443 pour HTTPS. Ils sont décrits ci-dessous dans la rubrique Connexions réseau.
4. Configurez la source NextGen à laquelle se connectera Malware Analysis. Il s'agit du Broker ou Concentrator.  
Malware Analysis est désormais prêt à commencer à analyser le trafic réseau.

## Connexions réseau

Les connexions réseau entrantes et sortantes doivent être configurées pour que l'appliance Malware Analysis puisse communiquer correctement avec les services et les sources RSA afin de recevoir les mises à jour logicielles et d'autres informations critiques.

Le pare-feu de votre réseau doit être configuré pour permettre à Malware Analysis d'accéder à Internet. Les serveurs proxy peuvent être utilisés pour faciliter ces connexions, le cas échéant.

### Connexions entrantes

TCP/22 - Accès SSH (Secure Shell) au serveur Malware Analysis pour examiner les fichiers logs et effectuer les corrections nécessaires. L'accès peut être limité aux adresses IP qui gèrent Malware Analysis.

- TCP/443 - Connexion Web HTTPS pour accéder à l'interface utilisateur de Malware Analysis.

- TCP/50008 - Port JMX pour résoudre les problèmes de performances, en utilisant une application telle que JVisualVM. (Facultatif) L'accès peut être limité aux adresses IP qui gèrent Malware Analysis.

### Connexions sortantes

- TCP/443 - Connexions HTTPS aux serveurs Web SSL. Certaines fonctionnalités Malware Analysis permettent d'envoyer des fichiers ou des documents vers des serveurs pour analyse, ce qui requiert une connexion sécurisée. L'utilisation d'un serveur proxy Web est prise en charge.
- (TCP/443 - Connexion SSL entre Malware Analysis vers le Cloud RSA. L'utilisation d'un serveur SOCKS Proxy est prise en charge. Les modifications de l'infrastructure client peuvent être nécessaires pour s'assurer que le port 443 est ouvert sur cloud.netwitness.com.)
- TCP/50103 - Port API REST utilisé pour communiquer avec un Broker (NetWitness Suite 10.3.x et versions antérieures).
- TCP/50105 - Port API REST utilisé pour communiquer avec un Concentrator (NetWitness Suite 10.3.x et versions antérieures).
- TCP/50003 TCP/56003 - Ports permettant de communiquer avec un service Broker (NetWitness Suite 10.4 et versions ultérieures).
- TCP/50005 TCP/56005 - Ports permettant de communiquer avec un service Concentrator (NetWitness Suite 10.4 et versions ultérieures).
- ICMP - Connexion JMS entre NetWitness Suite et le service Malware Analysis pour vérifier si le nom d'hôte et l'adresse IP saisis sont valides et si la connexion de test est établie.

## Ajouter un hôte et un service Malware Analysis

Vous pouvez ajouter un hôte et un service Malware Analysis à NetWitness Suite. Votre environnement NetWitness Suite détermine la façon dont vous ajoutez un hôte. Reportez-vous aux instructions de base pour ajouter un hôte (Ajouter ou mettre à jour un hôte) dans le Guide de mise en route de l'hôte et des services. Utilisez la procédure dans cette section uniquement si vous avez besoin d'ajouter un hôte Malware Analysis manuellement.

**Remarque :** Pour effectuer cette étape, le serveur de licences NetWitness Suite doit être configuré comme décrit dans le Guide d'octroi des licences.

- Ajoutez l'hôte Malware Analysis s'il existe une appliance Malware Analysis physique ou virtuelle.

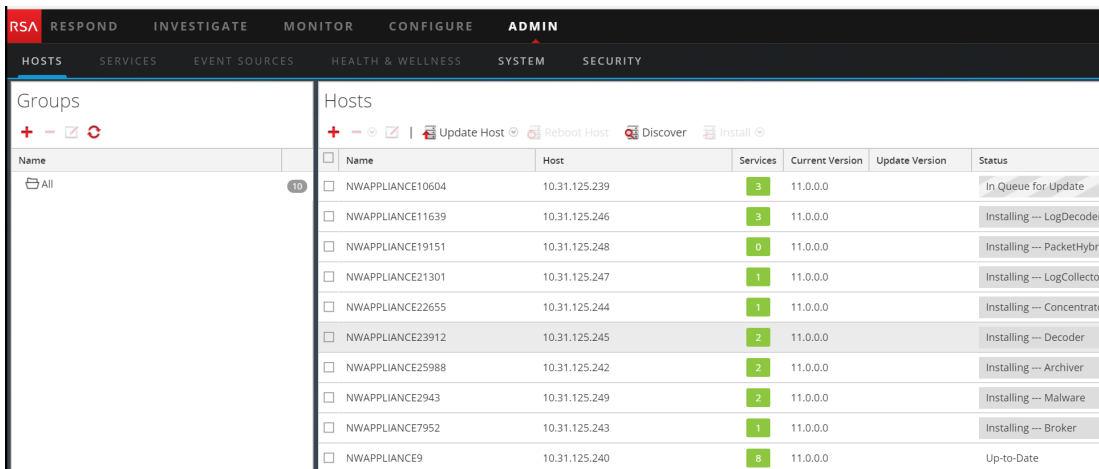
## Condition préalable

Si vous souhaitez ajouter un hôte et un service dans NetWitness Suite, vous devez avoir terminé la configuration des opérations et une instance de NetWitness Suite doit être installée et en cours d'exécution.

## Procédure

Pour ajouter manuellement un hôte Malware Analysis à NetWitness Suite :

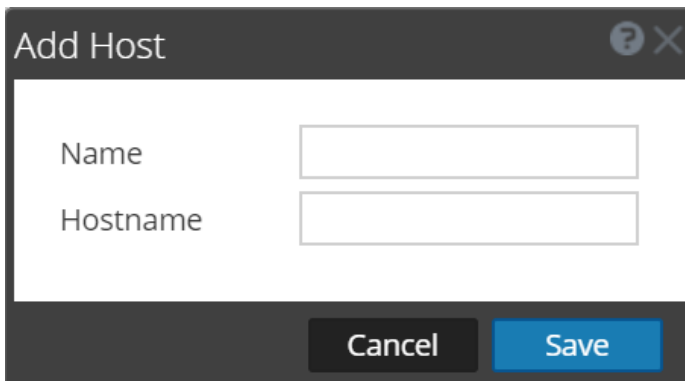
1. Connectez-vous à NetWitness Suite.
2. Dans Menu principal, sélectionnez **Administration > Hôtes**. La vue Administration > Hôtes s'affiche.



Name	Host	Services	Current Version	Update Version	Status
NWAPPLIANCE10604	10.31.125.239	3	11.0.0.0		In Queue for Update
NWAPPLIANCE11639	10.31.125.246	3	11.0.0.0		Installing --- LogDecoder
NWAPPLIANCE19151	10.31.125.248	0	11.0.0.0		Installing --- PacketHybrid
NWAPPLIANCE21301	10.31.125.247	1	11.0.0.0		Installing --- LogCollector
NWAPPLIANCE22655	10.31.125.244	1	11.0.0.0		Installing --- Concentrator
NWAPPLIANCE23912	10.31.125.245	2	11.0.0.0		Installing --- Decoder
NWAPPLIANCE25988	10.31.125.242	2	11.0.0.0		Installing --- Archiver
NWAPPLIANCE2943	10.31.125.249	2	11.0.0.0		Installing --- Malware
NWAPPLIANCE7952	10.31.125.243	1	11.0.0.0		Installing --- Broker
NWAPPLIANCE9	10.31.125.240	8	11.0.0.0		Up-to-Date

3. Dans la barre d'outils du panneau Hôtes, cliquez sur  .


La boîte de dialogue Ajouter un hôte s'affiche.

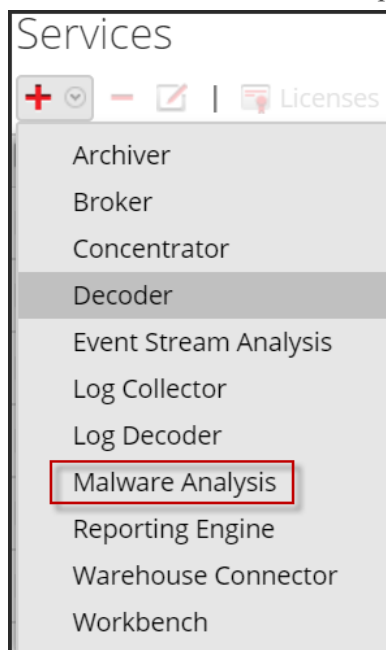


**Add Host** ? X

Name

Hostname

4. Dans le champ **Nom**, saisissez un nom pour l'hôte Malware Analysis. Dans le champ **Nom d'hôte**, saisissez le nom d'hôte, l'adresse IP virtuelle ou l'adresse IP sur Malware Analysis. Cliquez sur **Enregistrer**.
5. Dans la barre d'outils, sélectionnez **Services**.
6. Dans la barre d'outils du panneau **Services**, cliquez sur  et **Malware Analysis** dans la liste déroulante des services disponibles.



La boîte de dialogue Ajouter un service s'affiche avec le type de service Malware Analysis


7. Saisissez les informations suivantes :
  - Dans le champ **Nom**, saisissez un nom pour le service Malware Analysis.
  - Dans le champ **Hôte**, saisissez le nom d'hôte, l'adresse IP virtuelle ou l'adresse IP sur le Malware Analysis.
  - Dans le champ **Port**, saisissez **60007**.
  - (Facultatif) Sous **Options**, sélectionnez **Autoriser le service**.

The screenshot shows a dialog box titled "Add Service" with a question mark icon and a close button in the top right corner. The dialog contains the following fields and sections:

- Service:** Malware Analysis
- Host:** A dropdown menu that is currently empty.
- Name:** An empty text input field.
- Connection Details:** A section containing a **Port** field with the value "60007".
- Options:** A section containing a checkbox labeled "Entitle Service", which is currently unchecked.
- Test Connection:** A button that is currently disabled (greyed out).
- Buttons:** "Cancel" and "Save" buttons are located at the bottom of the dialog.

8. Cliquez sur **Tester la connexion**.

Lors de l'ajout du service, NetWitness Suite envoie des paquets ICMP au service pour vérifier si le nom d'hôte et l'adresse IP saisis sont valides et permettent une connexion de test réussie. Le résultat du test s'affiche dans la boîte de dialogue Ajouter un service. Si le test échoue, modifiez les informations du service et réessayez.

9. Si le résultat réussit, cliquez sur **Enregistrer**. La boîte de dialogue Ajouter un service se ferme et le service Malware Analysis est disponible pour NetWitness Suite. (Facultatif) Vérifiez l'état du service Malware Analysis. Dans la vue Services d'administration, sélectionnez le service Malware Analysis et sélectionnez  **Vue > Système**. Vous trouverez ci-dessous un échantillon des informations disponibles pour un service Malware Analysis.



The screenshot displays the RSA Malware Analysis interface. At the top, there is a navigation bar with tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, a secondary navigation bar includes HOSTS, SERVICES (which is selected), EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. A breadcrumb trail shows 'Change Service' | 'Malware Analytics' | 'System'. The main content area is divided into two sections: 'Service Information' and 'License Information'.

Service Information	
Name	Linux (Malware Analysis)
Version	11.0.0.0-8254-1
Memory Usage	126 MB (1.03% of 12274 MB)
Total Memory	32176 MB
Process Memory	27334 MB
CPU	0%
Running Since	2017-Jul-19 05:13:52
Uptime	13 days 04 hours 08 minutes 59 seconds
Host Max File Submission	2147483647
Host File Submission Count	74
Sandbox Max File Submission	2147483647
Sandbox File Submission Count	32

License Information	
Service ID	9b5a3f4f-ebf5-4461-8723-a6915be1c82f
Product	smcMalwareMetered
Licensed	
Type	Duration
Start Date	2017-07-11 08:00:00
Expiration Date	2017-10-10 07:59:59
Days Licensed	21
Days Remaining	69

Si le service ne dispose pas d'une licence, accédez à Administration > Système > panneau Gestion des licences, puis sélectionnez **Actualiser les licences** dans le menu **Actions d'attribution de licence**.

**Service Based Licenses**

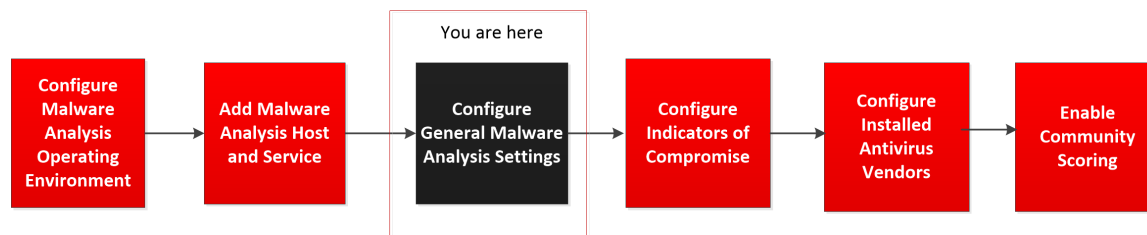
Status ^	Service Type	Available/Total
● Licensed	Archiver	0/1
● Licensed	Broker	0/1
● Licensed	Concentrator	0/1
● Licensed	Event Stream Analysis	0/1
● Licensed	Broker	0/0

**Metered Licenses**

Status ^	Service Type
● Within Usage Limit	Decoder
● Within Usage Limit	Log Decoder
● Within Usage Limit	Malware Analysis

## Configurer les paramètres généraux de Malware Analysis

Vous pouvez configurer plusieurs paramètres de base, nécessaires pour activer et calibrer la consommation des sessions, le téléchargement manuel des fichiers et les différents modules de score que Malware Analysis utilise pour analyser les données.



Vous pouvez également configurer le partage de fichiers avec le référentiel d'entreprise. Malware Analysis possède trois modes de consommation des sessions et fichiers. Vous pouvez utiliser n'importe quelle combinaison de ces trois modes pour lancer une analyse dans Malware Analysis. Ci-dessous les choix disponibles :

- **Rappel continu du service Core** : vous pouvez activer et configurer le rappel continu du service Core. Lorsqu'il est activé et configuré, Malware Analysis évalue en continu le service Core pour les sessions marquées pour l'analyse. Par défaut, le rappel continu est désactivé. Vous pouvez activer la protection contre les attaques par déni de service (DOS) durant le rappel continu. Vous pouvez tester la connexion au service Malware Analysis Service, qui est continuellement rappelé, à l'aide d'une option située sous l'onglet Intégration.

**Remarque** : Lorsque vous ajoutez un service Core en tant que service de rappel continu sur Malware Analysis version 10.3.5 et les versions antérieures, utilisez le port REST. Par exemple, ajoutez un Concentrator à Malware analysis 10.3.5 à l'aide du port REST (50105) au lieu du port NexGen natif (50005).

- **Analyse à la demande du service Core** : vous pouvez analyser les sessions à partir d'Investigation, lancé directement dans NetWitness Suite. Cette méthode permet de contrôler manuellement la consommation des sessions Core. De plus, elle permet de renforcer le contrôle du traitement des fichiers de ces sessions (via l'envoi pour traitement à un sandbox, par exemple). Vous pouvez contourner les restrictions par défaut de certains types de documents, et envoyer ces derniers pour traitement à la communauté ou à un sandbox, indépendamment du paramètre configuré.
- **Téléchargement manuel des fichiers** : vous pouvez télécharger manuellement un ou plusieurs fichiers à analyser en accédant à un dossier visible sur votre ordinateur, puis en sélectionnant les fichiers souhaités. Vous pouvez configurer la taille maximale des fichiers téléchargés.

## Afficher les paramètres de base

Pour afficher les paramètres de base :

1. Dans **Menu principal**, sélectionnez **Administration >Services**.
2. Dans la grille **Services**, sélectionnez un service Malware Analysis, puis cliquez sur



> **Vue > Configuration**.

La configuration du service s'ouvre sur l'onglet **Général**.

The screenshot shows the configuration page for Malware Analysis. It is divided into two main sections: 'Continuous Scan Configuration' and 'Modules Configuration'. The 'Continuous Scan Configuration' section includes settings for 'Enabled', 'Query', 'Query Expiry', 'Query Interval', 'Meta Limit', 'Time Boundary', 'Source Host', 'Source Port (NwPort)', 'Username', 'User Password', 'SSL', 'Denial of Service (DOS) Prevention', 'DOS Session Rate Window Length (Seconds)', 'DOS Number Sessions per Rate Window', 'DOS Session Lockout Time (Seconds)', and 'DOS Garbage Collecton Interval (Seconds)'. The 'Modules Configuration' section is organized into three categories: 'Static', 'Community', and 'Sandbox', each with its own set of configuration options like 'Enabled', 'Bypass PDF', 'Bypass Office', and 'Bypass Executable'.

Continuous Scan Configuration		Modules Configuration	
Name	Config Value	Name	Config Value
Enabled	<input checked="" type="checkbox"/>	Static	
Query	select * where content='spectrum.consume'    content='spectrum.c...	Enabled	<input checked="" type="checkbox"/>
Query Expiry	3600	Bypass PDF	<input type="checkbox"/>
Query Interval	5	Bypass Office	<input type="checkbox"/>
Meta Limit	25000	Bypass Executable	<input type="checkbox"/>
Time Boundary	24	Validate Windows PE Authentic Settings via Cloud	<input type="checkbox"/>
Source Host	10.31.125.244	Community	
Source Port (NwPort)	56005	Enabled	<input checked="" type="checkbox"/>
Username	admin	Bypass PDF	<input type="checkbox"/>
User Password	*****	Bypass Office	<input type="checkbox"/>
SSL	<input checked="" type="checkbox"/>	Bypass Executable	<input type="checkbox"/>
Denial of Service (DOS) Prevention	<input type="checkbox"/>	Sandbox	
DOS Session Rate Window Length (Seconds)	60	Enabled	<input checked="" type="checkbox"/>
DOS Number Sessions per Rate Window	200	Bypass PDF	<input type="checkbox"/>
DOS Session Lockout Time (Seconds)	60	Bypass Office	<input type="checkbox"/>
DOS Garbage Collecton Interval (Seconds)	120	Bypass Executable	<input type="checkbox"/>

## Configurer le rappel continu

Malware Analysis est plafonné à une certaine limite. Par conséquent, vous pouvez envoyer 1 000 fichiers par jour au Cloud ThreatGrid afin qu'ils soient traités dans un sandbox. Pour vous permettre d'optimiser l'utilisation du sandbox, la configuration de Malware Analysis propose plusieurs modes de consommation possibles pour Malware Analysis. Vous pouvez activer ou désactiver le rappel continu.

Les paramètres de prévention du déni de service (DOS) sont un point important à prendre en compte lors de la configuration du rappel continu. Par défaut, cette fonctionnalité est désactivée, car vous devez prendre soigneusement en compte les paramètres correspondant à votre environnement avant de l'activer.

Lorsque la prévention DOS est désactivée, Malware Analysis analyse les sessions en file d'attente dans l'ordre premier entré, premier sorti (FIFO, first-in, first-out).. Une attaque DOS peut remplir rapidement la file d'attente, si bien que Malware Analysis est occupé à traiter ces sessions en file d'attente alors qu'une attaque de malware se produit dans une session suivante. La session suivante subissant l'attaque réelle peut ne pas atteindre le début de la file d'attente et être analysée seulement après le début de l'attaque.

