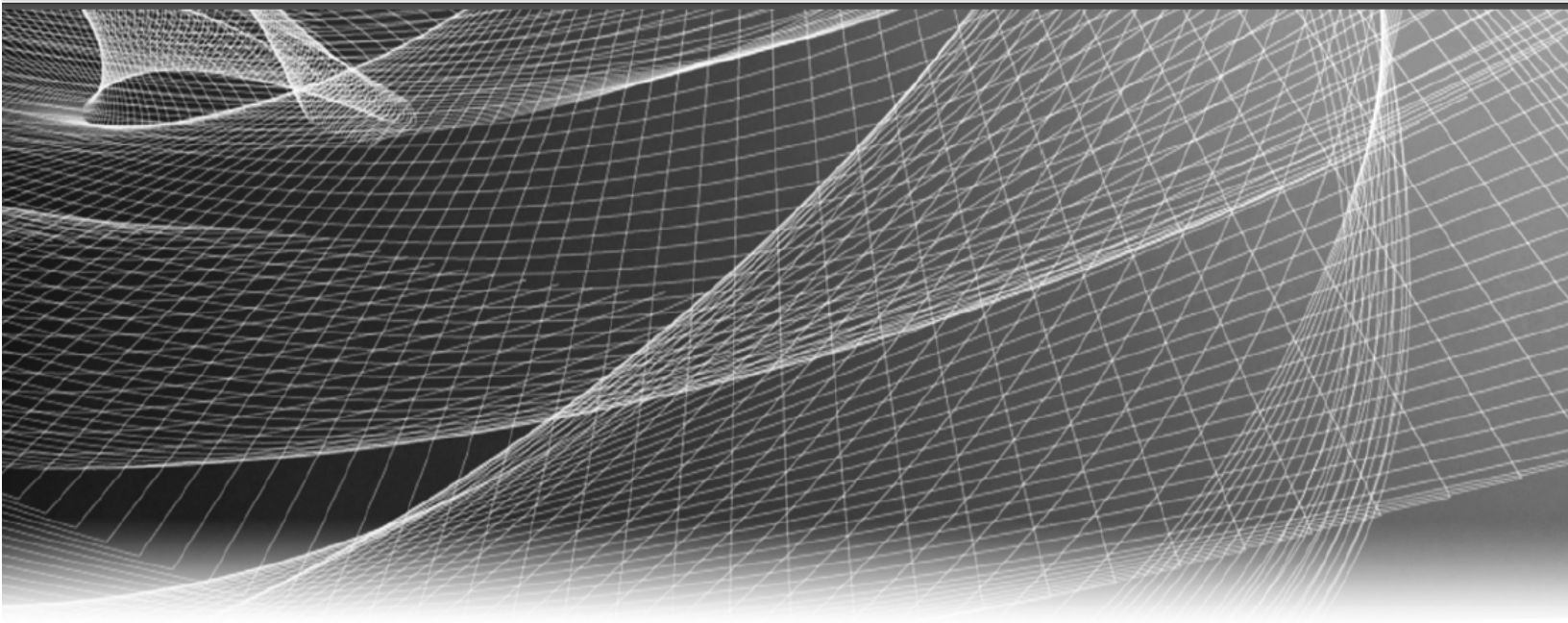

RSA Security Analytics

Guide d'intégration de RSA Archer

pour la version 10.6

RSA EMC²

Marques commerciales

Contrat de licence

Licences tierces

Remarque sur les technologies de chiffrement

Distribution

Sommaire

Intégration de RSA Archer **5**

Configurer Security Analytics pour une utilisation avec Archer **6**

Méthodes d'intégration 6

Service d'intégration Security Analytics Incident Management (SAIM) 7

RSA Unified Collector Framework (UCF) 7

Conditions préalables 8

Intégrations de RSA Unified Collector Framework 8

Créer des comptes utilisateurs RSA Archer pour les opérations de transmission (Push) et d'extraction (Pull) 9

Configurer les points de terminaison dans RSA Unified Collector Framework 10

Configurer l'action de sortie Syslog du Reporting Engine pour Security Analytics 10.5 ..14

Configurer les paramètres de notification Syslog pour ESA dans Security Analytics 10.5 ou version ultérieure 15

Configurer Incident Management pour une intégration à Archer SecOps 1.3 16

Étape 1 : Configurez la base de données Incident Management 16

Étape 2 : Sélectionnez le mode Security Analytics Incident Management 17

Étape 3 : Configurer le transfert vers le service Security Analytics Incident Management 18

