RSA NETWITNESS® SUITE

Guide d'intégration de RSA Archer

pour la version 11.0

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 : 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.

février 2018

Sommaire

Intégration de RSA Archer

Les administrateurs peuvent intégrer RSA NetWitness Suite avec RSA NetWitness Security Operations (SecOps) Manager pour envoyer des alertes et incidents de NetWitness Suite à Archer pour la gestion et la correction des incidents Ce guide fournit un workflow global pour configurer cette intégration.

Le tableau suivant répertorie les options d'intégration de NetWitness Suite 11.0 avec NetWitness SecOps Manager Version 1.3.1.2.

NetWitness SecOps Manager Version	Intégration de NetWitness Suite11.0	Référence
1.3.1.2	Event Stream Analysis (ESA)	Pour plus d'informations, reportez-vous à la rubrique « Configurer Event Stream Analysis pour une intégration à Archer SecOps ».
1.3.1.2	Reporting Engine (RE)	Pour plus d'informations, reportez-vous à la rubrique « Configurer Reporting Engine pour une intégration à Archer SecOps ».
1.3.1.2	Répondre	Pour plus d'informations, reportez-vous à la rubrique « Configurer Répondre pour une intégration à Archer SecOps 1.3.1.2 ».
1.3.1.2	Flux Archer	Pour plus d'informations, consultez la rubrique « Flux RSA Archer ».

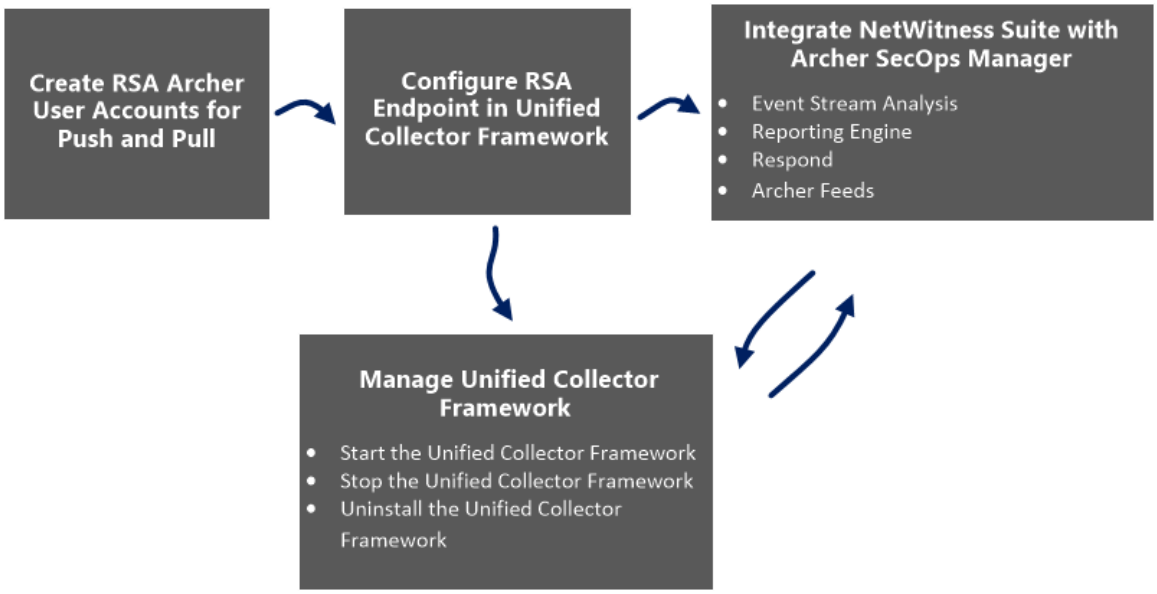
Configurer NetWitness pour une utilisation avec Archer

La solution RSA NetWitness SecOps Manager vous permet de rassembler tous les dispositifs d'alerte de sécurité exploitables pour vous permettre d'être plus efficace, plus pro-actif et plus ciblé dans vos réponses aux incidents et votre gestion du centre de supervision de la sécurité (SOC). Pour plus d'informations sur les fonctionnalités de RSA NetWitness SecOps, reportez-vous à la documentation RSA Archer sur le site RSA Archer Community ou le site de RSA Archer Exchange Community.

La version de RSA Archer détermine comment NetWitness Suite sera intégrée. Reportez-vous au *Guide d'installation de SecOps* pour en savoir plus sur les plates-formes Archer prises en charge.

NetWitness SecOps Manager 1.3.1.2 s'intègre avec NetWitness Suite à l'aide de la UCF RSA (Unified Collector Framework) qui comprend le service d'intégration Security Analytics Incident Management (IM) et le service SecOps Watchdog.

La figure suivante représente le flux d'intégration de NetWitness Suite 11.0 avec NetWitness SecOps Manager 1.3.1.2.



Créer des comptes utilisateurs RSA Archer pour les opérations de transmission (Push) et d'extraction (Pull)

Vous devez créer un compte utilisateur pour que le client de service Web puisse transférer les

données vers la plate-forme RSA Archer GRC.

Deux comptes utilisateurs RSA Archer sont requis pour éviter les conflits lors de l'envoi et de la réception des données de RSA NetWitness Suite.

Pour créer un compte utilisateur pour les transmissions (push) et les extractions (pull), procédez comme suit :

1. Dans l'interface utilisateur RSA Archer, cliquez sur **Administration** > **Contrôle d'accès** > **Utilisateurs** > **Ajouter nouveau**.
2. Dans les champs **Nom** et **Prénom**, saisissez un nom qui indique que le système UCF utilise ce compte pour transmettre les données à RSA Archer GRC. Par exemple, Utilisateur UCF, Transmission.

