RSA NETWITNESS® SUITE

Notes de mise à jour

pour la version 11.1.0.1

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, de la 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 : http://france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

Sommaire

Introduction

Ce document répertorie les améliorations et correctifs dans RSA NetWitness Suite 11.1.0.1. Lisez ce document avant de déployer ou de mettre à niveau RSA NetWitness Suite 11.1.0.1.

Numéros de build

Le tableau suivant répertorie les numéros de build des différents composants de RSA NetWitness Suite 11.1.0.1.

Composant	Numéro de version
Netwitness Suite Web Server	11.1.0.1-180413052407
Netwitness Suite Decoder	11.1.0.1-9043
Netwitness Suite Concentrator	11.1.0.1-9043
Netwitness Suite Broker	11.1.0.1-9043
Netwitness Suite Log Decoder	11.1.0.1-9043
Netwitness Suite Archiver (Workbench)	11.1.0.1-9043
Netwitness Suite Event Stream Analysis Server	11.1.0.1-436
Netwitness Suite Appliance	11.1.0.1-9043
Netwitness Suite Archiver	11.1.0.1-9043
Netwitness Suite Cloud Gateway Server	11.1.0.1-180413152801
Netwitness Suite Concentrator	11.1.0.1-9043
Netwitness Suite Console	11.1.0.1-9043
Netwitness Suite Endpoint Agents	11.1.0.1-1804190837
Netwitness Suite Endpoint Server	11.1.0.1-180419015718
Netwitness Suite Investigate Server	11.1.0.1-180417084126
Netwitness Suite Legacy Web Server	11.1.0.1-180413052407
Netwitness Suite Log Player	11.1.0.1-9043
Netwitness Suite Orchestration Server	11.1.0.1-180323104408
Netwitness Suite Respond Server	11.1.0.1-180322090443
Netwitness Suite SDK	11.1.0.1-9043

Nouveautés

Le correctif RSA NetWitness Suite 11.1.0.1 apporte des corrections à la version 11.1.0.0. Ce document décrit les améliorations et les corrections de cette version.

Endpoint Insights

Métadonnées Endpoint. Les API permettent d'afficher le mappage de métadonnées du point de terminaison par défaut ou de modifier le mappage de métadonnées de point de terminaison ; `get-default, get-custom, set-custom`. Pour plus d'informations sur ces API, reportez-vous au *Guide de configuration Endpoint Insights*.

NetWitness Investigate

Liste des services triée dans la vue Analyse des événements. Les services sont triés par ordre alphabétique dans le menu déroulant des services de la vue Analyse d'événements.

Indicateur des opérateurs lors de l'élaboration d'une requête dans l'Analyse d'événements. Lorsque les analystes ajoutent des filtres à une requête dans la vue Analyse d'événements, la liste déroulante des opérateurs, à saisie semi-automatique, affiche un chronomètre pour les opérations dont l'exécution prend plus de temps. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Investigate*.

Instructions de mise à jour

Vous devez lire les informations et suivre ces procédures de mise à jour RSA NetWitness Suite version 11.1.0.1.

Les stratégies de mise à jour suivantes sont prises en charge par RSA NetWitness Suite 11.1.0.1 :

- RSA NetWitness Suite 11.1.0.0 vers 11.1.0.1

Pour les stratégies de mise à jour prises en charge pour la version 11.1.0.0, reportez-vous au *Guide de mise à jour des versions 11.0.x vers 11.1*.

Vous pouvez mettre à jour le correctif 11.1.0.1 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 Suite 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

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 : 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** > **Vérifier les mises à jour** pour rechercher les mises à jour. La page Hôte affiche l'état **Mise à jour disponible**.
3. 11.1.0.1 est disponible dans la colonne « Version de la mise à jour ».

