RSA NETWITNESS® PLATFORM

Notes de mise à jour

pour la version 11.2

Informations de contact

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

Ce document répertorie les améliorations et correctifs dans RSA NetWitness® Platform 11.2.0.0. Lisez ce document avant de déployer ou d'effectuer la mise à niveau vers RSA NetWitness® Platform 11.2.0.0.

Actualités

La version RSA NetWitness® Platform 11.2.0.0 offre de nouvelles fonctionnalités et améliorations pour l'investigation des journaux, des paquets et des points de terminaison. Dans le cadre de cette version, l'analyse comportementale des utilisateurs et des entités est introduite pour détecter et enquêter sur les attaques et les anomalies basées sur l'identité.

NetWitness User and Entity Behavior Analysis (UEBA)

RSA NetWitness ® UEBA fait désormais partie de RSA NetWitness® Platform. NetWitness UEBA fournit des analyses comportementales complètes d'utilisateur et d'entité pour mieux détecter, enquêter et répondre aux attaques internes avancées et aux anomalies basées sur l'identité.

NetWitness UEBA dispose des fonctionnalités suivantes :

- Exploite des analyses de données statistiques dynamiques pour le comportement des valeurs de référence, la modélisation des comportements et l'analyse des groupes de pairs afin de détecter les comportements anormaux, les mouvements latéraux, les menaces d'initiés et l'exfiltration des données.
- Identifie les anomalies suspectes basées sur le comportement à l'aide d'algorithmes d'apprentissage automatique non supervisés.
- Génère un modèle de notation des risques liés aux identités et aux alertes pour ne relever que la sévérité et la priorité des indicateurs à haut risque, réduisant la fatigue liée aux alertes et les faux positifs.

Déploiement du service NetWitness UEBA. NetWitness UEBA peut être configuré et déployé à partir de NetWitness Platform Admin Server. NetWitness UEBA Server capture les données du journal Windows à partir des services NetWitness Platform, traite les données et affiche les résultats sur l'interface graphique NetWitness. Si l'agent NetWitness Insights Endpoint est déployé, les données du journal Windows collectées sont également analysées. Pour plus d'informations, reportez-vous au *Guide d'installation des hôtes physiques* ou au *Guide d'installation des hôtes virtuels*.

Dans la version 11.2, l'UEBA prend en charge nativement une variété de sources de journaux Windows, notamment :

- Windows Active Directory
- Activité d'ouverture de session et d'authentification Windows
- Serveurs de fichiers Windows

Valeurs de référence des comportements liés aux identités. Les modèles d'apprentissage automatique sont appliqués sur les données historiques et en temps réel afin de créer des valeurs de référence liées aux comportements, lesquelles permettent d'identifier les valeurs aberrantes et fournissent une visibilité sur les mesures organisationnelles et individuelles. La stratégie de modélisation standard exécute une période de formation de 30 jours. Si des données historiques supplémentaires sont stockées au-delà de la période de formation, celle-ci peut être modifiée pour s'exécuter à un délai antérieur. Seuls les comportements anormaux par rapport à ces valeurs de référence entraînent des anomalies ou des indicateurs de compromis.

Procédures d'enquête sur les alertes principales et les utilisateurs à haut risque. Les analystes peuvent utiliser un tableau de bord pré-défini (OOTB) ainsi que des rapports pour enquêter sur les alertes principales (alertes déclenchées par une séquence d'indicateurs durant une heure complète) et les utilisateurs à haut risque (utilisateurs présentant un score de risque élevé). Les analystes peuvent consulter les utilisateurs nécessitant une attention immédiate, effectuer des recherches approfondies et réduire les scores de risque.

Licence NetWitness UEBA. La licence NetWitness UEBA se base sur le nombre total d'utilisateurs de votre organisation. Les utilisateurs sont des personnes ayant accès au réseau et aux identifiants de connexion. Si le nombre d'utilisateurs dépasse cinq pour cent (5 %) de la licence achetée, vous devez acquérir de nouvelles licences. Pour plus d'informations, contactez votre gestionnaire de comptes RSA. Pour en savoir plus sur les licences, consultez le *guide de gestion des licences*.

Pour plus d'informations sur UEBA, consultez le *guide de l'utilisateur UEBA (User Entity and Behavior Analytics) NetWitness*.

NetWitness Respond

Accédez à l'analyse des événements directement à partir de la vue Détails de l'incident. Vous pouvez accéder en toute transparence à l'analyse des événements à partir de la vue Enquêter dans le panneau Indicateurs du scénario d'un incident. Pour étudier un incident de manière plus approfondie, vous pouvez cliquer sur le lien hypertexte du type d'événement d'un événement du scénario, afin d'ouvrir la vue Analyse d'événements dans Répondre.

Ajout de la possibilité d'envoyer des incidents au sein de NetWitness Respond to RSA Archer. Si RSA Archer est configuré en tant que source de données dans Context Hub, vous pouvez envoyer des incidents à Réponse aux cyberincidents et failles de sécurité IT Archer. Une fois configuré, vous verrez un bouton Envoyer à Archer et NetWitness Respond affichera l'état Envoyé à Archer. Vous aurez également la possibilité de filtrer la liste des incidents pour afficher les incidents envoyés à Archer. Lorsque vous envoyez un incident à Archer, le système crée automatiquement une entrée dans le journal pour l'incident.

Pivoter vers RSA Archer à partir d'Incidents. Vous pouvez pivoter vers RSA Archer pour afficher les détails de l'appareil et d'autres informations dans Réponse aux cyberincidents et failles de sécurité IT RSA Archer® pour les entités spécifiques. Ces entités sont l'adresse IP, l'hôte et l'adresse Mac. Dans le panneau de recherche contextuelle, vous pouvez afficher les attributs de l'entité soulignée, tels que les valeurs d'unité d'entreprise, le nom du périphérique, le type de périphérique, etc. Pour plus d'informations, reportez-vous au *Guide d'utilisation de NetWitness Respond*.

Optimisation de la création d'incidents manuels à partir de la vue Liste d'alertes. Vous pouvez ajouter une priorité, une personne affectée et des catégories lorsque vous créez un incident manuellement à partir d'alertes.

Ajout de la possibilité de masquer les types de nœuds dans le graphique nodal. Pour étudier de manière plus approfondie les interactions entre les entités sur le graphique nodal, vous pouvez sélectionner les types de nœuds que vous souhaitez inclure dans le graphique nodal. Cela peut être particulièrement utile si un graphique nodal contient plus de 100 nœuds.

Ajustement du filtre d'incidents pour les incidents attribués et non attribués. Dans le panneau Filtres de liste d'incidents, vous ne pouvez plus filtrer les personnes affectées et les incidents non attribués en même temps. Si vous sélectionnez « N'afficher que les incidents non attribués », le menu déroulant du filtre Personne attribuée est désormais désactivé. Si vous sélectionnez une personne attribuée dans le menu déroulant, l'option « N'afficher que les incidents non attribués » est désormais désactivée.

Amélioration de l'expérience client grâce à l'option de tri de la liste d'incidents. Vous pouvez cliquer n'importe où sur l'en-tête de colonne dans la liste afin de basculer le tri. Il n'est plus nécessaire de cliquer sur les flèches haut ou bas pour trier la liste.

Pour plus d'informations, reportez-vous au *Guide de l'utilisateur NetWitness Respond* et au *Guide de configuration de NetWitness Respond*.