Étape 4 : Transférez les alertes ECAT vers le service Security Analytics Incident Management 19

Étape 5 : Agrégez les alertes dans les incidents 19

Configurer l'action de sortie Syslog du Reporting Engine pour Security Analytics 20

Configurer la connexion SSL SA RE pour le serveur Syslog sécurisé 21

Configurer les règles dans Security Analytics 21

Ajouter des modèles d'alerte pour le Reporting Engine dans Security Analytics 22

Configurer les alertes dans Security Analytics 23

Configurer les paramètres de notification Syslog pour ESA dans Security Analytics 23

Configurer la connexion SSL SA ESA pour le serveur Syslog sécurisé dans Security Analytics 24

Ajouter des modèles d'alerte ESA dans Security Analytics 25

Créer des règles ESA dans Security Analytics 25

Feeds RSA Archer 26

Mettre à jour les services Concentrator et Decoder 27
Ajouter le point de terminaison RSA Archer Enterprise Management au système UCF ... 28
Mettre à jour le fichier Hôte RSA Security Analytics pour le mode SSL 30
Créer une tâche de feed récurrente 30
Gérer RSA Unified Collector Framework 32
Démarrer RSA Unified Collector Framework 32
Arrêter RSA Unified Collector Framework 32
Désinstaller RSA Unified Collector Framework 32

Dépanner l'intégration de RSA Archer 33

Configurer le magasin d'approbations de l'autorité de certification (AC) 33
Copier manuellement des certificats Enterprise Management 33
Certificats Security Analytics Incident Management 34
Incidents dans la solution RSA Archer Security Operations Management 34
Tâches de remédiation dans RSA Archer Security Operations Management 36
Erreurs entre RSA Security Analytics et RSA Unified Collector Framework 36

Intégration de RSA Archer

Les administrateurs peuvent intégrer de RSA Security Analytics avec RSA Archer Security Operations (SecOps) pour envoyer des alertes et les incidents à partir de Security Analytics vers Archer pour la gestion et la résolution des incidents. Ce guide fournit un workflow global pour la configuration de cette intégration.

Vous pouvez intégrer Security Analytics à RSA Archer SecOps pour effectuer les actions suivantes :

- Gestion des incidents : Tous les incidents créés dans Security Analytics peuvent être entièrement gérés dans Archer.
- Résolution des incidents : Les incidents sont traités dans Security Analytics, mais les tâches de correction sont éventuellement exportées dans Archer.

Version d'Archer SecOps	Security Analytics 10.5 Integration	Référence
1.1	Module Event Stream Analysis (ESA)	Consultez la section **Configurer un modèle** dans le guide *Configuration système* : Configuration système > Procédures standard > Configurer des modèles pour les notifications > Configurer un modèle
1.2	Gestion des incidents	Consultez la section **Configurer le paramètre d'intégration pour gérer les incidents dans RSA Archer Security Operations** dans le guide *Gestion des incidents* : Gestion des incidents > Intégration système > Configurer le paramètre d'intégration pour gérer les incidents dans RSA Archer Security Operations

Topics

- Configurer Security Analytics pour une utilisation avec Archer
- Dépanner l'intégration de RSA Archer

Configurer Security Analytics pour une utilisation avec Archer

RSA Security Analytics peut être configuré pour envoyer des alertes et des signalements d'incidents à RSA Archer à des fins de gestion et de correction des incidents. L'intégration de Security Analytics à RSA Archer SecOps permet d'effectuer les actions suivantes :

- Gestion des incidents : Tous les incidents créés dans Security Analytics peuvent être entièrement gérés dans Archer.
- Résolution des incidents : Les incidents sont traités dans Security Analytics, mais les tâches de remédiation sont éventuellement exportées dans Archer.

La solution RSA Archer Security Operations Management 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 Archer Sec Ops, reportez-vous à la documentation RSA Archer sur le site RSA Archer Community ou le site de RSA Archer Exchange Community.

Reportez-vous au *Guide d'installation de SecOps* pour en savoir plus sur les plates-formes Archer prises en charge.

La version de RSA Archer détermine comment RSA Security Analytics sera intégrée.