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 **11.1.0.1** dans la colonne **Version de la mise à jour**.
   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 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 11.1.0.1, 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 Numéros 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 Suite 11.1.0.1 sur RSA Link (https://community.rsa.com/) > NetWitness Suite > Téléchargements des logs et paquets de RSA NetWitness dans un répertoire local :
  `netwitness-11.1.0.1.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 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 11.1.0.1 dans un répertoire créé sur le serveur NetWitness à l'emplacement `/tmp/upgrade/11.1.0.1` et extrayez le fichier zip.
   ```
   unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1
   ```

   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 11.1.0.1 --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
   11.1.0.1
   ```

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 client).

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 11.1.0.1 configuré dans le même répertoire que la version 11.1.0.0.

1. Placez la version 11.1.0.1 dans un répertoire créé sur le serveur NetWitness à l'emplacement `/tmp/upgrade/11.1.0.1` et extrayez le fichier zip.
   `unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1`

   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. Lancez la mise à jour à l'aide de la commande suivante :
   `upgrade-cli-client --init --version 11.1.0.1 --stage-dir /tmp/upgrade`
3. Mettez à jour le serveur NetWitness à l'aide de la commande suivante :
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.1`
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 client).

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 11.1.x.x à l'aide du package `pam_radius`, vous devez la reconfigurer dans la version 11.1.0.1 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
```

Problèmes résolus

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

Correctifs relatifs aux serveurs

Numéro de suivi	Description
ASOC-50835	Il manque le service Integration-server dans l'interface utilisateur après la mise à jour.

Correctifs relatifs à Enquêter

Numéro de suivi	Description
ASOC-50771	Si vous accédez à l'Analyse d'événements par la vue Événements, soit en cliquant sur le lien Analyse d'événements, soit en cliquant avec le bouton droit sur l'un des événements, les options de clic droit sur les valeurs de métadonnées ne fonctionnent pas.
ASOC-49854	Le chargement du service n'aboutit pas.
ASOC-51011	Les groupes de colonnes RSA Endpoint Analysis, RSA Outbound SSL/TLS et RSA Outbound HTTP ne sont pas crées après la mise à niveau de 10.6.5 vers 11.x.
ASOC-48710	Le message « Une erreur inattendue est survenue » apparaît lorsque l'accès est supprimé ou des sessions déployées.
ASOC-50924	Le pivotement de l'Analyse d'événements à partir d'Endpoint est pris en charge uniquement pour le protocole IPv4.
ASOC-50712	Impossible d'ajouter des entités de métadonnées à un groupe de colonnes personnalisées dans la vue Événements lorsque l'option Optimiser les charges de la page Procédure d'enquête est désactivée.

Correctifs relatifs à Endpoint Insights

Numéro de suivi	Description
ASOC-49846	Aucune option n'est disponible pour désactiver la collecte de logs dans un agent Windows.
ASOC-49957	Un message d'avertissement a été écrit dans les logs (/var/log/messages). Ce message a maintenant été supprimé.
ASOC-50782	Dans 11.1.0.1, les noms de package du programme d'installation Linux ont été modifiés : • nwe-agent.rpm remplacé par nwe-agent.i686.rpm pour Linux 32 bits. • nwe-agent(64-bit).rpm remplacé par nwe-agent.x86_64.rpm pour Linux 64 bits.
ASOC-50162	L'intégration méta Endpoint est mise à jour afin que les mappages pour les clés méta s'alignent mieux sur les métadonnées générées à partir des logs et des paquets.

Correctifs relatifs à Telemetry

Numéro de suivi	Description
ASOC-50740	Telemetry JSON a été mis à jour avec les détails d'attribution de compte au niveau des services comme Decoder, Log Decoder et Malware.

Correctifs relatifs à Répondre

Numéro de suivi	Description
ASOC-51133	Répondre ne gère pas correctement la charge liée aux notifications et se bloque.

Correctifs relatifs à Context Hub

Numéro de suivi	Description
ASOC-51110	La règle ESA associée à une liste CH était désactivée au moment du redémarrage du système.
ASOC-51069	Le déploiement d'une règle ESA associée à une longue liste context-hub échoue.

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.

Remarque : les problèmes connus dans les versions antérieures à 11.1.0.0 peuvent être résolus dans les service packs. Reportez-vous à chaque service pack ou notes de mise à jour disponibles sur RSA Link : https://community.rsa.com/.

