RSA NETWITNESS® PLATFORM

Notes de mise à jour

pour la version 11.2.0.1

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

Notes de mise à jour

Ce document répertorie les correctifs dans NetWitness Platform 11.2.0.1. Lisez ce document avant de déployer ou de mettre à niveau NetWitness Platform 11.2.0.1

Problèmes résolus

Ce document répertorie les problèmes résolus dans NetWitness Platform 11.2.0.1.

Correctifs relatifs aux serveurs

Numéro de suivi	Description
ASOC-64089	La langue des paramètres d'application est réinitialisée lorsque la localisation est activée. Dans NetWitness Platform 11.2.0.0, vous ne pouvez pas définir le français, l'allemand ou le japonais comme préférence de langue.

Correctifs relatifs à Malware Analysis

Numéro de suivi	Description
SACE-9874	Lorsque vous utilisez une version antérieure de l'appel d'URL de hachage, Malware Analysis n'affiche pas les détails du fournisseur anti-virus.

Correctifs de gestion de la source d'événements

Numéro de suivi	Description
ASOC-62575	Le service SMS peut se bloquer sur les systèmes comportant un grand nombre de sources d'événement actives, lorsque ceux-ci ne peuvent suivre le rythme de traitement des messages de statistique des journaux. L'erreur `java.lang.OutOfMemoryError: Java heap space` s'affiche alors.

Correctifs relatifs aux services Core

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

Numéro de suivi	Description
SACE-10191	Le service Log Decoder se régénère lorsque save.session.count est défini sur Automatique.
SACE-10283	Le metaDB sur Log Decoder se régénère en raison d'une structure de répertoire de l'analyseur incorrecte.
SACE-10336	Network Decoder se bloque en raison du pilote de carte réseau 10G.

Numéros de build

Le tableau suivant répertorie les numéros de build des différents composants de NetWitness Platform 11.2.0.1.

Composant	Numéro de version
NetWitness Platform Decoder	11.2.0.1-9473.5
NetWitness Platform Concentrator	11.2.0.1-9473.5
NetWitness Platform Broker	11.2.0.1-9473.5
NetWitness Platform Log Decoder	11.2.0.1-9473.5
NetWitness Platform Archiver (Workbench)	11.2.0.1-9473.5
NetWitness Platform Event Stream Analysis Server	11.2.0.1-448.5
NetWitness Platform Appliance	11.2.0.1-9473.5
NetWitness Platform Archiver	11.2.0.1-9473.5
NetWitness Platform Console	11.2.0.1-9473.5
NetWitness Platform Legacy Web Server	11.2.0.1-181010193532.5
NetWitness Platform Log Player	11.2.0.1-9473.5
NetWitness Platform SDK	11.2.0.1-9473.5

Instructions de mise à jour

Vous devez lire les informations et suivre les procédures de mise à jour vers NetWitness Platform version 11.2.0.1.

Les stratégies de mise à jour suivantes sont prises en charge pour NetWitness Platform version 11.2.0.1 :

- NetWitness Platform 11.2.0.0 vers 11.2.0.1
- NetWitness Platform 11.1.0.3 vers 11.2.0.1

Pour les stratégies de mise à jour prises en charge pour la version 11.2.0.0, reportez-vous au *Guide de mise à jour des versions 11.0.x.x ou 11.1.x.x vers 11.2*

Vous pouvez mettre à jour le correctif 11.2.0.1 à l'aide de l'une des options suivantes :

- Si le serveur NetWitness possède une connexion Internet vers les Services Live, l'interface utilisateur de NetWitness Platform peut être utilisée pour appliquer le correctif.
- Si le serveur NetWitness ne possède pas de connexion Internet vers les Services Live, vous pouvez utiliser l'interface de ligne de commande pour appliquer le correctif.

Tâches de mise à jour

Tâche 1 : Désactiver les services Decoder

Avant de procéder à la mise à niveau vers 11.2.0.1, vous devez désactiver Capture AutoStart sur les services Network Decoder et Network Hybrid.

Pour désactiver le champ de Capture Autostart :

1. Accédez à **ADMIN**> **Services**.
   La vue Services d'administration s'affiche.
2. Sélectionnez un service Network Decoder ou Network Hybrid et sélectionnez  > **Vue** > **Config**.
   La vue Configuration des services s'affiche pour le service Network Decoder ou Network Hybrid sélectionné.
3. Dans le panneau **Décoder Configuration**, désactivez le champ **Capture Autostart** et cliquez sur **Appliquer**

Tâche 2 : Mettre le correctif à jour

Vous pouvez choisir l'une des méthodes de mise à jour suivantes en fonction de votre connexion Internet.