NetWitness Investigate

Informations contextuelles pour une valeur méta dans la vue Analyse d'événement. Le panneau de recherche contextuelle, qui était précédemment disponible dans la vue Naviguer et la vue Événements, a été ajouté à la vue Analyse d'événement. Le panneau Recherche contextuelle vous permet de consulter les détails à propos des éléments associés à un événement (adresse IP, utilisateur, hôte, domaine, adresse MAC, nom de fichier, hachage de fichier) dans Context Hub. Vous pouvez interagir avec les valeurs méta d'un événement pour obtenir davantage d'informations, y compris les incidents associés, alertes, listes personnalisées, ressources Archer, informations Active Directory, et NetWitness Endpoint Thick Client. Pour plus d'informations, reportez-vous à « Afficher un contexte supplémentaire pour un point de données » dans le *guide de l'utilisateur NetWitness Investigate*.

Pivotez vers Archer à partir de valeurs méta dans la vue Analyse d'événement. Vous pouvez maintenant pivoter vers RSA Archer à partir de ces entités soulignées : adresse IP, Mac et hôte dans Analyse d'événements pour afficher les détails de l'appareil.

Requêtes sur formulaire libre dans la vue Analyse d'événement. Le mode Formulaire libre est une alternative au mode de requête de base (guidé) disponible dans les versions antérieures. En mode Formulaire libre, les analystes peuvent entrer des requêtes de texte complexes et basculer entre le mode libre et le mode guidé. Pour plus d'informations, consultez la section « Filtrer les résultats dans la vue Analyse d'événements » du *Guide de l'utilisateur NetWitness Investigate*.

Les améliorations apportées au profil incluent les groupes de profils, les modèles nouveaux et mis à jour, et notamment la preQuery pour un profil dans le fil d'Ariane. Pour plus d'informations, consultez « Utiliser des profils pour encapsuler les vues personnalisées » dans le *guide d'utilisation NetWitness Investigate*.

- Les groupes de profil vous permettent d'organiser des profils en groupes logiques, par exemple, différents groupes de profil pour différents cas d'utilisation ou différents utilisateurs. Vous pouvez déplacer des

profils existants et nouveaux dans des groupes de profil.

- Un nouveau profil préconfiguré appelé RSA Endpoint Analysis utilise un preQuery de `device.type=nwendpoint` et le groupe de méta ainsi que les groupes de colonne de RSA Endpoint.
- Dans le profil d'analyse des menaces RSA, les trois clés méta suivantes sont remplacées :
  `risk.warning` est désormais `behavior of compromise (boc)`
  `risk.suspicious` est désormais `indicator of compromise (ioc)`
  `risk.informational` est désormais `enabler of compromise (eoc)`
- Lorsqu'un profil est sélectionné dans la vue Naviguer ou dans la vue Événements, la PreQuery pour le profil apparaît dans le fil d'Ariane.

Optimisation de la configuration des options de recherche. Le menu de paramétrage des options de recherche a été réorganisé pour faciliter la compréhension et le choix. Pour plus d'informations, consultez la section « Reconstruire la vue Naviguer et la vue Événements » du *Guide d'utilisation de NetWitness Investigate*.

Améliorations apportées au panneau Analyse de texte. Dans la vue Analyse d'événements, plusieurs améliorations traitent de la convivialité dans l'affichage des données.

- Les commandes de pagination des événements permettent une plus grande flexibilité pour parcourir la liste de événements.
- Si un événement reconstruit dans le panneau Analyse de texte comporte une requête ou une réponse dépassant le nombre maximal d'octets, l'en-tête indique que le message a été tronqué. Le maximum de données est fourni lors de l'affichage de l'analyse de texte d'un événement trop volumineux pour le rendu.

Gestion de la source d'événements

Identifier les sources d'événements inactives. Ce nouvel attribut affiche le nombre de jours écoulés depuis la dernière réception d'un journal à partir de chaque source d'événement. Vous pouvez utiliser cet attribut pour regrouper les sources d'événements inactives pendant une période spécifiée (par exemple, 90 jours), pour révision ou suppression en bloc.

Context Hub

Option d'importation ou d'exportation d'attributs. Les attributs dans le panneau de recherche contextuelle peuvent désormais être gérés afin d'aider les utilisateurs à afficher les attributs destinés aux détails de l'appareil RSA Archer. Vous pouvez configurer l'attribut d'intérêt à partir de l'application de l'appareil de RSA Archer et afficher ces attributs dans le panneau de contexte. Pour ce faire, vous pouvez exporter les attributs existants, ajouter le nouvel attribut et importer le jeu d'attributs mis à jour. Ces attributs sont reflétés dans l'ordre importé dans le panneau de recherche contextuelle lorsque vous affichez le contexte d'un incident ou d'un événement dans la vue Analyse d'événement. Pour plus d'informations, consultez le *Guide de configuration de Context Hub*.

Services implémentés avec NetWitness Server

Nouveau service de contenu. Le nouveau service de **contenu** gère les règles d'analyseur fournies par RSA et créées par l'utilisateur. Vous pouvez maintenant ajouter des règles d'analyseur dans l'interface utilisateur. Le service de contenu est utilisé dans l'onglet Règles des mappages de logs, qui est décrit dans la section Analyse des logs plus loin dans ce document.

Log et Network Decoder

Prise en charge des fichiers pcapng standard. Pour fournir un format de base de données plus ouvert, le Network Decoder peut maintenant écrire des fichiers au format pcapng standard. Cette fonctionnalité est activée par défaut si vous installez directement la version 11.2. Si vous effectuez une mise à niveau d'une version précédente vers la version 11.2, vous devez activer manuellement les fichiers de base de données au format pcapng, ce qui peut entraîner une diminution approximative de 4 % de l'espace disque (car les fichiers pcapng requièrent plus d'espace que les fichiers nwdb). Vous pouvez également utiliser le format pcapng avec une capture de 10 Gbps, ce qui ne diminue pas significativement les performances (< 1 %).

Pour activer le nouveau nœud de configuration :
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

Nouvel analyseur GeoIP2. Le nouvel analyseur GeoIP2 convertit les adresses IP en emplacements géographiques, fournit le dernier package MaxMind GeoIP et prend en charge les adresses IPv6, ainsi que IPv4. L'analyseur GeoIP2 lit à partir de `ip.src`, `ip.dst`, `ipv6.src` et `ipv6.dst` pour générer des informations GeoIP, et est activé dans Decoder par défaut. Pour plus d'informations, consultez la section « Analyseurs GeoIP2 et GeoIP » dans le *Guide de configuration de Decoder et Log Decoder*. .

Recherches GeoIP sur les métadonnées IPv4 IPv6. Vous pouvez maintenant effectuer des recherches GeoIP sur toutes les métadonnées IPv4 ou IPv6 afin de comprendre les informations géographiques dans les scénarios lorsque `ip.src` et `ip.dst` ne sont pas le point central de l'analyse.

- Il existe une nouvelle API Lua qui fournit aux analyseurs Lua un accès complet à toutes les informations GeoIP2. L'API Lua renvoie les informations demandées à partir de la base de données GeoIP2. L'analyseur est alors libre d'utiliser ces informations pour créer un méta ou pour effectuer sa propre analyse.
- Vous pouvez configurer l'analyseur GeoIP2 natif afin de générer des métadonnées GeoIP2 sur n'importe quelle clé IPv4 ou IPv6 à l'aide du nœud `configparsers.options`.

Pour plus d'informations, consultez la section « Analyseurs GeoIP2 et GeoIP » dans le *Guide de configuration de Decoder et Log Decoder*.