Mise à niveau

Les problèmes connus suivants se produisent au cours de la mise à niveau à partir de la version 11.1.0.x :

Les incidents Endpoint ne sont pas créés

Numéro de suivi : ASOC-51480

Problème : Les événements Endpoint avec une adresse IP source fonctionnent correctement, mais les événements Endpoint avec l'adresse IP du détecteur ne sont pas agrégées par la règle d'incidents Endpoint et ne créent pas d'incidents. Dans NetWitness Suite 11.1, le champ Regrouper par de la règle d'incident « Alertes de risque élevé : NetWitness Endpoint » est passée de « Valeur de risque » à « Adresse IP source ».

Contournement : Pour les mises à niveau de 10.6.x vers 11.1 :

1. Accédez à **CONFIGURER** > **Règles de l'incident**. La vue Liste des règles d'incident s'affiche.
2. Cliquez sur le lien dans le champ **Nom** de la règle d'incident **Alertes de risque élevé : NetWitness Endpoint** pour la modifier.
3. Modifiez le champ **Regrouper par** sur **Valeur de risque**.

Pour les nouvelles installations :

1. Accédez à **CONFIGURER** > **Règles de l'incident**. La vue Liste des règles d'incident s'affiche.
2. Cliquez sur le lien dans le champ **Nom** de la règle d'incident **Alertes de risque élevé : NetWitness Endpoint** pour la modifier.
3. Modifiez la valeur du champ **GroupBy** sur **Valeur de risque** ou toute autre valeur du champ Regrouper par.

Alertes dupliquées dans Répondre

Numéro de suivi : ASOC-50994

Problème : Les alertes dupliquées dans Répondre sont observées de par part de certaines sources comme le Reporting Engine.

Contournement : Suivez ces étapes pour supprimer les échanges fédérés obsolètes qui causeraient des alertes dupliquées dans Répondre :

1. Connectez-vous au cluster https://<adminServerIP>:15671/ Rabbitmq avec les informations d'identification suivantes.

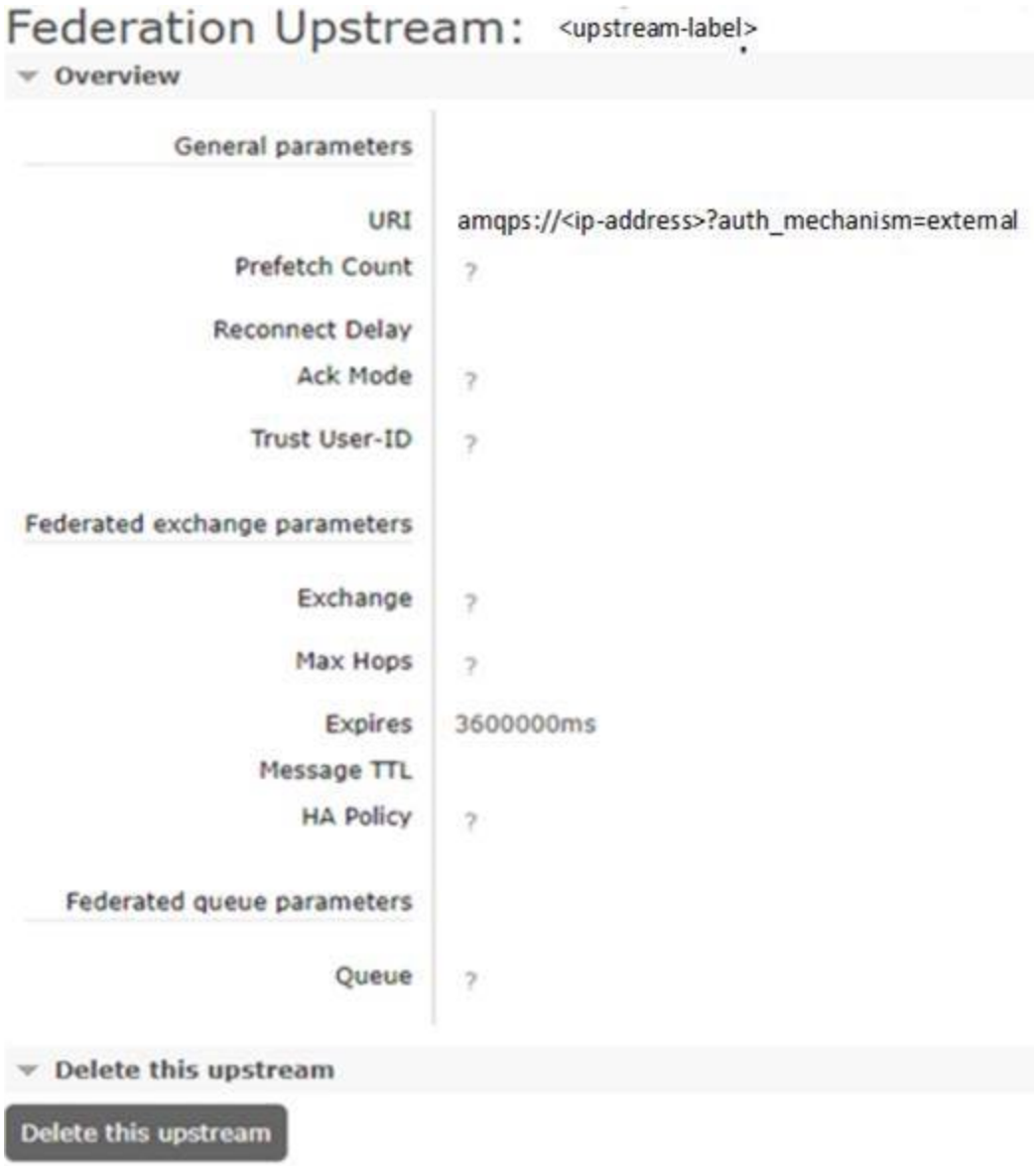
```
username: deploy_admin
```

```
password: <deployment-password-used-during-NW-Server-host-11.x-setup>
```

