RSA NETWITNESS® SUITE

Notes de mise à jour

pour la version 11.0.0.0

Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

Coordonnées

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

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, accédez à 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 présente les nouveautés et modifications introduites dans RSA NetWitness Suite 11.0.0.0, ainsi que les procédures de contournement des problèmes connus. Lisez ce document avant de déployer ou de mettre à niveau RSA NetWitness Suite 11.0.0.0.

RSA NetWitness Suite 11.0.0.0 intègre certaines des fonctionnalités clés de Security Analytics, ainsi que les outils de détection des menaces avancées pour permettre aux analystes, à tous les niveaux, de découvrir les menaces de sécurité et d'y répondre.

Nouveautés

RSA NetWitness Suite 11.0.0.0 offre des améliorations significatives au workflow des analystes, ainsi que des fonctions qui permettent aux analystes d'effectuer des recherches plus facilement à tous les niveaux d'expérience. Les administrateurs bénéficient d'une prise en charge améliorée, ainsi que de fonctions simplifiées de maintenance de services et d'hôtes. Netwitness Suite 11.0.0.0 comprend les nouvelles fonctions et améliorations suivantes.

Interface utilisateur

Navigation basée sur des rôles. L'interface utilisateur est divisée en cinq zones fonctionnelles principales : Répondre, Enquêter, Surveiller, Configurer et Administrateur, pour s'adapter aux rôles classiques du centre des opérations de sécurité. L'interface est mise à jour pour plus de modernité et pour améliorer le workflow pour les analystes et les chercheurs de cybermenaces. Pour plus d'informations sur la nouvelle interface de navigation et pour obtenir des conseils importants pour vous familiariser avec NetWitness Suite 11.0.0.0, reportez-vous au *Guide de mise en route de NetWitness Suite*.

Répondre

- **Amélioration de l'expérience des analystes**. NetWitness Suite 11.0.0.0 offre une nouvelle façon de gérer les incidents. Répondre remplace la Gestion des incidents de la version 10.6. Pour plus d'informations sur Répondre, reportez-vous au *Guide d'utilisation de NetWitness Respond*.
- **Nouvelle vue Répondre**. La vue Répondre aide les analystes et les responsables de la réponse aux incidents à comprendre la portée globale d'un incident et à identifier ces incidents de manière rapide et efficace.
- **Alertes consolidées**. Les analystes peuvent afficher toutes les alertes de menace reçues par RSA NetWitness Suite 11.0.0.0 dans un emplacement unique. Cela peut inclure des alertes comme les règles de corrélation ESA, la détection automatisée des menaces ESA, Malware Analytics et les alertes de reporting.
- **Liste d'incidents prioritaires**. La Liste des incidents présente aux analystes une file d'attente d'incidents par ordre de gravité pour faciliter le tri.
- **Ajouter des indicateurs associés à la demande**. Les analystes peuvent rechercher des indicateurs associés et les ajouter à un incident.

- **Suivre les tâches de l'incident jusqu'à la fin**. Les analystes peuvent créer des tâches au sein des incidents et gérer toutes les tâches à partir d'un emplacement central.
- **Collaborer avec d'autres analystes**. Les analystes peuvent publier des notes et examiner l'historique de l'activité sur un incident.
- **Scénario d'incident consolidé**. Une liste chronologique des indicateurs (alertes) affiche les événements et les enrichissements provenant de plusieurs sources de données.
- **Graphique de nœud interactif présentant des relations d'entité**. Vous pouvez effectuer une recherche verticale dans les détails d'hôte ou d'un utilisateur et pivoter vers la vue Enquêter pour exécuter une procédure d'enquête plus approfondie.
- **Informations contextuelles à la demande dans la vue Répondre**. Les analystes peuvent réduire le temps nécessaire pour la détection et la réponse à l'aide des informations contextuelles issues des sources de données telles que les listes, RSA Archer, Active Directory, RSA NetWitness Endpoint, les alertes, les incidents et Live Connect. Les analystes peuvent survoler des entités soulignées pour afficher des info-bulles de contexte. Ces info-bulles affichent un résumé rapide du type de données contextuelles disponibles pour l'entité sélectionnée et fournissent des liens vers d'autres actions d'enquête. Vous pouvez également accéder à un panneau de recherche contextuelle qui affiche des informations contextuelles plus détaillées pour l'entité sélectionnée.

Enquêter

- **Visibilité sur les données de point de terminaison**. Lorsque NetWitness Suite est configuré pour utiliser des données à partir de RSA NetWitness Endpoint, les analystes peuvent afficher les données de point de terminaison dans Enquêter. Grâce à cette amélioration, trois types d'événements (réseau, log et point de terminaison) sont exposés dans Enquêter, et tous les événements peuvent être analysés de la même manière. Pour plus d'informations, consultez le *Guide d'utilisation Enquêter et Malware Analysis*.
- **Analyse d'événements**. La fonction Analyse d'événements fournit aux analystes de nouvelles façons d'analyser les événements lors de la reconstruction d'un événement en tant que texte, paquet ou analyse de fichiers. Pour plus d'informations, reportez-vous à « Analyser les événements dans la vue Analyse d'événements » dans le *Guide d'utilisation d'Enquêter et de Malware Analysis*.

- **Fonctions d'analyse de paquets**.
  - Les attributs dans l'en-tête et le pied de page de paquet dans le format hexadécimal et ASCII sont mis en surbrillance en bleu ; lorsque vous placez le curseur sur un attribut mis en surbrillance, des informations supplémentaires s'affichent dans une zone de survol.
  - Les signatures de fichier courant sont mises en surbrillance avec un arrière-plan orange. Lorsque vous placez le curseur sur le texte en surbrillance, la description de la signature du type de fichier potentiel s'affiche dans une zone de survol.
  - Il existe quatre options pour le téléchargement : l'événement en tant que PCAP, toutes les charges utiles, les charges utiles de demande uniquement et les charges utiles de réponse uniquement.
  - Ombrage de caractères dans la charge utile du paquet pour distinguer les caractères hexadécimaux afin d'aider les analystes à trouver des modèles.
  - Possibilité d'afficher les charges utiles uniquement en supprimant les en-têtes et les pieds de page des paquets à partir de la restitution de l'événement.
- **Fonctions d'analyse de texte**.
  - Possibilité de télécharger un événement de log ou un point de terminaison dans plusieurs formats.
  - Affichez le codage et le décodage URL et Base64 dans une zone de survol lorsque le texte est sélectionné. Vous pouvez également copier le texte sélectionné.
  - Affichez le texte compressé ou non compressé pour une session de réseau HTTP.
  - Mettez en surbrillance les paires clé méta/valeur méta (non sensible à la casse) dans l'analyse de texte.
- **Fonctions d'analyse de fichier**. Lorsque vous téléchargez des fichiers, ils sont exportés en tant qu'archive zip protégée par un mot de passe. Le mot de passe par défaut est `netwitness`. L'exportation de fichiers sous cette forme garantit que l'archive ne sera pas mise en quarantaine par les logiciels antivirus. De plus, les fichiers potentiellement malveillants ne sont pas automatiquement ouverts par l'application par défaut et exécutés.

Reporting

- **Source de données par défaut pour les graphiques**. Les graphiques s'exécutent sur une source de données par défaut si la source de données n'est pas spécifiée. Par défaut, tous les tableaux de bord préconfigurés sont également exécutés sur la source de données par défaut, sauf si la source de données est spécifiée.
- **Reporting sur RespondDB**. Vous pouvez exécuter et afficher les rapports sur les données Répondre pour une meilleure visibilité au cours du processus de détection. Toutes les données clés d'alerte et d'incident sont disponibles dans la vue Répondre pour le reporting.
- **Syntaxe des règles NWDB de correction automatique**. Les analyseurs de base NWDB utilisent un parser Strict (attend une évaluation correcte de la syntaxe de requête), ce qui permet une validation stricte de la syntaxe des règles NWDB. Pour une expérience transparente de mise à niveau, les règles possédant une syntaxe non valide sont corrigées automatiquement lors de la première exécution après une mise à niveau. Pour plus d'informations, consultez le *Guide de Reporting pour la version 11.0*.

Tableaux de bord

- **Nouveaux tableaux de bord préconfigurés (OOTB)**. Les tableaux de bord préconfigurés apportent une valeur ajoutée immédiate aux responsables du SOC, aux analystes et aux administrateurs système, et sont disponibles dans le cadre de l'installation de NetWitness. Les tableaux de bord préconfigurés suivants ont été introduites dans cette version :
  - Procédure d'enquête
  - Opérations - Analyse de fichiers
  - Opérations - Analyse de protocole
  - Menaces - Indicateurs de programme malveillant
- **Fonctionnalité améliorée pour les tableaux de bord**. Les administrateurs peuvent créer et gérer des tableaux de bord en toute simplicité à l'aide de l'interface utilisateur intuitive :
  - Vous pouvez associer les valeurs principales de la procédure d'enquête et les dashlets de graphique en temps réel avec un tableau de bord connexe pour afficher des informations détaillées. Une option Afficher plus est disponible sur le dashlet sélectionné. Pour plus

d'informations, reportez-vous au *Guide de mise en route de NetWitness Suite*.

- Ajoutez un dashlet en tant que graphique de carte géographique pour obtenir un aperçu rapide de l'emplacement géographique. L'état du réseau et le trafic s'affichent. Les graphiques Geomap incluent des fonctions de zoom, de zoom arrière et d'exportation du graphique.
- Personnalisez l'aspect du tableau de bord en ajoutant, en supprimant et en réorganisant des dashlets.
- Activez ou désactivez des dashlets individuels en fonction de vos besoins.
- Filtrez les valeurs du graphique à partir du tableau de bord pendant 24 heures ou de façon permanente, si l'analyste souhaite masquer certaines valeurs évidentes pendant une durée spécifique pour se concentrer sur les autres valeurs.
- Configurez la mise en page du tableau de bord en sélectionnant les largeurs de dashlet disponibles (1/2, 1/3, 2/3, 1).
- Gérez les tableaux de bord en configurant le tableau de bord entier, modifiez les dernières heures et les paramètres d'intervalle d'actualisation.
- Affichez les dernières heures et les dernières informations actualisées pour le dashlet de graphique du rapporteur.
- Exportez ou importez des tableaux de bord avec les entités dépendantes dans un format .zip afin d'éviter l'importation ou l'exportation distincte de dépendances.

