RSA NETWITNESS® PLATFORM

Notes de mise à jour

pour la version 11.2.1

Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

Sommaire

Introduction

Ce document répertorie les améliorations et correctifs dans NetWitness Platform 11.2.1.0. Lisez ce document avant de déployer ou d'effectuer la mise à niveau vers NetWitness Platform 11.2.1.0.

Actualités

La version NetWitness Platform 11.2.1.0 fournit l'amélioration suivante.

NetWitness User and Entity Behavior Analysis (UEBA)

Prise en charge du modèle d'accès distant.UEBA modélise désormais l'accès utilisateur aux ordinateurs distants à l'aide du protocole du bureau à distance. Ce modèle définit les ordinateurs distants les plus couramment consultés par l'utilisateur et signale tout accès anormal. Pour plus d'informations, reportez-vous au *guide d'utilisation RSA NetWitness UEBA*.

Problèmes résolus

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

Sécurité

Numéro de suivi	Description
ASOC-61704	Mise à jour de sécurité Yum-utils https://access.redhat.com/errata/RHSA-2018:2285
ASOC-61929	Sécurité du noyau Mise à jour https://access.redhat.com/errata/RHSA-2018:2384
ASOC-60399	Mise à jour de sécurité Openjdk https://access.redhat.com/errata/RHSA-2018:2242
ASOC-59638	Sécurité Gnupg2 Mise à jour https://access.redhat.com/errata/RHSA-2018:2181

Numéro de suivi	Description
ASOC-62742	Postgresql Mises à jour de la sécurité https://access.redhat.com/errata/RHSA-2018:2557
ASOC-62744	Mise à jour de sécurité Bind https://access.redhat.com/errata/RHSA-2018:2570
ASOC-59640	Sécurité python Mise à jour https://access.redhat.com/errata/RHSA-2018:2123

Serveur

Numéro de suivi	Description
SACE-10385/ SACE-10364	La vue Santé et bien-être n'affiche pas les pages mises à jour.
SACE-9850	Sur la vue Graphiques, le tri par ordre croissant et décroissant n'affiche pas les résultats.

Reporting

Numéro de suivi	Description
SACE-10456	Dans la vue Règles, lors de la définition d'une clause WHERE, un espace supplémentaire est automatiquement ajouté après chaque condition.

Enquêter

Numéro de suivi	Description
SACE-10329	Lorsque vous exécutez une requête sur la vue Procédure d'enquête, la boîte de dialogue de requête ne vous permet pas d'entrer plus de six caractères.

Numéro de suivi	Description
SACE-10162	La requête d'investigation avec groupes méta ne prend pas en charge les adresses IP au format CIDR.
SACE-10060	Les clés méta avec un type de nombre entier n'affichent pas d'options pour les opérateurs dans la liste déroulante Intelli Sense.

Intégrité

Numéro de suivi	Description
SACE-10237	Lorsque vous exportez des sources d'événements, un fichier CSV non valide est créé.

Event Stream Analysis

Numéro de suivi	Description
SACE-9793	Une erreur se produit lorsque le service Whois est configuré.

Services de base

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

Numéro de suivi	Description
SACE-10222	Certains journaux sont manquants dans le fichier de sortie lorsque Concentrator est activé.

Numéros de build

Le tableau suivant répertorie les numéros de build des différents composants de NetWitness Platform 11.2.1.0.

Composant	Numéro de version
NetWitness Platform Web Server	11.2.1-x
NetWitness Platform Decoder	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Broker	11.2.1-x
NetWitness Platform Log Decoder	11.2.1-x
NetWitness Platform Archiver (Workbench)	11.2.1-x
NetWitness Platform Event Stream Analysis Server	11.2.1-x
NetWitness Platform Appliance	11.2.1-x
NetWitness Platform Archiver	11.2.1-x
NetWitness Platform Cloud Gateway Server	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Console	11.2.1-x
NetWitness Platform Endpoint Server	11.2.1-x
NetWitness Platform Investigate Server	11.2.1-x
NetWitness Platform Legacy Web Server	11.2.1-x
NetWitness Platform Log Player	11.2.1-x
NetWitness Platform Respond Server	11.2.1-x
NetWitness Platform SDK	11.2.1-x

Instructions de la mise à niveau

Les stratégies de mise à niveau suivantes sont prises en charge par NetWitness Platform 11.2.1.0 :

- RSA NetWitness® Platform 11.1.0.0 vers 11.2.1.0
- RSA NetWitness® Platform 11.1.0.1 vers 11.2.1.0
- RSA NetWitness® Platform 11.1.0.2 vers 11.2.1.0
- RSA NetWitness® Platform 11.1.0.3 vers 11.2.1.0
- RSA NetWitness® Platform 11.2.0.0 vers 11.2.1.0
- RSA NetWitness® Platform 11.2.0.1 vers 11.2.1.0

Pour obtenir des informations détaillées sur les procédures de mise à jour vers la version 11.2.1.0, consultez les instructions de mise à jour de la section Installation et mise à niveau

Problèmes connus

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

Remarque : Les problèmes connus dans les versions antérieures à 11.2.1.0 peuvent être résolus dans les correctifs. Reportez-vous aux notes de mise à jour de correctif disponibles sur RSA Link : https://community.rsa.com/.

UEBA

Les statistiques en double sont répertoriées sous la politique UEBA.

Numéro de suivi : ASOC-70119

Problème : Après avoir créé une règle sous la stratégie UEBA, les valeurs dupliquées s'affichent sous le menu déroulant Statistiques.

Contournement :

1. Connectez-vous à MongoDB à l'aide de la commande suivante :
   ```
   mongo admin -u deploy_admin -p {Saisissez le mot de passe}
   ```
2. Exécutez la commande suivante sous MongoDB
   ```
   use sms;
   db.getCollection('sms_statdefinition').find({componentId
   :"presidioairflow"})
   db.getCollection('sms_statdefinition').deleteMany({componentId
   :"presidioairflow"}) :
   ```

Le service UEBA affiche une version incorrecte.

Numéro de suivi : ASOC-69605

Problème : Après avoir mis à jour NetWitness Platform vers la version 11.2.1, la vue **ADMIN > Hôtes** affiche une version UEBA incorrecte.

Contournement : Vous devez mettre à jour le service UEBA.

1. Accédez à **ADMIN > Hôtes**.
2. Sélectionnez l'hôte UEBA
3. Cliquez sur **Mettre à jour** > **Mettre à jour l'hôte** dans la barre d'outils.
4. Cliquez sur **Commencer la mise à jour**.

Documentation produit

Cette version est fournie avec la documentation suivante :

Documentation	URL d'emplacement
Documentation en ligne RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112
Instructions de mise à niveau de RSA NetWitness Platform 11.2	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D

Réactions sur la documentation du produit

vous pouvez envoyer un e-mail à l'adresse sahelpfeedback@emc.com pour faire part de vos réactions sur la documentation RSA NetWitness Platform.

Contacter le support client

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

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

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

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

Historique des révisions

Révision	Date	Description
1	17 décembre 2018	Deuxième version