Lorsque la prévention DOS est activée, Malware Analysis traite trop de sessions issues d'une seule adresse IP comme une attaque DOS. Si une adresse IP dépasse le nombre de sessions par fenêtre de taux, Malware Analysis commence à ignorer les sessions issues de cette adresse jusqu'à ce que le délai de blocage de session soit atteint. Malware Analysis reprend ensuite l'analyse des sessions issues de cette adresse IP. Les sessions ignorées issues de cette adresse IP ne sont pas du tout analysées. Une attaque de malware peut donc échapper au contrôle pendant la période de blocage de session.

À l'aide du paramètre Intervalle de Garbage Collection DOS, Malware Analysis efface le stockage en mémoire d'une source IP au bout d'un nombre de secondes spécifié.. Les adresses IP qui connaissent peu d'activité pendant cet intervalle sont effacées de la mémoire. Si une adresse IP est active à une fréquence qui dépasse l'intervalle de Garbage Collection DOS, Malware Analysis risque de ne pas identifier une attaque DOS.

Pour configurer le rappel continu de Malware Analysis, dans la section Configuration de l'analyse continue, procédez comme suit :

1. Sous **Admin**, cliquez sur **Services**.
2. Dans l'onglet **Général**, sous **Configuration de l'analyse continue**, vous pouvez configurer le rappel continu.

The screenshot shows the configuration page for Malware Analysis. The 'General' tab is selected, and the 'Continuous Scan Configuration' section is visible. The configuration is as follows:

Name	Config Value
Enabled	<input checked="" type="checkbox"/>
Query	select * where content='spectrum.consume'    content='spectrum.consume11'
Query Expiry	3600
Query Interval	5
Meta Limit	25000
Time Boundary	24
Source Host	10.31.125.244
<b>Source Port (NwPort)</b>	<b>56005</b>
Username	admin
User Password	*****
SSL	<input checked="" type="checkbox"/>
Denial of Service (DOS) Prevention	<input type="checkbox"/>
DOS Session Rate Window Length (Seconds)	60
DOS Number Sessions per Rate Window	200
DOS Session Lockout Time (Seconds)	60
DOS Garbage Collecton Interval (Seconds)	120

3. Pour activer le rappel continu, cliquez sur **Activé**.
4. (Facultatif) Si vous souhaitez changer les valeurs par défaut de l'interrogation, saisissez de nouvelles valeurs pour les options **Expiration de la requête**, **Intervalle de requête**, **Limite des métavaleurs** et **Limite temporelle**.
5. Pour configurer l'apppliance Malware Analysis que Malware Analysis interroge pour récupérer les données d'analyse, spécifiez l'**Hôte source** et le **Port source (NwPort)**.
6. (Facultatif) Si vous souhaitez changer les informations d'identification de connexion par défaut pour l'apppliance Malware Analysis, indiquez le **Nom d'utilisateur** et le **Mot de passe utilisateur**.
7. Si vous souhaitez utiliser SSL pour la communication entre l'apppliance Malware Analysis et le service Core, activez le **SSL**.
8. (Facultatif) Si vous souhaitez configurer la protection contre les attaques par déni de service (DOS) :
  - a. Activez le paramètre **Prévention du déni de service (DOS Denial of Service)**.
  - b. Configurez les limites relatives aux sessions avec protection contre les attaques DOS :
    - Dans le champ **Longueur de la fenêtre des taux de session DOS**, spécifiez le nombre de secondes de la période pendant laquelle Malware Analysis compte les sessions pour une seule adresse IP. La fenêtre s'appelle une fenêtre de taux et un

compteur est activé lorsque la première session est reçue de cette IP source. La valeur par défaut est 60 secondes.

- Spécifiez le nombre de sessions autorisées par fenêtre des taux via le paramètre **Nombre de sessions DOS par fenêtre de taux**. La valeur par défaut est 200 sessions. Lorsque le nombre de sessions est atteint dans la fenêtre de taux, Malware Analysis commence par ignorer les sessions issues de l'adresse IP et les sessions ignorées issues de cette adresse IP ne sont pas du tout analysées. Malware Analysis continue d'ignorer les sessions jusqu'à ce que le délai de blocage soit atteint.
  - Spécifiez la durée du délai de blocage (pendant lequel les sessions issues de l'adresse IP sont ignorées et non analysées) dans le champ **Délai de blocage de la session DOS (secondes)**. La valeur par défaut est 60 secondes. Lorsque le délai de blocage est dépassé, Malware Analysis reprend l'analyse des sessions issues de cette adresse IP.
  - Spécifiez l'intervalle d'inactivité d'une adresse IP avant que NetWitness Suite ne supprime l'objet en mémoire pour la source IP, dans le champ **Intervalle de Garbage Collection DOS (secondes)**. La valeur par défaut est 120 secondes.
9. Cliquez sur **Appliquer** pour appliquer les modifications.  
Les modifications prennent effet immédiatement lorsque Malware Analysis reçoit de nouveaux paquets.
  10. Testez la connexion du service Malware Analysis au service Core sélectionné sous l'onglet **Intégration** en cliquant sur le bouton **Tester la connexion** dans la section **Test de connexion à l'analyse continue**.

## Configurer les paramètres de téléchargement manuel des fichiers

Pour configurer la taille maximale de fichier autorisée lors du téléchargement manuel des fichiers :

1. Dans la section Divers, saisissez la taille de fichier maximale autorisée, en mégaoctets, pour les fichiers téléchargés manuellement dans le cadre de l'analyse Malware Analysis.

Miscellaneous	
Name	Config Value
Maximum File Size (MB)	64

Buttons: Bypass Exe, Preserve C, GFI Sand, Enabled, Apply

2. Cliquez sur **Appliquer**.  
Les modifications prennent effet immédiatement.

## Configurer le référentiel d'entreprise

Malware Analysis peut stocker un nombre limité de fichiers sur l'apppliance. La configuration du référentiel d'entreprise propose une période de rétention du système de fichiers de 60 jours. Ce paramètre détermine la durée pendant laquelle les fichiers sont conservés dans l'apppliance Malware Analysis. Une fois supprimés, les anciens fichiers ne peuvent pas être restaurés. Chaque jour, Malware Analysis supprime les fichiers qui dépassent la période de rétention du système de fichiers pour éviter tout gaspillage de l'espace disque.

Le paramètre de la période de rétention du système de fichiers est le seul élément qui détermine le moment où les fichiers sont supprimés. Les fichiers ne sont pas supprimés en fonction de la quantité d'espace disque utilisée. Si le paramètre doit être changé, l'administrateur doit configurer la période de rétention en fonction de l'utilisation d'espace prévue pendant le nombre de jours de rétention spécifié.

Les paramètres visibles du référentiel d'entreprise dans l'interface utilisateur de NetWitness Suite sont :

- L'emplacement du référentiel d'entreprise est `/var/lib/netwitness/malware-analytics-server/spectrum`. Ne modifiez pas cette valeur.
- Le protocole de partage de fichiers, qui permet via l'un des protocoles de partage de fichiers de copier des fichiers à partir du service Malware Analysis.
- La période de rétention des fichiers en nombre de jours.

Pour configurer le partage de fichiers, dans la section Référentiel d'entreprise, procédez comme suit :

1. Cliquez sur Protocole de partage de fichiers pour sélectionner FTP ou SAMBA.
2. Sélectionnez le nombre de jours de conservation des fichiers dans le référentiel d'entreprise avant leur suppression.
3. Cliquez sur **Appliquer**.

Les modifications prennent effet immédiatement.

## Calibrer les modules de score

La section Configuration des modules permet de configurer les composants suivants de Malware Analysis à :


- Désactiver complètement une partie ou l'ensemble des trois modules de score (Static, Community et Sandbox). Avant de désactiver ou d'activer un module de score, assurez-vous de bien comprendre ce qu'il détecte.

- Malware Analysis marque les sessions contenant des fichiers Microsoft Office, Windows PE et PDF pour utilisation par le service Malware Analysis. Vous pouvez configurer Malware Analysis afin qu'il ignore complètement les documents Windows PE, Microsoft Office et PDF. Si tel est le cas, une meilleure option consiste à modifier vos paramètres Core pour ignorer ces fichiers afin qu'ils ne soient pas marqués pour une consommation par Malware Analysis.

Voici un exemple d'application du calibrage du module de score : lors de la création de groupes de règles, ou de l'analyse des performances système, vous pouvez tester différents scénarios dans lesquels les documents PDF ne sont pas analysés, contrairement aux documents Microsoft Office et Windows PE. Vous pouvez tester le scénario dans chacun des trois modules de score. Si vous constatez une amélioration notable des performances système, vous pouvez appliquer cette observation à une plus grande échelle.

## Configurer le score d'analyse Static

### Modules Configuration

Name	Config Value
 <b>Static</b>	
Enabled	<input checked="" type="checkbox"/>
Bypass PDF	<input type="checkbox"/>
Bypass Office	<input type="checkbox"/>
Bypass Executable	<input type="checkbox"/>
Validate Windows PE Authenticate Settings via ...	<input type="checkbox"/>

Pour configurer le score d'analyse Static, dans la section **Configuration des modules** :

- Par défaut, le module Static est activé. Pour activer ou désactiver complètement l'analyse Static, activez la case à cocher **Activé**.
- Pour configurer la gestion des fichiers PDF, Microsoft Office et Windows PE dans une session, activez l'une des cases à cocher **Ignorer les fichiers PDF**, **Ignorer les fichiers Office** et **Ignorer les fichiers exécutables**.
- Pour configurer votre préférence de validation Authenticode des fichiers Windows PE signés numériquement, activez la case à cocher **Valider les paramètres d'authentification de Windows PE via le Cloud**. Pour empêcher les fichiers Windows PE signés numériquement



d'être transmis au service RSA Cloud à des fins de validation, désactivez la case à cocher. Une fois cette option désactivée, toutes les analyses du module Static sont effectuées localement (en ignorant la validation Authenticode). Quel que soit ce paramètre, les documents PDF et Microsoft Office ne sont pas soumis à la validation Authenticode, et ne sont pas transmis sur le réseau durant l'analyse Static.

4. Cliquez sur **Appliquer**. Les modifications prennent effet immédiatement lorsque Malware Analysis reçoit de nouveaux paquets.

### Configurer le score d'analyse des pairs

Une fois le module Community activé, la communauté de sécurité analyse tous les documents dont le traitement n'est pas bloqué. Cela est rendu possible par l'envoi d'attributs de fichier et de session réseau pour traitement au service RSA Cloud. Le service RSA Cloud peut ensuite établir une connexion externe aux partenaires de la communauté de sécurité pour traiter les informations.

Le contenu du fichier n'est jamais envoyé à la communauté pour analyse. En revanche, le hachage MD5/SHA1 du fichier est envoyé à des fins de détection antivirus et de comparaison aux listes noires. De même, les métadonnées de session sont collectées et analysées dans le cadre de ce processus. Les éléments de métadonnées tels que les URL et les noms de domaine sont examinés et transmis au service RSA Cloud pour permettre l'identification des URL/domaines ayant une réputation douteuse.

Vous pouvez activer l'analyse des pairs et limiter les types de documents traités. Le contenu du fichier ne risque pas (à l'exception du hachage) d'être envoyé à l'extérieur de votre réseau.

**Remarque :** Pour accéder au service RSA Cloud où a lieu le traitement, vous devez inscrire votre service Malware Analysis auprès du Support Clients RSA. Vous disposez de deux méthodes possibles : inscrire le service via les options de l'onglet Intégration ou contacter le Support Clients RSA.

Pour configurer le score d'analyse des pairs, dans la section Configuration des modules, procédez comme suit :

Community	
Enabled	<input type="checkbox"/>
<b>Bypass PDF</b>	<input checked="" type="checkbox"/>
Bypass Office	<input checked="" type="checkbox"/>
Bypass Executable	<input type="checkbox"/>

1. Pour activer ou désactiver complètement l'analyse des pairs, activez la case à cocher **Activé**. La valeur par défaut est **Désactivé**.
2. Pour configurer la gestion des fichiers PDF, Microsoft Office et Windows PE dans une session, cochez les cases correspondantes : **Ignorer les fichiers PDF**, **Ignorer les fichiers Office**, **Ignorer les fichiers exécutables**.
3. Cliquez sur **Appliquer** pour enregistrer les modifications et les appliquer dès que Malware Analysis reçoit de nouveaux paquets.

## Configurer le score d'analyse Sandbox

Par défaut, le module Sandbox est désactivé et les fichiers Microsoft Office et PDF ne sont pas traités. Le but est de définir les paramètres les plus restrictifs possibles pour forcer l'utilisateur à spécifier si les données potentiellement sensibles peuvent être envoyées ou non hors du réseau à des fins de traitement. Si le traitement d'un type de documents n'est pas bloqué, le fichier entier (et pas seulement le hachage) est envoyé au serveur sandbox de destination.

En outre, vous pouvez choisir de conserver le nom de fichier d'origine lors de l'analyse Sandbox.

**Remarque :** Si vous ne spécifiez pas le paramètre d'origine **Conserver le nom de fichier d'origine lors de l'exécution de l'analyse Sandbox**, NetWitness Suite hache les fichiers.

Sandbox	
Enabled	<input checked="" type="checkbox"/>
Bypass PDF	<input type="checkbox"/>
Bypass Office	<input type="checkbox"/>
Bypass Executable	<input type="checkbox"/>
Preserve Original File Name when Performing Sandb...	<input type="checkbox"/>

Lorsque vous activez le module Sandbox, vous devez spécifier si le traitement est effectué à l'aide d'un sandbox GFI local, un sandbox ThreatGrid ou une version Cloud du sandbox ThreatGrid. La version Cloud du sandbox ThreatGrid est fournie directement par ThreatGrid. Elle nécessite une clé d'activation que vous devez vous procurer auprès de ThreatGrid et configurer sous l'onglet ThreatGRID.

### Paramètres de GFI Sandbox

Pour utiliser un sandbox GFI installé localement, vous devez activer GFI, puis fournir le nom et le port du serveur de sandbox GFI. Les paramètres Période maximale d'interrogation et Intervalle de rappel déterminent le temps de traitement d'un échantillon soumis, ainsi que la fréquence de vérification de son état (en secondes). L'option Ignorer les paramètres proxy Web vous permet d'indiquer à Malware Analysis que vous souhaitez contourner un proxy web lors de l'établissement de la connexion. Si aucun Proxy Web n'a été configuré dans Malware Analysis, le paramètre est ignoré.

GFI Sandbox (Local)	
Enabled	<input type="checkbox"/>
Server Name	localhost
Server Port	80
Max Poll Period	1800
Ignore Web Proxy Settings	<input type="checkbox"/>

### Paramètres de ThreatGrid Sandbox

**Remarque :** Avant d'activer le score ThreatGrid, vous devez configurer une clé de service fournie par ThreatGrid afin que ce dernier puisse reconnaître la légitimité des échantillons soumis à partir de ce site. Utilisez NetWitness Suite pour vous inscrire et obtenir une clé API ThreatGrid. Vous pourrez ensuite activer et configurer un sandbox ThreatGrid installé localement, ou la version Cloud du sandbox ThreatGrid. Consultez la tâche détaillée suivante : [Inscrivez-vous pour recevoir une clé API ThreatGrid.](#)

L'option Ignorer les paramètres proxy Web vous permet d'indiquer à Malware Analysis que vous souhaitez contourner un proxy web lors de l'établissement de la connexion. Si aucun Proxy Web n'a été configuré dans Malware Analysis, le paramètre est ignoré.

Pour configurer le score Sandbox, dans la section Configuration des modules, procédez comme suit :

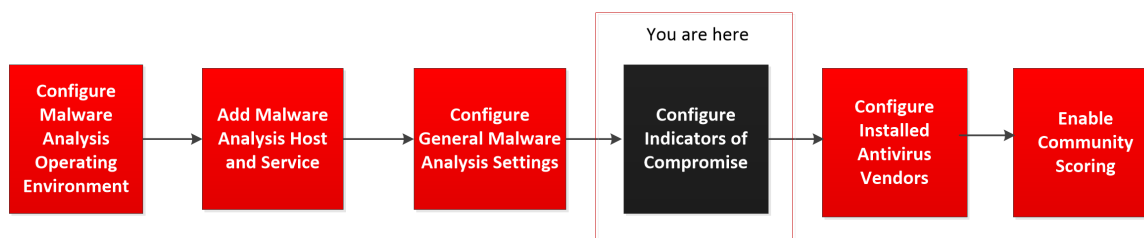
1. Pour activer ou désactiver complètement l'analyse Sandbox, activez la case à cocher **Activé**. La valeur par défaut est **Désactivé**.
2. Pour configurer la gestion des fichiers PDF, Microsoft Office et Windows PE dans une session, cochez l'une des cases **Ignorer les fichiers PDF**, **Ignorer les fichiers Office**, **Ignorer les fichiers exécutables**.

3. Configurez le fournisseur de sandbox actif. Vous disposez de trois options :
  - a. Pour utiliser une instance installée localement du sandbox GFI, fournissez le nom et le port du serveur de sandbox GFI, renseignez les paramètres Période maximale d'interrogation et Intervalle d'interrogation, puis activez éventuellement la case à cocher Ignorer les paramètres proxy Web.
  - b. Pour utiliser une instance de ThreatGrid installée localement, activez le score ThreatGrid, fournissez la clé de service ThreatGrid, puis activez éventuellement la case à cocher Ignorer les paramètres proxy Web.
  - c. Pour utiliser le Cloud ThreatGrid, vous devez d'abord vous inscrire et obtenir une clé API ThreatGrid. Activez ensuite le score ThreatGrid, fournissez la clé de service ThreatGrid, saisissez l'URL du serveur ThreatGrid (<https://panacea.threatgrid.com>), puis activez éventuellement la case à cocher Ignorer les paramètres proxy Web.
4. Cliquez sur **Appliquer**.

Les modifications prennent effet immédiatement.

## Configurer les Indicateurs de compromission

Les Indicateurs de compromission (IOC) des modules de score Malware Analysis sont configurés puisque chaque module de score Malware Analysis (Network, Static, Community, Sandbox et YARA) dispose d'un ensemble d'indicateurs de compromission (IOC) par défaut, qu'il utilise pour évaluer les données de fichier et de session afin de déterminer la probabilité de présence d'un malware.



Chaque IOC se voit attribuer une pondération de score numérique comprise entre 100 (bon) et 400 (médiocre). Lorsqu'un IOC se déclenche, la pondération de score numérique est prise en compte dans le score total de la session ou du fichier en cours d'analyse. Les pondérations de score individuelles de tous les IOC correspondants sont agrégées pour produire le score résultant de chaque session ou fichier. Le score agrégé est modifié de telle sorte qu'il ne dépasse pas la plage de score valide (comprise entre 100 et 400).

**Remarque :** La pondération de score attribuée à un IOC ne correspond pas toujours à la valeur de score explicite agrégée : il ne s'agit pas d'une simple addition des pondérations de score de chaque IOC qui se déclenche. En réalité, le score de l'IOC est une pondération ou un indicateur d'importance pris en compte dans le calcul d'un score global.

Les paramètres de configuration des indicateurs de compromission (IOC) de Malware Analysis se trouvent dans la vue Configuration des services > onglet Indicateurs de compromission. Voici un exemple de l'onglet.

