RSA NETWITNESS® PLATFORM

Notes de mise à jour

pour RSA NetWitness Platform 11.3

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, une documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

Sommaire

Introduction **4**

Nouveautés **4**

NetWitness Endpoint 4

NetWitness Respond 7

NetWitness UEBA 8

NetWitness Investigate 9

Event Stream Analysis (ESA) 11

Log Collectors 12

Services de base 13

Administration 14

Octroi de licences 15

Authentification sensible aux menaces 16

Problèmes résolus **16**

Sécurité 16

Enquêter 16

Répondre 17

Event Stream Analysis (ESA) 17

Services de base 18

Mise à niveau 18

Notes de mise à niveau **18**

Documentation produit **18**

Problèmes connus 19

Réactions sur la documentation du produit 19

Fonctions non prises en charge **20**

Fonctions non prises en charge dans les versions 11.1.0.0 ou ultérieures 20

Contacter le support client **21**

Historique des révisions **21**

Introduction

Ce document répertorie les améliorations et correctifs dans RSA NetWitness® Platform 11.3.0.0. Lisez ce document avant de déployer ou de mettre à niveau RSA NetWitness® Platform 11.3.0.0.

Nouveautés

RSA NetWitness® Platform 11.3.0.0 fournit de nouvelles fonctions et améliorations pour chaque rôle dans le Centre des opérations de sécurité. Ces composants sont les suivants :

- Fonctions supplémentaires d'analyse des hôtes et des fichiers pour des activités malveillantes ou suspectes.
- Améliorations de la convivialité pour faciliter le travail des responsables de la réponse aux menaces et des responsables de la recherche des menaces.
- Améliorations apportées aux règles et aux licences pour aider les administrateurs à gérer leurs environnements plus efficacement.

NetWitness Endpoint

Agents Endpoint

Dans la version 11.3, l'agent prend en charge les fonctionnalités EDR (Endpoint Detection and Response) avec Windows Log Collection.

L'agent avancé (sous licence) fournit des fonctions EDR avec une surveillance continue des activités sur l'hôte pour une visibilité approfondie et une analyse de l'ensemble du comportement et des processus sur le point de terminaison. L'agent enregistre les données relatives à chaque action critique, telles que les processus, les fichiers, les modifications du Registre et les connexions réseau, et les publie en tant qu'événements, en temps quasi-réel, sur le serveur. L'agent peut détecter des anomalies telles que des accroches d'image, des accroches de noyau, des divergences de registre et des threads suspects. En outre, il collecte les logs Windows. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint*.

Voici les principales caractéristiques :

- Interactions de la console utilisateur cruciales pour enquêter sur les attaques de logiciels malveillants utilisant des fichiers légitimes Windows, tels que `cmd.exe` ou `powershell.exe` pour exécuter des commandes sur un hôte compromis.

- Visibilité des chaînes d'arguments de ligne de commande qui sont importantes pour l'investigation et les procédures d'enquête.
- Détection de scripts basés sur fichier ou sans fichier en signalant les scripts directement sur les événements de processus plutôt que sur les moteurs de script. Les moteurs actuellement pris en charge sont les suivants : `powershell`, `cmd`, `cscript`, `wscript`, `rundll32`, `mshtml` et `javascript`.
- Agent Journaux infalsifiables - clés de Registre, les fichiers `exe` et `sys` des agents en mode utilisateur et en mode noyau sont protégés.

Les agents Endpoint peuvent fonctionner en mode Informations ou Avancé selon la configuration de la règle. Pour plus d'informations sur les règles, consultez le *Guide de configuration NetWitness Endpoint*.

Principales améliorations apportées aux agents 11.3 par rapport aux anciens agents NetWitness Endpoint

- Dépendances découplées avec les structures internes du noyau.
- Amélioration des performances du blocage de fichiers avec une augmentation considérable du nombre de hachages qui peuvent être bloqués.
- Limites de capture d'événements améliorées. Les événements ne sont plus liés au hachage exécutable, mais à l'ensemble de la chaîne de création.
- Meilleure compatibilité et interopérabilité avec les applications tierces.

Systèmes d'exploitation pris en charge

Les systèmes d'exploitation suivants sont désormais pris en charge :

- Windows 2019 Server
- Windows 10 (32 et 64 bits) (jusqu'à la version 1809)
- Red Hat Linux 7.x
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)

Les agents peuvent également être installés sur une infrastructure de poste de travail virtuel (VDI) sur des environnements VMware. Pour plus d'informations, consultez le *Guide d'installation de l'agent NetWitness Endpoint*.