2. Accédez à **Admin** > **Fédération en amont**.
3. Sélectionnez l'URI avec l'**adresse IP hôte du serveur NW** vers celui-ci. La vue **Fédération en amont** s'affiche.
4. Assurez-vous que l'URI est similaire à la valeur suivante

```
amqps : // <adminServerIP>?auth_mechanism=external
```

5. Cliquez sur **Supprimer en amont** pour supprimer l'URI.



Endpoint Insights

Après la mise à jour de l'agent, la version de l'agent n'est pas reflétée dans l'interface utilisateur

Numéro de suivi : ASOC-52761

Problème : Lorsque vous mettez à jour la version de l'agent à partir de 11.1 à 11.1.0.1, la version de l'agent présente 11.1 dans la vue Hôtes.

Contournement : Dans la vue **Enquêter** > **Hôtes**, sélectionnez l'hôte sur lequel vous avez installé la dernière version de l'agent, puis cliquez sur **Lancer la numérisation**. La version de l'agent est mise à jour vers 11.1.0.1.

Impossible de transférer des logs sur 6514, lorsque seul TLS 1.2 est activé dans le Log Decoder

Numéro de suivi : ASOC-52761

Problème : Dans le Log Decoder, si vous avez défini `/sys/config/ssl.context.options` sur `SSL_OP_NO_SSLv2,SSL_OP_NO_SSLv3,SSL_OP_NO_TLSv1,SSL_OP_NO_TLSv1_1` et autorisé uniquement TLS1.2 à accepter des logs, le transfert de log ne fonctionne pas lorsqu'il est transmis à 6514 à partir d'agents déployés dans Windows 7 SP1 et Windows 2008.

Contournement : Reportez-vous à l'article sur la façon d'activer TLS 1.2 : https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows.

Documentation produit

Cette version est fournie avec la documentation suivante :

Document	Emplacement
RSA NetWitness Suite 11.1.0.0 Documentation en ligne	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Instructions de la mise à niveau	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 Liste de contrôle Mise à niveau	https://community.rsa.com/community/products/netwitness/111
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	http://france.emc.com/support/rsa/contact/phone-numbers.htm
Communauté	https://community.rsa.com/docs/DOC-1294
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
0.1	17 avril	Version préliminaire RTO