General		Indicators of Compromise	IOC Summary	Auditing	Hash	AV	Proxy	ThreatGRID	Integration
Module: Community		Description: <input type="text"/>		Search: <input type="text"/>		<input type="button" value="Enable All"/> <input type="button" value="Enable"/> <input type="button" value="Disable All"/> <input type="button" value="Disable"/> <input type="button" value="Reset All"/> <input type="button" value="Reset"/> <input type="button" value="Save"/>			
<input type="checkbox"/>	Enabled	High Confidence	Description	Score	File Type				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Community Lists DNS Nameserver as Having Blacklisted Domains	15	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Community Lists Domain as Blacklisted	50	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Community Lists TLD (dest.tld) as Malicious	90	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Community Lists WHOIS Registrar as Having Blacklisted Domains	15	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: DNS TTL is Abnormally Low	5	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Event alias.host Resolves to IP Addresses in Multiple AS Numbers	25	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Event alias.host Resolves to IP Addresses in Multiple Countries	5	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Event alias.host Resolves to More than One IP Address	5	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Event alias.host Resolves to a Valid IPv6 Address	-10	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - Domain: Whois Date of Registration (alias.host) Indicates newly registered domain	10	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: AntVirus (Primary Vendor) Flagged File	100	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: AntVirus (Secondary Vendor) Flagged File	50	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: AntVirus did not Flag File	5	Windows PE				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: Community Identifies Provided File as Goodware	-50	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: Community Identifies Provided File as Goodware (low trust value)	-25	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: Community has assigned a Threat Level Assessment	10	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Community - File Hash: File Identified as Blacklisted (not trusted)	100	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community - File Hash: File Identified as WhiteListed (trusted)	-100	ALL				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Community: Service Failure	1	ALL				

Si vous prenez l'IOC **Community -Hachage de fichier : Fichier signalé par l'antivirus (fournisseur principal)** comme exemple, la pondération de score de l'IOC peut être définie à 100. Toutefois, Malware Analysis dilue cette valeur en fonction du pourcentage des principaux fournisseurs antivirus qui considèrent l'échantillon comme malveillant. Plus le nombre de fournisseurs qui estiment que l'échantillon est malveillant est proche de 100 %, plus la probabilité est grande que la totalité des 100 points soit utilisée pour agréger un score. Au fur et à mesure que le pourcentage se rapproche de 0 %, l'utilisation de la totalité des 100 points dans le score agrégé chute en proportion.

Les indicateurs de compromission principaux utilisent une logique mise en œuvre nativement dans Malware Analysis. Vous ne pouvez pas modifier cette logique. Vous pouvez seulement modifier l'IOC pour augmenter ou réduire son impact sur le score, pour indiquer un paramètre de confiance, ou encore pour l'activer ou le désactiver. Le scénario classique consiste à modifier un ensemble limité de valeurs de pondération de score d'IOC à la baisse pour les IOC qui font augmenter le score final et qui provoquent des résultats d'analyse faussement positifs. Il existe une solution extrême en matière de réglage : elle consiste à désactiver les IOC entièrement s'ils contribuent régulièrement à fournir des résultats faussement positifs. Par ailleurs, vous pouvez désactiver tous les IOC et choisir d'activer seulement un petit nombre d'entre eux. Par exemple, vous pouvez désactiver tous les IOC à l'exception de ceux qui détectent les correspondances des antivirus. À l'aide de Malware Analysis dans cette configuration extrêmement limitée, vous pouvez réduire les résultats de Malware Analysis de sorte que seules les correspondances A/V connues génèrent des résultats.



Vous pouvez configurer cette fonctionnalité de plusieurs façons :

- Désactivez les IOC afin qu'ils ne soient pas évalués dans le cadre du module de score auquel ils sont attribués.
- Modifiez la pondération de score d'un IOC afin d'augmenter ou de réduire son impact sur le score agrégé.
- Marquez les IOC qui vous semblent de bons indicateurs de malware, et affichez une balise de forte probabilité sur les sessions qui ont déclenché ces IOC dans les résultats de Malware Analysis.
- Personnalisez les paramètres de score et de probabilité de manière unique pour le type de fichiers analysé. Un type de fichiers est préattribué à chaque IOC auquel il est appliqué. Les valeurs possibles sont **TOUS**, **PDF**, **Microsoft Office** et **Windows PE**. L'IOC ayant le type de fichiers le plus approprié est utilisé durant l'analyse des fichiers. Par exemple, si un fichier PDF est analysé, un IOC dont le type de fichiers est **PDF** est choisi à la place du même IOC dont le type de fichiers est **TOUS**. En l'absence de correspondance avec un type de fichiers spécifique, l'IOC dont le type de fichiers est **TOUS** est sélectionné.
- Recherchez les règles à afficher dans la grille en fonction d'une correspondance avec la description de la règle.

## Filterer les IOC affichés par module

Vous pouvez filtrer les IOC affichés par module de score : l'un des quatre modules intégrés ou YARA. Les IOC YARA sont imbriqués dans les IOC natifs de chaque catégorie. Bien que les IOC YARA ne soient pas identifiés comme tels dans les autres affichages, vous pouvez sélectionner YARA dans la liste de sélection Module pour voir la liste des règles YARA.

Pour visualiser les IOC de l'un des quatre modules de score, ou de YARA :

1. Dans le menu **Menu principal**, sélectionnez **Admin > Services**.
2. Sélectionnez un service Malware Analysis.
3. Dans la ligne, sélectionnez   > **Vue > Configuration**.
4. Cliquez sur l'onglet **Indicateurs de compromission**.
5. Dans la liste de sélection **Module**, sélectionnez Tous, NextGen, Static, Community, Sandbox ou Yara.

Les règles et paramètres configurés pour le module sont affichés.

Enabled	Description	Score	File Type
<input type="checkbox"/>	Community - File Hash: AntiVirus did not Flag File	5	Windows PE
<input checked="" type="checkbox"/>	Community: Service Failure	1	ALL
<input checked="" type="checkbox"/>	Community - File Hash: File Identified as WhiteListed (trusted)	-100	ALL
<input checked="" type="checkbox"/>	Community - File Hash: File Identified as Blacklisted (not trusted)	100	ALL
<input checked="" type="checkbox"/>	Community - File Hash: Community has assigned a Threat Level Assessment	10	ALL
<input checked="" type="checkbox"/>	Community - File Hash: Community Identifies Provided File as Goodware (low trust value)	-25	ALL
<input checked="" type="checkbox"/>	Community - File Hash: Community Identifies Provided File as Goodware	-50	ALL
<input checked="" type="checkbox"/>	Community - File Hash: AntiVirus (Secondary Vendor) Flagged File	50	ALL
<input checked="" type="checkbox"/>	Community - File Hash: AntiVirus (Primary Vendor) Flagged File	100	ALL
<input checked="" type="checkbox"/>	Community - Domain: Whois Date of Registration (alias.host) indicates newly registered domain	10	ALL
<input checked="" type="checkbox"/>	Community - Domain: Event alias.host Resolves to a Valid IPv6 Address	-10	ALL
<input checked="" type="checkbox"/>	Community - Domain: Event alias.host Resolves to More than One IP Address	5	ALL
<input checked="" type="checkbox"/>	Community - Domain: Event alias.host Resolves to IP Addresses in Multiple Countries	5	ALL
<input checked="" type="checkbox"/>	Community - Domain: Event alias.host Resolves to IP Addresses in Multiple AS Numbers	25	ALL
<input checked="" type="checkbox"/>	Community - Domain: DNS TTL is Abnormally Low	5	ALL
<input checked="" type="checkbox"/>	Community - Domain: Community Lists WHOIS Registrar as Having Blacklisted Domains	15	ALL
<input checked="" type="checkbox"/>	Community - Domain: Community Lists TLD (dest.tld) as Malicious	50	ALL
<input checked="" type="checkbox"/>	Community - Domain: Community Lists Domain as Blacklisted	50	ALL
<input checked="" type="checkbox"/>	Community - Domain: Community Lists DNS Management as Having Blacklisted Domains	15	ALL

## Filter les modules affichés pour montrer uniquement les modules modifiés

L'onglet **Indicateurs de compromission** identifie visuellement les IOC modifiés localement. Lorsqu'un IOC est modifié, par exemple, la pondération de score change. En outre, le nom est affiché en rouge et comprend un indicateur de modification ajouté au nom de l'IOC. L'indicateur de modification est ++ et peut être utilisé comme mécanisme de filtrage durant la recherche d'IOC.

Pour limiter l'affichage aux IOC modifiés localement :

1. Dans le champ **Description**, saisissez ++.
2. Cliquez sur **Rechercher**.


La vue est filtrée pour afficher uniquement les IOC modifiés.

## Activer et désactiver les IOC d'un module de score

Lorsqu'un IOC est désactivé, il n'a plus d'impact sur le score d'agrégation du module de score auquel il appartient. Si l'IOC a des instances multiples (différenciées uniquement par le type de fichiers), la désactivation d'un IOC spécifique d'un type de fichiers entraîne l'utilisation d'une version de l'IOC indépendante du type de fichiers pour l'attribution du score.

Par exemple, s'il existe un même IOC avec le type de fichiers **TOUS** et le type de fichiers **Windows PE**, la désactivation de l'instance **Windows PE** de l'IOC entraîne l'utilisation de la version **TOUS** pour l'attribution du score. Pour désactiver complètement l'IOC pour **Windows PE**, tout en laissant l'IOC activé pour d'autres types de fichiers, définissez la pondération de score de l'instance **Windows PE** de l'IOC à la valeur zéro, comme indiqué ci-dessous. Ainsi, l'IOC reste activé pour les fichiers Windows PE (bien que sa pondération soit égale à zéro et qu'il soit supprimé de l'affichage des résultats d'analyse), sans affecter les autres types de fichiers. Les types de fichiers restants continuent d'utiliser l'instance **TOUS** de l'IOC.

Pour activer ou désactiver un IOC afin qu'il ne soit plus pris en compte dans un module de score :

1. Dans le menu **Menu principal**, sélectionnez **Admin > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue Config**.
3. Cliquez sur l'onglet **Indicateurs de compromission**.
4. Dans la liste de sélection **Module**, sélectionnez un module de score : Tous, Community, Network, Sandbox, Static ou Yara.  
Les règles et paramètres configurés pour le module sont affichés.
5. Exécutez l'une des opérations suivantes :
  - a. Activez la case à cocher **Activé** dans la colonne située en regard de la règle que vous souhaitez activer.
  - b. Sélectionnez une ou plusieurs règles, puis cliquez dans la barre d'outils sur **Activer** ou **Désactiver**.
  - c. Pour basculer entre Activé et Désactivé pour toutes les règles affichées sur la page, activez la case à cocher **Activé** dans le titre de la colonne.
  - d. Pour activer ou désactiver toutes les règles du module de score, cliquez dans la barre d'outils sur **Activer tout** ou **Désactiver tout**.
6. Pour enregistrer les modifications de la page, cliquez sur **Enregistrer** dans la barre d'outils.

**Remarque :** Les règles dont les paramètres sont modifiés sont affichées avec un angle rouge. Si vous naviguez vers une autre page avant d'enregistrer, toutes les modifications de cette page seront perdues.

## Modifier la pondération de score d'un IOC

La modification de la pondération de score d'un IOC augmente ou réduit l'impact global de l'IOC sur le score d'agrégation du module dans lequel il est configuré. Pour augmenter ou réduire l'impact global de l'IOC, réduisez la valeur actuelle en définissant un nouveau paramètre.

- Les valeurs comprises entre -100 et -1 indiquent que la session ou le fichier en cours d'analyse n'est pas susceptible d'être un malware (-100 étant la probabilité la plus faible).
- Les valeurs comprises entre 1 et 100 indiquent qu'il est probable que le fichier ou la session en cours d'analyse soit un malware (100 étant la probabilité la plus forte).
- Si vous définissez la valeur à zéro, l'IOC reste activé mais n'a plus d'impact sur le score d'agrégation. En outre, l'IOC est supprimé de l'affichage des résultats d'analyse. Définir la valeur à zéro est une méthode qui permet de désactiver l'instance spécifique d'un type de fichiers d'un IOC tout en gardant intacte l'instance indépendante du type de fichiers d'origine de la règle pour l'attribution d'un score aux types de fichiers restants.

Pour modifier la pondération de score :



1. Dans **Menu principal**, sélectionnez **Admin > Services**.
2. Sélectionnez un service Malware Analysis.
3. Dans la **barre d'outils**, sélectionnez **Vue > Configuration**.
4. Cliquez sur l'onglet **Indicateurs de compromission**.
5. Dans la liste de sélection **Module**, sélectionnez un module de score : Tous, Network, Static, Community, Sandbox ou Yara.  
Les règles et paramètres configurés pour le module sont affichés.
6. Exécutez l'une des opérations suivantes :
  - a. Faites glisser le curseur de score vers la gauche ou vers la droite pour augmenter ou réduire la pondération de score.
  - b. Cliquez directement sur la pondération de score affichée, puis saisissez une pondération de score.
7. Pour enregistrer les modifications de la page, cliquez sur **Enregistrer** dans la barre d'outils.

**Remarque :** Les règles dont les paramètres sont modifiés sont affichées avec un angle rouge. Si vous naviguez vers une autre page avant d'enregistrer, toutes les modifications de cette page seront perdues.

## Définir l'indicateur de forte probabilité d'un IOC

Le paramètre Forte probabilité permet de baliser des IOC spécifiques en tant qu'indicateurs de présence d'un malware avec un haut degré de probabilité. Par exemple, l'IOC **Community - Hachage de fichier : Fichier signalé par l'antivirus (fournisseur principal)** présente une faible probabilité de faux positif, ainsi qu'une forte probabilité de malware. En balisant cet IOC (et d'autres) en tant qu'indicateur de forte probabilité, vous pouvez utiliser un filtre dans les résultats de Malware Analysis pour limiter l'affichage aux sessions qui incluent une ou plusieurs règles de forte probabilité. Ainsi, l'affichage est limité à un sous-ensemble de résultats dont la pertinence est associée à un degré de probabilité plus important. L'affichage de résultats qui ne se limitent pas aux IOC à forte probabilité vous permet tout de même de vérifier les résultats incertains. Cela aboutit à des résultats moins susceptibles d'être de faux négatifs. Le filtrage ou non des résultats en fonction du degré de probabilité correspond à un exemple d'utilisation valide dans le workflow NetWitness Suite.

Pour définir l'indicateur de forte probabilité :

1. Sous l'onglet **Indicateurs de compromission**, sélectionnez un module de score dans la liste de sélection **Module** : Tous, Réseau, Statique, Communauté, Sandbox ou Yara.  
Les règles et paramètres configurés pour le module sont affichés.
2. Activez la case à cocher **Forte probabilité** dans la colonne située en regard d'une règle que vous souhaitez baliser ou non comme étant hautement susceptible d'indiquer la présence de malware dans une session en cas de concordance.
3. Pour enregistrer les modifications de la page, cliquez sur **Enregistrer** dans la barre d'outils.

**Remarque :** Les règles dont les paramètres sont modifiés sont affichées avec un angle rouge. Si vous naviguez vers une autre page avant d'enregistrer, toutes les modifications de cette page seront perdues.

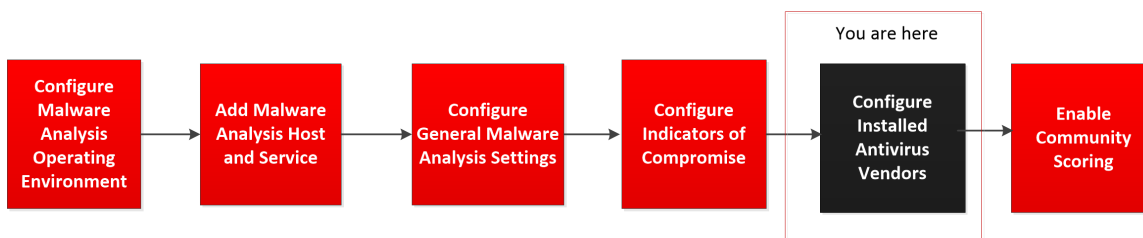
## Réinitialiser les paramètres par défaut des IOC

1. Sous l'onglet **Indicateurs de compromission**, sélectionnez un module de score dans la liste de sélection Module : Tous, Réseau, Statique, Communauté, Sandbox ou Yara.  
Les règles et paramètres configurés pour le module sont affichés.
2. Si vous souhaitez rétablir les paramètres par défaut de toutes les règles de la page active, cliquez dans la barre d'outils sur **Réinitialiser**.
3. Si vous souhaitez rétablir les paramètres par défaut de toutes les règles du module de score sélectionné, cliquez dans la barre d'outils sur **Réinitialiser tout**.
4. Pour enregistrer les modifications de la page, cliquez sur **Enregistrer** dans la barre d'outils.

## Configurer les fournisseurs d'antivirus installés

Vous pouvez comparer les résultats de l'analyse des fichiers provenant de vos fournisseurs d'antivirus installés par rapport aux résultats de la Communauté provenant de la base de connaissances Malware Analysis. Pendant qu'un fichier fait l'objet d'une analyse de la communauté, Malware Analysis consulte une base de connaissances d'antivirus pour déterminer si l'échantillon est déjà identifié comme étant malveillant. Si le fichier est reconnu comme malveillant, NetWitness Suite marque le fichier pour indiquer si un fournisseur d'antivirus primaire ou un fournisseur d'antivirus secondaire a identifié l'échantillon. NetWitness Suite classe les fournisseurs comme primaires et secondaires pour refléter le niveau de réputation de ces fournisseurs dans le secteur, et les Indicateurs de compromission factorisent cette réputation dans la note. Par exemple, la détection réalisée uniquement par des fournisseurs d'antivirus secondaires peut présenter une note inférieure à celle liée à la détection par des fournisseurs principaux.


**Remarque :** Lors du choix du logiciel de fournisseur d'antivirus à installer sur votre réseau, il est fortement recommandé d'en inclure au moins un provenant de la liste des fournisseurs principaux NetWitness Suite.





Vous pouvez identifier les fournisseurs d'antivirus installés sur votre réseau dans NetWitness Suite. NetWitness Suite compare les résultats des antivirus pendant l'analyse de la communauté par rapport aux résultats des fournisseurs installés sélectionnés sous l'onglet Antivirus. Si une correspondance est détectée, le fichier analysé est marqué pour indiquer que votre logiciel antivirus primaire ou secondaire, installé localement, a détecté l'échantillon.


L'exemple ci-dessous présente les résultats de l'analyse de communauté pour un fichier qui présentait une note de 100. Sous **Indicateurs de compromis**, vous pouvez voir que le fichier a été marqué par les fournisseurs d'AV répertoriés dans la communauté. Sous **Résultats du fournisseur d'antivirus**, NetWitness Suite indique si les fournisseurs antivirus (AV) installés dans votre environnement ont signalé le fichier comme malveillant. Si vos fournisseurs d'AV installés ont détecté le virus, le nom du malware s'affiche. Si vos fournisseurs d'AV installés n'ont pas détecté le virus, **--Non détecté--** s'affiche en regard du nom du fournisseur d'AV. Sous **Fournisseurs non installés**, vous pouvez cliquer sur + pour développer la section et voir si d'autres fournisseurs non installés sur votre système ont détecté le virus.