Live

- **Prise en charge du serveur TAXII**. Le serveur TAXII est pris en charge pour acquérir des informations sur les menaces mises en forme STIX dans NetWitness Suite. Les serveurs TAXII suivants sont qualifiés pour NetWitness Suite :
  - Hail a TAXII
  - Anomali Limo
  - Soltra Edge
  - OpenTAXII
- **Serveur activé SSL**. Vous pouvez activer le protocole de transfert SSL/TLS pour les serveurs TAXII et REST.

- **Nettoyage automatique des données TAXII**. Vous pouvez spécifier une période d'expiration, dans le champ Supprimer les données STIX antérieures à, afin que les packages STIX extraits du serveur TAXII et antérieurs à la période spécifiée soient supprimés de MongoDB. Cela limite le nombre d'indicateurs obsolètes dans Netwitness Suite.
- **Interface de catégorie améliorée**. Vous pouvez parcourir les catégories de contenu disponibles via Live pour voir le contenu disponible en fonction des exemples d'utilisation. Pour plus d'informations, consultez le *Guide de gestion des services Live*.

Event Stream Analysis et ESA Analytics

- **Ajout d'un nouveau service ESA Analytics (ESA Analytics Server)**. Il existe désormais deux services pouvant s'exécuter sur un hôte ESA :
  - Event Stream Analysis (règles de corrélation ESA)
  - Event Stream Analytics Server (ESA Analytics) Le service ESA Analytics est utilisé pour la détection automatisée des menaces. Pour plus d'informations sur la détection automatisée des menaces avancées, reportez-vous au *Guide de détection automatisée des menaces pour NetWitness Suite* et à la section « Configurer ESA Analytics » du *Guide de Configuration ESA*.
- **Les modules ESA Analytics préconfigurés ne nécessitent pas de connaissances des règles ESA**. La détection automatisée des menaces propose actuellement deux modules : Commande et Contrôle (C2) pour les paquets et C2 pour les logs.
- **Mappez tous vos modules ESA Analytics aux sources de données Concentrator depuis un emplacement central (ADMIN > Système)**. Les modules ESA Analytics sont configurés au niveau du système, afin que vous puissiez mieux gérer les déploiements et les mises à jour des mappages de module.
- **Les alertes se trouvent désormais dans la vue Répondre (RÉPONDRE > Alertes)**. La liste Alertes dans la vue Répondre affiche toutes les alertes et tous les indicateurs de menace reçus par NetWitness Suite. Vous pouvez filtrer la liste Alertes en fonction du type de source « Event Stream Analysis » pour afficher uniquement les alertes ESA. Pour les utilisateurs 10.6, la vue Alertes > Récapitulatif n'est plus disponible.
- **Ajout d'une nouvelle interface utilisateur pour configurer le service de recherche Whois (ADMIN > Système > Whois)**. Les analystes doivent configurer le service de

recherche Whois dans l'interface utilisateur de NetWitness Suite et non dans la vue Explorer. Une fois Whois configuré, il est disponible pour l'ensemble de vos modules ESA Analytics.

- **Les connexions de sources de données externes ESA nécessitent désormais TLSv1.2**. Pour des raisons de sécurité, les connexions internes et externes dans NetWitness Suite 11.0.0.0 exigent TLSv1.2. Si vous utilisez une source de données externes telle que MS SQL Server, MongoDB, MySQL ou Postgres pour vos données d'enrichissement (Configurer > Règles ESA > Paramètres), assurez-vous que votre serveur source de données est conforme TLSv1.2.

Services de base

- **Nouveaux services**. Les services suivants ont été introduits dans NetWitness Suite 11.0.0.0. Pour plus d'informations, consultez le *Guide des hôtes et services* :
  - **Serveur d'administration**. Le NetWitness Administration Server est le service back-end pour les tâches d'administration dans l'interface utilisateur NetWitness. Il permet d'extraire l'authentification, la gestion des préférences globales et la prise en charge de l'autorisation pour l'interface utilisateur.
  - **Serveur de configuration**. Le serveur de configuration NetWitness est chargé de stocker et de manipuler les collections de configuration. Une collection de configuration est un groupe de configurations logiques géré de manière indépendante.
  - **Serveur d'orchestration**. Le serveur d'orchestration NetWitness est responsable de la mise en service, de l'installation et de la configuration de tous les services qui constituent un déploiement NetWitness. Il permet d'extraire la logique de déploiement de plate-forme à partir des services NetWitness.
  - **Serveur de sécurité**. Le serveur de sécurité NetWitness gère l'infrastructure de sécurité d'un déploiement NetWitness. Il est responsable de tous les aspects de la sécurité, y compris :
    - Utilisateurs et comptes d'authentification
    - Contrôle d'accès basé sur les rôles
    - Le déploiement de l'infrastructure à clé publique (PKI)
  - **Serveur Enquêter**. Le serveur Enquêter de NetWitness est responsable de la

procédure d'enquête.

- **Serveur Répondre**. Le serveur Répondre remplace le service Incident Management.

- **Déchiffrement des paquets entrants vers un Decoder**. La commande `sslKeys` prend en charge le téléchargement de clés de cryptage privées dans un Decoder pour décrypter les paquets entrants avant l'étape d'analyse, afin que les parsers activés voient la charge utile du paquet non crypté et créent les données méta en conséquence. Pour plus d'informations, consultez le *Guide de configuration de Decoder et Log Decoder*.
- **Options de parser améliorées** : `decoder/parsers/config/parsers.option`. Ce nœud de configuration se compose d'une série de StringParams, où le parser reçoit une liste d'options en tant que paires nom = « valeur ». Le nouveau nœud de configuration est disponible pour le parser Entropy natif et les parsers Lua. Pour plus d'informations, reportez-vous au *Guide d'optimisation de base de données principale*.
- **Les parsers qui ne fournissent plus de valeur sont supprimés du Decoder**. Les parsers intégrés plus anciens décrits ci-dessous ont été retirés des Decoders.
  - Ces parsers natifs ont été supprimés des Decoders, car ils ne fournissent plus de valeurs : LotusNotes, MSN, SAMETIME, YMSG, AIM, Net2Phone, YCHAT et WEBMAIL.
  - Les parsers AIM natifs ont été supprimés, car AIM_Lua couvre cette fonctionnalité.
  - Le parser WebMail a été supprimé, car il n'est plus pertinent et WebMail est chiffrée ; il n'existe pas de remplacement de Lua. La fonction du parser WebMail consistait à capturer le code HTML depuis Gmail, Yahoo et Hotmail, et à extraire les métadonnées intéressantes. Les fournisseurs de ces applications WebMail modifient leur code HTML si souvent que le parser est inutile.
- **Nouveau parser Entropy natif**. L'analyseur Entropy analyse toutes les sessions réseau en mode natif sur le Decoder pour calculer les fonctionnalités liées à Entropy. Le résultat comporte plusieurs nombres qui indiquent si le trafic a été chiffré ou compressé, ou est conforme à une répartition des octets attendue. Entropy est une mesure du caractère aléatoire des données. Une valeur élevée Entropy d'une demande ou d'une réponse indique que le trafic est probablement chiffré ou compressé et qu'une session réseau tente de dissimuler des informations. Pour plus d'informations, consultez la section « Configuration du parser Entropy natif » dans le *Guide de configuration de Decoder et Log Decoder***.**
- **Réindexation de la base de données en arrière-plan pendant que le service de base est en ligne**. En fonctionnement normal, les modifications apportées à la configuration d'index sont uniquement appliquées aux nouvelles données qui entrent dans la collecte.

Reconstruire l'index sur toutes les données de la collecte est un processus qui prend du temps, car il nécessite la lecture de tout le stockage de la métabase de données sur le disque. À partir de la version 11.0.0.0, il est possible de reconstruire l'index lorsque le service de base est en ligne. Les services de la version 11.0.0.0 reconstruisent les index en arrière-plan chaque fois que le service détecte qu'une partie de la session et les métabases de données sont non indexées. Pour plus d'informations, reportez-vous au *Guide d'optimisation de base de données principale*.

- **Validation des fichiers de configuration d'index de service avant d'enregistrer ou de redémarrer**. Un contrôle strict des fichiers d'index pour valider tous les éléments et attributs est effectué lorsque les fichiers sont enregistrés et lorsque le service est démarré. Lorsque vous tentez d'enregistrer un fichier de configuration d'index qui n'est pas correctement formé, il est rejeté ; un message s'affiche dans l'interface utilisateur et le fichier n'est pas enregistré. Un contrôle strict se produit également lorsqu'un service est démarré. Toutefois, pour éviter les problèmes de mise à niveau à partir de la version 10.x, les erreurs sont consignées en tant qu'avertissements. Si vous tentez de modifier un fichier d'index avec des avertissements consignés à partir de l'interface utilisateur, l'enregistrement du fichier d'index sera annulé jusqu'à ce que les problèmes aient été résolus.
- **Nouvelles statistiques d'utilisation du CPU de contenu.** À compter de cette version, le Decoder fournit des statistiques d'utilisation de CPU pour tout le contenu installé. Les nouveaux moniteurs d'utilisation du CPU révèlent le temps CPU utilisé par les parsers, les feeds, les règles d'application et l'analyse lexicale. Les statistiques apparaissent sous forme de nœuds Statistiques dans l'arborescence des services de la vue Explorer lorsque `/decoder/parsers/config/detailed.stats` est activé et que le Decoder capture les statistiques. Chaque élément de contenu est comptabilisé comme une valeur unique en pourcentage (0-100), quel que soit le nombre de threads d'analyse en cours d'exécution. Le pourcentage représente une moyenne mensuelle de l'utilisation du CPU pour le contenu sur tous les threads.
- **Amélioration de la capacité RBAC**. Dans RSA Security Analytics version 10.6, Role-Based Access Control (RBAC) pour la commande `/sdk packets` était soit activé, soit désactivé, par l'utilisateur. Les utilisateurs avec un accès restreint n'ont généralement plus d'accès. La génération de fichier pcap à partir d'Investigation n'était donc pas autorisée, même pour les sessions qui n'avaient pas de restrictions. Dans RSA NetWitness Suite 11.0.0.0, RBAC fonctionne uniquement pour les paquets. Les sessions qui sont restreintes seront simplement ignorées pendant la génération de fichier pcap dans

Procédure d'enquête. Des paquets seront renvoyés dans les sessions qui sont autorisées. Pour plus d'informations sur RBAC, reportez-vous à la rubrique *Guide de la sécurité du système et de la gestion des utilisateurs*.