Déploiements évolutifs et distribués

Vous pouvez faire évoluer votre déploiement en ajoutant plusieurs fichiers log hybrides Endpoint, en fonction du nombre, de l'emplacement, de la distribution des agents et des données collectées à partir des points de terminaison. Installez Endpoint Broker pour obtenir une vue consolidée de tous les serveurs Endpoint de votre déploiement. Pour plus d'informations, consultez le *Guide de l'utilisateur NetWitness Endpoint* et au *Guide de configuration de NetWitness Endpoint*.

Groupes et règles

Pour gérer et mettre à jour efficacement les configurations d'agent Endpoint, les administrateurs peuvent regrouper les agents et gérer leur comportement à l'aide de règles. Les administrateurs peuvent utiliser des règles par défaut ou personnalisées. Vous pouvez activer la configuration Windows Log via la règle de journal Windows au lieu de la générer via le packager d'agent. Pour plus d'informations, consultez le *Guide de configuration NetWitness Endpoint*.

Analyser les fichiers et les hôtes à l'aide du score de risque

Les analystes peuvent enquêter sur un fichier ou un hôte à l'aide des scores de risque compris entre 1 et 100. Le contexte détaillé des responsables des risques (alertes et événements) est disponible pour vous aider à identifier rapidement les activités suspectes ou malveillantes. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint*.

Visualisation des processus

Pour une meilleure expérience en tant qu'analyste lors de la procédure d'enquête, une interface utilisateur intuitive est introduite pour :

- Comprendre l'ensemble de la chaîne d'événements de processus, traitez les relations parent-enfant et tous les événements associés dans une vue chronologique.
- Analyser les attributs de processus importants, tels que le nom d'utilisateur, les arguments de lancement, la réputation, l'état du fichier, le signataire, la signature et le chemin d'accès au fichier.

Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint*.

Analyse de fichiers et réponse

Les analystes peuvent :

- Analyser les fichiers à l'aide de la réputation de fichiers (tel que connus, non valides, suspects) à partir du Context Hub, du score de risque et de l'état du certificat.
- Effectuer une recherche externe à l'aide de Google ou VirusTotal.
- Télécharger un fichier et effectuer une analyse approfondie des fichiers, comme la recherche de chaîne et le contenu textuel pour les scripts.

Après la procédure d'enquête, les analystes peuvent :

- Attribuer des états aux fichiers pour les classer par catégorie : liste noire, liste blanche, etc.
- Corriger les menaces en bloquant les fichiers malveillants ou infectés.

Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint*.

Règles d'application pour les IIOC existants

Les IIOC existants de NetWitness Endpoint 4.4.0. x sont disponibles en tant que règles d'application prêtes à l'emploi dans NetWitness Platform 11.3. Pour plus d'informations, consultez le *Guide de configuration NetWitness Endpoint*.

Ajout de règles d'évaluation des risques liés aux points de terminaison pour ESA

Outre les règles d'exemple ESA, la plate-forme NetWitness inclut désormais un bundle de notation des risques Endpoint avec environ 400 règles. Ces règles génèrent des alertes qui sont utilisées pour calculer les scores de risque pour les fichiers suspects et les hôtes qui définissent les seuils de score de risque. Si vous disposez de NetWitness Endpoint, vous pouvez ajouter ce bundle de règles à un déploiement de règle ESA de la même manière que vous ajoutez une règle ESA. Cependant, vous devez spécifier les sources de données Endpoint (Concentrators) lors des déploiements de règles ESA. Pour plus d'informations, consultez le *Guide de configuration ESA*.

Mises à jour de la vue Enquêter > Vue Analyse d'événements pour les événements Endpoint

- L'analyse de texte pour les événements Vue Analyse d'événements fournit un texte explicite expliquant l'événement. Vous pouvez également afficher les métadonnées avec des valeurs supérieures à 255 caractères.
- Pour chaque session, vous pouvez afficher l'événement dans l'analyse de processus, ou afficher les détails de l'hôte associé à l'événement en pivotant vers la vue Détails de l'hôte.

NetWitness Respond

La liste des événements a été repensée pour les événements NetWitness Endpoint.

Pour améliorer l'expérience de l'analyste et intégrer des événements Endpoint dans NetWitness Respond, la liste d'événements repensée dispose d'une mise en page flexible qui permet de mieux restituer diverses données. La liste repensée permet aux analystes de comprendre et de trier rapidement les événements avec un aperçu des événements plus analysables, qui est personnalisé pour les détails de NetWitness Endpoint et des événements à la volée. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Respond*.

Amélioration du filtre de la liste des alertes pour NetWitness Endpoint

Lorsque vous filtrez la liste des alertes pour la source Endpoint, elle inclut les alertes NetWitness Endpoint 4.4. x et NetWitness Endpoint 11.x.