- RSA Archer Security Operations Management 1.2 s'intègre à RSA Security Analytics à l'aide de RSA UCF (Unified Collector Framework) qui comprend le service d'intégration SAIM et RCF (RSA Connector Framework).
- RSA Archer Security Operations Management 1.3 s'intègre à RSA Security Analytics à l'aide de RSA UCF (Unified Collector Framework) qui comprend le service d'intégration SAIM et le service SecOps Watchdog.

Méthodes d'intégration

Vous devez configurer les paramètres d'intégration système pour gérer le workflow d'incidents dans RSA Archer Security Operations Management. Lorsque ces paramètres sont configurés, les incidents et les tâches de remédiation ne sont plus visibles dans RSA Security Analytics.

Pour plus d'informations sur la configuration des paramètres d'intégration système pour gérer le workflow d'incidents dans RSA Archer Security Operations, reportez-vous à la rubrique **Configurer le paramètre d'intégration pour gérer les incidents dans RSA Archer Security Operations** dans le*Guide d'Incident Manager* (Incident Management> Intégration système > Configurer le paramètre d'intégration pour gérer les incidents dans RSA Archer Security Operations).

Service d'intégration Security Analytics Incident Management (SAIM)

Le service d'intégration Security Analytics Incident Management (SAIM) intègre les solutions RSA Archer Security Operations Management 1.2 et 1.3 au module RSA Security Analytics Incident Management. Vous pouvez choisir l'une des options d'intégration suivantes :

- Gérer le workflow complet des incidents dans RSA Archer Security Operations Management. Si vous sélectionnez cette option, le service d'intégration Security Analytics Incident Management transfère les incidents du module Security Analytics Incident Management vers la solution.
- Gérer le workflow des incidents dans le module Security Analytics Incident Management et permettre aux analystes de faire remonter les tâches de remédiation et les violations de données existantes vers la solution RSA Archer Security Operations Management. Si vous sélectionnez cette option, le service d'intégration Security Analytics Incident Management 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 Security Analytics et le service d'intégration Security Analytics Incident Management.

RSA Unified Collector Framework (UCF)

RSA Security Analytics s'intègre à RSA Archer SecOps 1.3 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 Archer Security Operations Management. Lorsque vous intégrez le module RSA Security Analytics Incident Management, vous pouvez choisir l'une des options d'intégration suivantes :

- Gérez le workflow complet des incidents dans RSA Archer Security Operations Management. Si vous sélectionnez cette option, Unified Collector Framework transfère les incidents du module Security Analytics Incident Management vers la solution.

- Gérer le workflow des incidents dans le module Security Analytics Incident Management et permettre aux analystes de faire remonter les tâches de remédiation et les violations de données existantes vers la solution RSA Archer Security Operations Management. Si vous sélectionnez cette option, 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 Security Analytics et Unified Collector Framework.
• L'intégration du module RSA Security Analytics Incident à Reporting Engine ou ESA peut engendrer la création d'événements ou d'incidents dupliqués dans RSA Archer SecOps.

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

Conditions préalables

- Installez RSA Archer Security Operations Management. Reportez-vous à la documentation RSA Archer sur le site RSA Archer Community ou à partir de l'onglet Contenu du site https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Security Analytics 10.5 ou une version ultérieure est compatible avec SecOps 1.2 et SecOps 1.3. Security Analytics 10.5 est également compatible avec SecOps 1.1, cependant, ce n'est pas recommandé.
- Il est recommandé d'effectuer une mise à niveau vers SecOps 1.3 en cas d'utilisation de Security Analytics 10.6.
- Vérifiez que le module Incident Management est configuré dans RSA Security Analytics.
- Pour Archer SecOps 1.3, vous devez créer un compte utilisateur pour que le client de service Web puisse transférer les données vers la plate-forme RSA Archer GRC.

Intégrations de RSA Unified Collector Framework

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

- Security Analytics Incident Management (SA IM)
- Security Analytics Reporting Engine (SA RE)
- Security Analytics Event Stream Analysis (SA ESA)

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

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

1. Cliquez sur **Administration** > **Contrôle d'accès** > **Gérer les 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 ce 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 Security Analytics 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 Syslog Archer Push
- Security Analytics Incident Management (SA IM)
- Point de terminaison du plug-in Archer Pull Enterprise Management
- Sélection du mode : Mode SecOps ou Non-SecOps.
- Serveur Syslog
- Enterprise Management

Remarque :
• Si le mode Non-SecOps est sélectionné, les incidents sont gérés dans SA IM au lieu de RSA Archer Security Operations Management.
• Vous devez configurer les ports TCP, TCP sécurisé et UDP.
• Vérifiez que le nom du sujet du certificat de votre serveur RSA Archer GRC correspond au nom de l'hôte.