Hachage du certificat TLS. Le Network Decoder peut produire des hachages de certificats qui sont visibles dans le flux de paquets. Ces hachages sont la valeur SHA-1 de tout certificat codé DER rencontré lors d'une négociation TLS. Les données hachées sont écrites dans la clé `cert.checksum`. Les hachages produits peuvent être utilisés pour comparer le trafic réseau avec les hachages des listes noires SSL publiques. Pour plus d'informations, consultez « Hachage de certificat TLS » dans le *Guide de configuration de Decoder et Log Decoder*.

Interface utilisateur

L'onglet Règles des analyseurs de logs a été déplacé. L'onglet Règles des analyseurs de logs, situé dans ADMIN > Sources d'événements pour la version 11.1, a été déplacé vers CONFIGURER dans la version 11.2.

Ajout d'une prise en charge linguistique supplémentaire. Dans les Préférences utilisateur, il existe une nouvelle option Langue, qui vous permet de sélectionner une autre langue disponible. La langue sélectionnée modifie le texte sur la plate-forme NetWitness. Pour plus d'informations, reportez-vous au *Guide de mise en route de NetWitness Platform*.

Nouveau nom NetWitness. Le produit NetWitness 11.2 a été rebaptisé dans l'interface utilisateur, la documentation et d'autres occurrences pertinentes comme suit :

1. RSA NetWitness® Suite vers RSA NetWitness® Platform
2. RSA NetWitness® Packets vers RSA NetWitness® Network
3. Journaux et paquets RSA NetWitness® vers journaux et réseau RSA NetWitness®
4. Type d'hôte de paquet hybride vers type d'hôte réseau hybride
5. Type d'hôte Packet Decoder vers le type d'hôte Network Decoder
6. RSA NetWitness ® SecOps Manager à RSA Archer ® Réponse aux cyberincidents et failles de sécurité IT

Administration

Actions des menus contextuels configurables dans Procédure d'enquête. Les actions de clic droit disponibles dans Procédure d'enquête peuvent désormais être configurées à l'aide de l'interface utilisateur du menu contextuel Actions via divers champs et groupes. Vous pouvez créer de nouvelles actions de menu contextuel et les gérer à l'aide des actions du menu contextuel disponibles sous ADMIN > Système. Les actions du menu contextuel configurées à l'aide de l'interface utilisateur peuvent s'afficher sous la forme d'une action de clic droit sur les clés méta dans l'onglet Procédure d'enquête, sous les vues Naviguer, Événements et Analyse d'événements. Dans Analyse des événements, les actions de clic droit sont également prises en charge sur les clés méta.

Bannière de connexion améliorée disponible. La bannière de connexion dispose désormais d'un texte entièrement personnalisable et de mesures de sécurité accrues.

Analyse des logs

L'onglet Règles des analyseurs de logs a été amélioré. RSA a ajouté la possibilité d'étendre les analyseurs de journal existants, d'ajouter des analyseurs de journal personnalisés et de mettre à jour les règles d'analyseur de journal pour vos analyseurs de journal. Les règles d'analyseur de journal modifient la façon dont les métadonnées sont extraites des journaux des sources d'événements. Vous pouvez ajouter des règles d'analyseur de journal qui étendent les analyseurs de journal existants dans votre système, ainsi que l'analyseur de journal par défaut, qui extrait des données méta des messages qui pourraient autrement être répertoriés comme inconnus. Pour plus d'informations, consultez le *guide de personnalisation de l'analyseur de journal* disponible dans RSA Link. Concernant la version 11.1, les règles d'analyseur de journal étaient en lecture seule.

Instructions de la mise à niveau

Les stratégies de mise à niveau suivantes sont prises en charge par RSA NetWitness® Platform 11.2.0.0 :

- RSA NetWitness® Platform 10.6.6.x vers 11.2.0.0
- RSA NetWitness® Platform 11.0.x ou 11.1.x vers 11.2.0.0

Pour obtenir des informations détaillées sur les procédures de mise à jour vers la version 11.2.0.0, consultez les instructions de mise à jour de la section Installation et mise à niveau.

Problèmes résolus

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

Sécurité

Numéro de suivi	Description
ASOC-58379	Mise à jour de sécurité modérée CentOS 7 glibc https://access.redhat.com/errata/RHSA-2018:0805
ASOC-58373	Mise à jour de sécurité du noyau CentOS 7 https://access.redhat.com/errata/RHSA-2018:1629
ASOC-58376	Mise à jour de sécurité dhcp : https://access.redhat.com/errata/RHSA-2018:1453
ASOC-58374	Mise à jour de sécurité procps-ng https://access.redhat.com/errata/RHSA-2018:1700
ASOC-58381	Mise à jour de sécurité ntp https://access.redhat.com/errata/RHSA-2018:0855
ASOC-58384	Mise à jour de sécurité gcc https://access.redhat.com/errata/RHSA-2018:0849
ASOC-58380	Mise à jour de sécurité krb5 https://access.redhat.com/errata/RHSA-2018:0666
ASOC-50151	Mise à jour de sécurité openssh https://access.redhat.com/errata/RHSA-2018:0980
ASOC-58367	Mise à jour de sécurité openjdk https://access.redhat.com/errata/RHSA-2018:1649
ASOC-58377	Mise à jour de sécurité libvorbis https://access.redhat.com/errata/RHSA-2018:1058

Numéro de suivi	Description
ASOC-52448	Mise à jour de sécurité Authconfig https://access.redhat.com/errata/RHSA-2017:2285
ASOC-52439	Mise à jour de sécurité Libx11 https://access.redhat.com/errata/RHSA-2017:1865
ASOC-52443	Mise à jour de sécurité NetworkManager https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52444	Mise à jour de sécurité Bash https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52445	Mise à jour de sécurité Openldap https://access.redhat.com/errata/RHSA-2017:1852
ASOC-49815	Mise à jour de sécurité Systemd https://access.redhat.com/errata/RHSA-2018:0260

Problèmes généraux liés aux applications

Numéro de suivi	Description
ASOC-46483	Le système déconnecte les utilisateurs inactifs dans Répondre et certaines vues Enquêter

Enquêter

Numéro de suivi	Description
ASOC-51011	Trois nouveaux groupes de méta pour 11.0 et les mêmes groupes de colonnes pour 11.1 ne sont pas créés lorsque vous effectuez la mise à niveau à partir de 10.6.5 vers 11.x : RSA Endpoint Analysis, RSA Outbound HTTP, RSA Outbound SSL/TLS.
ASOC-50702	Après la mise à niveau vers 11.1, il existe des types de données non concordants entre le Log Decoder (table-map.xml) et les définitions du Concentrator (index-concentrator.xml).