   Remarque : Lors de la configuration du compte Extraction, saisissez un nom indiquant que le système UCF utilise ce compte pour extraire les données de RSA Archer GRC. Par exemple, Utilisateur UCF, Extraction.
3. (Facultatif) Saisissez un nom d'utilisateur pour le nouveau compte utilisateur.

   Remarque : Si vous ne spécifiez pas de nom d'utilisateur, la plate-forme RSA Archer GRC crée le nom d'utilisateur à partir des nom et prénom saisis lors de l'enregistrement du nouveau compte utilisateur.
4. Dans la section **Informations de contact**, dans le champ **E-mail**, saisissez une adresse électronique à associer à ce nouveau compte utilisateur
5. Dans la section **Localisation**, sélectionnez le fuseau horaire UTC (Coordinated Universal Time).

   Remarque : Le système UCF utilise l'heure UTC comme ligne de base pour tous les calculs liés à l'heure.
6. Dans la section **Maintenance du compte**, saisissez un mot de passe, puis confirmez-le pour le nouveau compte utilisateur.

   Remarque : Relevez le nom d'utilisateur et le mot de passe que vous venez de créer pour le nouveau compte utilisateur. Vous devez saisir ces informations d'identification lorsque vous configurez le système UCF pour qu'il communique avec la plate-forme RSA Archer GRC via le client de service Web.
7. Désactivez l'option **Forcer le changement du mot de passe à la prochaine connexion**.
8. Dans le champ **Paramètre de sécurité**, sélectionnez le paramètre de sécurité à attribuer à l'utilisateur.

Remarque : Si vous attribuez un paramètre de sécurité par défaut avec un intervalle de modification du mot de passe de 90 jours, vous devez également mettre à jour le mot de passe du compte utilisateur stocké dans le service d'intégration SA IM tous les 90 jours. Pour éviter une telle opération, vous pouvez éventuellement créer un nouveau paramètre de sécurité pour le compte utilisateur du service d'intégration SA IM et définir l'intervalle de modification du mot de passe sur la valeur maximale autorisée par les normes de votre entreprise.

9. Cliquez sur l'onglet **Groupes** pour effectuer les actions suivantes :
   a. Dans la section **Groupes**, cliquez sur **Recherche**.
   b. Dans la fenêtre **Groupes disponibles**, développez Groupes.
   c. Faites défiler l'écran vers le bas, puis sélectionnez SOC : Administrateur de solutions et EM : Lecture seule
   d. Cliquez sur **OK**.
10. Cliquez sur **Appliquer**, puis sur **Enregistrer**.
11. Si la langue et les paramètres régionaux de votre système RSA Archer GRC ne sont pas configurés en mode anglais (États-Unis), procédez comme suit :
    a. Ouvrez le compte utilisateur que vous venez de créer et dans la section **Localisation**, au sein du champ Paramètres régionaux, sélectionnez **Anglais (États-Unis)**, puis cliquez sur **Enregistrer**.
    b. Sur le système Windows hébergeant votre plate-forme RSA Archer GRC, ouvrez le Gestionnaire des services IIS (Internet Information Services).
    c. Développez votre site RSA Archer GRC, cliquez sur **Globalisation .Net**, dans les deux champs **Culture** et **Culture d'interface utilisateur**, sélectionnez **Anglais (États-Unis)**, puis cliquez sur **Appliquer**.
    d. Redémarrez votre site RSA Archer GRC.
12. Répétez les étapes 1-11 pour créer un deuxième compte utilisateur pour que le système UCF puisse extraire les données de RSA Archer GRC.

Configurer les points de terminaison dans RSA Unified Collector Framework

Les points de terminaison fournissent les détails de connexion requis par le système UCF pour atteindre vos deux systèmes RSA NetWitness Suite et RSA Archer GRC.

Remarque : Certains points de terminaison sont nécessaires pour utiliser différentes intégrations. La liste suivante affiche les points de terminaison obligatoires.

Intégration des points de terminaison obligatoires

- Point de terminaison Archer Push
- Point de terminaison Archer Pull
- Sélection du mode : Mode SecOps ou Non SecOps.

Remarque :
• Si le mode Non SecOps est sélectionné, les incidents sont gérés dans NetWitness Suite Respond au lieu de RSA Archer Security Operations Management.
• Vous devez configurer le port selon le protocole (TCP, UDP ou TCP sécurisé).
• Vérifiez que le nom du sujet du certificat de votre serveur RSA Archer GRC correspond au nom de l'hôte.

Procédure

1. Sur le système UCF, ouvrez le Gestionnaire de connexions, comme suit :
   a. Ouvrez une invite de commande.
   b. `Remplacez les répertoires par <rép_installation>\SA IM integration service\data-collector`
   c. `Saisissez : runConnectionManager.bat`
2. Dans le **Gestionnaire de connexions**, saisissez **1** pour ajouter un point de terminaison.
3. Ajoutez un point de terminaison pour transmettre les données à RSA Archer Security Operations Management, comme suit :
   a. Saisissez le numéro correspondant à Archer.

      Remarque : La connexion SSL doit être activée pour ajouter les points de terminaison RSA Archer.

   b. Pour le nom du point de terminaison, saisissez **push**.
   c. Saisissez l'URL de votre système RSA Archer GRC.
   d. Saisissez le nom d'instance de votre système RSA Archer GRC.
   e. Saisissez le nom d'utilisateur du compte utilisateur que vous avez créé pour transmettre les données à votre système RSA Archer GRC.

f. Saisissez le mot de passe du compte utilisateur que vous avez créé pour transmettre les données à votre système RSA Archer GRC, puis confirmez le mot de passe.

g. Lorsque vous y êtes invité(e) si ce compte est utilisé pour l'extraction des données, saisissez **False**.