Ajout d'une règle d'incident UEBA

Une nouvelle règle d'incident par défaut UEBA (User Entity Behavior Analytics) est disponible, ce qui capture le comportement de l'entité utilisateur groupé par ID de classifieur pour créer des incidents à partir des alertes.

Mise à jour de la règle de l'incident NetWitness Endpoint

Si vous disposez de NetWitness Endpoint, la règle d'incident par défaut Alertes de risque élevé : NetWitness Endpoint capture les alertes générées par NetWitness Endpoint avec un score de risque élevé ou critique. Cette règle regroupe désormais les alertes en incidents par nom d'hôte. Pour plus d'informations, consultez le *Guide de configuration NetWitness Respond*.

Ajout de la possibilité de créer automatiquement des incidents d'évaluation des risques Endpoint

Si vous disposez de NetWitness Endpoint, vous pouvez configurer les paramètres du seuil de notation des risques Endpoint pour créer automatiquement des incidents de notation des risques pour les fichiers et les hôtes suspects dépassant les seuils de score de risque définis. Pour plus d'informations sur la configuration des paramètres de seuil des scores de risque, reportez-vous au *Guide de configuration de NetWitness Respond*. Pour plus d'informations sur NetWitness Endpoint, reportez-vous au *Guide de configuration NetWitness Endpoint*.

Pivoter vers les vues Enquêter > Hôtes et fichiers à partir de la vue Répondre

Pour une procédure d'enquête détaillée sur un incident, les analystes peuvent accéder aux vues Enquêter > Hôtes et fichiers via des info-bulles contextuelles dans la vue Répondre.

Rechercher l'état et les informations de réputation des fichiers à partir de la vue Répondre

Dans la vue Répondre et les vues Enquêter où Context Hub est intégré à la plate-forme NetWitness, les analystes peuvent passer le pointeur de la souris sur une entité de hachage de fichier pour ouvrir une info-bulle contextuelle, qui affiche l'état de réputation du fichier. Les analystes peuvent également cliquer sur un bouton Afficher le contexte pour ouvrir un panneau de recherche contextuelle avec des informations supplémentaires sur les fichiers.

NetWitness UEBA

Analytique avancée à l'aide de RSA NetWitness Endpoint

UEBA est intégré à NetWitness Endpoint pour améliorer la couverture de la détection actuelle sur NetWitness Platform. L'objectif de cette intégration est d'identifier l'activité potentielle du pirate. Il s'agit principalement de deux sources de données principales :

- Exécutions du processus
- Modifications du Registre

Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness UEBA*.

Accéder aux détails de l'hôte ou analyser les vues de processus à partir de la vue Profil utilisateur

Un analyste peut pivoter vers la vue Détails de l'hôte ou la vue Analyser le processus à partir de la vue Profil utilisateur pour rechercher des informations plus détaillées sur un processus anormal ou sur un hôte associé aux risques de l'utilisateur. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness UEBA*.

Prise en charge d'autres sources de données

NetWitness UEBA prend désormais en charge la source de données RSA SecurID.

NetWitness Investigate

Les analystes peuvent afficher un grand nombre d'événements simultanément dans la liste des événements de la vue Analyse d'événements

Jusqu'à 50 000 événements sont chargés dans la liste des événements par ordre croissant en fonction de la durée de la collecte. Un indicateur de numéro de ligne toutes les 100 lignes facilite la navigation dans la liste. Les fonctions de l'interface utilisateur vous permettent de comprendre ce qui est affiché et l'ordre de tri. Pour des informations détaillées, consultez la section « Filtrage d'événements dans la vue Analyse d'événements » du *Guide de l'utilisateur NetWitness Investigate*.

Les analystes peuvent voir l'état détaillé d'une requête dans la vue Analyse d'événements

Cliquer sur l'icône d'informations () dans le générateur de requête de l'Analyse d'événements, permet d'ouvrir la console de requête, une nouvelle fonction de l'interface utilisateur qui fournit une barre d'état, des avertissements, des erreurs et d'autres informations sur ce qui se produit lorsqu'une requête est en cours d'exécution. Lorsqu'une requête est terminée, la console de requête affiche la plage horaire, la requête, les services interrogés, tous les services qui n'ont pas pu être interrogés, et la durée de chaque service pour trouver des résultats et récupérer des événements en fonction de la requête. Vous pouvez copier la requête entière sous forme de texte. Pour plus d'informations, consultez la section « Filtrer les résultats dans la vue Analyse d'événements » du *Guide d'utilisation de NetWitness Investigate*.