Procédure

1. Sur votre système UCF, ouvrez le gestionnaire de connexions, comme suit :
   a. Ouvrez une invite de commande.
   b. Remplacez les répertoires par <*rép_install*>\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. Ajoutez un point de terminaison pour RSA Security Analytics Incident Management, comme suit :

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 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 Security Analytics, procédez comme suit :

i. Saisissez **Oui**.

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

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.

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

a. Saisissez le numéro correspondant à Sélection du mode.

b. Sélectionnez l'une des options suivantes :

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

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

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

b. Fournissez les informations suivantes (en anglais) :

- Description du champ
- SSL configuré
- Port TCP
- Sécurisez le port TCP si le client Syslog envoie le message Syslog en mode TCP sécurisé.

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

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**.

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.

8. Pour tester le client Syslog, saisissez le numéro correspondant à la ligne Tester le client Syslog. Utilisez la fonctionnalité Tester le client Syslog avec les fichiers issus de *<rép_install>*\SA IM integration service\config\mapping\test-files\.
9. Dans le gestionnaire de connexions, saisissez **5** pour tester chaque point de terminaison.

Configurer l'action de sortie Syslog du Reporting Engine pour Security Analytics 10.5

Remarque : Cette procédure est destinée à SecOps 1.3 avec Security Analytics 10.5.

1. Dans Security Analytics, accédez à **Administration** > **Services**.
2. Sélectionnez votre service Reporting Engine, puis cliquez sur **Système** > **Config**.
3. Cliquez sur l'onglet **Actions de sortie**.

4. Dans la section Configuration SA, dans le champ Nom d'hôte, saisissez le nom d'hôte ou l'adresse IP de votre serveur Reporting Engine.

   Remarque : Si vous ne saisissez aucune valeur dans ce champ, le lien dans l'application d'alerte RSA Archer Security ne fonctionnera pas dans Security Analytics.

5. 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**.

Configurer les paramètres de notification Syslog pour ESA dans Security Analytics 10.5 ou version ultérieure

Cette procédure est destinée à SecOps 1.3 avec Security Analytics 10.5 ou version ultérieure.

1. Cliquez sur **Administration** > **Système** > **Notifications globales**.
2. Cliquez sur l'onglet **Sortie**.
3. Définissez et activez une notification Syslog pour ESA.
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 :

Champ	Description
Nom du serveur	Nom d'hôte ou adresse IP du système ayant permis d'installer le composant UCF.
Port de serveur	Numéro du port sur lequel vous souhaitez que le système UCF écoute les messages d'alerte Syslog.
Site	Site Syslog.
Protocole	Choix du protocole.

7. Cliquez sur **Enregistrer**.

Configurer Incident Management pour une intégration à Archer SecOps 1.3

Pour configurer Incident Management pour Archer SecOps 1.3, effectuez les opérations suivantes dans Security Analytics :

Tâche / Link pour obtenir des Instructions
Étape 1 : Configurez la base de données Incident Management
Étape 2 : Sélectionnez le mode Security Analytics Incident Management
Étape 3 : Configurer le transfert vers le service Security Analytics Incident Management
Étape 4 : Transférez les alertes ECAT vers le service Security Analytics Incident Management
Étape 5 : Agrégez les alertes dans les incidents

Étape 1 : Configurez la base de données Incident Management

Vous devez configurer la base de données du service de gestion des incidents (Incident Management) pour qu'elle puisse être utilisée.

Pour configurer une base de données pour le service Incident Management :

1. Dans le menu Security Analytics, sélectionnez **Administration** > **Services**.

   La vue Services s'affiche.

2. Dans le panneau Service, sélectionnez le service Incident Management et cliquez sur  **> Vue > Explorer**.

   La vue Explorer les services s'affiche.

3. Dans le panneau des options, sélectionnez **Service > Configuration > base de données**.

   La vue de la base de données s'affiche dans le panneau de droite.