Méthode en ligne (connectivité aux Services Live) : Effectuez la mise à jour à l'aide de l'interface utilisateur NetWitness

Vous pouvez utiliser cette méthode si le serveur NetWitness est connecté aux Services Live et peut obtenir le package.

Remarque : Une mise à jour est disponible de 11.1.0.3 vers 11.2.0.1, en utilisant la méthode en ligne. Si vous effectuez la mise à jour à partir de 11.1.0.x vers 11.2.0.1, vous devez d'abord effectuer une mise à niveau vers NetWitness Platform 11.2.0.0, et ensuite faire la mise à jour vers 11.2.0.1.

Remarque : Si le serveur NetWitness n'a pas d'accès aux Services Live, utilisez la Méthode hors ligne (pas de connectivité aux Services Live) : Mise à jour à l'aide de l'interface de ligne de commande .

Conditions préalables

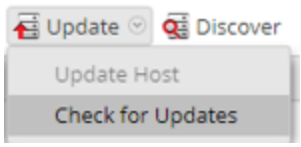
Vérifiez que :

1. L'option « Télécharger automatiquement les informations sur les nouvelles mises à jour tous les jours » est cochée et appliquée dans **ADMIN** > **Système** > **Mises à jour**.
2. Accédez à **ADMIN** > **Hôtes** > **Mettre à jour** > **Rechercher les mises à jour** pour rechercher les mises à jour. La page Hôte affiche l'état **Mise à jour disponible**.
3. 11.2.0.1 est disponible dans la colonne « Mettre à jour la version ».

Remarque : Si vous disposez de certificats personnalisés, déplacez tous les certificats personnalisés du répertoire `/etc/pki/nw/trust/import/` vers `/root/cert`. Suivez ces étapes pour déplacer les certificats :
1.) `mkdir /root/cert.`
2.) `mv /etc/pki/nw/trust/import/* /root/cert.`

Procédure

1. Accédez à **ADMIN** > **Hôtes**.
2. Sélectionnez l'hôte du serveur NetWitness (nw-server).
3. Vérifiez les dernières mises à jour.



4. Mise à jour disponible s'affiche dans la colonne **État** si vous disposez d'une version mise à jour dans le référentiel de mises à jour local pour l'hôte sélectionné.

5. Sélectionnez **11.2.0.1** dans la colonne **Mettre à jour la version**.
   Si vous :
   - Pour afficher une boîte de dialogue avec les principales caractéristiques de la mise à jour et les informations sur les mises à jour, cliquez sur l'icône d'informations ( ) à droite du numéro de version de mise à jour.
   - Impossible de trouver la version souhaitée, sélectionnez **Mettre à jour > Rechercher les mises à jour** pour vérifier le référentiel pour les mises à jour disponibles. Si une mise à jour est disponible, le message « Les nouvelles mises à jour sont disponibles » s'affiche et la colonne **État** se met automatiquement à jour pour afficher les mises à jour disponibles. Par défaut, seules les mises à jour prises en charge par l'hôte sélectionné sont affichées.
6. Cliquez sur **Mettre à jour** > **Mettre à jour l'hôte** dans la barre d'outils.
7. Cliquez sur **Commencer la mise à jour**.
8. Cliquez sur **Redémarrer l'hôte**.
9. Répétez les étapes 6 à 8 pour les autres hôtes.

Remarque : Vous pouvez sélectionner plusieurs hôtes à mettre à jour simultanément, mais seulement après la mise à jour et le redémarrage du serveur d'administration NetWitness. Tous les hôtes ESA, Endpoint Insights et Malware Analysis doivent être mis à jour vers la même version que celle du serveur d'administration NW ou NetWitness.

Remarque : Tous les composants n'ont pas été mis à jour vers la version 11.2.0.1, donc après avoir effectué les étapes de mise à jour, il est normal que certains composants disposent de numéros de version différents. Pour obtenir la liste des composants qui ont été mis à jour vers cette version, reportez-vous à la section Numéro de build.

Méthode hors ligne (pas de connectivité aux Services Live) : Mise à jour à l'aide de l'interface de ligne de commande

Vous pouvez utiliser cette méthode si le serveur NetWitness n'est pas connecté aux Services Live.