Workflow d'analyse amélioré dans la vue Naviguer, la vue Événements et la vue Analyse d'événements

Pour faciliter l'exécution des procédures d'enquête, les analystes ont mis en œuvre les améliorations suivantes :

- Lorsque vous passez d'une page à une autre dans la vue Événements, les événements de log se chargent plus rapidement en raison de la mise en cache des résultats de requête.
- La période utilisée dans la navigation est utilisée lors de la transition vers la vue Événements.
- Dans la vue Naviguer, une description de clé méta facilement compréhensible s'affiche en regard du nom de la clé méta. Pour obtenir des informations détaillées, consultez la section « Vue Naviguer » du *Guide d'utilisation de NetWitness Investigate*.

- Une entrée de période personnalisée a été ajoutée dans la vue Analyse d'événements. En plus des périodes prédéfinies, vous pouvez saisir une période personnalisée, puis cliquer sur le jour, le mois, l'année, l'heure et les minutes pour modifier la période directement dans le fil d'Ariane. Pour plus d'informations, consultez la section « Filtrer les résultats dans la vue Analyse d'événements » du *Guide d'utilisation de NetWitness Investigate*.

Les informations détaillées sur les événements chargés dans la vue Événements s'affichent dans le pied de page

Le message dans le pied de page aide les analystes à comprendre ce qu'ils visualisent dans la vue Événements. Si aucun événement n'est chargé, le message suivant s'affiche : « 0 correspondance d'événements ». D'autres messages vous permettent de savoir si la limite d'analyse ou la limite de résultats définie par l'administrateur a été atteinte et quels services affichent les résultats. Par exemple, le message suivant vous indique que la limite d'analyse a été atteinte et que des données supplémentaires sont disponibles pour l'analyse : « Affichage de 1-25 sur 100 000 + correspondances d'événements (la limite d'analyse de 100 000 événements a été atteinte). » Pour obtenir des informations détaillées, consultez la section « Vue Événements » du *Guide d'utilisation de NetWitness Investigate*.

Accélération de la recherche et de la requête dans la vue Naviguer et la vue Événements

Lorsque les analystes travaillant dans la vue Naviguer interrogent un Broker ou un Concentrator, les requêtes suivantes qui partagent tout ou partie des critères d'une requête précédente renvoient des résultats plus rapidement en utilisant une nouvelle mise en cache intégrée dans les services. Dans la vue Événements, les requêtes utilisant des opérations complexes avec des valeurs de texte sont mises en cache afin que les requêtes suivantes qui partagent tout ou partie des critères d'une requête précédente renvoient des résultats plus rapidement.

Nouvelles fonctions du générateur de requête dans la vue Analyse d'événements

- Vous pouvez créer des filtres complexes dans le générateur de requête en Mode Guidé à l'aide du filtre de formulaire libre dans le sous-menu Options avancées, qui se trouve dans tous les menus déroulants du Mode Guidé. Le Mode Formulaire libre est toujours disponible si vous souhaitez coller une longue requête complexe.
- Lorsque vous envoyez une requête qui contient des filtres de formulaire libre, les filtres de forme libre sont validés côté serveur avant l'exécution. Si l'un des filtres n'est pas valide, la requête n'est pas exécutée.
- Lorsqu'une requête est en cours d'exécution, vous pouvez annuler la requête en cours. Lorsqu'une requête est annulée, le nombre d'événements du panneau Événements, le message du pied de page et la console de requête reflètent le nombre d'événements récupérés plutôt que le nombre total d'événements trouvés.

Pour plus d'informations, consultez la section « Filtrer les événements dans la vue Analyse d'événements » du *Guide d'utilisation de NetWitness Investigate*.

Mises à jour des clés méta dans le groupe de colonnes Endpoint Analysis

Le groupe de colonnes Endpoint Analysis est mis à jour pour inclure les nouvelles clés méta pour la procédure d'enquête Endpoint, qui apparaissent lors de l'affichage d'un événement Endpoint dans la vue Événements et la vue Analyse d'événements.

Nouvelle option de préférence permettant de contrôler la mise à jour automatique de la période dans le fil d'Ariane

Dans la vue Analyse d'événements, une nouvelle préférence de la boîte de dialogue Préférences de l'événement contrôle la mise à jour automatique de la période dans le fil d'Ariane. Lorsque vous affichez les résultats d'une période spécifique, le service est interrogé à des intervalles d'une minute pour détecter s'il existe de nouveaux résultats, mais les nouveaux résultats ne sont pas chargés dans la vue actuelle. Par défaut, la période du fil d'Ariane reste synchronisée avec la recherche en cours. Vous pouvez choisir de mettre automatiquement à jour la période dans le fil d'Ariane lorsque le service indique que les derniers résultats ont été mis à jour en sélectionnant la case à cocher **Mettre à jour la période automatiquement**. Lorsque la période est mise à jour et que le bouton Envoyer une requête est activé, vous pouvez obtenir les résultats mis à jour.