4. Fournissez les informations suivantes :

   - Hôte : nom de l'hôte ou adresse IP de l'hôte ESA sélectionné en tant que base de données
   - Nom de la base de données : im (valeur par défaut)
   - Port : 27017 (valeur par défaut)

- Nom d'utilisateur : nom d'utilisateur du compte utilisateur pour la base de données IM (ESA crée un utilisateur im avec les privilèges adéquats)
- Mot de passe : mot de passe que vous avez sélectionné pour l'utilisateur im

5. Redémarrez le service Gestion des incidents à l'aide de la commande suivante :

```
service rsa-im restart
```

Remarque : Il est important de redémarrer le service Incident Management pour terminer la configuration de la base de données.

Étape 2 : Sélectionnez le mode Security Analytics Incident Management

Pour sélectionner la méthode de gestion du workflow d'incidents dans Security Analytics :

1. Dans le menu Security Analytics, sélectionnez **Incidents > Configurer**.
2. Cliquez sur l'onglet **Intégration**.
3. Sélectionnez l'une des options suivantes :
   - Gérer le workflow d'incidents dans RSA Security Analytics.
     - Autoriser les analystes à faire remonter les tâches de remédiation de la file d'attente cible **Opérations** en tant que tickets.
     - Autoriser les analystes à faire remonter les tâches de remédiation de la file d'attente cible **GRC** en tant que conclusions.
     - Autoriser les analystes à signaler les violations de données et à déclencher le processus de réponse aux violations dans la solution RSA Archer Security Operations Management

       Pour plus d'informations, reportez-vous à la section **Configurer le paramètre d'intégration pour gérer des incidents dans Security Analytics** dans le *Guide d'Incident Management*.
   - Gérer le workflow d'incidents de manière exclusive dans RSA Archer Security Operations Management.
4. Cliquez sur **Appliquer**.

Remarque : Cette étape s'applique également à l'intégration à Archer SecOps 1.2.

Étape 3 : Configurer le transfert vers le service Security Analytics Incident Management

- Pour transférer les alertes Security Analytics Event Stream Analysis vers Security Analytics Incident Management, procédez comme suit :
  a. Dans le menu Security Analytics, sélectionnez **Administration > Services > Service ESA**.
  b. Sélectionnez un service ESA et  **> Vue > Configuration**.
  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. Si nécessaire, activez la case à cocher **Transférer les alertes vers le bus de messages**, puis cliquez sur **Appliquer**.
- Pour transférer les alertes Security Analytics Reporting Engine vers Security Analytics Incident Management, procédez comme suit :
  a. Dans Security Analytics, cliquez sur **Administration > Services > Service Reporting Engine**.
  b. Cliquez sur  **> Vue > Configuration** 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 IM**, puis cliquez sur **Appliquer**.
- Pour transférer les alertes Security Analytics Malware Analysis vers Security Analytics Incident Management, procédez comme suit :
  a. Dans Security Analytics, cliquez sur **Administration > Services > Service Malware Analysis**.
  b. Cliquez sur  >**Vue** > **Configuration** pour le service MA.
  c. Cliquez sur l'onglet **Audit**.
  d. Dans la section Alertes Incident Management, 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 : Transférez les alertes ECAT vers le service Security Analytics Incident Management

Les alertes RSA ECAT peuvent être envoyées à RSA Archer GRC via Security Analytics Incident Management.

1. Configurer des alertes par bus de messages :*Configurer les alertes ECAT via le bus de messages*.
2. Dans RSA ECAT, cliquez sur **Configurer > Composants de surveillance et externes**.
3. Dans la fenêtre Configuration des composants externes, sélectionnez Incident Message Broker.
4. Cliquez sur Add (+).
5. Renseignez les champs suivants :
   - Nom de l'instance
   - Nom d'hôte/IP du serveur. Saisissez l'adresse DNS ou l'adresse IP de l'hôte du serveur RSA Security Analytics.
   - Numéro de port. Le port par défaut est 5671.
6. Cliquez sur **Enregistrer**.

Étape 5 : Agrégez les alertes dans les incidents

Les alertes arrivant dans Security Analytics Incident Management 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 Incident Management** dans le *Guide de configuration d'Incident Management*.

Pour configurer l'agrégation des alertes :

1. Dans Security Analytics, accédez à **Incidents > Configurer > Règles d'agrégation**.
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 Add (+).

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 l'action de sortie Syslog du Reporting Engine pour Security Analytics

1. Dans Security Analytics, accédez à **Administration > Services**.
2. Sélectionnez votre service Reporting Engine, puis cliquez sur Système > Config.
3. Cliquez sur l'onglet **Actions de sortie**.
4. Dans la section Configuration SA, dans le champ Nom d'hôte, saisissez le nom d'hôte ou l'adresse IP de votre serveur Reporting Engine.
5. 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**.