100
COMMUNITY ANALYSIS RESULTS



 DNS (Lowest TTL)  
N/A

 DNS (ASNs)  
N/A

 DNS (A Records)  
N/A

 DNS (Geolocation)  
N/A

INDICATORS OF COMPROMISE



Community - File Hash: AntiVirus (Primary Vendor) Flagged File

AntiVirus Matched 5 of 13 AV Providers: AVG: IRC/BackDoor.Flood, McAfee-Gateway: Artemis!7D708F247CC6, TrendMicroHouseCall: Mal\_Zap, Fortinet: W32/Inject.8A2F!tr, TrendMicro: Mal\_Zap

AV VENDOR RESULTS


Your AntiVirus vendor(s) flagged this file as being malicious.


Installed AV Vendors

	AVG	IRC/BackDoor.Flood
	McAfee-Gateway	Artemis!7D708F247CC6

Not Installed AV Vendors


N/A
SANDBOX ANALYSIS RESULTS

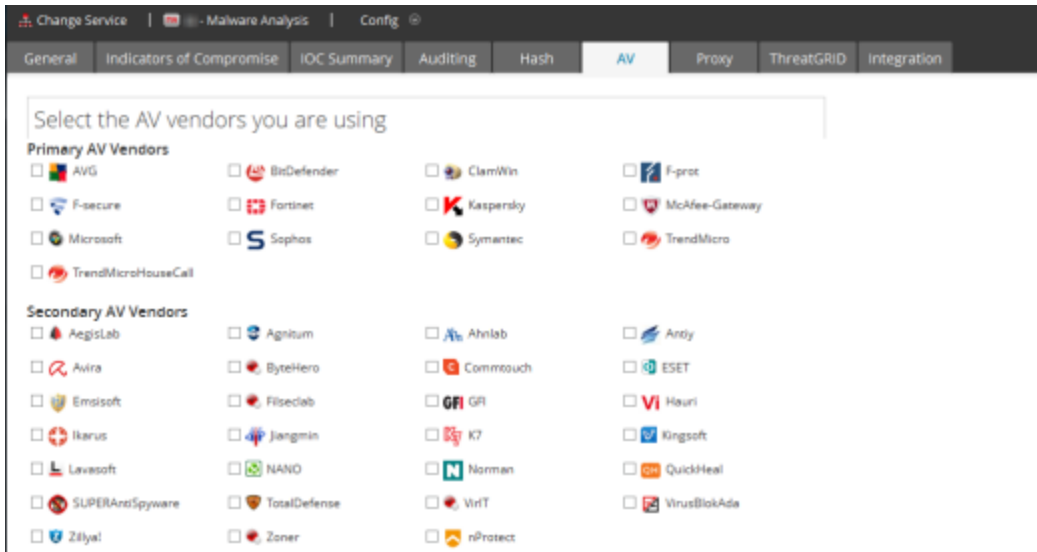
 Number Files Downloaded  
N/A

 Number Outgoing Sockets  
N/A

## Identifier le logiciel AV installé

Pour identifier le logiciel antivirus installé sur votre réseau :

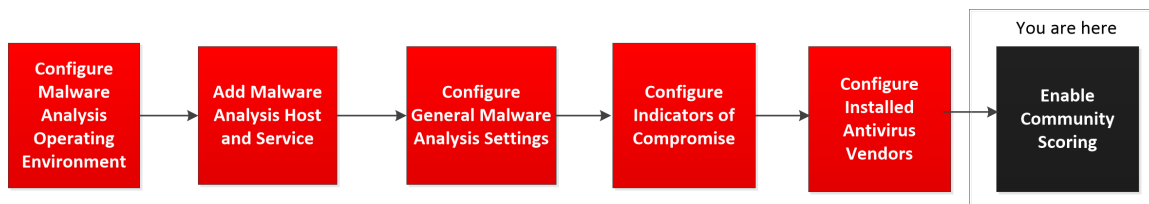
1. Dans le **Menu principal**, sélectionnez > **ADMINServices**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue Config**.
3. Dans la **vue Configuration des services**, sélectionnez l'onglet **AV**.




4. Sélectionnez la case à cocher près de chaque fournisseur d'antivirus (principal ou autre) dont le logiciel est installé sur votre réseau.
5. Pour enregistrer les modifications, cliquez sur **Appliquer**.  
Les résultats de l'analyse Communauté indiqueront si votre logiciel a signalé un événement.
6. (Facultatif) Si vous souhaitez réinitialiser la liste de logiciels antivirus installés sur la valeur par défaut (aucun), cliquez sur **Réinitialiser**.  
Toutes les sélections sont supprimées.
7. Pour enregistrer les modifications, cliquez sur **Appliquer**.

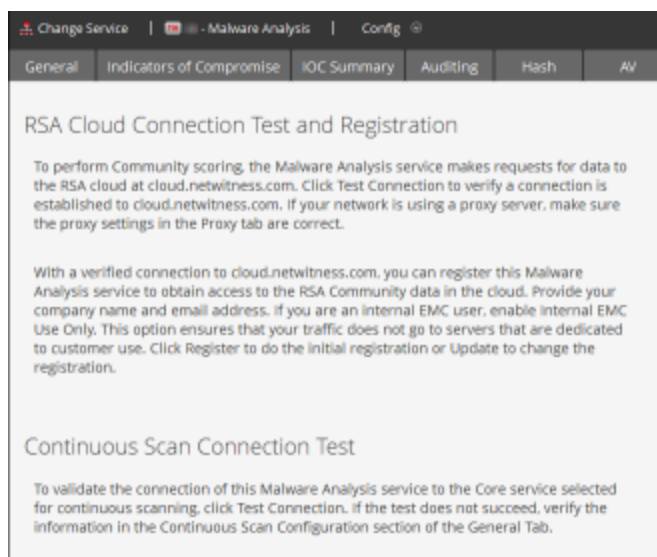
## Activer l'analyse de la communauté

Un administrateur peut activer l'analyse de la communauté. 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 activer l'analyse de communauté, vous devez vous enregistrer avec le Cloud RSA et tester la connexion au Cloud, puis tester la connexion entre le Cloud RSA et le service que vous avez configuré pour l'analyse continue.



Vous trouverez une description complète des méthodes d'analyse dans [Comment fonctionne Malware Analysis](#).

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue > Config**.
3. Dans la **Vue Configuration des services**, sélectionnez l'onglet **Intégration**.



4. Faites défiler jusqu'au Test de connexion à l'analyse continue et cliquez sur **Test et enregistrement de la connexion au Cloud RSA**.  
NetWitness Suite teste les communications avec le site sur <https://cloud.netwitness.com>. Si votre société utilise un proxy pour le trafic sortant, vérifiez vos paramètres de proxy. Une connexion valide est nécessaire pour s'enregistrer auprès du service de la communauté RSA.
5. Saisissez le nom de votre entreprise et l'e-mail du contact. Cliquez sur **S'inscrire**.  
Si tous les champs obligatoires sont complétés, votre enregistrement est terminé. Le libellé du bouton utilisé pour l'enregistrement devient Mettre à jour.
6. Pour vérifier que le service Malware Analysis peut se connecter au service Core sélectionné pour l'analyse continue, cliquez sur **Test de connexion à l'analyse continue**.

NetWitness Suite lance un contrôle basé sur l'hôte source, le port source, le nom d'utilisateur et le mot de passe d'utilisateur spécifiés dans l'onglet Général. Lorsque le test s'exécute correctement, les analystes peuvent voir le score de communauté dans Malware Analysis.

## (Facultatif) Configurer l'auditing sur l'hôte Malware Analysis

Cette rubrique présente les fonctionnalités configurables du log d'audit Malware Analysis et les procédures de configuration des fonctionnalités. Malware Analysis est capable de générer des alertes d'audit basées sur des seuils de modules de notation configurés. Une fois que le score d'analyse d'un fichier dans une session d'analyse atteint ou dépasse le ou les seuils configurés, une alerte d'audit est générée. Le seuil permet aux sessions et aux fichiers qui atteignent un score suffisamment élevé d'être de potentiels programmes malveillants candidats pour générer automatiquement une alerte.

Les alertes peuvent être configurées pour être formatées comme entrées SNMP, Syslog ou File. La prise en charge de plusieurs formats d'audit fournit une méthode permettant aux systèmes externes d'acquérir des événements d'audit en fonction de leur capacité à analyser les formats pris en charge.

En plus des sessions d'analyse d'audit, les événements suivants déclencheront une alerte d'audit :

- Réussites et échec de la connexion utilisateur
- Modifications des paramètres de configuration système
- Redémarrage du serveur
- Mise à niveau ou installation de version du serveur

Les paramètres de configuration d'audit pour Malware Analysis se trouvent dans la vue Configuration des services > onglet Audit.

The screenshot shows the configuration interface for Malware Analysis, specifically the Auditing tab. The interface is organized into several sections:



- Audit Thresholds:** A table with columns 'Name' and 'Config Value'. It includes sliders for Community Threshold, Static Threshold, Network Threshold, and Sandbox Threshold, all set to 50. There is also a checkbox for 'Notify when Installed AV Misses and Primary AV Detects'.
- Incident Management Alerting:** A table with columns 'Name' and 'Config Value'. It includes a checkbox for 'Enabled'.
- File Auditing:** A table with columns 'Name' and 'Config Value'. It includes checkboxes for 'Enable File Auditing', a text input for 'Archive File Count' (set to 20), and a text input for 'Max File Size' (set to 10485760).
- SNMP Auditing:** A table with columns 'Name' and 'Config Value'. It includes a checkbox for 'Enabled', and text inputs for 'Server Name' (127.0.0.1), 'Server Port' (1610), 'SNMP Version' (v2c), and 'Trap OID' (1.3.6.1.4.1.36807.1.8).
- Syslog Auditing:** A table with columns 'Name' and 'Config Value'. It includes a checkbox for 'Enabled', and text inputs for 'Server Name' (localhost), 'Server Port' (514), and 'Facility' (USER).

An 'Apply' button is located at the bottom center of the configuration area.

## Configurer le seuil d'audit



L'unique but des seuils vise à spécifier les critères qui doivent être atteints avant qu'une alerte soit générée pour une session/un fichier analysé(e). Si l'audit est activé, chaque fichier/session noté(e) est examiné(e) afin de déterminer si le score dans chaque module de notation atteint ou dépasse le seuil d'audit configuré. Si c'est le cas, une alerte est générée à l'aide du format d'alerte d'audit configuré (par ex., SNMP, Syslog ou File). Par exemple, en configurant SNMP et en définissant le seuil de communauté sur 90, toutes les sessions/tous les fichiers qui obtiennent un score supérieur ou égal à 90 dans le module Score de communauté génère un trap SNMP. Si tous les seuils sont définis sur 90, alors aucune alerte n'est générée, sauf si une session ou un fichier obtient un score supérieur ou égal à 90 dans les modules de notation Network, Static, Community et Sandbox.

Pour configurer le seuil d'audit :

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez   > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez sur l'onglet **Audit**.
4. Dans la section **Seuils d'audit** :
  - a. Définissez les seuils pour **Communauté, Statique, Réseau** et **Sandbox** en utilisant l'une des méthodes suivantes pour chacun des modules de notation :
    - Dans le curseur, cliquez puis faites glisser la poignée dans un sens ou dans l'autre.
    - Dans le champ de valeur, saisissez un nombre compris entre 0 et 100 inclus.
  - b. (Facultatif pour 10.3 SP2) Sélectionnez un ou plusieurs déclencheurs pour enregistrer un message et le livrer via toutes les méthodes d'audit activées.
  - c. Cliquez sur **Appliquer**.
    - Le réglage du seuil prend effet immédiatement pour toutes les méthodes d'audit activées : SNMP, fichier et Syslog.
    - Les messages enregistrés sont envoyés vers toutes les méthodes d'audit activées : SNMP, fichier et Syslog.

## Configurer Alerte de gestion des incidents

Lorsque la Gestion des incidents est activée, elle peut auditer des alertes Malware Analysis pour alimenter le workflow Gestion des incidents.

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez   > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **Audit**.



4. Dans la section **Alerte de gestion des incidents**, cochez la case **Activée** puis cliquez sur **Appliquer**.

L'alerte prend effet immédiatement.

## Configuration de l'audit SNMP

Le SNMP est un protocole standard Internet pour la gestion des services sur des réseaux IP. Lorsque l'audit SNMP est activé, Malware Analysis peut envoyer un événement d'audit comme trap SNMP à l'hôte du trap SNMP configuré. En plus du score et de l'ID d'événement, l'alerte inclut tous les métas de sessions ainsi que les métadonnées générées. Cela est utile pour les utilisateurs qui souhaitent fournir des données d'événements à des systèmes tiers.

Pour configurer l'audit SNMP :

1. Dans le Menu principal, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez   > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **Audit**.
4. Dans la section **Audit SNMP**, cochez la case pour activer l'audit SNMP.
5. Configurez le port et le nom de serveur SNMP.
6. Configurez la version SNMP et OID de trap pour l'envoi de traps.
7. Configurez la communauté Malware Analysis, puis réessayez l'expiration du délai des paramètres lors de l'envoi de traps.
8. Cliquez sur **Appliquer**.

Les paramètres d'audit SNMP prennent effet immédiatement.

## Configurer Paramètres d'audit des fichiers

Lorsque l'audit des fichiers est activé, le fichier log d'audit est conservé dans le Répertoire personnel Malware Analysis. L'emplacement par défaut de ce fichier est le suivant :


```
/var/lib/netwitness/malware-analytics-  
server/spectrum/logs/audit/audit.log.
```

Chaque log, lorsqu'il atteint la taille de fichier maximum, est archivé et un nouveau log est créé. La taille de ces logs d'audit et leur nombre sont deux paramètres configurables.

**Attention :** Évitez de définir la taille de fichier max et le nombre de fichier d'archive sur des valeurs trop élevées. En effet, cela peut avoir un effet négatif sur l'espace disque disponible sur l'appliance Malware Analysis.

Pour configurer les paramètres d'audit de fichier :



1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **Audit**.
4. Dans la section **Audit de fichiers**, cochez la case pour activer l'audit de fichiers.
5. (Facultatif) Définissez Nombre de fichiers d'archive et Taille max. de fichier.
6. Cliquez sur **Appliquer**.


Les paramètres d'audit de fichier prennent effet immédiatement.

## Configurer Paramètres d'audit Syslog

En cas d'activation, Syslog propose l'audit via l'utilisation du protocole syslog RFC 5424. Les réglementations, telles que SOX, PCI DSS, HIPAA, et bien d'autres contraignent les organisations à mettre en œuvre des mesures de sécurité globales, qui incluent souvent la collecte et l'analyse de logs provenant de nombreuses sources différentes. Le format Syslog a fait la preuve de son efficacité pour consolider les logs car il existe de nombreux outils open source et propriétaires pour le reporting et l'analyse.

En plus du score et de l'ID d'événement, le syslog inclut tous les métas de sessions ainsi que les métadonnées générées. Cela est utile pour les utilisateurs qui souhaitent fournir des données d'événements à des systèmes tiers.

Pour configurer les paramètres d'audit de syslog :

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **Audit**.
4. Dans la section **Audit Syslog**, cochez la case pour activer l'audit de syslog.
5. Configurez l'hôte où s'exécute le processus syslog cible puis le port sur l'hôte où le processus syslog est à l'écoute.
6. Configurez la fonction, l'encodage, le format, la longueur max et l'horodatage pour les messages syslog sortants.

**Remarque :** (Facultatif) Configurez Identifier la chaîne pour l'ajouter au début des alertes syslog.

Pour le format CEF, veuillez vous reporter à [Créer une alerte personnalisée au format CEF](#) pour en savoir plus.

7. Cliquez sur **Appliquer**.

Les paramètres d'audit syslog prennent effet immédiatement.

## (Facultatif) Configurer le filtre de hachage

Cette rubrique présente les filtres de hachage, qui offrent une méthode pour identifier comme malveillants ou sûrs des fichiers stockés dans Malware Analysis. Le filtrage de hachage permet d'établir la liste des fichiers identifiés comme étant malveillants ou sûrs. Sous l'onglet Hachage, vous pouvez régler l'analyse des événements Malware Analysis en fonction des hachages de fichier. Lorsqu'un hachage de fichier est identifié comme correct, Malware Analysis n'analyse pas le fichier lorsqu'il réapparaît. Lorsqu'un hachage de fichier est identifié comme incorrect, Malware Analysis ajoute automatiquement un grand nombre de points au score de la communauté. Malware Analysis analyse tout de même le fichier pour déterminer si de nouvelles informations sont disponibles.

**Remarque :** Si un événement contient un seul fichier considéré comme correct, Malware Analysis filtre l'événement entier mais ne l'affiche pas dans les résultats Malware Analysis.


Pour ajouter des filtres de hachage à la liste, suivez l'une ou l'autre de ces méthodes manuelles :

1. Menu contextuel dans la vue Détails des événements : Cliquez avec le bouton droit de la souris sur un fichier. Le menu contextuel qui s'ouvre permet de marquer le hachage du fichier sélectionné comme correct (normal) ou incorrect (malveillant).
2. Barre d'outils de l'onglet Hachage : Cliquez sur le bouton Ajouter sous l'onglet Hachage pour ajouter un hachage de fichier et une taille de fichier. Vous pouvez éventuellement marquer le hachage comme fiable.

Une méthode automatisée s'offre à vous pour ajouter des filtres de hachage dans Malware Analysis, qui consiste à importer une liste de hachage en bloc à partir du dossier surveillé. Les hachages importés par l'intermédiaire du dossier surveillé ne figurent pas dans la liste de hachage. Si l'importation en bloc et le répertoire de suivi (/var/netwitness/malware-analytics-server/spectrum/hashWatch) sont configurés sur le serveur Malware Analysis, copiez une liste de hachage dans le dossier surveillé pour qu'elle soit importée automatiquement sur le système. Les hachages importés en bloc en appliquant cette méthode remplacent ceux qui avaient précédemment été importés à partir du dossier surveillé.

### Afficher la liste de hachage

Pour afficher la liste de hachage :

1. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
2. Dans la grille Services, sélectionnez un service Malware Analysis, puis  > **Vue > Configuration**.
3. Cliquez sur l'onglet **Hachage**.

La liste de hachage s'affiche sous l'onglet Hachage. Seuls les hachages de fichier ajoutés en appliquant une des méthodes mentionnées y figurent.

## Ajouter un hachage de fichier au filtre de hachage

Pour ajouter un hachage de fichier au filtre de hachage :

1. Sous l'onglet **Hachage**, cliquez sur **Ajouter** dans la barre d'outils.

La boîte de dialogue Ajouter un hachage s'ouvre.

2. Si le hachage est digne de confiance, sélectionnez **Fiable**.
3. Indiquez l'algorithme MD5 ainsi que la taille de fichier (en octets).
4. Cliquez sur **Enregistrer**.

Le hachage de fichier est ajouté à la liste et utilisé pour procéder au filtrage dans Malware Analysis.

## Marquer un hachage comme fiable ou non fiable

Pour marquer un hachage comme fiable ou non fiable :

1. Sous l'onglet **Hachage**, cliquez dans la colonne **Fiable** du hachage concerné pour lui associer l'option Fiable ou Non fiable.
2. Dans la barre d'outils, cliquez sur **Enregistrer la modification**.