- **Nouvelle possibilité pour analyser les sessions Web compressées**. Les Decoders peuvent effectuer une analyse supplémentaire des sessions HTTP avec la langue de parser Lua. Les parsers Lua peuvent demander la décompression d'instances individuelles de compression dans une session HTTP. Il s'agit d'une fonction similaire fournie avec les parsers Flex précédents.
- **Gestion de l'expiration améliorée pour les expirations de délai de requête**. Modification du comportement d'expiration par défaut pour toutes les requêtes RESTful sur illimité, afin que les mécanismes d'annulation de requête normaux gèrent l'expiration. Avec une expiration de session REST API supprimée, l'expiration soumise par le paramètre `query.timeout` dans la session de l'utilisateur sera le facteur déterminant pour l'expiration du délai de requête.
- **Capture Decoder de VLAN sur plusieurs interfaces réseau à l'aide de packet_mmap**. Possibilité de sélectionner un sous-ensemble d'interfaces de capture en ajoutant la configuration pour le paramètre de configuration `/decoder/config/capture.device.params` Pour plus d'informations, consultez la section « Configurer les paramètres de capture » dans le *Guide de configuration de Decoder et Log Decoder*.
- **Capture de paquets à partir de F5 BIG-IP VE dans AWS**. Lorsque vous déployez un Decoder pour la capture de réseau Cloud, l'administrateur peut configurer des Decoders pour acquérir les données du réseau à partir de l'infrastructure Cloud d'AWS à l'aide de F5 BIG-IP Virtual Edition.
- **Comparaison de clé méta dans les règles d'application**. Les règles d'application dans les Decoders peuvent comparer les valeurs des différentes clés méta dans une session. Les clés méta peuvent désormais être utilisées sur le côté droit des opérateurs binaires. Les opérateurs pris en charge incluent les opérateurs relationnels (`=, !=,<, <=, >, >=`) ainsi que `contains`, `begins`, `ends`, `count`, `ucount` et `length`. Pour plus d'informations, consultez la section « Syntaxe des règles de capture » dans le *Guide de configuration de Decoder et Log Decoder*.
- **Amélioration de langage de règle et de requête pour les plages de temps relatives**. Les points de temps relatifs permettent à une clause `where` de référencer une valeur avec un décalage fixe, par rapport aux premiers ou derniers éléments méta vus dans la

collection. Pour plus d'informations sur les changements de syntaxe de requête, reportez-vous au *Guide d'optimisation de base de données principale*.

- **Indexation de texte de log améliorée**. Le niveau de base de l'analyse de log est défini de sorte que le texte de tous les logs non analysés soit analysé afin de rechercher ces éléments d'entité clé, même si aucun parser n'est activé : horodatage syslog, horodatage RFC 3339, adresses IP, adresses e-mail, composants d'URL et noms de domaine. Tout ce qui peut être raisonnablement identifié en tant que ces types de données est automatiquement marqué avec l'élément méta approprié.
- **Possibilité de reconstruire le flux réseau à partir de plusieurs sessions**. Améliore la combinaison de sessions fractionnées. Le Decoder assure le suivi du flux réseau tant qu'il dispose de ressources de mémoire suffisantes. Par conséquent, lorsque plus de paquets arrivent sur le même flux réseau, le Decoder ajoute des éléments méta divisés aux sessions ultérieures. À l'aide d'une combinaison de méta divisées et de la clé du flux, il est possible de reconstituer le flux réseau à partir de plusieurs sessions.

Sécurité

- Prise en charge supplémentaire pour les autorités de certification intermédiaire.
- Conditions de sécurité améliorées
- Le mode FIPS est activé par défaut sur tous les services à l'exception du Log Collector et du Log Decoder. Le mode FIPS ne peut pas être désactivé sur tous les services sauf Log Collector, Log Decoder et Decoder.
- Les modules cryptographiques certifiés FIPS 140-2 sont activés pour tous les services qui exécutent des opérations cryptographiques. Pour les services suivants, bien que le Module cryptographique FIPS soit utilisé, l'utilisation de suites de chiffrement FIPS n'est pas appliquée :
  - NTP : Port UDP 123
  - TCP : Port SSH 22
  - TCP : Port Loopback API Salt 8000
  - CollectD
  - Log Collector
  - Log Decoder

Remarque : Par défaut, les périphériques de base qui n'étaient pas en mode de mise en application FIPS dans la version 10.6.4 ne seront pas en mode de mise en application FIPS dans la version 11.0.0.0 après une mise à niveau. Cette opération affecte les services Log Decoder, Log Collector et de paquet Decoder.

Plate-forme

- **Configuration Decoder 10G simplifiée**. Vous pouvez installer le Decoder et les RPM pfring séparément et dans n'importe quel ordre. L'ordre dans lequel les RPM sont installés n'a aucune importance. Le Decoder peut localiser l'adaptateur 10G et démarrer la capture.

Administration

- **Amélioration des performances et évolutivité** de NetWitness Suite avec les améliorations suivantes :
  - Hôte et fourniture de service plus rapides.
  - Capacités de référentiel YUM externe qui offrent la possibilité d'installer rapidement le logiciel.
  - Les services tiers et NW ont été dissociées pour fournir des options de scale-dans les prochaines versions.
- **Simplification du processus de création et de gestion des services et des hôtes.** Ajout de la possibilité de provisionner les hôtes simultanément à partir de la ligne de commande ou de l'interface utilisateur.
- **Prise en charge pour les référentiels YUM gérés en externe**. Prise en charge pour les référentiels YUM gérés en externe.

Analyse des logs

Découverte de source d'événement. La découverte de source d'événement améliore la précision d'analyse de log et fournit un workflow pour détecter et corriger les sources d'événements non découvertes correctement ou complètement, comprenant :

- Liste unique et centralisée de toutes les sources d'événements
- Détails de chaque source d'événement
  - Types de sources d'événement découverts
  - Probabilité que le type de source d'événement ait été correctement identifié

  - Permet aux administrateurs de trouver les sources d'événements posant problème
- Détails de chaque source et type d'événement
  - Logs pour chaque type de source d'événement
  - Attributs importés ou définis
  - Permet à l'administrateur de déterminer si la source d'événement est correcte
- Possibilité d'accuser réception ou de définir les types de sources d'événement corrects
- La boîte de dialogue Gérer les mappages de parser permet aux administrateurs de mapper les parsers appropriés de manière centralisée pour les adresses IP sélectionnées.

Context Hub

- **Introduit de nouvelles sources de données**
  - **RSA Archer**. Les données de degré de criticité de ressources de RSA Archer sont utilisées afin de hiérarchiser les événements de sécurité en fonction de l'impact sur l'entreprise, et afin d'atténuer les menaces les plus dommageables. L'analyste peut agir en fonction du degré de criticité. Pour plus d'informations, consultez le *Guide de configuration de Context Hub*.
  - **Active Directory**. Les informations d'identité à partir d'Active Directory sont utilisées par un analyste pour accélérer la détection et la réponse pour un utilisateur sélectionné. Ces informations peuvent être utilisées pour mener une procédure d'enquête plus approfondie sur un utilisateur.
  - **Listes à plusieurs colonnes**. Les analystes peuvent afficher les informations contextuelles lorsqu'une liste est configurée en tant que source de données. Par exemple, si l'analyste possède une liste d'adresses IP sur liste noire, elle peut être configurée en tant que source de données de liste à une colonne ou à plusieurs colonnes. Puis, les données contextuelles pour les données importées peuvent être récupérées et affichées dans les vues Répondre et Enquêter. D'autres actions peuvent ensuite être effectuées en fonction.
- **Indicateur de contexte à la volée**. Un bref récapitulatif des données contextuelles pour permettre à un analyste de sélectionner les méta pour approfondie la procédure d'enquête dans la vue Nodale et Événements de la vue Répondre. Cette option est disponible lorsqu'un utilisateur survole la méta spécifique. Elle permet à l'analyste de pivoter vers Enquêter, Pivoter vers le point de terminaison et Ajouter à la liste/supprimer de la liste.

- **Panneau Recherche contextuelle**. Les informations contextuelles des sources de données configurées s'affichent pour permettre aux analystes d'exécuter d'autres actions de procédure d'enquête.
- **Recherche de domaine et de hachage de fichier**. Un analyste peut effectuer une recherche pour trouver des domaines et des hachages de fichier dans Context Hub, en plus des adresses IP, afin d'obtenir un context étendu sur différents types d'indicateur lors d'une procédure d'enquête.
- **Balises d'indication des risques**. En plus de la recherche Live Connect, l'analyste peut obtenir des informations de risque étendues (Évaluation des risques et Motif du risque). Cela inclut le niveau de risque d'un indicateur, ainsi que le motif de l'évaluation en cours. En outre, de nouveaux attributs sont disponibles pour chaque type d'indicateur :
  - Adresse IP
    - Identité (ASN, pays enregistré et entreprise)
    - Fichiers et domaines connexes
  - Domaine
    - Identité (informations WHOIS : nom de l'abonné, entreprise, adresse, e-mail, etc.)
    - Adresses IP et fichiers associés
  - Hachage de fichier
    - Identité (nom de fichier, taille, description, MD5, SHA1 et date/heure de dernière modification)
    - Informations sur le certificat (émetteur, date de début et date d'expiration, informations sur la signature, objet, etc.).
    - Adresses IP et domaines connexes
- **Commentaires d'évaluation des risques Live Connect**. Un analyste peut fournir des commentaires en fonction de son niveau de hiérarchie, de sa confiance et des indicateurs de risque. En outre, il peut fournir des commentaires détaillés sur un indicateur dans Live Connect. L'évaluation se compose de : Balises d'indicateur de risque (contexte sur la raison pour laquelle un indicateur est suspect), confiance, état du risque et niveau d'analyste (pour fournir du contexte sur la manière dont un indicateur a été découvert ou diagnostiqué). Pour plus d'informations, reportez-vous au Guide d'utilisation de NetWitness Respond.

Notes de mise à niveau

Les stratégies de mise à niveau suivantes sont prises en charge par RSA NetWitness Suite 11.0.0.0 :

- RSA NetWitness Suite 10.6.4.x vers 11.0.0.0

Pour obtenir des informations détaillées sur les procédures de mise à jour vers la version 11.0.0.0, consultez les instructions de mise à jour de la section Documentation produit.