Configurer la connexion SSL SA RE 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 qui se trouve dans <*rép_ install*>\RSA\SA IM integration service\cert-tool\certs to the Security Analytics server at **/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65-0.b17.el6_7.x86_64/jre/lib/security**
2. Exécutez la commande suivante :

   ```
   keytool -import -file keystore.crt.der -alias ucf-syslog -
   keystore cacerts -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 la page d'administration de l'interface utilisateur de SA.
   - Cliquez sur **Vue > Explorer** du service Reporting Engine.
   - Développez com.rsa.soc.re.
   - Développez sslContextConfiguration et définissez ServerCertificateValidationEnabled sur **true**.
4. Redémarrez le service RE.

Configurer les règles dans Security Analytics

1. Cliquez sur **Rapports > Gérer**.
2. Dans Groupes, cliquez sur **Règles**.
3. Cliquez sur Add (+).
4. Saisissez le nom du nouveau groupe.

5. Sélectionnez le groupe que vous avez créé, puis dans la barre d'outils Règle, cliquez sur **Ajouter (+)**.
6. Dans le champ Nom Syslog, saisissez un nom pour la configuration Syslog du composant SecOps permettant de configurer les alertes.
7. Dans le champ Type de règle, sélectionnez Base de données NetWitness.
8. Saisissez un nom pour la règle.
9. 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.

10. Cliquez sur **Enregistrer**.

Remarque : Pour visualiser le même nombre dalertes dans SA RE et RSA Archer GRC, vérifiez que vous avez sélectionné Une fois pour une exécution dans les onglets Syslog et Enregistrement.

Ajouter des modèles d'alerte pour le Reporting Engine dans Security Analytics

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 :

<*rép_install*>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates

1. Cliquez sur **Rapports > Gérer > Alertes**.
2. Cliquez sur l'onglet **Modèle**.
3. Cliquez sur Add (+).
4. Dans le champ Nom, saisissez le nom du modèle.
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.

Configurer les alertes dans Security Analytics

Dans RSA Security Analytics 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 **Rapports > Gérer > Alertes**.
2. Cliquez sur Add (+).
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 d'alerte RSA Archer Security ne fonctionnera pas dans Security Analytics.
6. Dans le champ Sources de données, sélectionnez votre source de données.
7. Dans la section Notification, sélectionnez **Syslog**.
8. Cliquez sur Add (+).
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**.

Configurer les paramètres de notification Syslog pour ESA dans Security Analytics

1. Cliquez sur **Administration** > **Système** > **Notifications globales**.
2. Cliquez sur l'onglet **Sortie**.
3. Définissez et activez une notification Syslog pour ESA.
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 :

- Serveur
- Name
- Nom d'hôte ou adresse IP du système ayant permis d'installer le composant UCF.
- Serveur
- Port
- Numéro du port sur lequel vous souhaitez que le système UCF écoute
- les messages d'alerte Syslog.

Gestionnaire :

- Spécifiez le site Syslog

Protocole :

- Choix du protocole.

7. Cliquez sur **Enregistrer**.

Configurer la connexion SSL SA ESA pour le serveur Syslog sécurisé dans Security Analytics

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

1. Accédez à **Administration > Services**.
2. Sélectionnez le service ESA. Accédez à **Explorer > Configuration > SSL** .
3. Définissez ServerCertificateValidationEnabled sur **true**.
4. Copiez le certificat keystore.crt.der à partir de la machine UCF qui se trouve dans <*rép_ install*>\SAIM integration service\cert-tool\certs dans le champ ESA accessible depuis **/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65.0.b17.el6_7.x86_64/jre/lib/security**.
5. Exécutez la commande suivante :