Numéro de suivi	Description
ASOC-50924	Une requête directe ou une requête via Link qui utilise une valeur méta IPV6 avec des caractères spéciaux non pris en charge génère une erreur dans la vue Analyse d'événements et la vue Naviguer.
ASOC-50771	Si vous accédez à l'Analyse d'événement depuis la vue Événements, soit en cliquant sur le lien Analyse d'événement, soit en cliquant avec le bouton droit sur l'un des événements, les options de clic droit sur les valeurs de métadonnées ne fonctionnent pas.
ASOC-49854	Le sélecteur de service continue de charger indéfiniment.
ASOC-50712	Impossible d'ajouter des entités de métadonnées à un groupe de colonnes personnalisé dans la vue Événements lorsque l'option Optimiser les charges de la page Procédure d'enquête est désactivée.
ASOC-50349	Il est possible de créer des groupes de colonnes personnalisés contenant des entités méta dans la vue Événements, mais lorsque le groupe de colonnes personnalisé est utilisé dans la vue Analyse d'événement, vous ne voyez pas les clés méta comprises dans l'entité méta dans les résultats.
ASOC-50041	Lorsque vous cliquez avec le bouton droit sur une valeur méta qui contient un point-virgule dans la vue Analyse d'événements et essayez d'appliquer la recherche verticale dans un nouvel onglet de la vue Naviguer, un message d'erreur apparaît : Impossible d'élaborer la visualisation.
ASOC-45198	Lorsque vous modifiez l'URL et que la nouvelle URL concerne un événement restreint, le contenu reconstitué pour la requête précédente persiste dans la vue Analyse d'événement et aucun message d'erreur ne s'affiche.
ASOC-48945	Lorsque vous saisissez une requête dans une session à laquelle vous n'avez pas accès dans la vue Analyse d'événement, aucune donnée ne s'affiche et il n'y a aucun message d'erreur.
ASOC-48710	Lors de la procédure d'enquête dans la vue Analyse d'événement, le message d'erreur suivant est renvoyé : « Une erreur imprévue s'est produite. »

Répondre

Numéro de suivi	Description
ASOC-40749	L'administrateur Répondre ne peut pas interroger Enquêter ou afficher les dashlets Live dans le tableau de bord

Numéro de suivi	Description
ASOC-41891	Le lien Security Analytics Incident Management dans NetWitness SecOps Manager 1.3.1.2 n'est pas valide dans NetWitness Suite 11.1.0.0.
ASOC-46834	Impossible de sélectionner Domaine de C&C suspect et Domaine dans le générateur de règles
ASOC-50911	L'agrégation s'arrête après la reconnexion à Mongo
ASOC-51480	Les événements de point de terminaison avec une adresse IP de détecteur ne sont pas agrégés par la règle d'incident de point de terminaison et ne créent pas d'incidents avec la condition de correspondance de la règle d'incident par défaut actuelle. Consultez la rubrique « Configurer et vérifier les règles d'incident par défaut » dans le *Guide de configuration NetWitness Respond*.

Event Stream Analysis (ESA)

Numéro de suivi	Description
ASOC-50201	Lorsque vous déployez de nouvelles règles ESA à la vue Santé et bien-être et créez une nouvelle politique sous Analytique des flux d'événements à l'aide de la statistique Utilisation de la mémoire des règles ESA, toutes les règles ESA déployées ne sont pas répertoriées.

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.

Fonctions disponibles dans les prochaines versions

Les fonctions suivantes ne sont pas disponibles dans la version 11.2 et le seront dans les versions à venir.

Non.	Fonction	Remarques
1	Reporting IPDB	Le service IPDB Extractor n'est pas pris en charge dans la version 11.2.0.0 et le sera dans les versions ultérieures.

Non.	Fonction	Remarques
2	STIG	Si vous disposez d'un hôte renforcé STIG, vous ne pouvez pas effectuer une mise à niveau vers la version 11.2.0.0 car les scripts de sauvegarde ne prennent pas en charge cette fonction.
3	Prise en charge de plusieurs serveurs Security Analytics (NetWitness Server)	Le déploiement de plusieurs serveurs n'est pas prise en charge.
4	Authentification PKI	La fonction d'authentification PKI n'est pas disponible dans la version 11.2.0.0.
6	Analyse des points de terminaison	Les fonctions d'analyse comme la valeur de risque ou le calcul de l'IOC ne sont pas prises en charge sur les données d'analyse de point de terminaison
7	Correction du point de terminaison	Cette fonctionnalité Répondre (maîtrise/blocage) n'est pas prise en charge.
8	Suivi du point de terminaison	Le suivi des événements réseau n'est pas pris en charge.
9	Mode noyau du point de terminaison	L'agent du point de terminaison fonctionne actuellement en mode utilisateur et ne prend pas en charge le mode de détection noyau
10	Réputation de fichiers du point de terminaison	La réputation de fichiers, comme les recherches OPSWAT, YARA et Reversing Lab, n'est pas prise en charge et ne peut pas, par conséquent, mettre les fichiers sur liste blanche ou noire.

Problèmes connus

Cette section décrit les problèmes non résolus dans cette version. S'il existe une solution de contournement, elle est présentée ou référencée de façon détaillée.

Problèmes connus lors de la mise à niveau vers 11.2

Les problèmes connus suivants se produisent au cours de la mise à niveau de 10.6.6.x vers 11.2 ou de la mise à jour depuis la version 11.1 ou 11.1.x vers 11.2. :

Le feed récurrent STIX ne parvient pas à effectuer la mise à niveau depuis la version 10.6.6 vers 11.2

Numéro de suivi : ASOC-61227

Problème : Lorsque vous effectuez une mise à niveau depuis Security Analytics 10.6.6 vers NetWitness Platform 11.2, le feed récurrent STIX que vous avez créé à l'aide de l'URL HTTPS ne fonctionne pas. En effet, tous les certificats sont approuvés par défaut dans la version 10.6.x. Toutefois, cela n'est pas le cas dans la version 11.2. Dans la version 11.2, l'option Approuver tous les certificats est disponible, mais elle est désactivée par défaut.

Contournement : Accédez à Configurer > Feeds personnalisés et modifiez le feed défaillant. Activez l'option Tout approuver ou chargez un certificat SSL valide pour résoudre le problème. Pour toute autre question, contactez le service clientèle RSA.

Lors de la mise à niveau vers NetWitness Platform 11.2, les détails de licence ne sont pas conservés dans le Cloud AWS

Numéro de suivi : ASOC-61614

Problème : Lorsque vous effectuez une mise à niveau depuis Security Analytics 10.6.6 vers NetWitness Platform 11.2, l'identifiant du serveur de licence n'est pas conservé. Le serveur d'administration n'est donc pas en mesure d'obtenir les détails du serveur de licences auprès du système back-end externe, par conséquent les services ne peuvent être mis sous licence.

Contournement : Suivez les étapes indiquées dans la rubrique « Accès à Download Central » et « Inscription du serveur (en ligne) » dans le *guide de gestion des licences* pour obtenir les détails de la licence à partir du système principal externe et enregistrer le nouvel identifiant de serveur de licences.

Après la mise à niveau de 10.6.6 vers 11.2.0.0, les licences hors ligne ne sont pas conservées.

Numéro de suivi : ASOC-41757

Problème : Même si vous téléchargez un nouveau fichier bin de réponse à partir de Download Central, les licences hors ligne ne fonctionnent pas. Bien que les anciens fichiers soient restaurés dans `/var/lib/fneserver`, les licences restent désactivées.

Contournement : Effectuez les étapes suivantes pour restaurer les licences :

1. Générez un nouveau fichier bin de réponse à partir de Download Central.
2. Activez SSH sur un hôte du serveur de Netwitness 11.2.0.0 (AdminServer).
3. Déplacer des fichiers ra* (3 fichiers) hors de `/var/lib/fneserver/`
4. Connectez-vous à l'interface utilisateur de RSA NetWitness 11.2.0.0 avec des informations d'identification d'administrateur et accédez à **ADMIN** > **Système** > **onglet Détails de la licence**.
5. Cliquez sur **Actualiser les licences**.
6. Téléchargez le fichier de réponse obtenu auprès de Download Central. Accédez à **ADMIN** > **Système** > **Octroi de licence** > **Paramètres**
7. Cliquez sur **Télécharger la réponse**.