Problèmes résolus

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

Correctifs relatifs aux serveurs

Numéro de suivi	Description
SATCE-1477/ASOC-24080	Les paramètres de bascule de CEF Parser sont effacés lors de la modification des paramètres d'analyseur dans l'interface utilisateur
SACE-7121/ASOC-30636	Des feeds personnalisés incluant du contenu CSV ne correspondent pas aux valeurs de métadonnées et les guillemets ne s'affichent pas correctement.

Correctifs relatifs à l'intégrité

Numéro de suivi	Description
ASOC-9225	Erreur de page qui ne s'affiche pas dans le navigateur Internet Explorer 10 lors de la connexion
SACE-6720	Tous les filtres sont supprimés sur la page Surveillance

Correctifs relatifs au Log Collector

Numéro de suivi	Description
SAENG-2476	Des messages d'erreur récurrents sont affichés si le nom de domaine n'est pas résolu dans la zone LWCS
ASOC-9586	Message inexact généré en cas d'erreur liée à la Collection AWS
ASOC-26826	La configuration du filtre de collecte des fichiers ne fonctionne pas

Correctifs relatifs à Event Stream Analysis

Numéro de suivi	Description
ASOC-6633	Configuration des règles d'évaluation : Les valeurs hors limites sont plafonnées

Correctifs relatifs aux services Core

Les services Core comprennent les services Broker, Concentrator, Decoder et Log Decoder.

Numéro de suivi	Description
ASOC-18044	Les flux Metacallback ne prennent pas en charge les plages d'index (plage d'adresses IP ou CIDR)

Fonctions non prises en charge

Les tableaux suivants fournissent des informations sur les fonctions qui ne sont plus prises en charge dans RSA NetWitness Suite 11.0.0.0 ou versions ultérieures.

Fonctions non prises en charge dans les versions 11.0.0.0 ou ultérieures

N°	Fonction	Remarques
1	Malware Colo	Malware Colo n'est pas pris en charge dans les versions 11.0.0.0 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 sur des Decoders	Warehouse Connector n'est pas installé par défaut sur les Decoders et les Log Decoders. Warehouse Connector doit être installé et configuré après la configuration du Decoder.
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. La modification de la bannière de connexion n'est pas prise en charge. 4. Utilisateur de test/recherche AD.
5.	Pivotal	Pivotal n'est pas pris en charge. HortonWorks est pris en charge.

Fonctions disponibles dans les prochaines versions

Les fonctions suivantes ne sont pas disponibles dans la version 11.0.0.0 et le seront dans les versions à venir.

N°	Fonction	Remarques
1	Reporting IPDB	Le service IPDB Extractor n'est pas pris en charge dans la version 11.0.0.0 et le sera dans les versions ultérieures.
2	STIG	Si vous disposez d'un hôte renforcé STIG, vous ne pouvez pas effectuer une mise à niveau vers la version 11.0.0.0 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 11.0.0.0
5	Warehouse Analytics	Warehouse Analytics n'est pas pris en charge dans la version 11.0.0.0 et le sera dans les versions ultérieures.

Problèmes connus

Cette section décrit les problèmes non résolus dans cette version. S'il existe une procédure de contournement ou un correctif, ils sont présentés ou référencés de façon détaillée.

Problèmes connus lors de la mise à niveau vers 11.0.0.0

Les problèmes connus suivants se produisent au cours de la mise à niveau de 10.6.x à 11.0.0.0 :

Après la mise à niveau de 10.6.4.x vers 11.0.0.0, 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 toujours 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. Connectez-vous à Netwitness Server 11.0.0.0 (AdminServer).
3. Déplacer des fichiers ra* (3 fichiers) hors de `/var/lib/fneserver/`
4. Connectez-vous à l'interface utilisateur de RSA NetWitness 11.0.0.0 avec des informations d'identification d'administrateur et accédez à Admin > Système > onglet Tour d'horizon de l'attribution de licence.
5. Sous le menu Actions d'attribution de licence, cliquez sur Actualiser les licences.
6. Puis, téléchargez le fichier de réponse reçu depuis Download Central sous Admin > Système > Attribution de licence > onglet Paramètres > Télécharger la réponse.

Remarque : la mise à niveau avec le mode en ligne (RSA Netwitness Suite 11.0.0.0 connecté à Internet) fonctionne correctement et toutes les licences sont restaurées après la mise à niveau vers 11.0.0.0

Les attributs d'utilisateur ou de rôle pour limiter l'accès aux données via le préfixe de requête ne sont pas pris en charge

Numéro de suivi : ASOC-42734

Problème : Si vous avez configuré des attributs d'utilisateur ou de rôle pour limiter l'accès aux données via le préfixe de requête dans 10.6.4.x et effectuez la mise à niveau vers 11.0, l'opération échoue...

Contournement : Vous devez appliquer le correctif RSA NetWitness Suite 11.0.0.1 pour résoudre cette situation.

Une fois la mise à niveau vers 11.0 effectuée, les utilisateurs configurés avec Active Directory ne seront pas en mesure de se connecter à l'interface utilisateur de Netwitness Suite

Numéro de suivi : ASOC-42738

Problème : Si vous avez des utilisateurs Active Directory configurés pour les connexions d'utilisateur externes dans 10.6.4.1 ou version antérieure et effectuez la mise à niveau vers 11.0, ces utilisateurs ne seront pas en mesure de se connecter à l'interface utilisateur de Netwitness Suite.

Contournement : Exécutez l'une des étapes suivantes :

- Appliquer le correctif 10.6.4.2 avant de passer à la version 11.0.0.0.
- Si, pour une raison quelconque, le correctif 10.6.4.2 n'est pas appliqué, appliquez le correctif 11.0.0.1, puis effectuez la migration de l'authentification externe.

Échec de la connexion utilisateur

Numéro de suivi : ASOC-43523

Problème : Les utilisateurs ne peuvent pas se connecter à l'interface utilisateur de NetWitness Suite lors de l'installation de 11.0.0.0 ou de la mise à niveau vers 11.0.0.0. En effet, l'interface utilisateur ne peut pas récupérer les informations du compte utilisateur à partir de MongoDB.

Contournement : Vous devez appliquer le correctif RSA NetWitness Suite 11.0.0.1.

Après la mise à niveau vers 11.0.0.0, aucune nouvelle source d'événements ne peut pas être ajoutée dans un déploiement de mode mixte.

Numéro de suivi : ASOC-41867

Problème : lorsque vous mettez à niveau vers 11.0.0.0 et vous connectez aux Log Collectors 10.6.4, les connexions de test échouent sur l'interface utilisateur Modifier. C'est parce que l'interface utilisateur convertit la valeur de Date de début de collecte (int) au format de date de chaîne « 1970-01-01 00:00:00 ». Vous continuerez à collecter des événements à partir de la source d'événement existante, mais ne serez pas en mesure d'ajouter une nouvelle source d'événement. Toutefois, en cas de connexion de test en masse, toutes les valeurs sont extraites directement à partir de l'interface REST et « Test de connexion » est transmis avec succès.

Contournement : Utilisez l'interface REST pour ajouter une nouvelle source d'événement dans un mode mixte.

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 10.6.4.

Remarque : Même si FIPS est activé dans 10.6.4, 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 10.6.4.

   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 le paquet Decoder, dans `/sys/config`, définissez `ssl.fips` sur ON et redémarrez le service.

Les liens Procédure d'enquête sont désactivés pour les graphiques statiques

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 n'existe aucun 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 obtenir les liens de la procédure d'enquête.

Erreur d'installation sur la post-orchestration de l'interface utilisateur de Warehouse Connector ou mise à jour de 11.0 à 11.0.0.1 pour une instance de Log Collector/Log Decoder

Problème : Sur une instance de Log Collector/Log Decoder, lorsque que WC est orchestré ou s'il est mis à jour

de 11.0 à 11.0.0.1, l'état En échec peut s'afficher dans la console et une erreur d'installation

s'affiche dans l'interface utilisateur.

Contournement : Pour obtenir des instructions sur la façon de résoudre ce problème, reportez-vous à l'article de base de connaissances

suivant : https://community.rsa.com/docs/DOC-84635.

Warehouse Connector n'est pas installé sur les Decoders

Problème : Warehouse Connector n'est pas installé par défaut sur les Decoders.

Contournement : Si, après une mise à niveau, il est nécessaire d'rétablir une connexion Warehouse, un utilitaire permettant de réinstaller le service est fourni. L'utilitaire est déployé pendant la phase d'amorçage. Pour installer Warehouse Connector, vous devez exécuter la commande suivante et spécifier l'hôte par ID (--host-id), nom (--host-name) ou adresse (--host-addr). La version la plus récente disponible sera installée par défaut, sauf si une version spécifique est spécifiée avec --version. Pour installer Warehouse Connector sur un hôte, exécutez la commande suivante sur le serveur d'administration :

```
[root]warehouse-installer --host-id <uuid of the host>
Details about the command:
Location: /usr/bin
Utility Name: warehouse-installer
```

Usage :

```
[root@nw11pds5 bin]# warehouse-installer --help
Warehouse Connector Installer
warehouse-installer [options]
Install options:
--host-id <id> Specify host to install (by ID)
--host-name <name> Specify host to install (by name)
--host-addr <address> Specify host to install (by address)
--version <#.#.#.#> Install version (defaults to latest)
General options:
```

```
-v, --verbose Enable verbose output
```

Clés méta pour la procédure d'enquête et la recherche ajoutées au fichier Concentrator Index par défaut.

Numéro de suivi : ASOC-22338, ASOC-22895, ASOC-19406

Problème : Si vous avez ajouté les clés méta suivantes en tant que clés personnalisées à votre fichier index-concentrator-custom.xml, elles peuvent être supprimées après la mise à niveau et sont désormais des clés méta standard dans le fichier index-concentrator.xml. Les clés méta sont : direction, netname, ioc, eoc, boc, analysis.file, analysis.session, analysis.service, inv.category, inv.context.

Contournement : Supprimez les clés répertoriées dans le fichier index-concentrator-custom.xml.

Tableaux de bord en double pour les indicateurs de menace.

Numéro de suivi : ASOC-41701

Problème : Le tableau de bord, Threat-Indicators, a été mis à jour pour générer des rapports par rapport aux nouvelles clés méta de recherche et a été renommé Threat-Malware Indicators. Lors de la mise à niveau, ils s'affichent tous deux dans l'interface utilisateur au lieu de l'ancien remplacé.