Accéder à UEBA à partir de la vue Enquêter > Détails de l'hôte

Si NetWitness UEBA est installé, vous pouvez analyser les risques associés aux utilisateurs connectés à l'hôte en les associant à la vue Utilisateurs. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness UEBA*.

Event Stream Analysis (ESA)

Introduction d'un nouveau service de corrélation ESA amélioré pour les règles de corrélation ESA

Le service de corrélation ESA de la plate-forme NetWitness 11.3 remplace le service Event Stream Analysis disponible dans les versions précédentes. Tout comme le service Event Stream Analysis, le service de corrélation ESA s'installe sur les types d'hôte principal et secondaire ESA.

Il existe deux services ESA pouvant s'exécuter sur un hôte ESA :

- Corrélation ESA (Règles de corrélation ESA)
- Event Stream Analytics Server (ESA Analytics)

Le service de serveur Contexthub, qui fournit une fonction de recherche d'enrichissement dans les vues Répondre et Enquêter, s'exécute uniquement sur un hôte principal ESA.

Prise en charge de différentes sources de données pour les règles de corrélation ESA

Au lieu d'ajouter des sources de données, telles que des concentrators, à l'ensemble du service, vous pouvez spécifier des sources de données différentes pour chaque déploiement de règle ESA. Par exemple, vous voudrez peut-être utiliser des concentrators avec des données de paquets HTTP dans un déploiement et des concentrators avec des données de log HTTP dans un autre déploiement. Pour plus de détails, consultez le *Guide d'utilisation des alertes de corrélation ESA*.

Pour plus d'informations sur les mises à niveau pour les déploiements de règles ESA, consultez les instructions de mise à niveau et de mise à jour applicables, ainsi que le *Guide de configuration ESA*.

Prise en charge de l'ajustement du niveau de compression pour les concentrators sur ESA

Lorsque vous configurez un déploiement de règle ESA et que vous configurez un concentrator à utiliser comme source de données, vous avez la possibilité de définir le niveau de compression des données pour le concentrator sur ESA. Pour plus de détails, consultez le *Guide d'utilisation des alertes de corrélation ESA*.

Activer ou désactiver le transfert des alertes de règle ESA individuelles dans la vue Répondre

Vous pouvez activer ou désactiver les alertes pour chaque règle ESA. Pour plus d'informations, consultez le *Guide de configuration ESA*.

Version ESPER mise à niveau de la version 5.3 vers la version 7.1

Mise à niveau de ESPER vers la dernière version 7.1.

Log Collectors

Liste triée des Log Collectors et Virtual Log Collectors

Pour les services Log Collector, Local Collectors et Remote Collectors, les menus contextuels sont triés par ordre alphabétique pour faciliter la recherche du collector que vous souhaitez afficher :

- Sur un local collector, sous l'onglet Remote Collectors, le champ Remote Collectors de la boîte de dialogue Ajouter une source est trié.
- Dans un log Collector virtuel, l'onglet Local Collectors contient des champs triés pour les destinations et les sources.

Liste triée des Log Collectors et des Log Decoders

Dans la vue ADMIN > Intégrité > vue Surveillance des sources d'événements, les menus déroulants Log Collectors et Log Decoders sont triés par ordre alphabétique pour faciliter la recherche des éléments que vous souhaitez afficher.

Ports Syslog des Log Collectors locaux

Dans la version 11.3, les Log Collectors locaux (Logs Collectors résidant sur les appliances Log Decoder) sont capables de recevoir des syslog sur des ports autres que 514 et 6514 afin de prendre en charge la réception de messages syslog avec différents codages, tels que EUC-KR, ISO8897-9, etc. Le service Log Decoder est toujours le point de collecte pour la réception des logs ASCII/UTF-8 sur les ports 514 et 6514.

Amélioration de la logique directe pour les syslogs non conformes

Les Log collectors distants acceptent désormais tous les messages syslog non conformes, à l'exception de ceux avec un corps ou un en-tête de message vide. Les messages indésirables doivent être filtrés lors de la collecte syslog à l'aide de filtres d'événement. Pour plus d'informations, reportez-vous à la section « Configurer des filtres d'événements pour un Collector » dans le *Guide de Log* . Reportez-vous à syslog RFC3164 et RFC5424 pour plus de détails concernant le format syslog (https://www.ietf.org/standards/rfcs/).

Services de base

Analyseur Snort avec prise en charge UDM

La prise en charge de l'analyseur Snort a été mise à jour avec une nouvelle option, `udm=true`, qui utilise le jeu de clés UDM (Unified Data Model) aligné. Pour plus d'informations, consultez la section « Analyseurs Snort » dans le *Guide de configuration de Decoder et Log Decoder*.