Remarque : la mise à niveau avec le mode en ligne (RSA Netwitness Suite 11.2.0.0 connecté à Internet) fonctionne correctement et toutes les licences sont restaurées après la mise à niveau vers 11.2.0.0.

Les liens de la Procédure d'enquête sont désactivés pour les graphiques statiques au cours de la post-mise à niveau de 10.6.6 vers 11.2

Numéro de suivi : ASOC-42136

Problème : Le lien Procédure d'enquête est désactivé pour le graphique statique (le résultat du rapport est au format graphique) qui possède la source de données en tant que NetWitness Suite-Broker (ce service est disponible par défaut).

Contournement : Il existe deux méthodes de contournement pour ce problème :

- Les règles qui contiennent le résultat dans le graphique statique sont consultables dans le format Tabulaire et la Procédure d'enquête fonctionne comme prévu.
- Vous pouvez également procéder comme suit pour résoudre le problème :
  1. Supprimez et rajoutez NetWitness Suite-Broker en tant que source de données au Reporting Engine portant le même nom.
  2. Si les rapports avec des graphiques statiques sont des rapports planifiés, lors de la prochaine exécution, le lien Procédure d'enquête fonctionnera comme prévu.
  3. Si le rapport est un rapport Ad hoc, réexécutez-le pour restaurer les liens de la procédure d'enquête.

Lors de la mise à niveau de 10.6.6 vers 11.2, le dashlet de géo-mappage ne peut pas être créé à l'aide d'un graphique (OOTB) préconfiguré.

Numéro de suivi : ASOC-41896

Problème : Lorsque vous effectuez la mise à niveau vers Netwitness Suite 11.2.0.0, le dashlet de géo-mappage ne peut pas être créé à l'aide d'un graphique préconfiguré. Cela se produit si un tableau de bord personnalisé utilise un dashlet de géo-mappage, qui est créé à l'aide d'un graphique préconfiguré.

Contournement : La source de données doit être mise à jour manuellement pour ce graphique préconfiguré dont l'utilisation est nécessaire dans le dashlet avec géo-mappage. Vous pouvez également créer un graphique à l'aide de la même règle préconfigurée et utiliser le nouveau graphique dans le dashlet avec géo-mappage.

Suite à la mise à niveau de la version 11.x vers 11.2, si vous avez utilisé l'analyseur entropique et l'indexation de charge utile, il vous faudra ajouter la balise bucket à l'index de fichiers afin que l'analyseur entropique puisse utiliser des buckets d'index.

Numéro de suivi : ASOC-45721

Problème : Lorsque vous effectuez la mise à niveau depuis la version 11.0 à la version 11.2, si vous avez utilisé l'analyseur entropique sur le Decoder (paquets uniquement) et procédez à l'indexation de la charge utile, vous devez ajouter la balise bucket à votre fichier d'index pour tirer parti de la nouvelle fonctionnalité de buckets d'index.

Remarque : Si vous effectuez une mise à niveau depuis la version 11.1 ou versions ultérieures vers la version 11.2, vous n'avez pas besoin d'effectuer cette modification.

Contournement : Ajoutez une balise de bucket au fichier d'index afin que l'analyseur Entropy puisse utiliser les buckets d'index, comme suit :

1. Dans le menu NetWitness Suite, sélectionnez **Administration** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez chaque service Concentrator qui agrège le trafic des Decoders.
3. Sous  (Actions), sélectionnez **Vue** > **Config** et sélectionnez l'onglet **Fichiers**.
4. Sélectionnez `index-concentrator-custom.xml file` et définissez la balise `bucket` sur `true` pour `payload.req` et `payload.res`. Par exemple :
   ```
   <key description="Payload Size Request" format="UInt 32"
   level="IndexNone" bucket="true" name="payload.req"
   valueMax="500000"/>
   <key description="Payload Size Response" format=UInt32"
   level="IndexNone" bucket="true" name="payload.res"
   valueMaz="500000"/>
   ```
5. Cliquez sur **Appliquer**.
6. Pour que les modifications prennent effet dans le fichier `index-concentrator-custom.xml`, vous devez redémarrer le service Concentrator :
   ```
   systemctl restart nwconcentrator
   ```

UEBA

Lorsque le proxy est configuré, et en cas de mises à jour, les détails de la licence ne sont pas actualisés automatiquement

Numéro de suivi : ASOC-52366

Problème : Lorsque le proxy est configuré, et en cas de mises à jour, les détails de la licence ne sont pas actualisés automatiquement, même après avoir cliqué sur le bouton Actualiser dans la vue Détails de la licence. En effet, la communication avec le serveur de licences n'est pas établie.

Contournement : L'administrateur doit télécharger manuellement les détails de la licence en mode hors connexion et charger les détails les plus récents de la licence via l'interface utilisateur de NetWitness Platform. Pour plus d'informations, consultez le *guide de gestion des octrois de licences*.

Point d'extrémité

Nginx rejette les requêtes POST dépassant la taille de la demande de 1 Mo

Numéro de suivi : ASOC-56236

Problème : Le serveur Nginx est mis à niveau et la taille de la charge utile par défaut est définie sur 1 Mo. Cela provoque l'échec de toute demande de données POST dépassant 1 Mo.

Contournement : Ajoutez le paramètre suivant au fichier de configuration Nginx (`/etc/nginx/conf.d/nginx.conf`) et redémarrez le serveur Nginx.

```
client_max_body_size 100M
```

La génération ou la copie du fichier *nwelcfg ne met pas à jour l'horodatage

Numéro de suivi : ASOC-49847

Problème : Après avoir installé l'agent Endpoint Insights, si l'administrateur souhaite mettre à jour une nouvelle configuration de collecte de logs via l'une des méthodes de copie ou l'outil de gestion Endpoint tiers, l'horodatage du fichier de configuration reflète l'heure du serveur Endpoint et non celle de l'agent. En conséquence, si l'agent Endpoint se trouve sur un fuseau horaire différent par rapport au serveur Endpoint, l'horodatage n'est pas mis à jour correctement.

Contournement : Après avoir copié le fichier de configuration, exécutez la commande sur l'agent Endpoint : `copy /b <filename.nwelcfg> +,,` dans le dossier %programdata%\NWEAgent\ à l'emplacement du fichier nwelcfg.

Répondre

Lorsque toutes les alertes sont supprimées pour une règle d'alerte, le filtre de la règle n'est pas correctement supprimé

Numéro de suivi : ASOC-59243

Problème : Dans la vue Liste des alertes (Répondre > Alertes), vous pouvez filtrer les alertes par nom d'alerte, puis supprimer toutes les alertes portant ce nom. Si vous ne supprimez pas le filtre de nom d'alerte après avoir supprimé les alertes, le filtre sera toujours en place la prochaine fois que la vue Liste des alertes sera chargé, mais il ne sera plus visible sous la forme d'une case à cocher dans le panneau Filtres, car toutes les alertes portant ce nom auront été supprimées. Vous continuerez de ne voir aucun résultat lorsque vous accéderez à la vue Liste des alertes.

Contournement : Avant d'actualiser ou de recharger la vue Liste des alertes, vous pouvez supprimer le filtre en désactivant la case à cocher en regard du nom de l'alerte. Si vous avez déjà actualisé ou rechargé la vue Liste des alertes, la seule façon de supprimer le filtre masqué est d'appuyez sur le bouton **Réinitialiser les filtres**, ce qui aura pour effet de supprimer tous les filtres, y compris le filtre de nom d'alerte masqué.