Contournement : Activez les graphiques de rapport Threat-Malware Indicators et le tableau de bord, et désactivez l'ancien tableau de bord Threat-Indicators.

Lors de la mise à niveau, les politiques personnalisées Intégrité pour le serveur Context Hub ne sont pas disponibles.

Numéro de suivi : ASOC-41826

Problème : Lorsque vous effectuez une mise à niveau vers Netwitness Suite 11.0.0.0, les politiques personnalisées Intégrité configurées pour le serveur Context Hub ne seront pas disponibles.

Solution de contournement : vous devez définir ces règles personnalisées dans 11.0.0.0

Pour la mise à jour vers la version 11.0, les collections de restauration créées dans la version 10.4 de Workbench afficheront des champs de valeurs vides pour la période et la date de création

Numéro de suivi : ASOC-9035

Problème : les collections de restauration créées dans la version 10.4 de Workbench afficheront des champs de valeurs vides pour la période et la date de création, après la mise à niveau vers la version 11.0.0.0.

Contournement : Aucun.

Lors de la mise à niveau, 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 11.0.0.0, le dashlet de géo-mappage ne peut pas être créé à l'aide d'un graphique (OOTB) 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 (OOTB) préconfiguré.

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

Le service Warehouse Connector montre que SSL FIPS est désactivé.

Numéro de suivi : ASOC-41930

Problème : Lorsque vous effectuez une mise à niveau d'une configuration 10.6.x non-FIPS vers 11.0.0.0, même si le service Warehouse Connector est en cours d'exécution sur FIPS, l'interface utilisateur indique que SSL FIPS est désactivé.

Contournement : Vérifiez SSL FIPS sur la page de configuration (IU) et redémarrez le service Warehouse Connector.

Context Hub

OutOfMemoryError dans le service Context Hub

Numéro de suivi : ASOC-41664

Problème : Le service Context Hub s'exécute dans OutOfMemoryError et ne répond plus si un grand nombre de sources TAXII est configuré pour pouvoir extraire des données.

Solution de contournement : redémarrez le service Context Hub et assurez-vous que la plage de temps que vous sélectionnez cette option pour extraire les sources TAXII à partir du serveur TAXII ne dépasse pas six mois. Si le problème persiste même après la mise à jour de la plage de temps, reportez-vous à la rubrique Résolution des problèmes dans le *Guide de gestion des services Live*.

L'option Pivoter vers la fonction Enquêter de la vue Répondre ne permet pas d'accéder au lien correct.

Numéro de suivi : ASOC-40944

Problème : Dès que vous arrêtez et redémarrez le serveur RabbitMQ, l'option Pivoter vers la fonction Enquêter disponible dans l'écran de réponse n'est pas visible. Et le panneau contextuel de Pivoter vers la fonction Enquêter rouvre la même page.

Contournement : redémarrez le service jetty sur le serveur Netwitness, vous connecter à l'hôte de serveur Netwitness et exécuter la commande de redémarrage du service jetty.

L'augmentation des paramètres de limite pour les alertes et les incidents entraîne des erreurs de recherche.

Numéro de suivi : ASOC-40246

Problème : Par défaut, les paramètres de limite pour afficher le nombre d'alertes et d'incidents sont définis sur 50. Si la limite est augmentée et que vous affichez l'erreur de recherche, cela est dû à un grand nombre d'incidents et d'alertes. Cela se produit en raison d'une restriction de base de données interne.

Solution de contournement : restreindre et afficher les alertes et incidents à 50.

Les listes à colonne unique et à plusieurs colonnes ajoutées à partir de l'onglet Source de données ne sont pas prises en charge pour l'ajout à une liste et la suppression à partir d'une liste.

Numéro de suivi : ASOC-37998

Problème : Lorsque vous effectuez une recherche sur une méta de contexte spécifique dans la vue Procédure d'enquête, Événements ou Répondre, les noms de liste affichés sont ceux qui ont des valeurs correspondantes.

Lorsque vous cliquez avec le bouton droit de la souris sur une méta spécifique et sélectionnez l'option Ajouter à la liste ou Supprimer de la liste, les noms de liste à colonne unique et à plusieurs colonnes ajoutés depuis l'onglet source de données ne s'afficheront pas. Seules les listes ajoutées à partir de l'interface utilisateur à l'aide de l'onglet Liste sont affichées.

Contournement : Vous devez ajouter manuellement les valeurs qui ont été ajoutées depuis l'onglet Source de données dans le fichier CSV spécifique. Ainsi, la prochaine fois que le planificateur s'exécutera, les valeurs du fichier CSV mis à jour seront disponibles dans les listes spécifiques.

Liste vide importée

Numéro de suivi : ASOC-34187

Problème : Lorsque vous importez une liste dans laquelle il manque des guillemets, comme « 172.16.0.0, la liste est enregistrée sans données. En effet, le bug Apache (CSV-141) n'analyse pas le fichier CSV avec un format incorrect.

Contournement : Importez une liste avec des guillemets corrects. Par exemple, « 172.16.0.0 », « host.mycompany.com », etc.

L'établissement de la liaison SSL avec un certificat RSA Archer échoue lors de son ajout comme source de données

Numéro de suivi : ASOC-32654

Problème : Lorsque vous tentez d'ajouter RSA Archer en tant que source de données à l'aide d'informations d'identification valides, le test de connexion échoue (ARCHER-37085). Cela se produit lorsque l'option « Approuver tous les certificats » n'est pas cochée et que vous tentez de télécharger un certificat de confiance RSA Archer.

Contournement : Sélectionnez la case à cocher « Approuver tous les certificats » et ne téléchargez pas un certificat.

Problèmes généraux liés aux plates-formes

L'interface utilisateur NetWitness Suite peut cesser de répondre

Numéro de suivi : SACE-7751

Problème : L'interface utilisateur NetWitness Suite peut cesser de répondre lorsque le système tente de lire des logs Live Connect volumineux.

Contournement : Ce problème peut être résolu temporairement en redémarrant jettysrv.

Problème avec l'exportation des métas

Numéro de suivi : SACE-8116

Problème : Bien que l'exportation fonctionne, s'il existe plusieurs valeurs méta dans une session, la capacité actuelle ne peut exporter que l'une des valeurs méta. Par exemple, si vous disposez d'une session avec 100 valeurs méta alias.host, une seule valeur est exportée.

Contournement : Aucun.

L'utilisateur sélectionne l'extraction des métadonnées, mais aucune donnée n'est téléchargée

Numéro de suivi : ASOC-35600

Problème : Si vous choisissez d'exporter des métas pour un événement, le fichier d'exportation est téléchargé et enregistré avec le nom de fichier spécifié, mais aucune donnée n'est contenue dans le fichier téléchargé.

Contournement : Aucun.

Une boîte de dialogue contextuelle vide est renvoyée dans l'interface utilisateur NW pour un fichier STIX non valide

Numéro de suivi : ASOC-36138

Problème : Si vous essayez de télécharger un fichier STIX non valide, un message d'erreur doit être affiché, mais au lieu de cela, une boîte de dialogue contextuelle vide est renvoyée.

Contournement : Aucun.

L'exportation de log exporte toujours au format Log

Numéro de suivi : ASOC-38270

Problème : Dans l'interface utilisateur de Procédure d'enquête, si vous choisissez d'extraire un ou des logs à partir du serveur NetWitness, le log sera toujours exporté au format « Log ».

Contournement : Aucun.

Problèmes généraux liés aux applications

Les pages classiques de l'interface utilisateur NetWitness Suite ne se chargent pas lorsque le système est soumis à une utilisation intensive

Numéro de suivi : ASOC-41999

Problème : Les pages classiques de l'interface utilisateur NetWitness Suite ne se chargent pas lorsque le système est soumis à une utilisation intensive avec l'erreur « `OutOfMemoryError: Metaspace` ».

Contournement : Remplacez « `-XX:MaxMetaspaceSize=256m` » par « `-XX:MaxMetaspaceSize=512m` » dans le fichier `/etc/default/jetty` sur le nœud d'administration. Une fois que les modifications sont enregistrées, redémarrez le service jetty (`systemctl restart jetty`).

Habilitations

Une licence à suivi d'utilisation ne passe pas immédiatement en conformité lorsque aucun service ne lui est rattaché

Numéro de suivi : ASOC-9078

Problème : Par exemple, si une licence à suivi d'utilisation est disponible pour un Log Decoder et que vous disposez d'un Log Decoder répertorié sous celui-ci, les conditions suivantes peuvent se produire :

- Vous dépassez la capacité d'utilisation autorisée, ce qui génère une non-conformité.
- Vous décidez de déplacer le Log Decoder vers une licence basée sur les services disponible.
- Votre licence à suivi d'utilisation ne dispose d'aucun service en dessous.
- Votre licence à suivi d'utilisation revient à l'état de conformité au bout de sept jours.

Contournement : Aucun.

Un rapport d'utilisation global est généré chaque fois qu'un seul service est rattaché à une licence et l'option « Tout » est sélectionnée lors de l'exportation des statistiques d'utilisation

Numéro de suivi : ASOC-10079

Problème : pour tout type de licence (Tout/à suivi d'utilisation/basée sur le service), le fichier PDF/CSV agrégé doit être généré uniquement lorsqu'il y a plusieurs services répertoriés sous un type de licence.

Contournement : Aucun.

Répondre

Lors de la mise à niveau, la règle d'agrégation pour les alertes C2, condition Group By est incorrecte

Numéro de suivi : ASOC-41934

Problème : Lors de la mise à niveau vers 11.0.0.0, la règle d'agrégation C2 utilisée par la détection automatisée des menaces possède une valeur différente de condition Group By.

Contournement : Après la mise à niveau vers 11.0.0.0, modifiez la règle d'agrégation « Communication de commande et contrôle suspect par domaine » et remplacez la condition Group By par « Domain ». (Pour ce faire, accédez à CONFIGURER > Règles d'incidents > Règles d'agrégation, puis double-cliquez sur la règle Communication de commande et contrôle suspect pour la modifier.) Ceci agrégera les alertes et des incidents seront créés pour « C&C suspect ».

Impossible de créer un incident avec 1 000 alertes

Numéro de suivi : ASOC-41855

Problème : Lorsque vous tentez de créer manuellement un incident avec plus de 400 alertes sélectionnées dans la vue Liste des alertes, vous pouvez rencontrer des problèmes.