Déchiffrement Secure SMTP

La plate-forme NetWitness prend en charge le déchiffrement opportuniste SSL/TLS, qui répond à RFC 3207 (https://tools.ietf.org/html/rfc3207). Vous pouvez ajouter une option d'analyseur HTTPs qui fournit une liste de ports de destination au format CSV (valeurs séparées par des virgules) de la session dans laquelle la commande STARTTLS sera recherchée, avec au moins une clé de chiffrement ayant été téléchargée. Cela active la fonction STARTTLS. Pour plus d'informations, consultez la section « Déchiffrement Secure SMTP » dans le *Guide de configuration de Decoder et Log Decoder*.

L'analyseur GeoIP n'est plus pris en charge. Il a été remplacé par l'analyseur GeoIP2

L'analyseur GeoIP d'origine n'est plus pris en charge. Le nouvel analyseur GeoIP2 qui a été introduit dans la version 11.2 a entièrement remplacé cette solution. L'analyseur GeoIP2 prend en charge toutes les fonctionnalités précédentes, ainsi que le nouveau package MaxMind, y compris les conversions IPv4 et IPv6.

Limiter l'utilisation de la mémoire de requête avec le paramètre SDK max.query.memory

Ce paramètre `max.where.clause.sessions` impose une limite au nombre de sessions qui peuvent être scannées par une requête unique. Par exemple, si un utilisateur sélectionne toutes les méta de sa base de données, la base de données arrête de traiter les résultats une fois que le nombre de sessions lues pour cette requête atteint cette valeur de configuration. Ce paramètre sera obsolète dans une prochaine version. Utilisez le paramètre `max.query.memory` pour limiter l'utilisation de la mémoire globale de la requête.

Les disques PowerVault SED peuvent être utilisés pour le stockage externe

Vous pouvez maintenant configurer les disques PowerVault SED (disques à chiffrement automatique) pour l'utiliser comme un stockage externe pour stocker les données des fichiers log et des paquets en vue de leur extraction.

Les index N-Gram offrent de meilleures performances que dans la version 11.2, ce qui améliore les recherches de texte intégral

Des améliorations ont été apportées au taux d'insertion des index N-Gram pour les recherches de texte intégral. Les index en mode N-Gram sont approximativement deux fois plus rapides pour les mises à jour, ce qui signifie qu'ils peuvent être exploités dans un plus grand nombre de concentrators sans avoir d'impact sur les performances de l'agrégation. Par défaut, cette fonctionnalité est désactivée. Pour plus d'informations sur les index N-gram, reportez-vous à la section « Personnalisation de l'index » dans le *Guide d'optimisation de la base de données principale de NetWitness Platform*.

Nouvelle fonction `avglen` dans la syntaxe de requête de base de données

La fonction `avglen` a été ajoutée à la syntaxe de requête. Elle renvoie une valeur unique qui correspond à la durée moyenne d'une valeur méta dans une fonction.

Administration

Possibilité de configurer des composants hybrides sur des appliances principales (permettant d'utiliser plusieurs PowerVault pour les composants hybrides)

Vous pouvez installer des catégories hybrides, telles que des catégories de service Log Hybrid et Réseau (paquet) hybride, sur un hôte physique de la gamme 6 (R640). Vous avez ainsi la possibilité de rattacher plusieurs périphériques de stockage PowerVault externe à l'hôte physique de la gamme 6 (R640).

Authentification PKI (Public Key Infrastructure)

L'authentification PKI permet aux utilisateurs de s'authentifier et d'accéder à l'interface utilisateur de NetWitness Platform à l'aide de certificats numériques. Pour plus d'informations, reportez-vous à la section Authentification PKI dans le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Prise en charge de DISA STIG

RSA prend en charge toutes les règles d'audit du groupe de contrôles DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide) dans la version 11.3. Pour obtenir des informations détaillées sur le guide STIG pris en charge dans la version 11.3, reportez-vous au *Guide de maintenance du système*.

Commande de réémission de certificat

RSA a ajouté la commande `cert-reissue` et ses arguments afin que vous puissiez réémettre les certificats d'hôte. Après avoir mis à jour l'ensemble de vos hôtes vers la version 11.3, vous devez réémettre tous les certificats le plus tôt possible afin d'éviter qu'ils n'expirent. En cas d'expiration des certificats, le déploiement de NetWitness passe à l'état irrécupérable. Pour plus d'informations sur la façon de réémettre des certificats dans la version 11.3, reportez-vous au *Guide de configuration système*.