## Supprimer un hachage du filtre de hachage

Pour supprimer un hachage du filtre de hachage :

1. Sous l'onglet **Hachage**, sélectionnez un ou plusieurs hachages à supprimer du filtre.
2. Dans la barre d'outils, cliquez sur **Supprimer**.

Une boîte de dialogue s'ouvre pour confirmer l'opération et permet de l'annuler, le cas échéant.

3. Pour confirmer la suppression, cliquez sur **Oui**.

Le hachage de fichier est supprimé de la grille et n'est plus utilisé pour procéder au filtrage de hachage dans Malware Analysis.

## Rechercher un hachage de fichier

Sous l'onglet Hachage, vous pouvez rechercher un hachage de fichier figurant dans la grille.

Dans le champ MD5, indiquez le nom du hachage de fichier concerné, puis cliquez sur **Rechercher**. La liste des fichiers contenant le hachage s'affiche dans la grille.

## Importer une liste de hachage à l'aide du dossier surveillé

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 décrit ci-après dans un dossier (`/var/netwitness/malware-analytics-server/spectrum/hashWatch`) stocké sur l'apppliance Malware Analysis pour qu'il soit importé automatiquement dans la base de données de hachage locale. C'est la seule façon d'importer des hachages de fichier. Autrement, il faut autoriser un administrateur système à exposer le répertoire de suivi à un processus permettant d'y copier un fichier. Il s'agit d'une méthode d'importation en bloc destinée à gérer un volume élevé de hachages.

Le fichier doit être au format csv ; les données de chaque ligne ne sont pas séparées par des espaces. On part du principe que la liste de hachage n'inclut pas de doublons. Les valeurs en double sont ignorées au cours du traitement. Si des hachages en double sont rencontrés, le fichier log affiche le message suivant pour indiquer le nombre de hachages dupliqués figurant dans le fichier :

```
2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing -
/var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO
com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate
Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /
var/lib/rsa>malware/hashWatch/test.csv
```

Voici un exemple de liste de hachage dans le format de fichier par défaut.

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

Un fichier de configuration NetWitness Suite (`/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml`) spécifie le format et les options d'importation d'une liste de hachage. Voici un extrait du fichier de configuration.

```

<config>
  <enabled>true</enabled>
  <distributedCacheEnabled>true</distributedCacheEnabled>

  <watchDirectory>/
  /var/lib/rsamalware/hashWatch</watchDirectory>

  <processedDirectory>/
  var/lib/rsamalware/hashWatch/processed</processedDirectory>

  <erroredDirectory>/
  var/lib/rsamalware/hashWatch/error</erroredDirectory>
  <md5Col>0</md5Col>
  <fileSizeCol>-1</fileSizeCol>
  <isTrustedCol>1</isTrustedCol>
  <isTrust>>false</isTrust>
  <ignoreFirstLine>>false</ignoreFirstLine>
  <frequencyInMinutes>1</frequencyInMinutes>
  <isGzipCompressed>>false</isGzipCompressed>
</config>

```

Ligne	Description
<md5Col>0</md5Col>	Emplacement du hachage md5 dans chaque entrée. La valeur par défaut est la position <b>0</b> , soit la première place.
<fileSizeCol>1</fileSizeCol>	Emplacement de la taille du hachage dans chaque entrée. La valeur par défaut est la position <b>1</b> , soit la deuxième place. Si la taille du hachage ne figure pas dans le fichier csv, il faut définir la valeur <b>-1</b> .
<isTrustedCol>2</isTrustedCol>	Emplacement de la colonne Fiable dans chaque entrée. La valeur par défaut est la position <b>2</b> . Si le paramètre Fiable ne figure pas dans le fichier csv, il faut définir la valeur <b>-1</b> .
<isTrust>>false</isTrust>	La supposition par défaut pour le paramètre <b>Fiable</b> est <b>false</b> pour chaque entrée.
<ignoreFirstLine>>false</ignoreFirstLine>	Présence ou absence d'en-tête dans le hachage. La valeur par défaut est <b>false</b> . Si le hachage contient un en-tête, il faut définir la valeur <b>true</b> .

Ligne	Description
<code>&lt;frequencyInMinutes&gt;1&lt;/frequencyInMinutes&gt;</code>	Intervalle entre deux vérifications du répertoire de suivi par NetWitness Suite. La valeur par défaut est <b>1</b> minute.
<code>&lt;isGzipCompressed&gt;&gt;false&lt;/isGzipCompressed&gt;</code>	Compression du hachage à l'aide de Gzip. La valeur par défaut est <b>false</b> . Si le hachage est compressé à l'aide de Gzip, il faut définir la valeur <b>true</b> .

Après l'importation de la liste de hachage, le log système affiche des entrées similaires aux suivantes :

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processed -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

En cas de problème lors du chargement du fichier, le log système affiche des entrées similaires aux suivantes :

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
... Verbose log
2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Error Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

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

1. Copiez les listes de hachage que vous souhaitez importer dans le répertoire **`/var/netwitness/malware-analytics-sever/spectrum/hashWatch`**.  
Malware Analysis surveille automatiquement ce dossier et traite les fichiers qui y sont placés.  
Malware Analysis ajoute chaque hachage trouvé dans les listes de hachage au filtre de hachage.  
Le cas échéant, les erreurs de traitement sont consignées sous **`/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error`**  
Les fichiers traités sont répertoriés sous **`/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed`**  
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.


## (Facultatif) Configurer les paramètres proxy de Malware Analysis

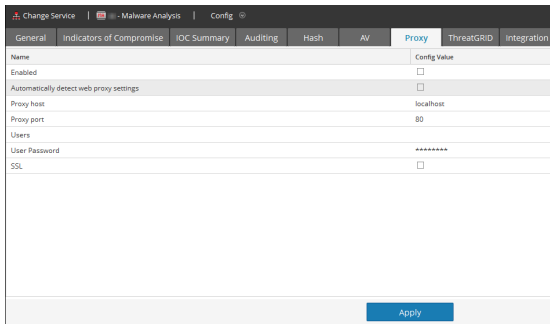
Cette rubrique décrit la configuration d'un proxy Web pour communiquer avec le service RSA Cloud et le service local ThreatGrid ou GFI. Les paramètres de la vue Configuration du service > onglet Proxy établissent une communication par proxy Web, que Malware Analysis peut utiliser pour communiquer avec RSA Cloud pour l'analyse de communauté et l'analyse sandbox. Une fois que le proxy est configuré :

- Malware Analysis communique via proxy Web proxy avec RSA Cloud pour l'analyse de communauté.
- Malware Analysis communique via proxy Web avec le service sandbox ThreatGrid ou GFI. L'utilisation de ce proxy Web peut dégrader les performances. Les sections de ThreatGrid et GFI de l'onglet Général disposent d'une option pour ignorer le proxy Web et communiquer directement avec sandbox en vue d'améliorer les performances.

### Configurer le proxy Web

Pour configurer le proxy Web pour Malware Analysis :

1. Accédez à la **ADMIN > vue Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez  > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **Proxy**.



4. Pour activer le proxy, cochez la case **Activé**.
5. (Facultatif) Pour détecter automatiquement les paramètres proxy du serveur Serveur NetWitness, cochez la case.  
Les champs Hôte proxy et Port proxy sont remplis automatiquement.
6. Si vous souhaitez utiliser un proxy différent, saisissez l'**Hôte proxy** et le **Port proxy**.
7. Saisissez le nom d'utilisateur et le mot de passe utilisés pour vous connecter à l'hôte proxy.
8. (Facultatif) Sélectionnez **SSL**, si l'hôte proxy communique sur SSL.
9. Cliquez sur **Appliquer**.

Les paramètres sont sauvegardés et prennent effet immédiatement.

**Remarque :** Malware Analysis ne prend pas en charge l'authentification de proxy Web NTLM.

## (Facultatif) Enregistrez-vous pour recevoir une clé API ThreatGrid



Cette rubrique présente la procédure permettant d'obtenir une clé API ThreatGrid d'évaluation à utiliser dans le sandbox ThreatGrid Cloud. Avant d'activer ThreatGrid en tant que service sandbox dans le module Sandbox, une clé de service fournie par ThreatGrid doit être configurée afin que ThreatGrid puisse reconnaître que les échantillons soumis à partir de ce site sont légitimes.


Si vous ne disposez pas d'une clé de service fournie par ThreatGrid, vous pouvez obtenir une clé à l'aide de cet onglet. La clé est fournie à titre d'évaluation.

Lorsque vous saisissez vos informations utilisateur et cliquez sur **Enregistrer**, une clé s'affiche dans cet onglet et est automatiquement ajoutée à la configuration ThreatGrid sous l'onglet **Général**. Quelques minutes plus tard, vous recevrez un e-mail de ThreatGrid contenant un lien vers la page sur laquelle vous pourrez vous connecter. Après avoir accepté les termes de la licence sur la page ThreatGrid, vous pouvez envoyer les fichiers pour analyse. ThreatGrid reconnaîtra les fichiers envoyés par Malware Analysis en vue d'une analyse dans le sandbox.



**Pour obtenir une clé API ThreatGrid d'évaluation :**

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Sélectionnez un service Malware Analysis, puis sélectionnez   > **Vue > Config**.
3. Dans la vue **Configuration des services**, sélectionnez l'onglet **ThreatGrid**.
4. Saisissez votre nom complet, votre fonction, le nom de votre organisation et votre adresse e-mail.
5. Pour vous connecter à ThreatGrid, saisissez un ID utilisateur et un mot de passe dans le champ prévu à cet effet.
6. Cliquez sur **S'inscrire**.  
Votre enregistrement est envoyé à ThreatGrid et une clé API s'affiche sous le bouton Enregistrer. Cette clé est automatiquement reportée sous l'onglet **Général**.
7. Sélectionnez cet onglet pour confirmer que la configuration ThreatGRID inclut désormais la clé API.

☒ ThreatGRID (Local)	
Enabled	<input checked="" type="checkbox"/>
Service Key	
URL	https://panacea.threatgrid.com
Ignore Web Proxy Settings	<input type="checkbox"/>

8. Lorsque vous recevez un e-mail de ThreatGrid contenant un lien de connexion, cliquez sur le lien pour vous connecter et acceptez les termes du contrat.  
Votre évaluation de ThreatGrid débute alors. Malware Analysis peut envoyer cinq fichiers par jour au Cloud ThreatGrid en vue de leur analyse dans le sandbox.

## Procédures supplémentaires pour la configuration de Malware Analysis

Cette rubrique décrit les procédures d'un administrateur peut effectuer pour réaliser un objectif qui ne fait pas partie de la configuration de base de Malware Analysis. Une fois Malware Analysis configuré, les administrateurs peuvent affiner le service et le personnaliser davantage, par exemple en implémentant le contenu YARA personnalisé.

- [Créer une alerte personnalisée au format CEF](#)
- [Activer le contenu YARA personnalisé](#)

### Créer une alerte personnalisée au format CEF

Cette rubrique donne des instructions sur la création d'alertes personnalisées au format Common Event Format (CEF) pour envoyer à un service qui intègre des événements CEF. Il s'agit d'une tâche de configuration avancée qui nécessite des connaissances suffisantes pour modifier manuellement le fichier de configuration `/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`. Avant de modifier le fichier, vous devez arrêter le service Malware Analysis sur le système d'exploitation. L'alerte CEF s'active lorsque vous redémarrez le service Malware Analysis.

#### Modèle CEF

Pour envoyer des événements à un service d'acquisition d'événements tel que CEF, NetWitness Suite traite ces événements via un fichier de configuration qui sert de modèle CEF, avant de les soumettre à une technologie de corrélation. Vous pouvez modifier le fichier de configuration selon vos besoins. Celui-ci spécifie la séquence et le mappage des champs syslog dans chaque alerte.

L'exemple de message syslog suivant présente les champs CEF dans la section extensions de l'alerte (après le dernier '|' dans l'alerte). Chaque champ peut être configuré pour indiquer la séquence (décrite dans la section Exemple ci-dessous). Les champs peuvent être exclus entièrement à partir de l'alerte via un paramètre de configuration.

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0
nextgen=25.0 community=100.0 sandbox=25.0 file.name=myFile.exe
file.size=1234556 file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563
event.type=MANUAL_UPLOAD event.id=0 country.dst.code=--
country.dst=Unavailable ip.src=0:0:0:0:0:0:0:1
ip.dst=0:0:0:0:0:0:0:1 event.uid=f7a6155a-31de-4fa6-ba16-
41fb9a8e5f26 ...
```

## Comprendre une entrée de fichier d'audit Syslog

La description de la structure de fichiers se base sur l'exemple suivant.

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected
suspicious
network event ID 857 session ID 73|2|
static=100.0 network=29.0 community=8.0 sandbox=N/R
file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consumell extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2
referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/
risk.info=http client server version mismatch
```

### Première ligne

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

Informations sur le journal	Description
Feb 6 10:02:28	Horodatage de l'entrée.
10.10.10.125	Adresse IP source de l'événement.
SpectrumServer125	Nom d'hôte source de l'événement.

### En-tête CEF (Common Event Format) d'audit

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
network event ID 857 session ID 73|2|
```

L'en-tête d'audit CEF est une liste dont les valeurs sont séparées par des barres obliques dans les champs suivants :

Informations sur le journal	Description
0	Version ArcSight CEF (Common Event Format) utilisée pour le Syslog d'audit.
NetWitness	Service ayant créé le message Syslog.
Spectrum	Malware Analysis est l'enregistreur de l'événement.
1.2.1.130	Version Malware Analysis.
event ID 857	ID d'événement réseau unique pour cet événement.
session ID 73	ID de session unique Core pour la session qui a inclus cet événement.
2	<p>Gravité, le nombre entier compris entre 1 et 6 indique le niveau de gravité du message.</p> <ul style="list-style-type: none"> <li>• 1 = INFORMATION_LEVEL</li> <li>• 2 = WARNING_LEVEL</li> <li>• 3 = ERROR_LEVEL</li> <li>• 4 = SUCCESS_LEVEL</li> <li>• 5 = FAILURE_LEVEL</li> <li>• 6 = AUDIT_FAILURE_LEVEL</li> </ul>

### Extension CEF d'audit

```
static=100.0 network=29.0 community=8.0 sandbox=N/R
file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
```

```
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consumell extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server
version mismatch
```

### Scores d'analyse

La première entrée de l'extension CEF d'audit fournit les quatre scores Malware Analysis pour l'événement : Statique, Réseau, Communauté et Sandbox

Informations sur le journal	Valeur d'échantillon
static	100.0
network	29.0
community	8.0 Un score de 0.0 peut être un score communautaire pour l'événement ou peut indiquer qu'il n'y a pas de services communautaires activés.
sandbox	N/R N/R signifie « non exécuté ». Cela indique que le sandbox GFI n'a pas été activé.

### Informations sur le fichier

Les trois prochaines entrées fournissent des informations sur les fichiers : nom du fichier, taille et hachage.

Informations sur le journal	Valeur d'échantillon
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0

Informations sur le journal	Valeur d'échantillon
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

### Métadonnées d'événement récupérées par NextGen

L'enregistrement se poursuit avec les métadonnées Core de l'événement. Les métadonnées du message sont liées à l'événement. La quantité de données contenues dans le message est tronquée à la longueur maximale d'octets configurée dans les paramètres Syslog. La valeur par défaut est 1024.

Informations sur le journal	Valeur d'échantillon
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149
client	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Privé
temps	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
Action	get
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	rtf
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6

Informations sur le journal	Valeur d'échantillon
tcp.flags	27
ip.src	10.25.50.61
tcp.dstport	80
threat.category	spectrum
eth.dst	00:0C:29:F8:50:2D
durée de vie	0
alert.id	nw32535
sessionid	73
moyen	1
taille	117864
contenu	spectrum.consume11
extension	doc
directory	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
service	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
serveur	Apache/2.2.13 (Fedora)
streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	http client server version mismatch

## Modifier le fichier de configuration

1. Arrêtez le service Malware Analysis.
2. Modifiez le fichier de configuration comme indiqué dans l'exemple.
3. Démarrez le service Malware Analysis.

Le service Malware Analysis commence à traiter les alertes via le fichier de configuration, puis envoie les alertes CEF aux services désignés.

## Exemple

Vous pouvez utiliser le fichier de configuration pour définir les champs qui doivent figurer dans l'alerte résultante, le libellé associé à chaque champ et l'ordre d'apparition des champs de données. Le fichier de configuration est constitué d'un ou de plusieurs blocs XML `MalwareCefExtension`, comme indiqué dans l'exemple ci-dessous. L'ordre de ces blocs dans le fichier de configuration détermine l'ordre des champs de données dans l'alerte CEF.

Dans l'exemple ci-dessous, l'alerte CEF comprend deux champs de données, `ip.src` suivi par `ip.dst`. `customKey` sert à indiquer le libellé du champ de données dans l'alerte. Cela permet à l'utilisateur de choisir un libellé personnalisé afin de forcer le format d'alerte et mieux répondre aux attentes du consommateur d'alerte. En d'autres termes, le format peut être réglé pour empêcher toute modification ou suppression indésirable apportée à un parseur d'alerte existant. Enfin, le paramètre `isDisplay` détermine si le champ est inclus dans la sortie d'alerte. Cela permet à l'utilisateur de désactiver les champs de données sans avoir à supprimer physiquement le bloc `MalwareCefExtension` de la configuration.

```
<config>
  <malwareExtensionList>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>ip.src</customKey>
      <malwareKey>ip.src</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>ip.dst</customKey>
      <malwareKey>ip.dst</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
  </malwareExtensionList>
</config>
```



À la fin du fichier de configuration, vous disposez de trois paramètres supplémentaires pour régler le format d'alerte. Il s'agit des paramètres suivants :

Paramètre	Description
<code>includesUnknownMeta</code>	<p>Le paramètre <code>true</code> ou <code>false</code> indique si les éléments de données inconnus sont inclus dans l'alerte résultante. Les métadonnées de session NextGen peuvent éventuellement être incluses dans une alerte CEF.</p> <p>Dans la mesure où des métadonnées de session supplémentaires peuvent être introduites via la création de parsers NextGen, il est possible que des métadonnées non contenues dans la configuration par défaut soient présentes. Vous pouvez affecter la valeur <code>true</code> à <code>includesUnknownMeta</code> pour inclure les métadonnées inconnues dans l'alerte et leur attribuer un libellé basé sur le nom de la clé méta NextGen. Pour forcer une clé personnalisée d'une métadonnée inconnue, vous devez modifier ce fichier et ajouter un nouveau bloc <code>MalwareCefExtension</code> au dictionnaire.</p> <p>Pour omettre les métadonnées inconnues de l'alerte, affectez la valeur <code>false</code> à <code>includesUnknownMeta</code>.</p>
<code>displayNulls</code>	<p>Le paramètre <code>true</code> ou <code>false</code> indique si les valeurs null sont incluses dans l'alerte. Si <code>displayNulls</code> a la valeur <code>false</code>, les champs de valeur null sont omis, même si la propriété <code>MalwareCefExtension isDisplay</code> est activée. Ainsi, la mise en forme dynamique des alertes peut exclure les champs de valeur null.</p>
<code>valueIfNull</code>	<p>Le paramètre <code>true</code> ou <code>false</code> vous permet de spécifier un espace réservé sous forme de chaîne (<code>n/a</code> par défaut) utilisable en tant que valeur pour tous les champs null. Si <code>displayNulls</code> a la valeur <code>true</code>, les champs de valeur null sont inclus dans les alertes. Leur valeur est définie en fonction de la valeur spécifiée dans <code>valueIfNull</code>.</p>

Ce qui suit représente le fichier de configuration CEF par défaut. Le fichier de configuration par défaut inclut toutes les métadonnées de session NextGen par défaut.