Contournement : Ne sélectionnez pas plus de 400 alertes lorsque vous créez un incident.

L'administrateur Répondre ne peut pas interroger Enquêter ou afficher les dashlets Live dans le tableau de bord

Numéro de suivi : ASOC-40749

Problème : Le rôle Respond_Administrator n'est pas autorisé à interroger Enquêter. Cela est nécessaire afin que l'administrateur Répondre puisse pivoter vers Enquêter ou créer des incidents à partir d'événements. Le rôle Respond_Administrator ne possède pas non plus l'autorisation Live : Accéder au module Live, requise pour afficher des dashlets Live dans le tableau de bord.

Contournement :

1. Créez manuellement le rôle Respond_Administrator sur les services de base. Pour ce faire, accédez à ADMIN > Services, sélectionnez un service de base, puis, dans la liste déroulante Actions, sélectionnez Vue > Sécurité > onglet Rôles. Cliquez sur + pour ajouter le rôle Respond_Administrator. Ajoutez les autorisations suivantes au rôle Respond_ Administrator :

- sdk.content
- sdk.meta
- sdk.packets
- storedproc.execute

Répliquez le rôle Respond_Administrator aux autres services de base pouvant être utilisés par les utilisateurs.

2. Dans ADMIN > Sécurité > onglet Rôle, ajoutez l'autorisation Live : Accéder au module Live pour le rôle Respond_Administrator.

Lorsque la licence de suivi d'utilisation ou basée sur service est mappée, les jours sous licence et la date de début sont mal affichés.

Numéro de suivi : ASOC-26334

Problème : Lorsque la licence de suivi d'utilisation ou basée sur service est mappée, les jours sous licence et la date de début sont mal affichés sur l'interface utilisateur. Cela se produit en raison d'un problème avec le système d'octroi de licence et si/quand une nouvelle licence est mappée. Toutefois, les données correctes (jours sous licence et date de début) sont reflétées dans l'interface utilisateur après quelques jours.

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.

Impossible d'interroger le domaine dans source/destination.device.geolocation

Numéro de suivi : ASOC-39938

Problème : L'emplacement géographique provenant des règles de corrélation ESA n'est pas disponible dans la vue Détails de l'incident, panneau Indicateurs. (Pour accéder au panneau Indicateurs associés, accédez à RÉPONDRE > Incidents, puis dans la Liste des incidents, cliquez sur le lien ID ou NOM de l'incident. Dans la barre d'outils de la vue Détails de l'incident, cliquez sur l'icône Journal, Tâche et Connexe. Le Journal s'affiche sur la droite. Cliquez sur l'onglet ASSOCIÉ.)

Contournement : Aucun. Il s'agit d'une nouvelle fonctionnalité ; ces données ne sont pas disponibles pour la recherche.

Le lien Security Analytics Incident Management dans NetWitness SecOps Manager 1.3.1.2 n'est pas valide dans NetWitness Suite 11.0.0.0

Numéro de suivi : ASOC-41891

Problème : NetWitness Suite 11.0.0.0 fonctionne uniquement avec NetWitness SecOps Manager 1.3.1.2. Cependant, le lien Security Analytics Incident Management dans NetWitness SecOps Manager 1.3.1.2 accède à la page existante Security Analytics Incident Management, qui n'est pas valide dans NetWitness Suite 11.0.0.0

Contournement : Aucun.

Les incidents et les tâches sont toujours disponibles lorsque l'intégration RSA NetWitness SecOps Manager est activée.

Numéro de suivi : ASOC-39886

Problème : Une fois l'intégration NetWitness SecOps Manager activée dans le service Serveur Répondre, tous les incidents sont gérés dans NetWitness SecOps Manager. Dans les versions précédentes, lorsque SecOps était activé, les incidents et les tâches de correction étaient masqués. Dans NetWitness Suite 11.0.0.0, 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 Suite. 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 NetWitness SecOps Manager.

Contournement : Si vous avez activé l'intégration SecOps Manager 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). Il s'agit du comportement attendu dans NetWitness Suite 11.0.0.0 (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.

Impossible de Pivoter vers la fonction Enquêter sur toutes les valeurs de nom d'utilisateur, nom de fichier et domaine lorsque plusieurs valeurs sont présentes.

Numéro de suivi : ASOC-37997

Problème : Si les champs de nom d'utilisateur contiennent des virgules qui ne représentent pas de séparateurs entre les valeurs, vous ne serez peut-être pas en mesure de pivoter vers la procédure d'enquête sur certaines métas, s'il existe plusieurs valeurs dans le champ.

Contournement : Vous pouvez interroger ou pivoter sur d'autres données, ou enquêter manuellement sur les métas. Vous pouvez toujours accéder à la méta via Enquêter.

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 métas DOMAINE et HÔTE ne s'affichent pas correctement dans la vue Répondre

Numéro de suivi : ASOC-37232

Problème : Les métas Domaine et Hôte peuvent être correctement étiquetées dans la vue Détails de l'incidents, dans Répondre, lorsque alias.host contient différents types de données. Le comportement du champ Domaine n'est pas cohérente et il peut être rempli avec des noms d'hôte.

Contournement : Aucun. Plusieurs types d'information continueront d'exister dans le champ Domaine.

Après la mise à niveau, impossible de filtrer les incidents en utilisant le champ Personne affectée

Numéro de suivi : ASOC-36973

Problème : Après la mise à jour des incidents de 10.6.x vers 11.0.0.0, les analystes ne sont pas en mesure de filtrer les incidents migrés en utilisant le champ Personne affectée (RÉPONDRE > Incidents - panneau Filtre).

Contournement : Aucun.

Répondre - Créez des incidents à partir des Alertes dans la vue Répondre - Liste des alertes

Numéro de suivi : ASOC-35811

Problème : Lorsque vous créez manuellement un incident à partir des alertes dans la vue Répondre - Liste des alertes (RÉPONDRE > Alertes) dans 11.0.0.0, vous disposez seulement de la fonctionnalité minimale pour créer un incident à partir des alertes. Vous pouvez uniquement fournir un nom pour l'incident et la priorité est Faible par défaut. Lorsque vous créez manuellement un incident, vous n'avez pas d'options supplémentaires, telles que l'ajout d'une priorité, d'une personne affectée ou d'une catégorie.

Contournement : Vous pouvez mettre à jour d'autres champs en modifiant manuellement l'incident après l'avoir créé, par exemple en remplaçant la priorité Faible par Élevée. Toutefois, vous ne pouvez pas ajouter une catégorie à un incident.

Domaines sur liste blanche lors de la fermeture d'incidents en tant que faux positif

Numéro de suivi : ASOC-25135

Problème : Dans 10.6.x, si un incident C&C suspecté a été marqué comme « Fermé – faux positif », une entrée a été créée dans la liste « Domaines sur liste blanche » de Context Hub. La vue Répondre doit comporter une fonction similaire.

Contournement : Les analystes peuvent ajouter manuellement des domaines à une liste blanche dans la vue Répondre. Le *Guide de l'utilisateur NetWitness Respond* fournit des procédures.

Les paramètres d'intégration pour le Gestionnaire SecOps doivent être exposés dans l'interface utilisateur

Numéro de suivi : ASOC-25127

Problème : Les paramètres d'intégration pour l'envoi de tous les incidents à RSA NetWitness SecOps Manager doivent être exposés dans l'interface utilisateur

Contournement : L'interface utilisateur pour l'intégration partielle RSA NetWitness SecOps Manager a été supprimée dans 11.0.0.0. Les administrateurs peuvent effectuer l'intégration dans la vue Explorateur pour le service de serveur Répondre.

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

Numéro de suivi : ASOC-16640

Problème : les valeurs de la procédure d'enquête ne sont pas mises en surbrillance lorsque des alertes dans Répondre sont ajoutées à un incident manuellement. Les alertes qui sont ajoutées dynamiquement à un incident sont mises en surbrillance.

Contournement : Aucun.

Log Collector

Rôle DPO manquant dans le Log Collector

Numéro de suivi : ASOC-7937

Problème : le nouveau rôle de responsable de la confidentialité des données n'existe pas dans le service Log Collector.

Contournement : Aucun.

La collection de points de contrôle ne fonctionne pas avec l'erreur « l'homologue a mis fin à la session »

Numéro de suivi : ASOC-8351

Problème : la collecte de points de contrôle ne fonctionne pas et les logs affichent l'erreur : **« L'homologue a mis fin à la session. »**

Contournement : pour résoudre ce problème :

1. Effectuez une sauvegarde, puis supprimez le fichier de position des points de contrôle (**/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_ Security.xml**).
2. Redémarrez le service pour régénérer le fichier.
3. (Facultatif) Si l'option **Nb max. d'interrogations liées au délai de mise en veille** est définie sur 0, définissez le paramètre sur 5.

Erreur de régulation de la bande passante entre le collecteur distant et le collecteur local

Numéro de suivi : ASOC-16717

Problème : les modifications apportées à la configuration de la régulation de bande passante pour contrôler la vitesse à laquelle le collecteur distant envoie les données d'événements à un collecteur local, ne sont pas conservées après un redémarrage.

Le script `set-shoveltransfer-limit.sh` permet de définir la régulation de la bande passante pour les données d'événements transférées d'un collecteur distant vers un collecteur local. Le script utilise à la fois les règles iptables et les filtres d'orientation du trafic du noyau Linux afin de contrôler la bande passante de téléchargement utilisée par le port RabbitMQ lors des transferts vers un collecteur en amont. Le script fonctionne correctement lors de l'exécution, mais ne parvient pas à conserver les valeurs des filtres d'orientation du trafic une fois que l'appliance est redémarrée.

Contournement : ajoutez l'exécution du script dans `/etc/rc.local` sur le collecteur distant, comme illustré dans l'exemple suivant :
`"/opt/netwitness/bin/set-shovel-transfer-limit.sh -s -r 4096kbit"`

Procédure d'enquête

Les attributs d'utilisateur et de rôle ne sont pas appliqués dans les nouveaux workflows Enquêter - Analyse des événements.

Numéro de suivi : ASOC-42735

Problème : NetWitness Suite 11.0 n'appliquent pas les attributs d'utilisateur et de rôle dans les nouveaux workflows Enquêter - Analyse des événements.

Contournement *:* Vous devez appliquer le correctif RSA NetWitness Suite 11.0.0.1 pour résoudre cette situation.