Hôte du serveur NW de secours à chaud (pour le basculement sur incident/haute disponibilité) - hôte physique uniquement

Le serveur NW de secours à chaud duplique les composants et les configurations critiques de votre hôte de serveur NW actif pour accroître la fiabilité. Le serveur NW de secours à chaud peut être configuré pour rester en mode veille et recevoir des sauvegardes de l'hôte du serveur NW actif à intervalles réguliers. Si le serveur NW actif tombe en panne (passe en mode hors ligne), il est possible d'exécuter la procédure de basculement sur incident et le serveur NW en veille devient actif. Pour plus d'informations sur la configuration et la gestion d'un serveur NW de secours à chaud dans la version 11.3, reportez-vous à NetWitness Platform - *Guide de déploiement*.

Nouvel outil permettant de consolider les données de configuration des hôtes et des services en une seule instance

L'outil NW-Consolidator est disponible pour les clients 10.6.6 sélectifs qui souhaitent migrer la configuration et les données de la version 10.6.6 vers la plate-forme NetWitness 11.3. Cet outil peut être utilisé si votre déploiement comporte plusieurs instances Security Analytics et Reporting Engine, et que vous souhaitez consolider la configuration des hôtes et des services, ainsi que les données dans une seule instance. Vous pouvez également consolider les données liées aux utilisateurs, aux groupes, aux rôles, aux sources et aux rapports.

Octroi de licences

Prise en charge des licences Endpoint et ESA et de la consolidation de toutes les habilitations pour les licences de débit

L'interface utilisateur des licences améliorées facilite l'affichage des informations de licence par les administrateurs. La page des détails de l'octroi de licence affiche l'utilisation du débit agrégé pour différentes habilitations avec des tendances d'utilisation du débit. Les administrateurs peuvent afficher toutes les licences du déploiement, y compris celles pour Endpoint et le serveur de corrélation ESA. En outre, les administrateurs peuvent configurer les licences pour plusieurs serveurs NetWitness, ainsi que des serveurs à chaud. Pour plus d'informations, consultez le *guide de gestion des octrois de licences*.

Authentification sensible aux menaces

Intégration de la plate-forme NetWitness avec RSA SecureID Access

L'intégration de la plate-forme NetWitness avec RSA SecureID Access vous permet d'identifier les utilisateurs suspects dans la plate-forme NetWitness et d'élever les niveaux d'accès ou de bloquer les utilisateurs dans RSA Secure ID Access en fonction du niveau d'assurance et des règles définies dans l'ID sécurisé. Le serveur NetWitness Respond envoie des identifiants e-mail des utilisateurs suspects des incidents à RSA SecurID Access. Pour configurer cette intégration sur le serveur Respond, reportez-vous au *Guide de configuration de Respond*.

Problèmes résolus

Cette section répertorie les problèmes résolus depuis la dernière version principale.

Sécurité

Numéro de suivi	Description
ASOC-59254	Mise à jour de sécurité du noyau https://access.redhat.com/errata/RHSA-2018:1965.
ASOC-58383	Mise à jour de sécurité policycoreutils https://access.redhat.com/errata/RHSA-2018:0913.
ASOC-58382	Mise à jour de sécurité https://access.redhat.com/errata/RHSA-2018:0998.

Enquêter

Numéro de suivi	Description
ASOC-61230	Lorsque vous importez des profils dans la vue Naviguer ou dans la vue Événements à l'aide de la boîte de dialogue Gérer les profils, les profils nouvellement importés ne sont pas ajoutés au menu déroulant Profils.

Numéro de suivi	Description
ASOC-60941	Les événements de réseau et de journal sont entrelacés et triés dans l'ordre chronologique dans la vue Événements, mais les événements sont triés différemment dans la vue Analyse d'événements. Dans la vue Analyse d'événements, les événements ne sont pas entrelacés comme ils devraient l'être ; au lieu de cela, tous les événements de journal triés dans l'ordre chronologique sont affichés avant tous les événements réseau triés dans l'ordre chronologique.
ASOC-50196	Si l'URL d'un point d'extraction est très long et que vous utilisez la requête dans la vue Analyse d'événements, une erreur (Erreur de requête 414) est renvoyée.
ASOC-49427	Le générateur de requête dans la vue Analyse d'événements ne répond pas aux filtres qui contiennent un espace.

Répondre

Numéro de suivi	Description
ASOC-59243	Lorsque toutes les alertes sont supprimées pour une règle d'alerte, le filtre de la règle n'est pas correctement supprimé.
ASOC-37533	Lorsqu'une table en mémoire personnalisée est créée et ajoutée en tant que source d'enrichissement dans ESA, ces informations ne sont pas affichées pour les alertes ESA.

Event Stream Analysis (ESA)

Numéro de suivi	Description
ASOC-60511	Les règles ESA CH sont désactivées pendant la mise à niveau ou le redémarrage de l'hôte ESA.
ASOC-60367	Les règles ESA avec des clés méta personnalisées ne se déploient pas sur le serveur ESA.
ASOC-26481	Impossible de définir le niveau de compression ESA comme dans d'autres appliances.