Les incidents ne sont pas marqués lorsqu'un utilisateur ajoute manuellement les alertes à un incident existant

Numéro de suivi : ASOC-52428

Problème : Les valeurs méta survolées sur les valeurs ne sont pas mises en surbrillance lorsque des alertes dans Répondre sont ajoutées à un incident manuellement. En revanche, les alertes ajoutées automatiquement ou dynamiquement à un incident s'affichent lorsqu'elles sont survolées.

Contournement : Aucun.

Le nom du fichier d'événement de malware comportant des caractères coréens ne s'affiche pas correctement dans la vue Répondre

Numéro de suivi : ASOC-40159

Problème : Si une alerte reçue de Malware Analysis comporte des caractères coréens, ils ne s'afficheront pas correctement dans la vue Répondre.

Contournement : Aucun.

Des règles ESA de gravité Élevée ou Faible ne pas générées dans l'interface utilisateur de RSA Archer

Numéro de suivi : ARCHER-47101

Problème : Lorsque les alertes ESA de gravité élevée ou faible sont transmises à RSA Archer, le champ Priorité d'alerte de sécurité n'est pas renseigné dans l'interface utilisateur RSA Archer.

Contournement : Aucun.

Les incidents et les tâches sont toujours disponibles lorsque l'intégration Réponse aux cyberincidents et failles de sécurité IT RSA Archer est activée.

Numéro de suivi : ASOC-39886

Problème : Après avoir activé l'intégration Réponse aux cyberincidents et failles de sécurité IT RSA Archer (NetWitness SecOps Manager) dans le service de serveur de réponse, tous les incidents sont gérés dans Réponse aux cyberincidents et failles de sécurité IT RSA Archer. Dans les versions précédentes, lorsque SecOps était activé, les incidents et les tâches de correction étaient masqués. Dans NetWitness Platform 11.0.0.x, les utilisateurs sont toujours en mesure d'accéder aux incidents et aux tâches dans la vue Répondre (RÉPONDRE > Incidents et RÉPONDRE > Tâches). Ils peuvent également créer des incidents dans NetWitness Platform. S'ils créent des incidents à partir de la vue Liste des alertes dans Répondre (RÉPONDRE > Alertes) ou à partir d'Enquêter, ces incidents ne parviendront pas à Réponse aux cyberincidents et failles de sécurité IT RSA Archer.

Contournement : Si vous avez activé l'intégration Réponse aux cyberincidents et failles de sécurité IT RSA Archer dans le service Serveur de réponse, n'utilisez pas les éléments suivants dans la vue Répondre : Vue Liste des incidents, vue Détails de l'incident et vue Liste des tâches. De plus, ne créez pas d'incidents dans la vue Liste des alertes de la vue Répondre ou dans Enquêter.

Pour les incidents migrés, le nombre d’événements affiche toujours 0 dans le volet Présentation

Numéro de suivi : ASOC-38026

Problème : Dans le champ Catalyseurs du panneau Vue d'ensemble des incidents, le nombre d'événements pour les incidents migrés affiche toujours 0 (zéro). Ce comportement est attendu dans NetWitness Platform 11.0.0.x et versions ultérieures. (Pour accéder au panneau Aperçu, accédez à Répondre > Incidents. Si vous cliquez sur un incident dans la Liste des incidents, le panneau Aperçu s'affiche à droite. Si vous cliquez sur un lien dans le champ ID ou NOM de la Liste des incidents, la vue Détails de l'incident s'ouvre avec le panneau Aperçu sur la gauche.)

Contournement : Aucun.

Les informations d'enrichissement de tableau dans la mémoire ne s'affichent pas pour les alertes ESA

Numéro de suivi : ASOC-37533

Problème : Vous ne pouvez pas afficher des enrichissements personnalisés pour les règles de corrélation ESA dans la vue Alertes de réponse.

Contournement : Aucun.

Les paramètres d'intégration de Réponse aux cyberincidents et failles de sécurité IT RSA Archer doivent être visibles dans l’interface utilisateur

Numéro de suivi : ASOC-25127

Problème : Les paramètres d'intégration pour l'envoi de tous les incidents à Réponse aux cyberincidents et failles de sécurité IT Archer (NetWitness SecOps Manager) doivent être exposés dans l'interface utilisateur

Contournement : L'interface utilisateur pour l'intégration partielle Réponse aux cyberincidents et failles de sécurité IT RSA Archer (NetWitness SecOps Manager) a été supprimée dans 11.0.0.x. Les administrateurs peuvent effectuer l'intégration dans la vue Explorateur pour le service de serveur Répondre.

Log Collector

FIPS est désactivé par défaut pour le service Log Collector

Numéro de suivi : ASOC-41841

Problème : FIPS est désactivé par défaut pour le service Log Collector, même si FIPS a été activé dans 11.2.0.0.

Remarque : Même si FIPS est activé dans 11.2.0.0., il est désactivé après la migration.

Contournement : Pour activer FIPS sur le service Log Collector, procédez comme suit :

1. Arrêtez le service Log Collector.
2. Ouvrez le fichier `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Modifiez la valeur de la variable suivante en **off** comme décrit ici :

   `Environment="OWB_ALLOW_NON_FIPS=on"`

   par

   `Environment="OWB_ALLOW_NON_FIPS=off"`
4. Rechargez le processus du système en exécutant la commande `systemctl daemon-reload`.
5. Redémarrez le service Log Collector.
6. Définissez le mode FIPS pour le service Log Collector dans l'interface utilisateur :

   Remarque : Cette étape n'est pas obligatoire en cas de mise à niveau, si FIPS a été activé sur 11.2.0.0.

   a. Accédez à **ADMIN** > **Services**.

   b. Sélectionnez le service Log Collector, puis accédez à **Vue** > **Config**.

   c. Dans le Mode SSL FIPS, cochez la case sous Valeur de configuration, puis cliquez sur **Appliquer**.

   Remarque : Pour activer Log Decoder et Packet Decoder, dans `/sys/config` définissez `ssl.fips` sur ON afin de redémarrer le service.

Enquêter

Les profils d'investigation importés ne s'affichent pas dans le menu déroulant Profils

Numéro de suivi : ASOC-61230

Problème : 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.

Contournement : Actualisez la fenêtre du navigateur pour voir les profils récemment ajoutés.

Dans la vue Analyse d'événement, les événements de journal et de réseau ne sont pas entrelacés

Numéro de suivi : ASOC-60941

Problème : 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'événement. Dans la vue Analyse d'événement, 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.

Contournement : Utilisez la vue Événements pour afficher les événements de réseau et de journal entrelacés.

Lorsqu'un PCAP volumineux est extrait de la vue Événements, s'il expire après 5 minutes, l'heure de la requête affiche 8 heures dans le message d'erreur de la barre des Tâches

Numéro de suivi : ASOC-60464

Problème : Lors de l'exportation d'un PCAP avec environ 100 000 sessions à partir de la vue Événements à l'aide d'Exporter > Exporter tous les PCAP, le téléchargement peut échouer en raison du délai d'appel des paquets de 5 minutes. Si l'appel expire, le message d'erreur dans la barre de tâches affiche un délai d'attente incorrect de 8 heures (28,8 millions ms).

Contournement : Aucun.