Dans un environnement en mode mixte, un analyste avec des autorisations insuffisantes peut télécharger des PCAP et des logs à partir d'un service 10.6.x dans la vue Enquêter > Analyse des événements, mais pas des fichiers ou des charges utiles.

Numéro de suivi : ASOC-41697, ASOC-41698

Problème : Le RBAC (contrôle d'accès basé sur les rôles) sur le serveur NW 11.0.0.0 n'est pas appliqué uniformément aux téléchargements lors de l'enquête sur les services 10.6.x. Si le paramètre sdk.packets n'a pas été désactivé, les analystes disposant des autorisations de rôle méta SDK mis en place pour limiter l'affichage et la reconstruction du contenu d'un événement peuvent télécharger le fichier PCAP et le log d'un événement dont le contenu est restreint. D'autres types de téléchargements semblent télécharger, puis génèrent des erreurs en raison d'un manque d'autorisations et les données restent protégées.

Contournement : Désactivez le paramètre sdk.packets des services de la version 10.6.x afin d'empêcher l'analyste de télécharger des PCAP ou des logs pendant la mise à niveau phasée. Lorsque la mise à niveau de tous les services est terminée, l'expérience RBAC sera cohérente entre tous les services. Reportez-vous à la section « Tâches de mise à niveau » dans le *Guide de mise à niveau des hôtes physiques* pour plus d'informations.

Dans un environnement mixte, la vue Reconstruction d'événement > Vue Fichier affiche le mot « terminé » au lieu de la liste des fichiers.

Numéro de suivi : ASOC-41703

Problème : La première fois qu'un utilisateur administrateur reconstruit un événement de service=other et un fichier .raw, le mot « fermé » peut s'afficher dans la vue Reconstruction d'événement au lieu du fichier .raw.

Contournement : Accédez à un autre événement dans la vue Événements et revenez à cet événement, ou effacez le cache de services pour voir le résultat correct. Autrement, l'utilisateur administrateur peut afficher le fichier dans la vue Analyse des événements. Le problème se produit uniquement lors de la mise à niveau en mode mixte. La meilleure solution consiste donc à terminer la mise à niveau des services connectés à NW 11.0.0.0. Reportez-vous à la section « Tâches de mise à niveau » dans le *Guide de mise à niveau des hôtes physiques* pour plus d'informations.

Dans un réseau en mode mixte et dans un réseau 11.0.0.0, un analyste faisant l'objet de restrictions de contenu peut télécharger le contenu à accès restreint, mais ne parvient pas à décompresser l'archive téléchargée, car l'archive zip ne contient pas le contenu à accès restreint.

Numéro de suivi : ASOC-41698, ASOC-41696

Problème : Lorsqu'un utilisateur qui ne dispose pas d'autorisations pour le contenu télécharge des fichiers, les restrictions relatives au contenu appliquées au moyen de RBAC sont préservées, mais l'expérience utilisateur n'est pas cohérente avec l'expérience utilisateur pour les autres types de téléchargements avec des autorisations insuffisantes. On le constate dans un environnement 11.0.0.0 et un environnement en mode mixte 11.0.0.0/10.6x. Un analyste dont les autorisations restreignent l'affichage de contenu dans la vue Reconstruction d'événement peut télécharger du contenu restreint sur des services 10.6.x connectés. L'analyste peut exporter des fichiers restreints au format Zip ou GZip, et la file d'attente de travail présente un téléchargement réussi. Toutefois, le fichier est téléchargé en tant que Zip ou au format tar, et l'archive ne peut pas être décompressée ; elle crée une copie « cpgz ».

Contournement : Aucun. Lorsque la mise à niveau de tous les services est terminée, l'expérience RBAC sera cohérente entre tous les services. Reportez-vous à la section « Tâches de mise à niveau » dans le Guide de mise à niveau des hôtes physiques pour plus d'informations.

Cliquer avec le bouton droit de la souris dans la vue Log ne lance pas de Reconstruction d'événement ou d'Analyse de l'événement lorsque vous cliquez sur une colonne Logs répartie sur plusieurs lignes.

Numéro de suivi : ASOC-37989

Problème : Dans la vue Log d'un événement, il n'est pas possible de cliquer avec le bouton droit de la souris pour lancer une Reconstruction d'événement ou une Analyse de l'événement lorsque la colonne Logs dans la vue Log est répartie sur plusieurs lignes.

Contournement : Les analystes peuvent cliquer avec le bouton droit de la souris sur une autre colonne qui n'est pas répartie sur plusieurs lignes, dans la même ligne d'événement.

Dans l'Analyse des événements, le message Paquets restitués ne s'affiche pas pour les événements possédant une faible charge utile, mais un grand nombre de paquets.

Numéro de suivi : ASOC-37348

Problème : Lorsqu'un événement contient plus de 2 500 paquets, un message doit s'afficher au bas des résultats pour afficher le nombre de paquets restitués. Ce message ne s'affiche pas pour les événements comptant 2 500 paquets ou plus et une très faible charge utile, car la charge utile entière peut être affichée dans la vue.

Contournement : Aucun.

Problèmes de téléchargement de PCAP et de charge utile dans la vue Analyse d'événements dans un environnement en mode mixte

Numéro de suivi : ASOC-37309

Problème : Le workflow Analyse d'événements nécessite que tous les services exécutent la version 11.0.0.0. Si le serveur NW, le Broker et le Concentrator exécutent la version 11.0.0.0 et si les Decoders exécutent la version 10.6.x, l'utilisateur administrateur ne sera pas en mesure de télécharger les fichiers, les logs, les PCAP et les charges utiles.

Contournement : Téléchargez les fichiers à partir de la Reconstruction d'événement.

Lors de l'affichage d'un fichier d'archive dans le panneau Analyse d'événements - Analyse de fichier, les noms de fichiers individuels dans l'archive ne s'affichent pas.

Numéro de suivi : ASOC-35607

Problème : Vous pouvez voir l'archive, mais pas les noms de fichiers qu'elle contient.

Contournement : Affichez l'événement dans la vue Enquêter - Reconstruction d'événement pour voir les noms de fichiers individuels.

La visualisation des coordonnées parallèles n'affiche pas les caractères spéciaux correctement

Numéro de suivi : ASOC-9346

Problème : Lors de la configuration de la clé méta content type en tant qu'une des métadonnées de l'axe, si la métavaleur contient des caractères spéciaux, les valeurs ne s'afficheront pas correctement.

Contournement : Aucun.

Workbench

Numéro de suivi : ASOC-6859

Problème : Une collection vide s'affiche sous l'onglet Collections si le service Workbench s'arrête ou redémarre pendant le processus de restauration

Contournement : Aucun.

La plage de données ne s'affiche pas pour la collecte si le service Workbench ou Jettysrv est redémarré alors que la restauration est en cours

Numéro de suivi : ASOC-6822

Problème : La plage de dates ne s'affiche pas pour la collecte si le service Workbench ou Jettysrv est redémarré alors que la restauration est en cours.

Contournement : Aucun.

Live

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.

Malware Analysis

Les utilisateurs dotés du rôle d'analyste ne sont pas en mesure d'exécuter l'analyse des programmes malveillants à la demande

Numéro de suivi : ASOC-5425

Problème : un utilisateur disposant du rôle d'analyste a accès aux modules Investigation et Malware Analysis. En revanche lorsque l'utilisateur tente d'exécuter l'analyse Malware Analysis à la demande à partir de l'écran de procédure d'enquête, il échoue à cause du nom d'utilisateur non valide. La tâche est soumise mais échoue à cause des informations d'identification.

Contournement : Aucun.

Si le périphérique de base n'est pas configuré avec l'adresse IP, l'option Afficher la session réseau est désactivée pour les événements Malware Analysis

Numéro de suivi : ASOC-5571

Problème : en raison du nouvel identifiant de service et des modifications apportées à ASG, Malware Analysis n'affiche pas l'option Afficher la session réseau depuis le récapitulatif des événements Malware. Il semble que l'ID de périphérique soit disponible avec la valeur nulle.

Contournement : Aucun.

Event Stream Analysis

Le déploiement (appelé synchronisation dans la version 10.4 et les versions antérieures) échoue si vous déployez cette règle à partir de RSA Live : Aucun trafic de logs détecté à partir du périphérique au cours de la période donnée

Numéro de suivi : SAENG-5888

Problème : le déploiement, anciennement appelé synchronisation, échoue pour la règle « Aucun trafic de logs détecté à partir du périphérique au cours de la période donnée » déployée à partir de Live. Ce problème ne se produit que si vous déployez les règles à partir de Live sur une installation 10.4 et que vous effectuez la synchronisation. Le problème est observé si vous mettez à jour votre système à partir d'une version antérieure à la 10.4 où les règles sont déployées à partir de Live avec un ID de module incorrect.

Contournement : supprimez les règles dont l'ID de module est incorrect et redéployez-les à partir de Live.

Le tri sensible à la casse ne fonctionne pas correctement dans la grille de toutes les règles ESA

Numéro de suivi : SAENG-3605

Problème : Lorsque les noms de règle commencent par une lettre minuscule et une lettre majuscule, l'ordre de tri ne fonctionne pas correctement dans la colonne Nom de la règle de la grille de toutes les règles ESA. Par exemple, la « règle 1 » n'est pas suivie de la « règle 2 » lors du tri par nom.

Contournement : Aucun.

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 Analysispeut 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> Explorateur**, puis 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 nom de la règle de transfert n'est pas mis à jour lorsque le nom de la règle avancée change

Numéro de suivi : ASOC-9585

Problème : Dans le cadre d'un déploiement intersite, lorsque vous modifiez le nom d'une règle avancée, la règle de transfert n'est pas modifiée. Cela peut entraîner une règle orpheline qui peut continuer à transférer les événements.

Contournement : Pour renommer une règle avancée intersite, créez une nouvelle règle et supprimez l'ancienne.

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 à la 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.

Configuration des règles d'évaluation : Les valeurs hors limites sont plafonnées

Numéro de suivi : ASOC-6633

Problème : lorsque vous configurez les paramètres des règles d'évaluation, vous pouvez configurer les valeurs suivantes :

- **MemoryCheckPeriod** : définit l'intervalle d'interrogation pour vérifier la consommation de mémoire ESA.
- **MemoryThresholdForTrialRules** : définit la valeur du seuil ; lorsqu'elle est atteinte, toutes les règles d'évaluation sont désactivées.