4. Ajoutez un point de terminaison pour extraire les données de RSA Archer Security Operations Management, comme suit :

   a. Saisissez le numéro correspondant à Archer.

   Remarque : La connexion SSL doit être activée pour ajouter les points de terminaison RSA Archer.

   b. Pour le nom du point de terminaison, saisissez **pull**.

   c. Saisissez l'URL de votre système RSA Archer GRC.

   d. Saisissez le nom d'instance de votre système RSA Archer GRC.

   e. Saisissez le nom d'utilisateur du compte utilisateur que vous avez créé pour extraire les données de votre système RSA Archer GRC.

   f. Saisissez le mot de passe du compte utilisateur que vous avez créé pour extraire les données de votre système RSA Archer, puis confirmez le mot de passe.

   g. Lorsque vous y êtes invité(e) si ce compte est utilisé pour l'extraction des données, saisissez **True**.

5. Ajouter un point de terminaison pour RSA NetWitness Suite

   - Pour RÉPONDRE

     a. Saisissez le numéro correspondant à Security Analytics IM.

     b. Saisissez un nom pour le point de terminaison.

     c. Saisissez l'adresse IP de l'hôte SA.

     d. Pour le port de messagerie SA, saisissez **5671**.

     e. Saisissez la file d'attente cible pour les tâches de remédiation. La sélection Tout s'applique à la fois à RSA Archer Integration (GRC) et au service d'assistance technique IT (Operations).

     f. Pour ajouter des certificats automatiquement au magasin de certificats de confiance NetWitness Suite, procédez comme suit :

i. Saisissez **Oui**.

ii. Saisissez le nom d'hôte, le nom d'utilisateur et le mot de passe de l'hôte NetWitness Suite.

> **Remarque :** Si un message d'erreur indique que l'échec de la configuration du magasin de certificats de confiance, reportez-vous à la rubrique Dépanner l'intégration de RSA Archer.

g. Dans le gestionnaire de connexions UCF, sélectionnez le mode, comme suit :

i. Saisissez le numéro correspondant à la Sélection du mode.

ii. Sélectionnez l'une des options suivantes :

- Gérer le workflow d'incidents dans RSA NetWitness Suite.
- Gérer le workflow d'incidents de manière exclusive dans RSA Archer Security Operations Management.

- Pour Reporting Engine et Event Stream Analysis

a. Pour utiliser les intégrations tierces, ajoutez le point de terminaison du serveur Syslog, comme suit :

i. Saisissez le numéro correspondant au point de terminaison du serveur Syslog.

ii. Saisissez ce qui suit :

- Nom défini par l'utilisateur
- Numéro de port TCP avec SSL configuré

> **Remarque :** Paramètre par défaut : 1515. Si vous ne souhaitez pas héberger le serveur Syslog avec ce mode, saisissez **0**.

- Numéro de port TCP : sélectionnez le port TCP si le client Syslog envoie le message Syslog en mode TCP.

> **Remarque :** Paramètre par défaut : 1514. Si vous ne souhaitez pas héberger le serveur Syslog avec ce mode, saisissez **0**.

- Numéro de port UDP : saisissez le port UDP si le client Syslog envoie le message Syslog en mode UDP.

> **Remarque :** Paramètre par défaut : 514. Si vous ne souhaitez pas héberger le serveur Syslog avec ce mode, saisissez **0**.

Par défaut, le serveur Syslog s'exécute dans les trois modes ci-dessus, sauf en cas de désactivation en saisissant **0**.

b. Pour tester le client Syslog, saisissez le numéro correspondant à la ligne Tester le client Syslog. Utiliser le client de Test Syslog avec les fichiers à partir de `<install_dir>\SA IM integration service\config\mapping\test-files\`.

6. Dans le Gestionnaire de connexions, saisissez **5** pour tester chaque point de terminaison.

Intégrer NetWitness Suite avec Archer SecOps Manager

Vous devez configurer les paramètres d'intégration système pour gérer le workflow d'incidents dans RSA NetWitness SecOps Manager.

Pour plus d'informations sur le mode de configuration des paramètres d'intégration système pour gérer le workflow d'incidents dans RSA Archer Security Operations, reportez-vous à la section « Configurer le paramètre d'intégration pour gérer les incidents dans RSA Archer Security Operations » dans le *Guide d'utilisation de NetWitness*.

RSA Unified Collector Framework (UCF)

RSA NetWitness Suite s'intègre à RSA Archer SecOps Manager 1.3.1.2 à l'aide de RSA Unified Collector Framework (UCF). RSA Unified Collector Framework (UCF) s'intègre avec tous les outils SIEM pris en charge et la solution RSA NetWitness SecOps Manager. Lors de l'intégration de RSA NetWitness Suite Respond, vous pouvez gérer le workflow d'incidents dans NetWitness Suite Respond et permettre aux analystes de faire remonter des tâches de correction et ouvrir des violations de données à gérer et corriger dans la solution RSA Archer Security Operations Management. Et le Unified Collector Framework transfère les tâches de remédiation (créées en tant que Conclusions), les violations de données, ou les deux.

Remarque :
• Vous devez configurer la même option dans RSA NetWitness Suite et Unified Collector Framework.
• L'intégration du module RSA NetWitness Respond à Reporting Engine ou Event Stream Analysis peut engendrer la création d'événements ou d'incidents dupliqués dans RSA Archer SecOps Manager.