Numéro de suivi	Description
ASOC-14157	ESA affiche des messages d'avertissement pour les opérateurs de baie.

Services de base

Numéro de suivi	Description
ASOC-41902	Le mode SSL FIPS (case à cocher) pour Broker, Concentrator et Archiver doit être désactivé.

Mise à niveau

Numéro de suivi	Description
ASOC-49843	Les modèles de journal d'audit ne sont pas mis à jour dans le fichier conf de sortie Logstash lors de la mise à niveau vers 11. x.
ASOC-42136	Après la mise à niveau, les liens Procédure d'enquête sont désactivés pour les graphiques statiques

Notes de mise à niveau

Les stratégies de mise à niveau suivantes sont prises en charge par RSA NetWitness® Platform 11.3.0.0 :

- RSA NetWitness® Platform 10.6.6.x vers 11.3.0.0
- RSA NetWitness® Platform 11.0.x, 11.1.x ou 11.2.x vers 11.3.0.0

Pour plus d'informations sur l'installation et la mise à niveau vers la version 11.3.0.0, reportez-vous aux Guides d'installation et de mise à niveau dans https://community.rsa.com/community/products/netwitness/113 > Guides d'installation et de mise à niveau.

Documentation produit

Cette version est fournie avec la documentation suivante :

Documentation	URL d'emplacement
Documentation en ligne RSA NetWitness Platform 11.3	https://community.rsa.com/community/products/netwitness/documentation
Instructions de mise à niveau de RSA NetWitness Platform 11.3 et listes de contrôle	https://community.rsa.com/community/products/netwitness/documentation
Guides de configuration matérielle de RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
Contenu RSA pour RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Problèmes connus

Les problèmes qui ne sont pas résolus dans cette version sont documentés ici :https://community.rsa.com/community/products/netwitness/documentation/known-issues. S'il existe une solution de contournement, elle est présentée ou référencée de façon détaillée.

Réactions sur la documentation du produit

Vous pouvez envoyer un e-mail à sahelpfeedback@rsa.com pour faire part de vos réactions sur la documentation de RSA NetWitness Platform.

Fonctions non prises en charge

Les tableaux suivants fournissent des informations sur les fonctions qui ne sont plus prises en charge dans RSA NetWitness® Platform 11.1 ou versions ultérieures.

Fonctions non prises en charge dans les versions 11.1.0.0 ou ultérieures

Non.	Fonction	Remarques
1	Malware Colo	Malware Colo n'est pas pris en charge dans les versions 11.1.0.0 et ultérieures. Malware Analysis est pris en charge à l'aide d'un module Malware Analysis autonome.
2	Déploiement tout-en-un	Le déploiement tout-en-un n'est pas pris en charge. Une nouvelle installation tout-en-un a été retirée.
3	Warehouse Connector autonome	Standalone Warehouse Connector n'est pas prise en charge.
4	Fonctionnalités d'administration	1. J'ai oublié mon mot de passe. 2. Notification par e-mail à l'utilisateur lors de l'expiration du mot de passe. 3. Utilisateur de test/recherche AD.
5.	Pivotal	Pivotal n'est pas pris en charge.
6.	Warehouse Analytics	Warehouse Analytics n'est pas pris en charge.

Non.	Fonction	Remarques
7.	Quelques fonctions du service Event Stream Analysis depuis la version 11.2 et les versions antérieures	Les fonctions du service Event Stream Analysis (11.2 et versions antérieures) qui ne figurent pas dans le service de corrélation ESA 11.3 : 1. Snapshot de la mémoire pour les règles d'évaluation 2. Méthode de notification ESA SNMP 3. Base de données en tant que source d'enrichissement (remplacée par la liste Context Hub) 4. Base de données en tant que Warehouse Analytics (remplacée par la liste Context Hub) 5. Connexion à la base de données en tant que Warehouse Analytics (remplacée par la liste Context Hub) 6. Ordonnancement temporel des captures 7. Pool de mémoire
8.	Endpoint Hybrid	Le type d'hôte Endpoint Hybrid n'est pas pris en charge dans les versions 11.3.0.0 et ultérieures.

Contacter le support client

Lorsque vous contactez l'assistance clientèle, vous devez être devant votre ordinateur. Soyez prêt à fournir les informations suivantes :

- Le numéro de version du produit ou de l'application RSA NetWitness Platform que vous utilisez.
- Le type de matériel que vous utilisez.

Si vous avez des questions ou si vous avez besoin d'aide, suivez les instructions fournies ici : https://community.rsa.com/docs/DOC-1294

Historique des révisions

Révision	Date	Description
1	13 mars 2019	Version pour les opérations