```
<config>
  <malwareExtensionList>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>static</customKey>
      <malwareKey>static</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>nextgen</customKey>
      <malwareKey>nextgen</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>community</customKey>
      <malwareKey>community</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>sandbox</customKey>
      <malwareKey>sandbox</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>file.name</customKey>
      <malwareKey>file.name</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
      <customKey>file.size</customKey>
      <malwareKey>file.size</malwareKey>
      <isDisplay>true</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
  </malwareExtensionList>
</config>
```

```

<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>

```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>
<malwareKey>country.dst.code</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
<isDisplay>>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
<malwareKey>agency.dst</malwareKey>
```

```
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
<malwareKey>threat.category</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>lifetime</customKey>
```

```

<malwareKey>lifetime</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
<malwareKey>latdec.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>

```

```
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>size</customKey>
<malwareKey>size</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```



```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>
<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
<isDisplay>>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
<isDisplay>>false</isDisplay>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filename</customKey>
```

```

<malwareKey>filename</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
<malwareKey>streams</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>

```

```
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referrer</customKey>
<malwareKey>referrer</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>
<malwareKey>risk.warning</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>attachment</customKey>
<malwareKey>attachment</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrar</customKey>
<malwareKey>whois.registrar</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrant</customKey>
<malwareKey>whois.registrant</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.date.creation</customKey>
<malwareKey>whois.date.creation</malwareKey>
<isDisplay>>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.server</customKey>
<malwareKey>whois.server</malwareKey>
<isDisplay>>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
</malwareExtensionList>
<includesUnknownMeta>>false</includesUnknownMeta>
<displayNulls>>false</displayNulls>
<valueIfNull>n/a</valueIfNull>
</config>
```

## Activer le contenu YARA personnalisé

Cette rubrique fournit les instructions permettant d'activer un contenu YARA personnalisé sur l'hôte NetWitness Suite sur lequel le service Malware Analysis est installé. 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 les indicateurs de compromission YARA intégrés disponibles dans RSA Live. Ceux-ci sont automatiquement téléchargés et activés sur les appliances souscrites.

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'appliance les utilise. Cette section fournit des instructions destinées à l'administrateur qui configure les appliances pour activer la création d'un contenu YARA personnalisé.

### Conditions préalables

Il s'agit d'une tâche de configuration avancée, ce qui nécessite des privilèges et des connaissances suffisantes pour configurer un GNU Compiler Collection (GCC) et la C++ Python development library pour la création YARA. En outre, vous devez être familier avec la documentation YARA standard. Les composants suivants sont requis :

- Perl-Compatible Regular Expression (PCRE) library : [pcre-8.33.tar.bz2](#)
- Yara 1.7 (rev:167) - ligne de commande YARA autonome : [yara-1.7.tar](#)
- Extension YARA pour Python : [yara-python-1.7.tar.gz](#)
- Documentation sur les règles YARA : [YARA User's Manual 1.6.pdf](#)

Les composants sont disponibles au téléchargement ici : <https://code.google.com/p/yara-project/downloads/list>

**Remarque :** À compter de l'écriture, YARA 2.0 est disponible mais non pris en charge pour Malware Analysis 10.5.

## Installer les bibliothèques et les applications nécessaires à la création YARA sur une appliance basée CentOS

Comme condition préalable à la création YARA sur l'hôte qui exécute CentOS, vous devez installer `make`, GNU Compiler Collection et C++ Python Development Library sur l'appliance. Pour installer les applications et les bibliothèques nécessaires à la création YARA :

1. Pour vérifier que le référentiel YUM standard figure dans le dossier `/etc/yum.repos.d`, et pas d'autres fichiers de référentiel, saisissez la commande suivante :

```
ls -al /etc/yum.repos.d
```

Les résultats doivent ressembler à ceci :

```
-rw-r-r-. 1 root root 1926 Jun 26 2012 CentOS-Base.repo
-rw-r-r-. 1 root root 637 Jun 26 2012 CentOS-Debuginfo.repo
-rw-r-r-. 1 root root 626 Jun 26 2012 CentOS-Media.repo
-rw-r-r-. 1 root root 2593 Jun 26 2012 CentOS-Vault.repo
```

2. Pour installer `make` sur l'appliance, saisissez les commandes suivantes :

- a. `yum search make`

Le message suivant a été retourné : `make.x86_64` : A GNU tool which simplifies the build process for user

- b. `yum install make.x86_64`

3. Pour installer et tester le GCC sur l'hôte, saisissez les commandes suivantes :

- a. `yum search gcc`

Les messages suivants s'affichent :

```
gcc-c++.x86_64 : C+ support for GCC
gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)
```

- b. Saisissez les commandes suivantes :

```
yum install gcc.x86_64
yum install gcc-c++.x86_64
```

- c. Pour tester la commande `gcc`, saisissez les commandes suivantes :

```
gcc -v
cc -v
```

4. Pour installer C++ Python development library sur l'appliance, saisissez les commandes suivantes :

- a. `yum search python dev`

Le message suivant a été retourné :

```
python-devel.x86_64 : The libraries and header files needed for
```

```
Python development
```

```
b. yum install python-devel.x86_64
```

## Configurer Yara

Pour créer un développement GCC et C++ Python Development Library dans lequel vous pouvez créer YARA sur l'hôte NetWitness Suite qui exécute Malware Analysis :

1. Exécutez l'une des opérations suivantes :
  - a. Si l'hôte sur lequel vous effectuez l'installation exécute Mac OS, installez xCode pour Mac OS.
  - b. Si l'hôte sur lequel vous effectuez l'installation exécute CentOS, installez make, GCC et C++ Python Development Library à l'aide de la ligne de commande YUM.

2. Pour installer la bibliothèque PCRE sur l'hôte, ouvrez une fenêtre de terminal et saisissez les commandes suivantes :

```
tar -xvf pcre-8.33.tar.bz2
cd pcre-8.33
./configure
make
sudo make install
```

3. Pour installer la ligne de commande YARA autonome, saisissez les commandes suivantes :

```
tar -xvf yara-1.7.tar
cd yara-1.7
./configure
make
sudo make install
```

4. Pour tester la ligne de commande YARA autonome :

- a. Saisissez la commande suivante :

```
yara
```

- b. Si la commande aboutit, passez à l'étape 7. Si la commande échoue et renvoie l'erreur `yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory`, saisissez la commande suivante pour vérifier le fichier `/etc/ld.so.conf` ou la variable d'environnement `LD_LIBRARY_PATH`.

```
ldconfig -v
```

5. Pour installer l'extension YARA pour Python, saisissez les commandes suivantes :

```
tar -xvf yara-python-1.7.tar.gz
```



```
cd yara-python-1.7
python setup.py build
sudo python setup.py install
```

6. Pour tester l'extension YARA :

a. Saisissez la commande suivante : **python**

b. À l'invite de commande Python (>>>), saisissez les commandes suivantes :

```
import yara
exit()
```

Lorsque cette configuration est terminée, les analystes peuvent créer des indicateurs de compromission YARA personnalisés pour l'utilisation sur un hôte Malware Analysis, comme décrit dans « Implémenter du contenu YARA personnalisé » dans le *Guide Investigation et Malware Analysis*

## Références de Malware Analysis

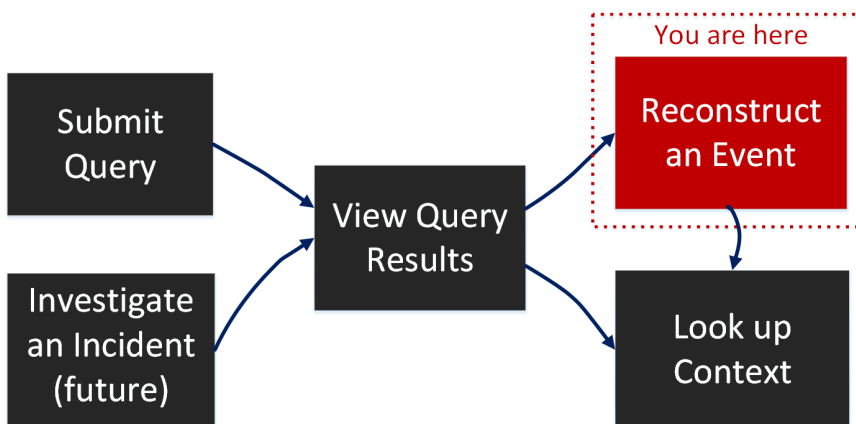
---

- [Vue Configuration des services - Onglet Audit](#)
- [Vue Configuration des services - onglet AV](#)
- [Vue Configuration des services - onglet Général](#)
- [Vue Configuration des services - Onglet Hachage](#)
- [Vue Configuration des services - onglet Indicateurs de compromission](#)
- [Vue Configuration des services - onglet Intégration](#)
- [Vue Configuration des services - onglet Récapitulatif des indicateurs de compromission des services](#)
- [Vue Configuration des services - onglet Proxy](#)
- [Vue Configuration des services - onglet ThreatGRID](#)

## Vue Configuration des services - Onglet Audit

Dans la Vue Événements et le panneau Nouveaux Vue Événements - Reconstruction (**Enquêter > panneau Événements > cliquez sur un événement**), vous pouvez afficher en toute sécurité une reconstruction d'un événement intéressant qui se trouve dans la vue Naviguer ou le panneau Événements.

### Workflow



### Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Responsable de la recherche des menaces	envoyer une requête	<a href="#">Mener une procédure d'enquête</a>
Responsable de la recherche des menaces	afficher les résultats de la requête	<a href="#">Analyser les événements dans la vue Analyse d'événements</a>
<b>Responsable de la recherche des menaces</b>	<b>reconstruire un événement*</b>	<a href="#">Reconstruire un événement</a>
Responsable de la recherche des menaces	exporter des fichiers à partir d'un événement	<a href="#">Reconstruire un événement</a>
Responsable de la recherche des menaces	Rechercher un contexte supplémentaire sur un événement	Recherche d'informations contextuelles

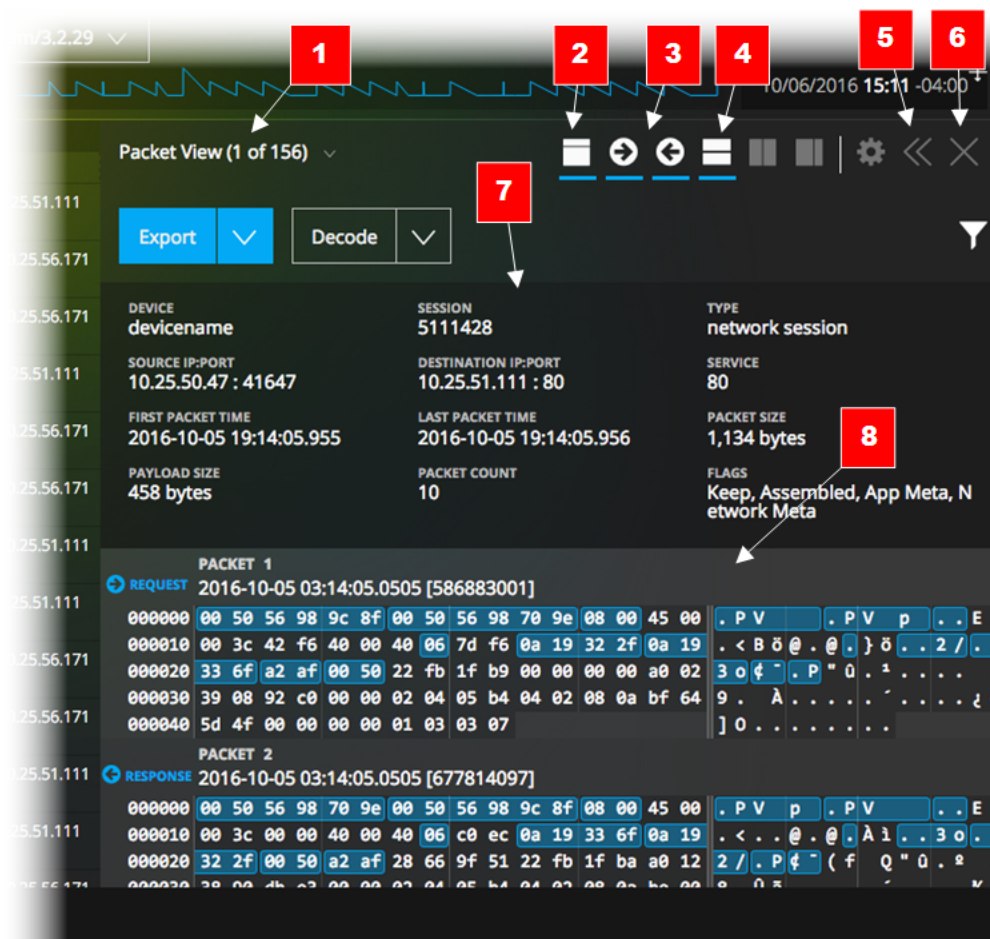
### Rubriques connexes

- [Fonctionnement de NetWitness Investigate](#)
- [Mener une procédure d'enquête](#)
- [Analyser les événements dans la vue Analyse d'événements](#)
- [Vue Naviguer](#)
- [Vue Analyse d'événements - Panneau Analyse de texte](#)

## Aperçu rapide

Le panneau Reconstruction d'Enquêteur affiche une reconstruction d'un seul événement dans Vue Paquet, Vue Fichiers et Vue Texte. Lorsque vous cliquez sur un événement dans le panneau Événements, le panneau Reconstruction adjacent présente la reconstruction de paquets de l'événement. Vous pouvez utiliser les options dans la barre d'outils Reconstruction d'événement pour modifier le type de reconstruction et l'orientation (demande ou réponse), pour masquer ou afficher le panneau d'en-tête et pour développer, réduire et fermer le panneau Reconstruction d'événement. Selon le type de reconstruction sélectionné et le contenu de la charge utile, des options supplémentaires sont disponibles. Vous pouvez, par exemple, afficher la charge utile uniquement dans la vue Texte, télécharger les fichiers dans la vue Fichiers et télécharger les fichiers PCAP dans la vue Paquet.

Vous trouverez ci-dessous un exemple d'une reconstruction de paquets.



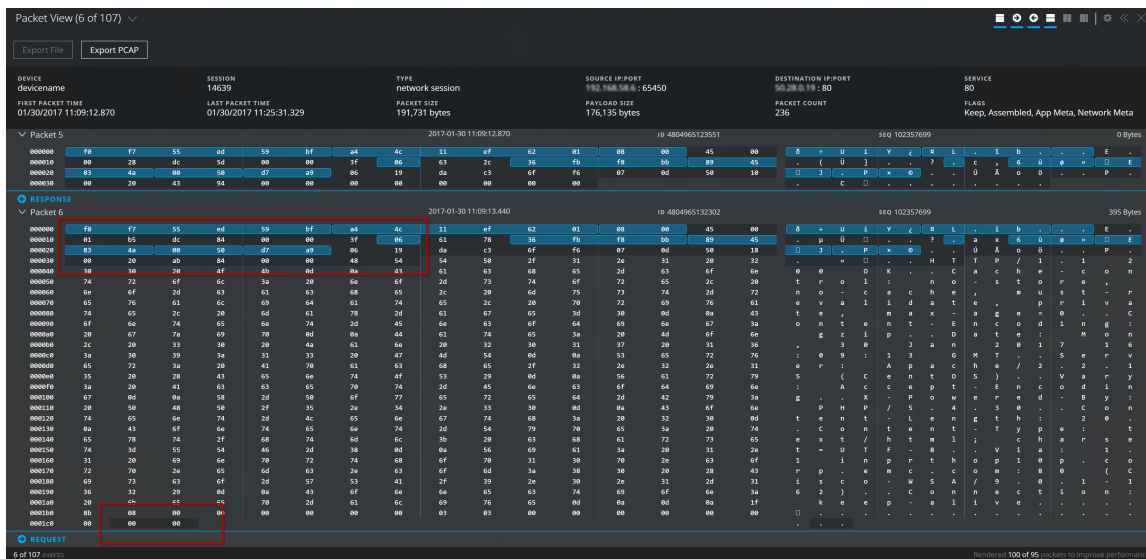
- 1 Onglets ou menu déroulant permettant de sélectionner le type de reconstruction : vue des paquets, du fichier ou du texte. Le type sélectionné s’affiche dans le libellé.
- 2 Cliquez sur cet élément pour masquer ou afficher le panneau de l’en-tête.
- 3 Cliquez sur ces icônes pour afficher la demande, la réponse ou les deux.
- 4 Cliquez sur cette icône pour afficher ou masquer le panneau Méta de l’événement, qui fournit une liste détaillée des métadonnées associées à l’événement.
- 5 Option permettant de développer ou de réduire le panneau Reconstruction horizontalement dans la vue Naviguer.
- 6 Option permettant de fermer le panneau Reconstruction.
- 7 L’en-tête affiche des informations récapitulatives sur l’événement en cours de reconstruction.
- 8 Répertorie chaque paquet de l’événement. Pour chaque paquet, vous pouvez voir le numéro, l’orientation (demande ou réponse) et le contenu du paquet dans un format binaire

sur la gauche, dans un format hexadécimal au milieu et dans un format texte sur la droite.

## Détails de la reconstruction de paquets

Dans la reconstruction de paquets, la vue Enquêteur indique le nombre de paquets, l'orientation du paquet (demande ou réponse), l'heure de début du paquet et son contenu.

Tous les paquets commencent par un en-tête, et certains ont un pied de page. Dans la vue Paquet, l'en-tête et le pied de page affichent un arrière-plan plus sombre qui vous permet de les distinguer de la charge utile du paquet. L'arrière-plan plus sombre de l'en-tête et du pied de page s'affiche au format hexadécimal et texte.



Le contenu du paquet est fourni au format hexadécimal et au format texte. Les métadonnées sont mises en surbrillance en bleu ; lorsque vous passez le pointeur de la souris sur les métadonnées, les informations relatives aux clés méta/métavaleurs s'affichent sous la forme d'une infobulle.

Des options supplémentaires dans la vue Paquet incluent la possibilité de télécharger le fichier PCAP de l'événement et d'afficher uniquement les charges utiles. Lorsque seule la charge utile est affichée, vous pouvez utiliser l'option Octets d'ombrage pour mieux différencier les schémas dans les données.

## Détails de la reconstruction de texte

Dans la reconstruction de texte, les événements de réseau et de log sont présentés différemment. Pour les événements de réseau, Enquêteur affiche l'orientation du paquet (demande ou réponse) et le contenu de chaque paquet au format texte.

Pour les événements de log (filtre sur Moyen = Log), il n'existe aucune demande ou réponse ; seul le log brut s'affiche dans la reconstruction de texte.

Un sous-ensemble des options de reconstruction est disponible dans la vue Texte. Vous pouvez :

- Masquer et afficher l'en-tête.
- Pour les événements de réseau, sélectionner l'affichage des demandes uniquement, des réponses uniquement, ou les deux.
- Pour les événements de réseau, exporter la session en tant que fichier PCAP.
- Pour les événements de log, exporter le log brut.
- Basculer entre une vue compressée et une vue décompressée des charges utiles. Lorsque la session est décompressée, les parties compressées du texte deviennent lisibles.
- Sélectionner le texte pour le décodage et l'encodage.

**Remarque :** cette fonction n'est pas disponible pour la vue Fichiers, pour les sessions réseau non http et pour les données de log.

## Détails de la reconstruction de fichier

Dans la reconstruction de fichier, Enquêteur contient une liste de fichiers associés à l'événement de réseau sélectionné.

The screenshot shows the RSA Malware Analysis interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The main area is titled 'QUERY EVENTS' and shows results for 'Concentrator67' on '04/17/1997 06:21:00 pm - 04/17/2017 06:21:59 pm' with 'service = 80'. A table of events is displayed on the left, with one event selected. The right pane shows 'File View' details for the selected event, including a 'Download File' button and a table of associated files.

TIME	EVENT TYPE	SIZE
10/15/2008 11...	Network	35 KB
10/15/2008 11...	Network	5 KB
10/15/2008 11...	Network	1 KB
10/15/2008 11...	Network	5 KB
10/15/2008 11...	Network	4 KB
10/15/2008 11...	Network	5 KB
10/15/2008 11...	Network	4 KB
10/15/2008 11...	Network	4 KB
10/15/2008 11...	Network	7 KB
10/15/2008 11...	Network	6 KB
10/15/2008 11...	Network	2 KB

DEVICE	SESSION	MEDIUM	TYPE	SOURCE IP:PORT	DESTINATION IP:PORT
Concentrator67	32	1	Network	172.20.0.35 : 50306	67.192.232.82 : 80

SERVICE	FIRST PACKET TIME	LAST PACKET TIME	PACKET SIZE	PAYLOAD SIZE	PACKET COUNT
80	10/15/2008 03:46:51.906 pm	10/15/2008 03:46:55.875 pm	4,911 bytes	4,133 bytes	14

FILE NAME	MIME TYPE	FILE SIZE	HASHES
<input checked="" type="checkbox"/> 32-107-0_1_e96d78a3-7450-4bb6-b087-5b4855d687a1.aspx	application/octet-stream	3.1 KB	SHA1: 3b7a3d96d36fd1b626a7ec32f8cbe MDS: 28063e8d5e9a80e6b74d0cfa987c

Vous pouvez sélectionner un seul fichier, un ou plusieurs fichiers, ou la totalité d'entre eux à exporter vers votre système de fichiers local. Lorsque des fichiers sont sélectionnés, le bouton Exporter des fichiers devient actif et reflète le nombre de fichiers sélectionnés. En cliquant sur ce bouton, les fichiers sélectionnés sont exportés en tant qu'archive zip, ce qui garantit que les fichiers potentiellement malveillants ne seront pas ouverts par l'application par défaut et exécutés. L'archive exportée est nommée à l'aide de la convention suivante :