UCF prend en charge plusieurs connexions d'outils SIEM simultanées, comme la prise en charge de NetWitness Suite Reporting Engine, HP ArcSight et NetWitness Suite Respond. En revanche, différentes instances d'un même outil SIEM ne peuvent pas être prises en charge, par exemple, deux serveurs NetWitness Suite connectés au même système UCF.

Conditions préalables

- Installez le package RSA_Archer_Security_Operations_Management sur Archer. Reportez-vous à la documentation RSA Archer sur RSA Archer Community ou à partir de l'onglet Content du site https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Installez NetWitness SecOps Manager.
- Assurez-vous de disposer de NetWitness Suite 11.0 car il est compatible avec NetWitness SecOps Manager 1.3.1.2.
- Assurez-vous que Respond est configuré dans RSA NetWitness Suite.

RSA Unified Collector Framework (UCF) vous permet d'intégrer votre système RSA Archer Security Operations Management aux composants suivants :

- NetWitness Suite Respond
- NetWitness Suite Reporting Engine
- NetWitness Suite Event Stream Analysis
- Feeds Archer

Configurer Respond pour l'intégration à Archer SecOps

Pour configurer Respond pour Archer SecOps, procédez comme suit dans NetWitness Suite :

Étape 1 : Sélectionnez le Mode de NetWitness Suite Respond

1. Sélectionnez **ADMIN > Services > Respond > Explorer**.
2. Accédez à `Respond/Aggregation/export`.
3. Activer le champ `archer-secops-integration-enabled` sur **true**.
4. Redémarrez le service Respond.

Étape 2 : Configurer NetWitness Suite Respond pour transférer les alertes vers UCF

1. Accédez à `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` dans la boîte middleware Secops.
2. Copiez `keystore.cert.pem` et `rootcastore.cert.pem` à partir du dossier certs (pour importer un dossier du serveur NW)
   ```
   cp rootcastore.crt.pem /etc/pki/nw/trust/import
   ```
   ```
   cp keystore.crt.pem /etc/pki/nw/trust/import
   ```
3. Ouvrez une session SSH sur le serveur NW

a. Exécutez la commande update-admin-node
```
orchestration-cli-client --update-admin-node
```

b. Redémarrez le service RabbitMQ
```
service rabbitmq-server restart
```

c. Créez l'utilisateur archer et définissez les autorisations pour l'hôte virtuel '/rsa/system'
```
rabbitmqctl add_user archer archer

rabbitmqctl clear_password archer

rabbitmqctl set_permissions -p /rsa/system archer ".*" ".*" ".*"
```

Étape 3 : Transférer les alertes vers NetWitness Suite Respond

- **Pour transférer les alertes NetWitness Suite Event Stream Analysis vers NetWitness Respond, procédez comme suit :**
  a. Sélectionnez **ADMIN > Services > service ESA**.
  b. Sélectionnez un service Event Stream Analysis, puis cliquez sur **> Vue > Config**.
  c. Cliquez sur l'onglet **Advanced**.
  d. Vérifiez que la case à cocher **Transférer les alertes vers le bus de messages** est sélectionnée par défaut. Sinon, activez la case à cocher **Transférer les alertes vers le bus de messages**, puis cliquez sur **Appliquer**.

- **Pour transférer les alertes NetWitness Suite Reporting Engine vers NetWitness Respond, procédez comme suit :**
  a. Sélectionnez **ADMIN > Services > service Reporting Engine**.
  b. Cliquez sur **> Vue > Config** pour le service Reporting Engine.
  c. Cliquez sur l'onglet **Général**.
  d. Dans la section **Configuration système**, activez la case à cocher **Transférer des alertes vers Respond**, puis cliquez sur **Appliquer**.

- **Pour transférer les alertes NetWitness Suite Malware Analysis vers NetWitness Respond, procédez comme suit :**
  a. Sélectionnez **ADMIN > Services > service Malware Analysis**
  b. Cliquez sur > **Vue** > **Config** pour le service Malware Analysis.
  c. Cliquez sur l'onglet **Audit**.

d. Dans la section **Répondre aux alertes**, vérifiez que la case à cocher **Valeur de configuration activée** est sélectionnée. Si la case à cocher n'est pas sélectionnée, puis cliquez sur **Appliquer**.

Étape 4 : Transférer les alertes vers NetWitness Suite Respond

Les alertes RSA Endpoint peuvent être envoyées à RSA Archer GRC via NetWitness Respond. Pour plus d'informations sur la façon de configurer des alertes NetWitness Endpoint via un bus de messages, consultez la rubrique « Configurer des alertes Endpoint via un bus de messages » dans le *Guide d'intégration de RSA NetWitness Endpoint*.

Étape 5 : Agrégez les alertes dans les incidents

Les alertes arrivant dans NetWitness Respond peuvent être automatiquement agrégées sous la forme d'incidents et transférées vers RSA Archer Security Operations Management. Les règles d'agrégation sont automatiquement exécutées chaque minute et permettent d'agréger les alertes en incidents en fonction des conditions de mise en correspondance et des options de regroupement sélectionnées. Pour plus d'informations sur l'agrégation des alertes, reportez-vous à la rubrique « Configurer les sources d'alertes pour afficher les alertes dans Respond » dans le *Guide de configuration de NetWitness Respond*.