  Si vous configurez ces paramètres avec des valeurs hors limites, les valeurs sont plafonnées aux valeurs minimale ou maximale du système, plutôt qu'aux valeurs définies dans les paramètres.

Contournement : Aucun.

Reporting Engine

Certains rapports de conformité ne peuvent pas être déployés à partir de Live

Numéro de suivi : SAENG-1334

Problème : Si les dépendances de certains des rapports de conformité dans Live ne sont pas déployées avant les rapports eux-mêmes, leur déploiement échouera.

Contournement : tentez un nouveau déploiement. Si le problème persiste, essayez de déployer la règle ou de répertorier les dépendances en premier, puis de déployer les rapports.

Certaines alertes Reporting peuvent échouer ou être retardées si la connexion RabbitMQ est bloquée

Numéro de suivi : SAENG-5329

Problème : si l'option **Transférer des alertes vers Répondre** est activée et si les connexions RabbitMQ au serveur Répondre sont bloquées, certains des threads de Reporting Engine peuvent être bloqués.

Contournement : désactivez l'option **Transférer des alertes vers Répondre** jusqu'à ce que le broker RabbitMQ du serveur NetWitness Suite, dans Répondre, démarre et puisse accepter les connexions.

Les mises à jour des paramètres de connexion de la page Maintenance ne sont pas répercutées aux sources de données Reporting

Numéro de suivi : ASOC-8149

Problème : en cas de changement ou de mise à jour des noms de services, ports ou paramètres de la page Maintenance, ces derniers ne sont pas propagés aux sources de données correspondantes ajoutées dans Reporting Engine.

Contournement : ajoutez des sources de données avec le service modifié et utilisez-les. En outre, si les noms des services existants sont modifiés, les plannings correspondants doivent être mis à jour dans Reporting.

Impossible d'accéder à la procédure d'enquête à partir des rapports NWDB si les paramètres de connexion de la page Maintenance sont mis à jour

Numéro de suivi : ASOC-8575

Problème : le lien de procédure d'enquête pour les valeurs méta des rapports exécutés ne s'affiche pas sur la page des résultats NWDB.

Contournement : Aucun. Problème qui sera résolu dans la prochaine version.

Les mises à jour des paramètres de connexion de la page Maintenance ne sont pas répercutées aux sources de données Reporting

Numéro de suivi : ASOC-8149

Problème : en cas de changement ou de mise à jour des noms de services, ports ou paramètres de la page Maintenance, ces derniers ne sont pas propagés aux sources de données correspondantes ajoutées dans Reporting Engine.

Contournement : ajoutez des sources de données avec le service modifié et utilisez-les. En outre, si les noms des services existants sont modifiés, les plannings correspondants doivent être mis à jour dans Reporting.

Reporting

Les métas de catégories pour la collecte d'incidents ne sont pas prises en charge.

Numéro de suivi : ASOC-40851

Problème : Lorsque vous utilisez les métas de catégories pour la collecte d'incidents, les résultats affichés possèdent un format incorrect. Par conséquent, cette méta n'est pas prise en charge et vous ne pouvez pas utiliser les métas de catégories dans une clause select ou where. En outre, elle n'est pas disponible dans la liste des métas pour la sélection dans la page Générateur de règles.

Contournement : Aucun.

Lors de l'interrogation sur la base de données Répondre, des lignes vides s'affichent.

Numéro de suivi : ASOC-37846

Problème : Lors de l'interrogation sur la base de données Répondre et si les données ne sont pas disponibles pour les colonnes demandées, des lignes vides s'affichent dans l'interface utilisateur.

Contournement : Aucun.

Le graphique avec les totaux affiche des données incorrectes.

Numéro de suivi : ASOC-37958

Problème : Le graphique avec les totaux affiche des données incorrectes lorsque le nombre total de valeurs est supérieur à la limite du graphique. Par exemple, si 16 valeurs numériques sont récupérées, seules 10 peuvent s'afficher sur le graphique.

Contournement : Aucun.

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 « Je prends 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.

Les résultats des tests de règle comportant un grand nombre de données ne s'affichent pas dans Internet Explorer 10

Numéro de suivi : SAENG-3926

Problème : lorsque vous cliquez sur **Tester la règle** à plusieurs reprises de façon rapide, les résultats contenant de nombreuses données ne s'affichent pas dans Internet Explorer 10.

Contournement : si ce problème se produit, essayez l'une des étapes suivantes :

- Fermez la fenêtre Tester la règle dans Internet Explorer 10, puis réexécutez le test.
- Utilisez d'autres navigateurs tels que Chrome ou Mozilla Firefox pour tester l'exécution de la règle.

Impossible d'ajouter des listes dynamiques lors de la modification d'un planning de rapport à partir de la page Afficher tous les plannings

Numéro de suivi : SAENG-5837

Problème : vous ne pouvez pas ajouter une liste dynamique à l'aide de l'option Modifier disponible sur la page « Afficher tous les plannings » à un planning existant.

Contournement : modifiez le planning à partir de la page Planning de rapport pour ajouter une liste dynamique.

Administration

L'événement d'audit de configuration capturé par NetWitness Suite ne fournit pas de contexte sur les services modifiés

Numéro de suivi : ASOC-8889

Problème : le serveur NetWitness Suite ne capture pas le service cible applicable pour les modifications de configuration dans les événements d'audit.

Contournement : Aucun.

Des journaux d'audit excessifs sont consignés en cas d'accès aux pages de l'interface utilisateur de NetWitness Suite ou d'importation, exportation, connexion ou déconnexion

Numéro de suivi : ASOC-8916

Problème : NetWitness Suite crée une quantité excessive de logs d'audit lorsque les utilisateurs de NetWitness Suite se connectent, se déconnectent, importent, exportent et accèdent aux pages de l'interface utilisateur NetWitness Suite.

Contournement : Aucun.

Logs d'audit : SA_SERVER ne capture pas la valeur de queryString

Numéro de suivi : ASOC-8994

Problème : lorsque vous modifiez le contenu du fichier d'un service de NetWitness Suite, les journaux d'audit du serveur NetWitness Suite n'indiquent pas les fichiers modifiés par l'utilisateur.

Contournement : Aucun.

L'e-mail d'expiration du mot de passe ne fournit pas d'informations sur la source

Numéro de suivi : ASOC-9187

Problème : L'e-mail d'expiration du mot de passe envoyé par le serveur NetWitness Suite ne mentionne pas le nom ni l'URL du serveur NetWitness Suite qui a envoyé l'e-mail. S'il existe plusieurs serveurs NetWitness Suite, vous ne savez peut-être pas où vous pouvez mettre à jour votre mot de passe.

Contournement : Aucun.

Les journaux d'audit n'indiquent pas la page (nom) de NetWitness Suite à laquelle l'utilisateur a tenté d'accéder sans autorisation

Numéro de suivi : ASOC-9323

Problème : lorsqu'un utilisateur tente d'accéder aux pages de l'interface utilisateur de NetWitness Suite sans les autorisations nécessaires, les journaux d'audit ne capturent pas les noms des pages en question.

Contournement : Aucun.

Gestion de la source d'événement

L'attribution d'un nouveau nom à l'hôte du Log Collector ou du Log Decoder n'apparaît pas dans la vue Gérer la source d'événements

Numéro de suivi : ASOC-9235

Problème : à la page **Administration > Host**, si vous modifiez le « nom » de l'appliance du Log Collector ou du Log Decoder, la modification n'apparaît pas à la page **Administration > Event Sources > Manage** dans les colonnes Log Collector ou Log Decoder.

Contournement : une fois que vous mettez à jour un nom dans la page Hôte, procédez comme suit :

1. Connexino en SSH à l'appliance NetWitness Suite.
2. Redémarrez le service SMS en exécutant la commande suivante : service rsa-sms restart.
3. Dans l'interface utilisateur de NetWitness Suite, attendez que la page **Gestion de la source d'événement** redevienne active, puis supprimez les sources d'événements portant les anciens noms du Log Collector ou du Log Decoder.

Si vous collectez des événements issus des sources d'événements supprimées, ils sont réintégrés automatiquement dans la page Gestion de la source d'événement avec le nouveau nom du Log Collector ou du Log Decoder.

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 11.0.0.0, les 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.

Les rôles système du Broker n'affichent pas les métaclés personnalisées définies dans le Concentrator

Numéro de suivi : ASOC-6749

Problème : si des clés méta personnalisées sont définies, les mêmes clés méta doivent également s'afficher dans le Broker. Cependant, les rôles système du Broker n'affichent pas les métadonnées personnalisées.

Contournement : vous pouvez copier le fichier langue et le fichier d'index personnalisé (si applicable) pour le Broker afin d'ajouter les rôles de clés méta SDK en tant que rôles système.

Configuration de flux personnalisée - Option Avancée Fichier XML : erreur non valide pour plusieurs rappels méta.

Numéro de suivi : ASOC-40867

Problème : Netwitness Suite ne prend pas en charge le téléchargement de flux 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 du décodeur directement. Cela n'est pas applicable au flux récurrent.

Possibilité de créer des flux basés sur IP pour la source et la destination à l'aide de CIDR ou d'une plage

Numéro de suivi : SATCE-628

Problème : lors de la création d'une source et d'une destination sur un Log Decoder, seule la clé méta source est renseignée. Vous ne pouvez pas utiliser un flux basé sur une plage ou sur CIDR. Vous devez répertorier chaque adresse IP unique.

Contournement : créez deux flux différents à l'aide des adresses IP et vous pourrez utiliser CIDR dans ces flux.

Documentation produit

Cette version est fournie avec la documentation suivante :

Document	Lieu
RSA NetWitness Suite 11.0 Documentation en ligne	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0 Instructions de la mise à niveau	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0 Liste de contrôle Mise à niveau	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite Guides de configuration du matériel	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Contacter le support client

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

RSA SecurCare	https://knowledge.rsasecurity.com
Tél.	+33 1 39 96 90 00, option 3
Contacts internationaux	https://france.emc.com/support/rsa/contact/phone-numbers.htm
E-mail	nwsupport@rsa.com
Communauté	https://community.rsa.com/community/rsa-customer-support
Support de base	Le support technique chargé de résoudre vos problèmes techniques est disponible de 08h00 à 17h00 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.

Préparation avant de contacter l'assistance clientèle

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 Suite que vous utilisez.
- Le type de matériel que vous utilisez.

Historique des révisions

Révision	Date	Description
1	24 octobre 2017	Disponibilité générale