Conditions préalables

Vérifiez que :

- Vous avez téléchargé le fichier suivant, qui contient tous les fichiers de mise à jour NetWitness Platform 11.2.0.1 sur RSA Link (https://community.rsa.com/) > NetWitness Platform > Réseau et journaux RSA NetWitness > Téléchargements > Téléchargements RSA vers un répertoire local : `netwitness-11.2.0.1.zip`

Procédure

Vous devez effectuer les étapes de mise à jour pour les serveurs d'administration NW et pour les serveurs des composants.

Remarque : Si vous effectuez une mise à jour depuis la version 11.1.0.3 vers 11.2.0.1, vous devez télécharger les fichiers NetWitness Platform 11.2.0.0 au format zip et les configurer dans le dossier intermédiaire avec les fichiers 11.2.0.1. Si vous effectuez la mise à jour depuis la version 11.1.0. x vers 11.2.0.1, vous devez d'abord effectuer une mise à niveau vers NetWitness Platform 11.2.0.0, puis faire la mise à jour vers 11.2.0.1.

Remarque : Si vous copiez et collez les commandes à partir du PDF dans le terminal SSH Linux, les caractères ne fonctionnent pas. Il est recommandé de saisir les commandes.

1. Placez la version 11.2.0.1 dans un répertoire créé sur le serveur NetWitness à l'emplacement `/tmp/upgrade/11.2.0.1` et extrayez le fichier zip.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Remarque : Si vous avez copié le fichier .zip dans le répertoire temporaire créé pour la décompression, assurez-vous de supprimer le fichier .zip initial que vous avez copié dans l'emplacement intermédiaire après l'extraction.

2. Initialisation de la mise à jour à l'aide de la commande suivante :
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Mise à jour du serveur NetWitness à l'aide de la commande suivante :
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Après la réussite de la mise à jour de l'hôte du composant, redémarrez l'hôte à partir de l'interface utilisateur NetWitness.
5. Répétez les étapes 3 et 4 pour chaque hôte de composant, modifiez l'adresse IP pour l'hôte du composant qui est en cours de mise à jour.

Remarque : Vous pouvez vérifier les versions de tous les hôtes à l'aide de la commande `upgrade-cli-client --list` sur le serveur NetWitness. Si vous souhaitez afficher le contenu de l'aide de `upgrade-cli-client`, utilisez la commande `upgrade-cli-client --help`.

Remarque : Si l'erreur suivante s'affiche pendant le processus de mise à jour :
`2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671] o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error; protocol method: #method<connection.close>(reply-code=320, reply-text=CONNECTION_FORCED - broker forced connection closure with reason 'shutdown', class-id=0, method-id=0)`
le correctif s'installe correctement. Aucune action n'est requise. Si vous rencontrez des erreurs supplémentaires lors de la mise à jour d'un hôte vers une nouvelle version, contactez le Support clients (Contacter le support clients).

Instructions relatives au référentiel externe pour la mise à jour via l'interface de ligne de commande

Remarque : Le référentiel externe à configurer doit disposer d'un référentiel 11.2.0.1 configuré dans le même répertoire que la version 11.2.0.0.

1. Placez la version 11.2.0.1 dans un répertoire créé sur le serveur NetWitness à l'emplacement `/tmp/upgrade/11.2.0.1` et extrayez le fichier zip.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Remarque : Si vous avez copié le fichier .zip dans le répertoire temporaire créé pour la décompression, assurez-vous de supprimer le fichier .zip initial que vous avez copié dans l'emplacement intermédiaire après l'extraction.

2. Initialisation de la mise à jour à l'aide de la commande suivante :
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Mise à jour du serveur NetWitness à l'aide de la commande suivante :
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Après la réussite de la mise à jour de l'hôte du composant, redémarrez l'hôte à partir de l'interface utilisateur NetWitness.
5. Répétez les étapes 3 et 4 pour chaque hôte de composant, modifiez l'adresse IP pour l'hôte du composant qui est en cours de mise à jour.

Remarque : Vous pouvez vérifier les versions de tous les hôtes à l'aide de la commande `upgrade-cli-client --list` sur le serveur NetWitness. Si vous souhaitez afficher le contenu de l'aide de `upgrade-cli-client`, utilisez la commande `upgrade-cli-client --help`.

Remarque : Si l'erreur suivante s'affiche pendant le processus de mise à jour :
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
le correctif s'installe correctement. Aucune action n'est requise. Si vous rencontrez des erreurs supplémentaires lors de la mise à jour d'un hôte vers une nouvelle version, contactez le Support clients (Contacter le support clients).