Les utilisateurs qui ne disposent pas des autorisations de serveur Investigate ne reçoivent pas de message d'erreur leur expliquant pourquoi ils n'ont pas accès à la vue Analyse d'événement

Numéro de suivi : ASOC-60366

Problème : Si l'administrateur n'a pas attribué une autorisation de serveur Investigate à un utilisateur, ce dernier devrait recevoir un message d'erreur lui refusant l'accès à une session dans la vue Analyse d'événement. Au lieu de cela, l'erreur de serveur interne s'affiche.

Contournement : Aucun.

Les valeurs méta Active Directory dans la vue Analyse d'événement, telles que le nom d'utilisateur, peuvent comporter des données de contexte disponibles, mais les valeurs méta ne sont pas soulignées en tant qu'indicateur

Numéro de suivi : ASOC-58853

Problème : Les analystes travaillant dans la vue Analyse d'événement ne verront pas un indicateur les informant que les métadonnées Active Directory disposent de l'enrichissement de contexte ; ils doivent pointer la souris sur une valeur méta Active Directory pour déterminer si un contexte lui est associé et ouvrir le panneau de recherche contextuelle.

Contournement : Pointez ou sélectionnez une valeur méta et cliquez sur le bouton **Afficher le contexte** pour déterminer s'il existe un contexte associé pour Active Directory.

Si l'URL d'un point d'extraction est très long et que vous utilisez la requête dans la vue de l'analyse des événements, une erreur (Erreur dans la requête 414) est renvoyée

Numéro de suivi : ASOC-50196

Problème : Plusieurs situations créent une très longue requête que le navigateur ne peut pas gérer, en particulier si vous utilisez Internet Explorer dont la limite de caractères est bien inférieure à celle de la plupart des navigateurs. Le fait de pivoter dans Analyse d'événements à partir de Reporting peut entraîner une requête de très longue, tout comme dans la vue Naviguer.

Contournement : Continuez de travailler dans la vue Naviguer ou Événements lorsque l'URL prend trop de temps dans la vue Analyse d'événements.

Le générateur de requête dans la vue Analyse d'événement ne répond pas aux filtres qui contiennent un espace

Numéro de suivi : ASOC-49427

Problème : Lors de l'ajout d'un filtre, si vous ajoutez un espace supplémentaire avant <meta key>, entre <meta key> et <operator>, et après <operator>, le générateur de requête ne répond plus et le bouton Interroger des événements est désactivé, et vous ne pouvez plus ajouter de filtres.

Contournement : Cliquez sur un filtre existant, puis cliquez sur le générateur de requête. Si cela ne fonctionne pas, actualisez la page.

Feeds personnalisés

L'état de la barre de progression du flux STIX est incomplet

Numéro de suivi : ASOC-40642

Problème : Dans certains cas, l'état de la barre de progression pour certains des flux STIX est incomplet même si les flux sont transférés avec succès au ou aux Decoders.

Contournement : Aucun.

Event Stream Analysis (ESA)

Les règles ESA CH sont désactivées pendant la mise à niveau ou le redémarrage de l'hôte ESA

Numéro de suivi : ASOC-60511

Problème : Si l'hôte ESA redémarre et que les règles Context Hub sont déployées sur ESA, les règles Context Hub peuvent être désactivées. Cela se produit à la suite d'une condition de concurrence entre l'ordre de démarrage des services Context Hub et Event Stream Analysis sur l'hôte ESA.

Contournement : Pour résoudre ce problème, effectuez l'une des actions suivantes :

- Accédez à l'onglet **CONFIGURER > Règles ESA > Services** et activez les règles désactivées qui dépendent de Context Hub.
- Redémarrez le service Event Stream Analysis.

Les règles ESA avec des données méta personnalisées ne se déploient pas sur le serveur ESA

Numéro de suivi : ASOC-60367

Problème : Si vous ajoutez de nouvelles clés méta personnalisées dans la version 11.2, les règles ESA utilisant ces clés méta risquent de ne pas être déployées. Cela se produit car le service Event Stream Analysis a besoin d'obtenir des informations auprès de Concentrator.

Contournement : Pour déployer une règle de corrélation ESA avec un méta personnalisé, procédez comme suit :

1. Ajoutez les clés non standard au fichier index-concentrator-custom.xml (ADMIN > Services > Sélectionner un Concentrator, puis sélectionner Actions > Vue > Config > onglet Fichiers).
2. Redémarrez Concentrator (ADMIN > Services > Sélectionnez un Concentrator, puis sélectionnez Actions > Redémarrer).
3. Assurez-vous que Concentrator est configuré comme source de données pour le service Event Stream Analysis (ADMIN > Services > sélectionnez le service Event Stream Analysis, puis sélectionnez Actions > Vue > Config > onglet Sources de données).
4. Redémarrez le service Event Stream Analysis (Actions > Redémarrer).
5. Assurez-vous que les nouvelles clés méta sont répertoriées dans les Références de clés méta (CONFIGURER > Règles ESA > onglet Paramètres > Références de clés méta).
6. Déployez la règle ESA avec un méta personnalisé.

Impossible de déployer la règle ESA avec méta de baie dans l'enrichissement

Numéro de suivi : ASOC-47584

Problème : Si un utilisateur configure une Table en mémoire en tant que Source d'enrichissement dans ESA, où une colonne du tableau présente le type String, une règle ESA est créée avec une condition de liste blanche et la colonne de liste de chaînes est mappée à une clé méta d'événement de baie de chaîne. Lorsque la règle est déployée, la règle est désactivée car la conversion de type de données de String[] à String n'est pas autorisée.

Contournement : Aucun.

Pour les règles ESA qui utilisent des sources d'enrichissement, l'option Ignorer la casse ne fonctionne pas pour la première instruction

Numéro de suivi : ASOC-49906

Problème : Lors de la création d'une règle ESA qui utilise une source d'enrichissement, si l'option Ignorer la casse est activée sur la première instruction d'enrichissement, aucun résultat n'est renvoyé. Notez que ce problème ne s'applique pas aux instructions qui viennent après la première instruction (c'est-à-dire, aux sous-instructions).

Contournement : Lorsque vous créez une nouvelle règle, l'option Ignorer la casse est maintenant désactivée. Pour les règles existantes dont l'option Ignorer la casse est activée pour une instruction d'enrichissement, l'option reste activée mais les utilisateurs sont invités à désactiver l'option lors de l'ouverture de la règle dans ESA, puis d'enregistrer la règle mise à jour.

Impossible de définir le niveau de compression ESA comme dans d'autres appliances

Numéro de suivi : ASOC-26481

Problème : Les administrateurs ne peuvent pas définir le niveau de compression dans ESA comme avec d'autres appliances, même avec la vue Explorer.

Contournement : Supprimez la source Concentrator d'ESA et ajoutez-la à nouveau afin que les changements au niveau de la compression soient pris en compte :

1. Supprimez la source de données Concentrator d'ESA. (Accédez à ADMIN > Services, sélectionnez le service Event Stream Analysis et dans le menu Actions, sélectionnez Vue > Config. Dans la vue Config, onglet Sources de données, supprimez la source de données Concentrator.)
2. Définissez le niveau de compression dans ESA. (Accédez à la vue Explorer, puis dans la liste de nœuds, accédez à Workflow/Source/nextgenAggregationSource et définissez CompressionLevel.)
3. Ajoutez de nouveau la Source de données Concentrator à ESA. (Revenez à la vue Config, onglet Sources de données et ajoutez la source de données Concentrator).