Pour configurer l'agrégation des alertes :

1. Sélectionnez **CONFIGURER > Règles de l'incident**.
2. Pour activer les règles fournies prêtes à l'emploi, procédez comme suit :
   a. Double-cliquez sur la règle.
   b. Sélectionnez **Activé**.
   c. Cliquez sur **Enregistrer**.
   d. Répétez les étapes a à c pour chaque règle.
3. Pour ajouter une nouvelle règle, procédez comme suit :
   a. Cliquez sur +.
   b. Sélectionnez **Activé**.
   c. Renseignez les champs suivants :
      - Nom de la règle
      - Action
      - Conditions de mise en correspondance
      - Options de regroupement
      - Options d'incident

- Priorité
- Notifications

4. Cliquez sur **Enregistrer**.

Configurer Reporting Engine pour l'intégration avec NetWitness SecOps Manager

Pour configurer l'action de sortie Syslog d'un Reporting Engine, procédez comme suit :

1. Sélectionnez **ADMIN > Services**.
2. Sélectionnez votre service Reporting Engine, puis cliquez sur **Vue** > **Config**.
3. Cliquez sur l'onglet **Actions de sortie**.
4. Dans la section **Configuration NetWitness Suite**, dans le champ **Nom d'hôte**, saisissez le nom d'hôte ou l'adresse IP de votre serveur Reporting Engine.
5. Dans la section **Configuration Syslog**, ajoutez la configuration Syslog comme suit :
   a. Dans le champ **Nom du serveur**, saisissez le nom d'hôte du système UCF.
   b. Dans le champ **Port de serveur**, saisissez le port que vous avez sélectionné lors de la configuration Syslog du système UCF.
   c. Dans le champ **Protocole**, sélectionnez le protocole de transport.

   Remarque : Si vous sélectionnez le mode TCP sécurisé, la connexion SSL doit être configurée.
6. Cliquez sur **Enregistrer**.

Pour configurer la connexion SSL NetWitness Suite Reporting Engine pour le serveur Syslog sécurisé :

Si le serveur Syslog est configuré en mode TCP sécurisé, configurez la connexion SSL.

1. Copiez le certificat `keystore.crt.der` à partir de la machine UCF vers la zone du serveur NetWitness Suite sur `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3.x86_64/jre/lib/security`
2. Exécutez la commande suivante :

```
keytool -import -file keystore.crt.der -alias ucf-syslog -keystore /etc/pki/nw/trust/truststore.jks -storepass changeit
```

Remarque : N'effectuez pas un copier-coller du code ci-dessus. Saisissez-le pour éviter de faire des erreurs.

3. Activez **ServerCertificateValidationEnabled** sur **true:**
   - Accédez à **ADMIN** > **Service**.
   - Cliquez sur > **Vue > Explorer** du service Reporting Engine.
   - Développez **com.rsa.soc.re** > **Configuration** > **SSLContextConfiguration**.
   - Développez **sslContextConfiguration** et définissez **ServerCertificateValidationEnabled** sur **true**.
4. Redémarrez le service Reporting Engine.

Pour configurer des règles dans NetWitness Suite :

1. Cliquez sur **SURVEILLER >Rapports > Gérer**.
   L'onglet Gérer s'affiche.
2. Dans le panneau **Groupes de règles**, cliquez sur +.
3. Saisissez le nom du nouveau groupe.
4. Sélectionnez le groupe que vous avez créé, puis dans la barre d'outils Règle, cliquez sur +.
5. Dans le champ **Type de règle**, sélectionnez Base de données NetWitness.
6. Saisissez un nom pour la règle.
7. Saisissez des valeurs dans les champs **Select** et **Where** en fonction de la règle que vous souhaitez créer.

   Remarque : Ajoutez la configuration Syslog au nom Syslog défini ci-dessus.
8. Cliquez sur **Enregistrer**.

Remarque : Pour visualiser le même nombre d'alertes dans Reporting Engine et RSA Archer GRC, vérifiez que vous avez sélectionné Une fois pour une exécution dans les onglets Syslog et Enregistrement.

Pour ajouter des modèles d'alerte pour le Reporting Engine dans NetWitness Suite :

La configuration Syslog du système UCF est fournie avec des modèles d'alerte prêts à l'emploi que vous pouvez utiliser lors de la création d'une alerte avec une action de sortie Syslog. Ces modèles définissent les critères permettant d'agréger les alertes en incidents sur votre plate-forme RSA Archer GRC.

Les exemples de modèles se trouvent à l'emplacement suivant sur le système UCF :

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates`

1. Cliquez sur **SURVEILLER > Rapports > Gérer > Alertes**.
2. Cliquez sur l'onglet **Modèle**.
3. Cliquez sur ✚.
4. Dans le champ **Nom**, saisissez le nom du modèle d'alerte.
5. Dans le champ **Message**, saisissez le message d'alerte.
6. Cliquez sur **Create**.
7. Répétez les étapes 3 à 6 pour chaque modèle d'alerte à ajouter.

Pour configurer des alertes dans NetWitness Suite :

Dans RSA NetWitness Suite Reporting Engine, une alerte est une règle que vous pouvez planifier pour une exécution continue et dont les conclusions peuvent se présenter sous différentes formes de sortie d'alerte.

1. Cliquez sur **SURVEILLER > Rapports > Gérer > Alertes**.
2. Cliquez sur ✚.
3. Sélectionnez **Activer**.
4. Sélectionnez la règle que vous avez créée.
5. Sélectionnez **Transmettre aux décodeurs**.

   Remarque : Si vous ne saisissez aucune valeur dans ce champ, le lien dans l'application Alertes de sécurité de RSA Archer ne fonctionnera pas dans RSA NetWitness Suite.
6. Dans le champ Sources de données, sélectionnez votre source de données.
7. Dans la section **Notification**, sélectionnez **Syslog**.
8. Cliquez sur ✚.
9. Complétez les champs de configuration Syslog.
10. Dans le champ **Modèle de corps**, sélectionnez le modèle que vous souhaitez utiliser pour cette alerte Syslog.
11. Cliquez sur **Enregistrer**.