```
<service-ID or host name>_SID<nnnnnnnn>_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<nnnnnnnn> est le numéro d'ID de la session
- FC<nnnnnnnn> est le nombre de fichiers contenus dans l'archive







Pour empêcher une archive d'être décompressée automatiquement lors de son téléchargement, NetWitness Suite exporte l'archive sous la protection d'un mot de passe. Pour ouvrir une archive, saisissez le mot de passe suivant : **netwitness**.

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

## Description détaillée

Fonction	Description
Menu du type de reconstruction	Dans ce menu, vous pouvez sélectionner le type de reconstruction : <b>Paquet</b> ou <b>Fichier</b> . Lorsque vous ouvrez une reconstruction pour la première fois, NetWitness Suite choisit la meilleure reconstruction par défaut.
Options de téléchargement	Options permettant d'exporter un log, un fichier PCAP ou des fichiers en vue d'une analyse plus approfondie et d'un partage avec d'autres utilisateurs.



Fonction	Description
	<p>Contrôle l’affichage d’un en-tête au-dessus de la liste des paquets ; vous pouvez cliquer sur cette icône pour afficher ou masquer l’en-tête. 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.</p> <p>L’en-tête fournit des informations sur l’événement reconstruit : nom du service qui a collecté le paquet, numéro de session ou d’événement, type d’événement (réseau), IP source : port, IP cible : port, type de service, heure du premier paquet dans l’événement, heure du dernier paquet dans l’événement, taille de l’événement, taille de la charge utile en octets, nombre de paquets et indicateurs appliqués à l’événement (conservation, assemblage, méta d’application, méta réseau).</p>
	<p>Deux commandes permettent d’afficher ou de masquer la demande et la réponse (voir <a href="#">Reconstruire un événement</a>).</p>
	<p>Affiche les détails méta de l’événement dans un autre panneau.</p>
	<p>(À venir) Menu Paramètres.</p>
	<p>Commandes de redimensionnement pour le panneau Reconstruction (voir <a href="#">Reconstruire un événement</a>).</p>
	<p>Ferme le panneau Reconstruction. La vue affiche désormais uniquement le panneau Événements.</p>

## Vue Configuration des services - onglet AV

Cette rubrique présente les fonctionnalités et fonctions de l'onglet Antivirus disponible dans la vue Configuration des services pour un service Malware Analysis. L'onglet Antivirus permet d'identifier les fournisseurs de logiciels antivirus dont les logiciels sont en cours d'utilisation sur votre réseau. NetWitness Suite peut inclure les résultats issus de ces fournisseurs dans la vue Résultats détaillés d'un événement qui a été analysé à l'aide de Malware Analysis.

Il s'agit d'un exemple de l'onglet Antivirus.

## Fonctions

L'onglet antivirus répertorie les fournisseurs d'antivirus dont les logiciels peuvent être installés sur votre réseau. Il existe deux catégories de fournisseurs : Principal, qui est le plus fiable, et Secondaire, qui est le moins connu. Une case à cocher et une icône sont placées en regard de chaque fournisseur. Un nom de fournisseur coché indique que vous avez installé le logiciel antivirus sélectionné de ce fournisseur dans votre environnement.

Ce tableau décrit les options de l'onglet Antivirus.

Fonction	Description
Case à cocher Fournisseur	Choisissez un ou plusieurs fournisseurs d'antivirus dans la liste fournie pour indiquer les produits qui ont été installés dans l'organisation locale.
Appliquer	Enregistre les modifications effectuées sous l'onglet Antivirus.
Réinitialiser	Restaure l'état initial de la liste Antivirus sans aucune sélection de fournisseurs.

## Vue Configuration des services - onglet Général

Cette rubrique présente les paramètres de configuration disponibles dans la vue Configuration des services > onglet Général pour Malware Analysis, qui contient des paramètres propres au service Malware Analysis. Dans cet onglet, vous configurez :

- Les paramètres de traitement pour les services Core qui capturent des données.
- Le référentiel pour les données capturées.
- Les catégories de notation statique, communauté et Sandbox utilisées pour analyser des données.

La tâche suivante fournit des procédures détaillées : [Configurer les paramètres généraux de Malware Analysis](#).

Il s'agit d'un exemple de l'onglet Général.

Cet onglet présente quatre sections : Configuration de l'analyse continue, Configuration du référentiel, Divers et Configuration des modules.

### Section Configuration de l'analyse continue

Ce tableau décrit les fonctions de la section Configuration de l'analyse continue.

Paramètre	Description
Activé	Permet d'activer ou de désactiver complètement le rappel continu du service Core. Par défaut, cette option n'est pas sélectionnée ( <b>désactivée</b> ).

Paramètre	Description
<b>Requête</b>	<p>Pendant son analyse du trafic réseau, Decoder crée un contenu appelé de champ de métadonnées avec une valeur de <b>spectrum.consume</b> dans des sessions qui sont supposées contenir un programme malveillant. Par défaut, Malware Analysis ne réalise des analyses que sur les événements qui ont cette métavaleur spécifique. En modifiant cette requête, Malware Analysis peut être configuré pour analyser différents types d'événements.</p> <p>Le fait de trop élargir cette requête peut forcer Malware Analysis à analyser trop d'événements, ce qui entraîne du retard ou une performance médiocre.</p> <p>La requête par défaut est <b>select * where content='spectrum.consume'</b></p>
<b>Expiration de la requête</b>	<p>Lorsque le Malware Analysis recherche les métadonnées sur le service Core, il obtient un résultat en quelques secondes. S'il y a un problème, de connectivité réseau par exemple, Malware Analysis abandonne la requête après cette période configurée.</p> <p>La valeur par défaut est de <b>3 600 secondes</b>.</p>
<b>Intervalle de requête</b>	<p>Fréquence, en minutes, d'interrogation pour les nouveaux fichiers et les nouvelles métadonnées de sessions.</p>
<b>Limite des métavaleurs</b>	<p>Chaque fois que le service Malware Analysis interroge le service Core, il extrait un volume de métadonnées, jusqu'à cette limite de métadonnées. En utilisant ce paramètre, conjointement avec l'intervalle de requête, vous pouvez régler la performance de Malware Analysis dans l'infrastructure Core.</p> <p>La valeur par défaut est <b>25 000</b>.</p>

Paramètre	Description
<b>Limite temporelle</b>	<p>Malware Analysis analyse des sessions qui se sont produites après la Limite temporelle. Ce paramètre est spécialement important lors de l'installation d'une nouvelle appliance Malware Analysis, car il détermine à quel moment dans le passé débiter l'analyse. Un réglage horaire trop éloigné dans le passé de la limite peut entraîner une analyse par Malware Analysis d'un trop grand nombre d'événements passés, causant un important retard avant que vous ne voyiez un trafic se produisant en temps réel.</p> <p>La valeur par défaut est de <b>24 heures</b>.</p>
<b>Hôte source</b>	<p>Nom d'hôte de l'appliance Malware Analysis.</p> <p>Il s'agit de l'adresse IP, ou du nom d'hôte, du service que Malware Analysis interroge pour récupérer ses données pour analyse. N'utilisez pas localhost comme hôte source.</p> <p>Selon le modèle de l'appliance et la configuration de l'infrastructure NetWitness Suite, cet hôte source peut varier.</p>
<b>Port source</b>	<p>Malware Analysis communique avec l'infrastructure NetWitness Suite en utilisant le service REST à l'écoute sur ce port. Ce numéro de port est spécifique au type du service Core qui est utilisé comme hôte source. Cela correspond aux connexions sortantes pour votre service Core.</p>
<b>Nom d'utilisateur</b>	<p>Nom d'utilisateur. La valeur par défaut est <b>admin</b>.</p> <p>Malware Analysis doit s'authentifier sur l'hôte source chaque fois qu'il cherche des données. Dans la plupart des cas, le compte utilisé par Malware Analysis est le même que celui utilisé pour accéder au service Core via NetWitness Suite. Toutefois, il est recommandé de créer un nouveau compte sur le service Core dédié à Malware Analysis.</p>
<b>Mot de passe d'utilisateur</b>	<p>Mot de passe d'utilisateur. La valeur par défaut est <b>netwitness</b>.</p>

Paramètre	Description
SSL	<p>Utilisez SSL lors de la communication avec Core. Si Malware Analysis utilise une connexion SSL pour communiquer avec un service Core, cochez cette option.</p> <p>Par défaut, l'option est désactivée.</p>
<b>Prévention du déni de service (DOS - Denial of Service)</b>	<p>La Prévention du déni de service (DOS - Denial of Service) fournit des protections contre les programmes malveillants qui génèrent intentionnellement des volumes élevés de connexions réseau entre deux points de terminaison incluant du contenu Windows PE. La génération d'un volume élevé de connexions gonfle artificiellement le volume de trafic que les services de sécurité surveillant le réseau doivent consommer et analyser, ce qui entraîne un déni de service. Cette fonctionnalité contribue à l'identification de ces sessions afin que le traitement d'analyse les ignore.</p> <p>Par défaut, l'option est désactivée.</p>

Paramètre	Description
<p><b>Longueur de la fenêtre des taux de session DOS (secondes)</b></p>	<p>Malware Analysis utilise ce paramètre avec les paramètres <b>Nombre de sessions DOS par fenêtre de taux</b> et <b>Heure de blocage de la session DOS (secondes)</b> pour identifier une attaque par déni de service et déterminer pendant combien de temps ignorer les sessions issues d'une seule adresse IP.</p> <p>Pour identifier une attaque par déni de service, Malware Analysis surveille le nombre de sessions établies par une seule adresse IP au cours d'une période spécifique. Le <b>Longueur de la fenêtre des taux de session DOS (secondes)</b> définit cette période. Si le nombre de sessions dépasse le paramètre <b>Nombre de sessions DOS par fenêtre de taux</b> dans le nombre de secondes défini dans <b>Longueur de la fenêtre des taux de session DOS</b>, Malware Analysis identifie l'activité comme une tentative de déni de service. Dans ce cas, le trafic provenant de l'adresse IP est ignoré pour la période indiquée dans <b>Temps de verrouillage de session DOS (secondes)</b>.</p> <p>La valeur par défaut est <b>60</b> secondes.</p>

Paramètre	Description
<b>Nombre de sessions DOS par fenêtre de taux</b>	<p>Malware Analysis utilise ce paramètre avec les paramètres <b>Longueur de la fenêtre des taux de session DOS (secondes)</b> et <b>Temps de verrouillage de session DOS (secondes)</b> pour identifier une attaque par déni de service et déterminer pendant combien de temps ignorer les sessions issues d'une adresse IP.</p> <p>Pour identifier une attaque par déni de service, Malware Analysis surveille le nombre de sessions établies par une seule source IP au cours d'une période spécifique. Le <b>Longueur de la fenêtre des taux de session DOS (secondes)</b> définit cette période. Si le nombre de sessions dépasse le paramètre <b>Nombre de sessions DOS par fenêtre de taux</b> dans le nombre de secondes défini dans <b>Longueur de la fenêtre des taux de session DOS</b>, Malware Analysis identifie l'activité comme une tentative de déni de service. Dans ce cas, le trafic est ignoré pour la période indiquée dans <b>Temps de verrouillage de session DOS (secondes)</b>.</p> <p>La valeur par défaut est <b>200</b> sessions.</p>



Paramètre	Description
<p><b>Heure de blocage de la session DOS (secondes)</b></p>	<p>Malware Analysis utilise ce paramètre avec les paramètres <b>Longueur de la fenêtre des taux de session DOS (secondes)</b> et <b>Nombre de sessions DOS par fenêtre de taux</b> pour identifier une attaque par déni de service et déterminer pendant combien de temps ignorer une telle attaque.</p> <p>Pour identifier une attaque par déni de service, Malware Analysis surveille le nombre de sessions établies par une seule adresse IP au cours d'une période spécifique. Le <b>Longueur de la fenêtre des taux de session DOS (secondes)</b> définit cette période. Si le nombre de sessions dépasse le paramètre <b>Nombre de sessions DOS par fenêtre de taux</b> dans le nombre de secondes défini dans <b>Longueur de la fenêtre des taux de session DOS</b>, Malware Analysis identifie l'activité comme une tentative de déni de service. Dans ce cas, le trafic est ignoré pour la période indiquée dans <b>Temps de verrouillage de session DOS (secondes)</b>.</p> <p>La valeur par défaut est <b>60</b> secondes.</p>
<p><b>Intervalle de Garbage Collection DOS (secondes)</b></p>	<p>Effectue une opération de récupération d'espace sur la structure de mémoire interne utilisée pour suivre les tentatives de déni de service.</p> <p>Si l'utilisation de la mémoire est anormalement élevée, vous pouvez diminuer ce paramètre pour libérer de la mémoire non utilisée plus souvent. Si l'utilisation de l'UC est anormalement élevée, vous pouvez accroître la valeur de ce paramètre pour éliminer le temps système de traitement (aux dépens de l'utilisation de la mémoire).</p> <p>La valeur par défaut est de <b>120</b> secondes.</p>

## Section Configuration du référentiel

Malware Analysis stocke tous les fichiers qui sont analysés pour une utilisation future. Ces fichiers peuvent être téléchargés via l'interface utilisateur ou ouverts via un des protocoles de partage de fichiers.

Ce tableau décrit les fonctions de la section Configuration du référentiel.

Paramètre	Description
<b>Directory Path</b>	Tous les fichiers sont stockés dans le répertoire suivant sur l'apppliance Malware Analysis : <b><code>/var/lib/netwitness/spectrum</code></b>
<b>Protocole de partage de fichiers</b>	Des valeurs possibles pour le protocole de partage de fichiers sont les suivantes : FTP, SAMBA et Aucun. Vous pouvez activer l'accès au FTP et le partage des fichiers SAMBA pour permettre à un utilisateur d'accéder aux fichiers stockés sur l'apppliance Malware Analysis à partir d'un site distant. Aucune information d'identification n'est requise pour accéder à ces fichiers. Le port requis pour l'accès FTP est TCP/21. Le protocole de partage de fichiers par défaut est <b>Aucun</b> .
<b>Conservation (en jours)</b>	Malware Analysis conserve des fichiers stockés dans le référentiel pendant un nombre de jours spécifié. Vous pouvez définir le nombre de jours de conservation des fichiers avant leur suppression. La valeur par défaut est <b>60</b> jours.

## Section Configuration diverse (10.3 SP2 et versions supérieures)

Ce tableau décrit les fonctions de la section Configuration diverse.

Paramètre	Description
<b>Taille de fichier maximale</b>	Limite la taille de chaque fichier que vous pouvez analyser manuellement. Ce paramètre s'applique à la fonction décrite dans « Télécharger des fichiers pour l'analyse de malware » dans le Guide sur Investigation et Malware Analysis. La valeur par défaut est <b>64 Mo</b> .  Si la limite de la taille de fichier est dépassée, vous empêche d'analyser le fichier.

## Section Configuration des modules

La section Configuration des modules permet la configuration des catégories de notation statique, communauté et Sandbox.

### Configuration de l'analyse statique

Le module statique est la seule catégorie de notation qui soit activé par défaut. Ce tableau décrit les paramètres de configuration de l'analyse statique.

Fonction	Description
<b>Activé</b>	Désactiver ou activer complètement l'analyse statique. Par défaut, cette option est sélectionnée ( <b>activée</b> ).
<b>Ignorer les fichiers PDF</b>	Désactive l'analyse des documents PDF. Par défaut, cette option n'est pas sélectionnée, tous les fichiers PDF sont soumis à une analyse statique.
<b>Ignorer les fichiers Office</b>	Désactive l'analyse des documents Office. Par défaut, cette option n'est pas sélectionnée, tous les fichiers Microsoft Office sont soumis à une analyse statique.
<b>Ignorer les fichiers exécutables</b>	Désactive l'analyse des documents Windows PE. Par défaut, cette option n'est pas sélectionnée, tous les fichiers Windows PE sont soumis à une analyse statique.