Le service Event Stream Analysis cesse de répondre lors de l'utilisation d'une agrégation basée sur une requête pour la détection automatisée des menaces pour les logs

Numéro de suivi : ASOC-25174

Problème : Event Stream Analysis peut cesser de répondre en raison d'une forte utilisation de ressources, et la configuration du script global (wrapper) doit peut-être être ajustée.

Contournement : vous devrez peut-être modifier les paramètres d'heure de la commande ping dans le fichier `wrapper.conf`. Effectuez les opérations suivantes :

1. Accédez à **Administration > Services > Event Stream Analysis> Explorer** et accédez au dossier **`/opt/rsa/esa/conf/`**.
2. Modifiez les paramètres avec les valeurs suivantes :
   `wrapper.ping.timeout=300`
3. Ajoutez les lignes suivantes à la fin du fichier :
   `wrapper.restart.delay=40`

```
wrapper.ping.timeout.action=RESTART
```

4. Redémarrez le service Event Stream Analysis.

ESA affiche des messages d'avertissement pour les opérateurs de baie

Numéro de suivi : ASOC-14157

Problème : lorsque vous écrivez une règle avancée, les opérateurs de baie, tels que « anyOf », échouent. Par exemple :

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

cette commande affiche une erreur similaire à la suivante :

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class
java.util.Vector
```

Contournement : pour effectuer une comparaison floue, convertissez d'abord la baie en chaîne. Par exemple :

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

Remarque : dans l'EPL, si vous avez utilisé des opérateurs de baie développés dans les versions 10.5, 10.5.0.1 et 10.6, vous devrez modifier l'EPL pour utiliser la solution de contournement ci-dessus.

Le déploiement échoue si le serveur qui héberge une base de données externe est défaillant

Numéro de suivi : ASOC-9011

Problème : vous configurez une connexion de base de données pour utiliser la base de données sous la forme d'une source d'enrichissement pour une règle. Une référence à la base de données est déployée sur chaque ESA, même si l'ESA ne déploie aucune règle qui utilise la base de données. Si le serveur qui héberge la base de données est défaillant, tout nouveau déploiement échoue.

Contournement : redémarrez le serveur qui héberge la base de données.

Reporting

Les options Masquer et Enquêter ne sont pas prises en charge dans les navigateurs Google Chrome ou Mozilla Firefox sur le système d'exploitation Windows 10

Numéro de suivi : ASOC-37590

Problème : Si vous utilisez les navigateurs Chrome ou Firefox sur un système d'exploitation Windows 10 et cliquez sur un point de données du graphique, les options Masquer et Enquêter ne s'affichent pas. Toutefois, ces options sont disponibles à l'aide du navigateur Internet Explorer.

Contournement : Désactivez la fonction tactile sur les navigateurs Chrome et Firefox. Pour désactiver cette option dans Chrome, procédez comme suit :

1. Accédez à - chrome://flags/ sur Firefox ou Chrome.
2. Sélectionnez l'option « Disabled » pour l'indicateur « Touch Events API ».
3. Redémarrez le navigateur.

Pour désactiver cette option dans Firefox, procédez comme suit :

1. Accédez à : « about:config ».
2. Cliquez sur « J'accepte le risque ».
3. Recherchez le « Nom de l'option » - « dom.w3c_touch_events.enabled ».
4. Saisissez 0 dans la colonne « Valeur ».
5. Redémarrez le navigateur.

Gestion de la source d'événements

La fenêtre Gérer les mappages d'analyseurs comporte un nom d'affichage vide pour les analyseurs de journal si la source d'événements a été créée manuellement

Numéro de suivi : ASOC-53914

Problème : Lorsque vous ouvrez la fenêtre Gérer les mappages d'analyseurs à partir d'ADMIN > Sources d'événements > vue Découverte, le nom d'affichage des sources d'événements mappées est vide pour les sources d'événements créées manuellement.

Contournement : Fermez la fenêtre d'adressage et rouvrez-la.

Les types ne sont pas tous affichés pour les adresses mappées automatiquement

Numéro de suivi : ASOC-48328

Problème : Si une nouvelle application est ajoutée à une source d'événement existante qui est automatiquement mappée, il se peut qu'il y ait un délai pour que ce type apparaisse dans Découverte de source d'événement et soit supprimé du mappage automatique.

Contournement : Aucun.

Le service SMS se bloque, en indiquant une erreur de mémoire insuffisante

Numéro de suivi : ASOC-62575

Problème : Le service SMS peut se bloquer sur les systèmes possédant un grand nombre de sources d'événements actives, lorsque ces derniers ne parviennent pas à suivre le rythme de traitement des messages de statistiques des journaux. Le message d'erreur suivant apparaît alors : **java.lang.OutOfMemoryError: Java heap space**.

Contournement : Si vous rencontrez ce problème, veuillez contacter le support RSA pour savoir comment résoudre ce problème.

Services de base

La case à cocher Mode SSL FIPS dans la vue Configuration des services doit être désactivée pour les Brokers, Concentrators et Archivers, étant donné que la modification de la valeur de la case à cocher ne désactive pas la mise en œuvre FIPS pour le service

Numéro de suivi : ASOC-41902

Problème : Dans la version 11.0.0.x ou versions ultérieures, Broker, Concentrator et Archiver sont toujours mis en œuvre avec FIPS et l'administrateur n'a pas la possibilité de basculer entre les modes FIPS et non FIPS. L'administrateur peut utiliser la case à cocher Mode SSL FIPS pour activer et désactiver le mode FIPS sur un Log Decoder, Packet Decoder ou Log Collector.

Contournement : Aucun.

Configuration de feed personnalisé - Option Avancée Fichier XML : erreur non valide pour plusieurs rappels méta

Numéro de suivi : ASOC-40867

Problème : Netwitness Platform ne prend pas en charge le chargement de feeds pour les fichiers XML lorsqu'il y a plusieurs rappels.

Contournement : La source ad hoc peut être téléchargée à l'aide de NwConsole, ou directement à l'aide de l'URL REST de Décoder. Cela n'est pas applicable au feed récurrent.

Documentation produit

Cette version est fournie avec la documentation suivante :

Documentation	URL d'emplacement
Documentation en ligne RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112
Instructions de mise à niveau de RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D
Listes de contrôle de la mise à niveau RSA NetWitness Platform 11.2	Liste de contrôle de la mise à niveau des hôtes virtuels pour la version 10.6.6.x vers 11.2) Liste de contrôle du Guide de la mise à niveau des hôtes physiques 10.6.6.x vers 11.2

Documentation	URL d'emplacement
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

Contacter le support client

Lorsque vous contactez le support client, 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.

Utilisez les informations de contact suivantes si vous avez des questions ou si vous avez besoin d'aide.

RSA Link	https://community.rsa.com dans le menu principal, cliquez sur **Mes dossiers**.
Tél.	+33 1 39 96 90 00, option 3
Contacts internationaux	http://france.emc.com/support/rsa/contact/phone-numbers.htm
Communauté	https://community.rsa.com/community/support
Support de base	Le support technique chargé de résoudre vos problèmes techniques est disponible de 8 h 00 à 17 h 00 heure locale, du lundi au vendredi.
Support amélioré	Le support technique est disponible par téléphone 24 heures sur 24, 7 jours sur 7, toute l'année pour des problèmes de gravité 1 et de gravité 2 uniquement.

Historique des révisions

Révision	Date	Description
1	15 août 2018	Version pour les opérations