Pour plus d'informations, reportez-vous à la section « Configurer Event Stream Analysis pour une intégration à Archer SecOps ».

Pour configurer les paramètres de notification Syslog d'Event Stream Analysis NetWitness Suite :

1. Cliquez sur **ADMIN** > **Système** > **Notifications globales**.
2. Cliquez sur l'onglet **Sortie**.
3. Définissez et activez une notification Syslog d'Event Stream Analysis.
4. Cliquez sur l'onglet **Serveurs**.
5. Définissez et activez un serveur de notification Syslog.
6. Dans la section Informations sur le serveur Syslog, saisissez ce qui suit :

   Description du champ :

   - Nom : spécifiez le nom personnalisé
   - IP du serveur (nom d'hôte) : spécifiez le nom d'hôte ou l'adresse IP du système ayant permis d'installer le composant UCF.
   - Port : spécifiez le numéro du port sur lequel vous souhaitez que le système UCF écoute.
   - Site : spécifiez le site Syslog
   - Protocole : sélectionnez le protocole.
7. Cliquez sur **Enregistrer**.

Pour configurer la connexion SSL NetWitness Suite Event Stream Analysis pour le serveur Syslog sécurisé :

Si le serveur Syslog est configuré en mode TCP sécurisé, configurez la connexion SSL.

1. Sélectionnez **ADMIN >Services**.
2. Sélectionnez le service Event Stream Analysis. Accédez à **Explorer > Configuration > SSL**.
3. Définissez **ServerCertificateValidationEnabled** sur **true**.
4. Copiez `rootcastore.cert.pem` de la machine UCF vers le serveur Event Stream Analysis sur `/etc/pki/ca-trust/source/anchors`.
5. Exécutez la commande suivante :

```
update-ca-trust
```

6. Redémarrez le service Event Stream Analysis.

Pour ajouter des modèles d'alerte Event Stream Analysis

La configuration Syslog du système UCF est fournie avec des modèles d'alerte prêts à l'emploi que vous pouvez utiliser lors de la création d'une alerte avec une action de sortie Syslog. Ces modèles définissent les critères permettant d'agréger les alertes en incidents sur votre plate-forme RSA Archer GRC.

Les exemples de modèles se trouvent à l'emplacement suivant sur le système UCF :

`<install_dir>\SA IM integration service\config\mapping\templates\SecOps_SA_`

`Templates\SecOps_SA_ESA_templates.txt`

1. Sélectionnez **ADMIN > Système > Notifications globales**.
2. Cliquez sur l'onglet **Modèles**.
3. Cliquez sur ✚.
4. Dans le champ **Type de modèle**, sélectionnez Event Stream Analysis.
5. Dans le champ **Nom**, saisissez le nom du modèle.
6. (Facultatif) Dans le champ **Description**, saisissez une brève description du modèle.
7. Dans le champ **Modèle**, saisissez le message d'alerte.
8. Cliquez sur **Enregistrer**.
9. Répétez les étapes 3-8 pour chaque modèle d'alerte à ajouter.

Pour créer des règles Event Stream Analysis

1. Cliquez sur **CONFIGURER** > **Règles ESA**.
2. Dans la **Bibliothèque de règles**, cliquez sur ✚.
3. Sélectionnez le **Générateur de règles**.
4. Dans le champ **Nom de la règle**, saisissez le nom de la règle.
5. Dans le champ **Description**, saisissez une description de la règle.
6. Sélectionnez une **Gravité**.
7. Dans la section **Condition**, procédez comme suit :
   a. Cliquez sur ✚ pour créer une instruction.
   b. Saisissez un nom, sélectionnez un type de condition et ajoutez les paires métadonnées/métavaleurs de votre instruction.

c. Cliquez sur **Enregistrer**.

d. Répétez les étapes a - c jusqu'à ce que toutes les instructions de votre règle soient créées.

8. Dans la section **Notifications**, sélectionnez **Syslog**.
9. Sélectionnez la notification, le serveur Syslog et le modèle qui ont été créés.
10. Cliquez sur **Enregistrer** et **Fermer**.
11. Cliquez sur **Configurer** > **Déploiements**.
12. Cliquez sur ✚ pour la section des services Event Stream Analysis.
13. Sélectionnez le service Event Stream Analysis.
14. Cliquez sur **Déployer maintenant**.
15. Dans la section **Règles Event Stream Analysis**, cliquez sur ✚ pour choisir la règle Event Stream Analysis que vous avez créée, puis cliquez sur **Déployer maintenant**.

Feeds RSA Archer

Par défaut, seuls les champs Adresse IP et Évaluation du degré de criticité au sein de l'application RSA Archer Devices sont renseignés dans RSA NetWitness Suite par le service d'intégration Security Analytics Incident Management. Vous pouvez personnaliser le plug-in Enterprise Management pour inclure les champs Business Unit et Facility qui font l'objet de références croisées dans l'application Devices au sein du feed. Pour plus de détails, reportez-vous à la documentation sur le site https://community.emc.com/community/connect/grc_ecosystem/rsa archer ou https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.

Remarque : Si vous envisagez de renseigner les champs Business Unit et Facility à partir de votre plate-forme RSA Archer GRC dans Live, vous devez également ajouter des clés à ces champs dans le fichier index-concentrator-custom.xml.

Mettre à jour les services Concentrator et Decoder

Le service d'intégration SA IM dans NetWitness SecOps Manager gère les fichiers d'un feed personnalisé et dépose ces fichiers dans un dossier local que vous spécifiez lors de la configuration du service d'intégration Enterprise Management. Le module Live de RSA NetWitness Suite récupère les fichiers de feed dans ce dossier. Ensuite, Live transmet le feed aux services Decoder qui commencent à créer les métadonnées en fonction du trafic réseau capturé et de la définition du feed. Pour que chaque Concentrator identifie les nouvelles métadonnées créées par les services Decoder, vous devez modifier `index-concentrator-custom.xml`, `index-logdecoder-custom.xml` et `index-decoder-custom.xml files`.