Fonction	Description
<b>Valider les paramètres d'authentification de Windows PE via le Cloud</b>	<p>Spécifiez si des fichiers Windows PE sont envoyés, ou non, au Cloud RSA-NetWitness pour validation Authenticode. La valeur par défaut est sélectionnée.</p> <ul style="list-style-type: none"> <li>Lorsqu'elle est sélectionnée, tout fichier Windows PE qui est signé numériquement est transmis sur le réseau (intégralement) au Cloud RSA-NetWitness pour validation. Si l'intention n'est pas d'empêcher les fichiers Windows PE de quitter le réseau client, vous devez désactiver cette option.</li> <li>Lorsqu'elle n'est pas sélectionnée, TOUTES les analyses statiques sont effectuées localement (en ignorant la validation Authenticode). En dépit de ce paramètre, les documents PDF et Microsoft Office ne sont pas soumis à la validation Authenticode et ne sont pas transmis sur le réseau pendant l'analyse statique.</li> </ul>

### Configuration de l'analyse de la communauté

Par défaut, le module de la communauté est désactivé et les options sont sélectionnées pour empêcher le traitement des fichiers PDF et Microsoft Office. L'objectif est de régler par défaut les paramètres sur les choix les plus restrictifs afin qu'aucun document sensible ne quitte le réseau, sauf si l'utilisateur en fait le choix. Ce tableau décrit les paramètres de configuration de l'analyse de la communauté.

Fonction	Description
<b>Activé</b>	Désactiver ou activer complètement l'analyse statique. Par défaut, cette option n'est pas sélectionnée ( <b>désactivée</b> ).
<b>Ignorer les fichiers PDF</b>	Désactive l'analyse des documents PDF. Par défaut, cette option est sélectionnée et les fichiers PDF ne sont pas traités.
<b>Ignorer les fichiers Office</b>	Désactive l'analyse des documents Office. Par défaut, cette option est sélectionnée et les fichiers Microsoft Office ne sont pas traités.
<b>Ignorer les fichiers exécutables</b>	Désactive l'analyse des documents Windows PE. Par défaut, cette option est sélectionnée et les documents Windows PE ne sont pas traités.

## Configuration de l'analyse Sandbox

Par défaut, le module Sandbox est désactivé et les fichiers Microsoft Office et PDF ne sont pas traités. L'objectif est de définir les paramètres les plus restrictifs possibles pour forcer l'utilisateur à spécifier si les données potentiellement sensibles peuvent être envoyées ou non hors du réseau à des fins de traitement. Si le traitement du type de document n'est pas empêché, le fichier est envoyé au serveur Sandbox de destination dans son intégralité (non limité à un hachage du contenu des fichiers).

Ce tableau décrit les paramètres de configuration de l'analyse Sandbox.

Fonction	Description
<b>Activé</b>	Désactiver ou activer complètement l'analyse Sandbox. Par défaut, cette option n'est pas sélectionnée ( <b>désactivée</b> ).
<b>Ignorer les fichiers PDF</b>	Désactive l'analyse des documents PDF. Par défaut, cette option est sélectionnée et les fichiers PDF ne sont pas traités. Lorsqu'elle n'est pas sélectionnée, tous les fichiers PDF sont soumis intégralement au Sandbox pour analyse.
<b>Ignorer les fichiers Office</b>	Désactive l'analyse des documents Office. Par défaut, cette option est sélectionnée et les fichiers Microsoft Office ne sont pas traités. Lorsqu'elle n'est pas sélectionnée, tous les fichiers Microsoft Office sont soumis intégralement au Sandbox pour analyse.
<b>Ignorer les fichiers exécutables</b>	Désactive l'analyse des documents Windows PE. Par défaut, cette option est sélectionnée et les documents Windows PE ne sont pas traités. Lorsqu'elle n'est pas sélectionnée, tous les documents Windows PE sont soumis intégralement au Sandbox pour analyse.
<b>Conserver le nom de fichier d'origine lors de l'exécution de l'analyse Sandbox</b>	Dans 10.3 SP2 et versions supérieures, activez la capacité de hachage pour les noms de fichiers lorsqu'ils sont envoyés à un Sandbox local. Par défaut, cette option n'est pas sélectionnée. <b>Remarque :</b> si vous ne sélectionnez pas ce paramètre, NetWitness Suite hache les fichiers.

## Paramètres de GFI Sandbox

Dans la section GFI Sandbox, vous pouvez activer le traitement sandbox par GFI et configurer le GFI Sandbox installé localement. Le tableau décrit les paramètres de configuration du GFI Sandbox.

Fonction	Description
<b>Activé</b>	Lorsqu'elle est activée, le traitement Sandbox est réalisé par une copie locale de GFI. La valeur par défaut est <b>désactivé</b> . Si vous activez GFI, vous devez configurer les paramètres restants.
<b>Nom du serveur</b>	Le nom de serveur GFI Sandbox. Aucune valeur par défaut
<b>Port de serveur</b>	Le port de serveur GFI Sandbox. La valeur par défaut est <b>80</b> .
<b>Période maximale d'interrogation</b>	Détermine le délai d'attente d'un échantillon soumis pour terminer le traitement. La valeur par défaut est <b>600 secondes</b> .
<b>Ignorer les paramètres proxy Web</b>	Indique à Malware Analysis d'ignorer le proxy Web, si celui-ci est configuré, lors de l'établissement de la connexion. Si aucun Proxy Web n'a été configuré dans Malware Analysis, le paramètre est ignoré.

## Paramètres de ThreatGrid Sandbox

Dans la section Sandbox ThreatGrid, vous pouvez activer le traitement Sandbox par ThreatGrid et choisir si vous voulez utiliser le ThreatGrid installé localement ou le ThreatGrid Cloud pour analyse Sandbox.

- Si vous avez une copie locale de ThreatGrid, configurez le traitement Sandbox pour utiliser la copie locale.
- Si aucune instance locale de ThreatGrid n'a été achetée et installée, configurez le ThreatGrid Cloud.

Le tableau décrit les paramètres de configuration de ThreatGrid Sandbox.

**Remarque :** avant d'activer ce service, vous devez configurer une clé de service fournie par ThreatGrid. La clé de service permet à ThreatGrid de reconnaître que les échantillons envoyés par ce site sont légitimes.

Fonction	Description
Activé	Lorsque cette option est activée, le traitement Sandbox est effectué par ThreatGrid, soit une copie locale, soit le ThreatGrid Cloud. La valeur par défaut est <b>désactivé</b> .
Clé de service	Avant d'activer le module Sandbox, une clé de service fournie par ThreatGrid doit être configurée. La clé de service permet à ThreatGrid de reconnaître que les échantillons envoyés par ce site sont légitimes.
URL	L'URL pour le serveur ThreatGrid à utiliser (si vous n'utilisez pas un ThreatGrid installé localement). Le ThreatGrid Cloud est accessible via <a href="https://panacea.threatgrid.com">https://panacea.threatgrid.com</a>
Ignorer les paramètres proxy Web	Indique à Malware Analysis d'ignorer le proxy Web, si celui-ci est configuré, lors de l'établissement de la connexion. Si aucun Proxy Web n'a été configuré dans Malware Analysis, le paramètre est ignoré.

## Vue Configuration des services - Onglet Hachage

Cette rubrique présente les fonctionnalités et fonctions disponibles dans la vue Configuration des services > onglet Hachage de Malware Analysis.

Dans cet onglet, vous pouvez gérer le filtrage de hachage dans Malware Analysis. La grille de hachage est initialement vide ; la grille répertorie les filtres qui ont été ajoutés à Malware Analysis. Dans cette vue, vous pouvez ajouter un filtre de hachage, le supprimer, le marquer comme approuvé ou non approuvé et enregistrer les modifications.

Il s'agit d'un exemple de l'onglet Hachage.

Il s'agit d'un exemple de la boîte de dialogue Ajouter un hachage.

## Fonctions

L'onglet **Hachage** se compose d'une barre d'outils et d'une grille de hachage paginable.

Ce tableau décrit la barre d'outils de l'onglet Hachage.

Fonction	Description
<b>Recherche MD5</b>	Saisissez un hachage MD5 pour lequel vous souhaitez rechercher les résultats dans la grille. La fonction de recherche est insensible à la casse.
<b>Add</b>	Affiche la boîte de dialogue Ajouter un hachage dans laquelle vous pouvez ajouter un nouveau hachage à la grille de hachage, spécifiez si le hachage est digne de confiance ou non et fournissez la taille du fichier de hachage.
<b>Enregistrer la modification</b>	Enregistre des ajouts ou des modifications aux tables de hachage dans la grille.
<b>Supprimer</b>	Supprime les hachages sélectionnés de la grille.

Ce tableau décrit les colonnes de la grille Hachage.

Fonction	Description
<b>Sélectionner la case à cocher</b>	Cliquez pour sélectionner une ligne. Cliquez dans l'en-tête de colonne pour sélectionner un en-tête.



<b>Fonction</b>	<b>Description</b>
<b>Fiable</b>	Marque un hachage comme fiable ou non fiable.
<b>MD5</b>	Identifie le hachage MD5.
<b>File Size</b>	Identifie la taille du fichier de hachage en kilo-octets.

## Vue Configuration des services - onglet Indicateurs de compromission

Cette rubrique présente les fonctionnalités et fonctions disponibles dans la vue Configuration des services > onglet Indicateurs de compromission, qui s'applique au service Malware Analysis. À l'aide de cet onglet, vous pouvez configurer la façon dont chacun des quatre modules de score utilise les règles disponibles pour attribuer un score aux données.

Il s'agit d'un exemple de l'onglet Indicateurs de compromis.

### Fonctions

L'onglet Indicateurs de compromis se compose d'une barre d'outils et d'une grille paginable.

Ce tableau décrit les fonctions de la grille.

Fonction	Description
Liste de sélection de module	Sélectionne le module de notation pour lequel vous souhaitez afficher les Indicateurs de compromis. Tous, Network, Static, Community, Sandbox ou Yara.
Champ de recherche	Saisissez le texte que vous recherchez dans le champ Description.
Option de recherche	Filtre la grille pour afficher uniquement les Descriptions qui correspondent au terme de recherche Description.
Option Activer tout	Cliquez pour activer toutes les règles pour le module de notation, au lieu d'activer toutes les règles sur la page à l'aide de la case à cocher.
Option Activer	Cliquez pour activer les règles sélectionnées.
Option Désactiver tout	Cliquez pour désactiver toutes les règles pour le module de notation, au lieu de désactiver toutes les règles sur la page à l'aide de la case à cocher.

Fonction	Description
Option Désactiver	Cliquez pour désactiver les règles sélectionnées.
Option Réinitialiser tout	Cliquez pour réinitialiser toutes les lignes sur la page à leurs valeurs par défaut.
Option Réinitialiser	Cliquez pour réinitialiser les lignes sélectionnées à leurs valeurs par défaut.
Option Enregistrer	Cliquez pour enregistrer les modifications que vous avez effectuées sur cette page. Si vous quittez la page sans enregistrer, les modifications sont perdues. La description de chaque ligne avec des modifications non sauvegardées présente un angle rouge.

Ce tableau décrit les fonctions de la barre d'outils.

Colonne	Description
Case de sélection	Cases à cocher pour sélectionner des lignes individuelles ou toutes les lignes sur la page.
Case à cocher activée	Si l'indicateur de compromis est activé, Malware Analysis utilise la règle pour noter les données de session.
Case à cocher Forte probabilité	Si elle est cochée, Malware Analysis traite la règle comme indiquant très probablement la présence d'un malware, et un événement qui déclenche la règle est marqué dans la grille des résultats.
Description	Décrit l'indicateur de compromis.

Colonne	Description
Note	Spécifie la note que vous souhaitez prendre en compte dans la note totale pour tout événement déclenchant la règle. La note par défaut s'affiche et vous pouvez augmenter ou diminuer la note en faisant glisser le curseur ou en saisissant un chiffre dans la zone de note.
Type de fichier	Affiche les types de fichiers auxquels la règle s'applique. Les valeurs possibles sont <b>TOUS</b> , <b>PDF</b> , <b>Microsoft Office</b> et <b>Windows PE</b> .

## Vue Configuration des services - onglet Intégration

Cette rubrique présente les fonctionnalités et fonctions de l'onglet Intégration disponible dans la vue Configuration des services (Administration) pour Malware Analysis. Cet onglet permet de tester les connexions et d'activer l'évaluation du score de la communauté en enregistrant le service Malware Analysis. Un administrateur peut tester la connexion au site cloud.netwitness.com et à un service Core configuré pour une analyse continue.

La figure suivante donne un exemple de l'onglet Intégration.

## Fonctions

Cet onglet présente deux sections : Test et enregistrement de la connexion au Cloud RSA et Test de connexion à l'analyse continue. Le tableau suivant décrit les fonctions disponibles.

Fonction	Description
<b>Bouton Test et enregistrement de la connexion au Cloud RSA</b>	Cliquer sur ce bouton teste une connexion active à cloud.netwitness.com. NetWitness Suite teste les communications avec le site et vérifie les paramètres de Proxy. Une connexion valide est nécessaire pour s'enregistrer auprès du service de la communauté RSA.
<b>Nom de la société</b>	Nom de votre société. Il s'agit d'un champ obligatoire.
<b>E-mail du contact</b>	Adresse e-mail du contact. Il s'agit d'un champ obligatoire.
<b>Case à cocher À usage interne d'EMC uniquement</b>	Ce champ est facultatif. Les clients, commerciaux ou utilisateurs de démonstrations EMC doivent cocher cette option pour que leurs demandes n'utilisent pas la bande passante sur le serveur de production. Lorsque cette case est cochée, le message d'avertissement suivant s'affiche : <code>Checking this box may cause a less robust performance because the production server isn't being used.</code>
<b>Bouton Enregistrer</b>	Lorsque vous cliquez sur le bouton Enregistrer, l'enregistrement est validé si tous les champs requis ont été complétés. Ce bouton prend l'intitulé Mettre à jour lorsque l'enregistrement est terminé.

Fonction	Description
<b>Bouton Update</b>	Ce bouton s'affiche une fois l'enregistrement terminé.
<b>Bouton Test de connexion à l'analyse continue</b>	Cliquez sur ce bouton pour vérifier que le service Malware Analysis peut se connecter au service Core sélectionné en vue d'une analyse continue (hôte source, port source, nom d'utilisateur et mot de passe d'utilisateur, tels qu'indiqués dans l'onglet Général).

## Vue Configuration des services - onglet Récapitulatif des indicateurs de compromission des services

Cette rubrique présente les fonctions et fonctionnalités disponibles dans la vue Configuration des services > onglet Récapitulatif des indicateurs de compromission. Cet onglet affiche des informations de synthèse sur les IOC. Pour chaque module d'évaluation, une grille répertorie les IOC configurés ainsi que les statistiques qui lui sont associées sur une période donnée. Ces statistiques incluent les données suivantes :

- Nombre d'événements pour une session réseau ou nombre de fichiers pour un événement statique, de communauté ou de sandbox marqués avec l'IOC.
- Score actuellement configuré pour l'IOC sous l'onglet Indicateurs de compromission.
- Scores renvoyés par chaque module d'évaluation.

Lorsque vous sélectionnez un événement, vous pouvez afficher les vues Événements de malware ou Fichiers de malware de l'IOC. Vous pouvez également accéder à l'IOC sélectionné sous l'onglet Indicateurs de compromission pour en modifier le score actuel.

Il s'agit d'un exemple de l'onglet Récapitulatif des indicateurs de compromission pour le réseau du module de notation.

## Fonctions

Le récapitulatif des indicateurs de compromission se décompose en quatre onglets, soit un par module d'évaluation : Réseau, Analyse statique, Communauté et Sandbox. Chaque onglet contient le même formulaire et les mêmes informations, ainsi qu'une barre d'outils et une grille paginable.

Ce tableau décrit les fonctions des différents onglets.

Fonction	Description
Période	Sélectionne la période sur laquelle doit porter le récapitulatif des indicateurs de compromission. Les valeurs possibles sont les suivantes : 5 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.

Fonction	Description
Colonne Description	Descriptions des IOC.
Colonne de décompte	Indique le nombre d'occurrences des IOC. Sous l'onglet Réseau, cette valeur correspond au nombre d'événements dans lesquels l'IOC a été détecté. Sous les autres onglets, cette valeur correspond au nombre de fichiers dans lesquels l'IOC a été détecté.
Colonne Score actuel	Indique le score actuel des IOC tel que configuré sous l'onglet Indicateurs de compromission.
Colonnes Analyse statique, Réseau, Communauté et Sandbox	Indiquent les scores que chacun des modules d'évaluation a donné aux IOC.
Menu déroulant Actions	Ce menu comporte deux options : Afficher les événements/fichiers et Modifier. La première affiche l'IOC dans la vue Événements ou Fichiers (Procédure d'enquête). Cette vue est également accessible en double-cliquant directement sur l'IOC. L'option Modifier permet d'afficher l'IOC sous l'onglet Indicateurs de compromission pour en modifier le score actuel.



## Vue Configuration des services - onglet Proxy

Cette rubrique présente les paramètres configurés sous l'onglet Proxy de la vue Configuration des services d'un service Malware Analysis. Cet onglet configure la communication Malware Analysis via proxy Web avec RSA Cloud pour l'analyse des pairs et avec le service sandbox pour l'analyse sandbox en vue de préserver l'anonymat. Si vous utilisez un service sandbox local, les communications via proxy Web sont inutiles et peuvent ralentir les performances. Lors de la configuration du module sandbox sous l'onglet **Général**, vous pouvez choisir de contourner le proxy Web configuré.

Il s'agit d'un exemple de l'onglet Proxy.

## Fonctions

Ce tableau décrit les fonctions de l'onglet Proxy.

Fonction	Description
Activé	Cochez la case pour activer la communication via proxy Web avec RSA Cloud pour l'analyse des pairs et avec le service sandbox pour l'analyse sandbox en vue de préserver l'anonymat.
Détecter automatiquement les paramètres du proxy Web	Cochez la case pour utiliser les paramètres configurés dans les paramètres du système.
Hôte proxy	Saisissez le nom d'hôte de l'hôte proxy.
Port proxy	Saisissez le port utilisé pour la communication sur l'hôte proxy.
Utilisateurs	Saisissez le nom d'utilisateur qui sert à se connecter à cet hôte proxy.
Mot de passe d'utilisateur	Saisissez le mot de passe de l'utilisateur qui sert à se connecter à l'hôte proxy.
SSL	(Facultatif) Cochez la case pour activer la communication via SSL.
Bouton Appliquer	Cliquez sur le bouton <b>Appliquer</b> pour soumettre les paramètres choisis.

## Vue Configuration des services - onglet ThreatGRID

Cette rubrique présente les paramètres requis pour obtenir une clé API ThreatGrid d'évaluation sous l'onglet Malware Analysis **ThreatGRID**. Cette méthode permet d'obtenir clé API ThreatGrid d'évaluation à utiliser dans le sandbox ThreatGrid Cloud. Avant d'activer ThreatGrid en tant que service sandbox dans le module Sandbox, une clé de service fournie par ThreatGrid doit être configurée afin que ThreatGrid puisse reconnaître que les échantillons soumis à partir de ce site sont légitimes.

Si vous ne disposez pas d'une clé de service fournie par ThreatGrid, vous pouvez obtenir une clé à l'aide de cet onglet. La clé est fournie à titre d'évaluation.

Il s'agit d'un exemple de l'onglet ThreatGRID.

## Fonctions

Ce tableau décrit les fonctions de l'onglet **ThreatGRID**.

Fonction	Description
Nom complet	Vos nom et prénom.
Titre	Votre fonction.
Nom de l'entreprise	Nom de votre organisation.
E-mail	Votre adresse e-mail.
ID utilisateur	Votre ID utilisateur pour accéder à ThreatGrid.
Mot de passe	Votre mot de passe pour accéder à ThreatGrid.
Bouton Enregistrer	Cliquez sur le bouton <b>Enregistrer</b> pour soumettre la demande.