Tâches consécutives à la mise à jour

(Facultatif) Tâche 1 - Déplacer les certificats personnalisés

Déplacez les certificats personnalisés à partir d'un répertoire externe vers le répertoire `/etc/pki/nw/trust/import`.

(Conditionnel) Tâche 2 - Reconfigurer l'authentification PAM pour Radius

Si vous avez configuré l'authentification PAM pour Radius dans la version 11.2.x.x à l'aide du package `pam_radius`, vous devez la reconfigurer dans la version 11.2.0.1 en utilisant le package `pam_radius_auth`.

Vous devez exécuter les commandes ci-dessous sur le serveur NW sur lequel réside le serveur d'administration.

Remarque : Si vous avez configuré `pam_radius` dans 11.x.x.x, effectuez les opérations suivantes pour désinstaller la version existante, ou passez à l'étape 2.

Étape 1 : Vérifiez la page existante et désinstallez la version actuelle `pam_radius`

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Étape 2 : Pour installer le package `pam_radius_auth` , exécutez la commande suivante

```
yum install pam_radius_auth
```

Étape 3 : Modifiez le fichier de configuration RADIUS, `/etc/raddb/server` comme suit et ajoutez les configurations pour le serveur radius :

```
# server[:port] shared_secret timeout (s)
server secret 3
```

Par exemple, 111.222.33.44 secret 1

Étape 4 : Modifiez le fichier de configuration PAM du serveur NetWitness `/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :

```
auth sufficient pam_radius_auth.so
```

Étape 5 : Donnez l'autorisation en écriture sur les fichiers `/etc/raddb/server` à l'aide de commande ci-dessous.

```
chown netwitness:netwitness /etc/raddb/server
```

Étape 6 : Pour copier la bibliothèque `pam_radius_auth`, exécutez la commande suivante.

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Étape 7 : Redémarrez le serveur jetty après avoir apporté des modifications aux configurations `pam_radius_auth`, exécutez la commande suivante.

```
systemctl restart jetty
```

Tâche 3 - Redémarrez le serveur Répondre.

Redémarrez le serveur Respond :

```
systemctl restart rsa-nw-respond-server
```

Tâche 4 - Mise à jour de l'emplacement du pilote 10G

Vous devez mettre à jour le pilote 10G à l'emplacement approprié dans le noyau actuel.

Étape 1 : Si vous utilisez le décodeur 10G, exécutez les commandes ci-dessous après avoir effectué la mise à niveau 11.2.0.1 et redémarrez l'appliance Décoder. Cliquez sur **Y** lorsque vous êtes invité à écraser le fichier.

- cp /var/lib/dkms/ixgbe-zc/5.3.7.14/$(uname -r)/x86_64/module/ixgbe_zc.ko.xz /lib/modules/$(uname -r)/extra/
- cp /var/lib/dkms/i40e-zc/2.4.6.14/$(uname -r)/x86_64/module/i40e_zc.ko.xz /lib/modules/$(uname -r)/extra/
- `cp /var/lib/dkms/pfring/6.5.0.14/$(uname -r)/x86_64/module/pf_ring.ko.xz /lib/modules/$(uname -r)/extra/`

Étape 2 : Si vous avez désactivé le champ **Capture Autostart** comme indiqué Tâche 1 : Désactiver les services Decoder, vous devez réactiver **Capture AutoStart** sur les services Network Decoder et Network Hybrid.

Pour activer le champ Capture Autostart :

1. Accédez à **ADMIN**> **Services**.
   La vue Services d'administration s'affiche.

2. Sélectionnez un service Network Decoder ou Network Hybrid, puis choisissez  > **Vue** > **Config**.
   La vue Configuration des services s'affiche pour le service Network Decoder ou Network Hybrid sélectionné.
3. Dans le panneau **Configuration de Decoder**, sélectionnez le champ **Capture Autostart** et cliquez sur **Appliquer**.

Documentation produit

Cette version est fournie avec la documentation suivante :

Document	Lieu
RSA NetWitness Platform Documentation en ligne de la version 11.2.0.0	https://community.rsa.com/community/products/netwitness/112

Réactions sur la documentation du produit

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

Contacter le support Client

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

RSA Link	https://community.rsa.com/
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/rsa-customer-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.

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

Historique des révisions

Révision	Date	Description
0.1	25 octobre	Version finale