1. Sélectionnez **Admin > Services**.
2. Sélectionnez votre service Concentrator, puis cliquez sur  > **Vue > Config**.
3. Cliquez sur l'onglet **Fichiers**.
4. Dans la liste déroulante, sélectionnez le fichier index-concentrator-custom.xml. Exécutez l'une des opérations suivantes :
   - Si le contenu existe déjà dans le fichier, ajoutez une clé pour le nouvel élément de métadonnées comme suit :

     ```
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     ```

     Remarque : N'effectuez pas un copier-coller du code. Saisissez-le pour éviter de faire des erreurs.
   - Si le fichier est vide, ajoutez le contenu suivant :

     ```
     <?xml version="1.0" encoding="utf-8"?>
     <language level="IndexNone" defaultAction="Auto">
     <key description="Criticality" format="Text" level="IndexValues"
     name="criticality" defaultAction="Open"/>
     </language>
     ```
5. Cliquez sur **Appliquer**.
6. Pour ajouter plusieurs périphériques, procédez comme suit :
   a. Cliquez sur **Push**.
   b. Sélectionnez les périphériques auxquels vous souhaitez transmettre ce fichier.
   c. Cliquez sur **OK**.
7. Répétez les étapes 1 à 7 pour les composants Log Decoder et Index Decoder à l'aide des fichiers index-logdecoder-custom.xml et index-decoder-custom.xml.
8. Arrêtez, puis redémarrez les services Concentrator et Decoder.

Ajouter le point de terminaison RSA Archer Enterprise Management au système UCF

1. Dans le gestionnaire de connexions UCF, sélectionnez le mode, comme suit :
   a. Saisissez le numéro correspondant à la Sélection du mode.
   b. Sélectionnez l'une des options suivantes :

- Gérer le workflow d'incidents dans RSA NetWitness Suite.
- Gérer le workflow d'incidents de manière exclusive dans RSA Archer Security Operations Management.

2. Ajoutez le point de terminaison RSA Archer Enterprise Management comme suit :
   a. Saisissez le numéro correspondant à la ligne Enterprise Management.
   b. Complétez les champs du tableau ci-dessous.

Champ	Description
Nom du point de terminaison	Nom facultatif du point de terminaison.
Port du serveur Web	Paramètre par défaut : 9090. Peut être configuré pour héberger l'adresse URL du serveur Web. L'URL et le numéro de port doivent être fournis en tant qu'URL du feed NetWitness Suite Live : http://hostname:port/archer/sa/feed
Degré de criticité	Degré de criticité des ressources à extraire de RSA Archer GRC. Si la valeur **false** est définie, extraction des ressources avec degré de criticité. Si la valeur **true** est définie, extraction des ressources avec uniquement un degré de criticité élevé (High). Pour effectuer la configuration manuellement, modifiez la propriété em.criticality dans le fichier de propriétés collector-config pour fournir une liste de degrés de criticité séparés par une virgule : LOW, MEDIUM, HIGH.
Répertoire Feed	Répertoire dans lequel le fichier CSV des ressources de RSA Archer GRC sont sauvegardées. **Remarque :** Le chemin d'accès au répertoire fourni doit être présent.
Nom d'utilisateur du serveur Web	Nom d'utilisateur permettant l'authentification sur le serveur Web EM. **Remarque :** Il est fourni lors de la configuration du feed NetWitness Suite Live.

Champ	Description
Mot de passe du serveur Web	Mot de passe permettant l'authentification sur le serveur Web EM. **Remarque :** Il est fourni lors de la configuration du feed NetWitness Suite Live.
Mode SSL	La valeur par défaut est Non. Si **Non**, l'adresse URL utilise `http mode: http://hostname:port/archer/sa/feed` Si vous n'avez pas mis à jour le fichier d'hôte, reportez-vous à la section « Mettre à jour le fichier hôte RSA NetWitness Suite ». **Remarque :** NetWitness Suite ne prend actuellement pas en charge les feeds récurrents Archer en mode SSL.

Mette à jour le fichier hôte RSA NetWitness Suite

1. Modifiez le fichier Hôte sur le serveur NetWitness Suite à l'emplacement suivant : vi /etc/hosts
2. Saisissez ce qui suit pour l'adresse IP de l'hôte UCF :

   ```
   <ucf-host-ip> <ucf-host-name>
   ```

3. Redémarrez le serveur NetWitness Suite en exécutant la commande suivante :

   ```
   service jetty restart
   ```

4. Lors de la configuration du feed NetWitness Suite Live, saisissez le nom d'hôte de l'URL au lieu de l'adresse IP et du numéro de port configurés pour le point de terminaison Enterprise Management sur le système UCF :

   ```
   http: //<ucf-host-name> : <EM_Port>/archer/sa/feed.
   ```

5. Vérifiez que la connexion est active.

Créer une tâche de feed récurrente

Pour que RSA NetWitness Suite puisse télécharger les fichiers de feed à partir du service d'intégration NetWitness Respond et transmettre les feeds aux services Decoder, vous devez créer une tâche de feed récurrente et définir les paramètres de feed.

Remarque : Pour RSA Archer SecOps 1.2 : Pour que RSA NetWitness Suite puisse télécharger les fichiers de feed à partir de votre machine RCF et transmettre les feeds aux services Decoder, vous devez créer une tâche de feed récurrente et définir les paramètres de feed. La procédure est similaire à RSA Archer SecOps 1.3, avec néanmoins quelques exceptions. Pour plus de détails, reportez-vous à la documentation sur le site RSA Archer Exchange Community.

1. Sélectionnez **CONFIGURER > Feeds personnalisés**.
2. Dans la vue Feeds, cliquez sur ✚.
3. Sélectionnez **Feed personnalisé**, puis cliquez sur **Suivant**.
4. Sélectionnez **Récurrent**.
5. Saisissez un nom pour le feed.
6. Dans le champ URL, saisissez l'un des éléments suivants :

   `http://ucf_hostname/archer/sa/feed`

   où *`http :ucf_hostname_or_ip:port`* est l'adresse de votre système du service d'intégration NetWitness Respond. Par exemple : `http://10.10.10.10:9090` .

   Remarque : Si Respond est en cours d'exécution en mode SSL, le nom d'hôte doit être utilisé dans l'URL.
7. Sélectionnez **Authentifié**.
8. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification du compte d'utilisateur que vous avez créées pour RSA NetWitness Suite en vue d'utiliser les fichiers d'accès du service d'intégration NetWitness Respond.
9. Définissez l'intervalle de récurrence du feed.
10. Dans la section **Période**, définissez une date de début et une date de fin pour le feed, puis cliquez sur **Suivant**.
11. Sélectionnez chaque service Decoder auquel vous souhaitez transmettre ce feed, puis cliquez sur **Suivant**.
12. Dans le champ **Type**, vérifiez que l'adresse IP est sélectionnée.
13. Dans le champ **Colonne index**, sélectionnez 1.
14. Dans la deuxième colonne, définissez la valeur Clé de degré de criticité, puis cliquez sur **Suivant**.
15. Vérifiez vos détails de configuration de feed, puis cliquez sur **Terminer**.

Gérer RSA Unified Collector Framework

Cette rubrique fournit d'autres tâches de configuration et de gestion de RSA Unified Collector Framework (UCF) pour l'intégration d'Archer SecOps 1.3.1.2.

Démarrer RSA Unified Collector Framework

1. Cliquez sur **Panneau de configuration > Outils d'administration > Services**.
2. Sélectionnez RSA Unified Collector Framework.
3. Cliquez sur **Démarrer**.

Arrêter RSA Unified Collector Framework

1. Cliquez sur **Panneau de configuration > Outils d'administration > Services**.
2. Arrêtez le service RSA SecOps WatchDog.

   Remarque : Si vous n'arrêtez pas le service Watchdog, celui-ci démarrera le service NetWitness Respond plus tôt que prévu.
3. Sélectionnez RSA Unified Collector Framework.
4. Cliquez sur **Arrêter**.

Remarque : Si le service met trop de temps à s'arrêter, utilisez le Gestionnaire des tâches pour mettre fin à RSASAIMDCService.

Désinstaller RSA Unified Collector Framework

1. Cliquez sur **Panneau de configuration**> **Programmes et fonctionnalités**.
2. Sélectionnez **RSA Unified Collector Framework**.
3. Cliquez sur **Désinstaller**.

Dépanner l'intégration de RSA Archer

Cette section donne des instructions pour résoudre les problèmes communs que vous pouvez rencontrer lors de la configuration d'Archer SecOps 1.3.1.2 avec NetWitness Suite Respond.

Configurer le magasin d'approbations de l'autorité de certification (AC)

Problème : Après avoir ajouté le point de terminaison pour NetWitness Suite Respond, le magasin d'approbations de l'autorité de certification ne parvient pas à se configurer.

Solution :

1. Assurez-vous que les informations d'identification SSH de l'hôte NetWitness Suite sont valides.
2. Si les informations d'identification sont correctes mais que des erreurs se produisent encore, copiez manuellement les certificats.

Tâches de remédiation dans RSA Archer Security Operations Manager

Problème : Les tâches de remédiation qui sont envoyées à la file d'attente des Opérations via UCF n'apparaissent pas dans RSA Archer Security Operations Management comme conclusions.

Solution :

1. Ouvrez Connection Manager :
   - Ouvrez une invite de commande
   - `Remplacez les répertoires par <rép_installation>\SA IM integration service\data-collector.`
   - `Saisissez : runConnectionManager.bat`
2. Saisissez 2 pour modifier le point de terminaison.
3. Saisissez 3 pour NetWitness Suite Respond.
4. Assurez-vous que la file d'attente est configurée sur Tous ou Opérations.

Erreurs entre RSA NetWitness Suite et RSA Unified Collector Framework

Problème : Dans `<install_dir>\SA IM integration service\logs\collector.log`, il existe des erreurs SSL entre RSA NetWitness Suite et RSA Unified Collector Framework.

Solution :

1. Vérifiez que les certificats SSL sont valides.

   Remarque : Les certificats NetWitness Suite Respond sont valables pendant deux ans.

2. Si vos certificats ont expiré, générez de nouveau et copiez les certificats expirés.

Pour générer de nouveau et copier les certificats, procédez comme suit :

1. Dans l'invite de commande, accédez à `<install_dir>\SA IM integration service\data-collector`.
2. Saisissez : `runConnectionManager.bat`
3. Saisissez le numéro de certificat Regenerate SA IM Integration Service.
4. Dans le point de terminaison NetWitness Suite Respond, dans le Gestionnaire de connexion, entrez le nombre correspondant à la modification du point de terminaison.
5. Saisissez Oui pour copier automatiquement les certificats dans la zone de stockage fiable NetWitness Suite.

Remarque : Si la copie des certificats a échoué, procédez manuellement.