```
keytool -import -file keystore.crt.der -alias ucf-syslog -keystore cacerts -
storepass changeit
```

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

6. Redémarrez le service ESA.

Ajouter des modèles d'alerte ESA dans Security Analytics

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 :

<*rép_install*>\SA IM integration service\config\mapping\templates\SecOps_SA_

Templates\SecOps_SA_ESA_templates.txt

Procédure :

1. Cliquez sur **Administration > Système > Notifications globales**.
2. Cliquez sur l'onglet **Modèles**.
3. Cliquez sur Add (+).
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.

Créer des règles ESA dans Security Analytics

1. Cliquez sur **Alertes** > **Configurer**.
2. Sélectionnez votre périphérique ESA.
3. Cliquez sur **Sélectionner**.
4. Dans la barre d'outils Règles ESA, cliquez sur +.
5. Sélectionnez le Générateur de règles.
6. Dans le champ Nom, saisissez le nom de la règle.
7. Dans le champ Description, saisissez une description de la règle.
8. Sélectionnez une gravité.
9. 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.

10. Dans la section Notifications, sélectionnez **Syslog**.
11. Sélectionnez la notification, le serveur Syslog et le modèle qui ont été créés.
12. Cliquez sur **Enregistrer**, puis **Fermer**.
13. Cliquez sur **Alertes** > **Configurer** > **Déploiements**.
14. Cliquez sur + pour la section Services ESA.
15. Sélectionnez le service ESA.
16. Cliquez sur **Déployer maintenant**.
17. Dans la section Règles ESA, cliquez sur + pour choisir la règle ESA 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 Security Analytics 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.

L'administrateur peut effectuer plusieurs tâches dans Security Analytics, notamment :

Tâche
Mettre à jour les services Concentrator et Decoder

Tâche
Ajouter le point de terminaison RSA Archer Enterprise Management au système UCF
Mettre à jour le fichier Hôte RSA Security Analytics pour le mode SSL
Créer une tâche de feed récurrente

Mettre à jour les services Concentrator et Decoder

Le service d'intégration Security Analytics Incident Management 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 Security Analytics Incident Management. Le module Live de RSA Security Analytics 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 service Concentrator tienne compte des nouvelles métadonnées créées par les services Decoder, vous devez modifier les fichiers index-concentrator-custom.xml, index-logdecoder-custom.xml et index-decoder-custom.xml.

1. Dans le menu Security Analytics, cliquez sur **Administration > Services**.
2. Sélectionnez votre service Concentrator, puis sélectionnez  > **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. Si aucun service ne s'affiche, cliquez sur **Appliquer**.
7. 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**.
8. 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.
9. 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 Sélection du mode.
   b. Sélectionnez l'une des options suivantes :
      - Gérer le workflow d'incidents dans RSA Security Analytics.
      - 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 SA Live : http(s)://hostname:port/archer/sa/feed

Champ	Description
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 SA Live.
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 SA Live.
Mode SSL	La valeur par défaut est Non. Si la valeur est **Non**, l'adresse URL utilise le mode http : http://hostname:port/archer/sa/feed Si la valeur est **Oui**, l'adresse URL utilise le mode http : https://hostname:port/archer/sa/feed Si vous n'avez pas mis à jour le fichier hôte, reportez-vous à la rubrique Mettre à jour le fichier Hôte RSA Security Analytics pour le mode SSL.

3. Si vous avez sélectionné le paramètre Oui pour le mode SSL, complétez les champs suivants :
   - Copiez les certificats dans le champ SA. Saisissez **Oui** pour que les certificats soient automatiquement copiés de RSA Archer Security Operations Management vers RSA Security Analytics.

- Hôte SA. Saisissez le nom d'hôte ou l'adresse IP du serveur SA.
- Nom d'utilisateur de l'hôte SA. Saisissez le nom d'utilisateur permettant de se connecter au serveur SA afin de copier les certificats.
- Mot de passe de l'hôte SA. Saisissez le mot de passe permettant de se connecter au serveur SA afin de copier les certificats.

Remarque : Si les opérations de copie des certificats et d'ajout du point de terminaison échouent, copiez les certificats manuellement. Reportez-vous à la section **Copiez manuellement les certificats Enterprise Management** dans Dépanner l'intégration de RSA Archer. Après avoir copié les certificats, vous devez ajouter le plug-in Enterprise Management sans copier automatiquement les certificats.

Mettre à jour le fichier Hôte RSA Security Analytics pour le mode SSL

1. Modifiez le fichier Hôte sur le serveur SA 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 SA en exécutant la commande suivante :

   ```
   restart jettysrv
   ```

4. Lors de la configuration du feed SA 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 :

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

5. Vérifiez que la connexion est active.

Créer une tâche de feed récurrente

Pour que RSA Security Analytics puisse télécharger les fichiers de feed à partir du service d'intégration Security Analytics Incident Management 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 Security Analytics 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. Dans le menu Security Analytics, cliquez sur **Live > Feeds**.
2. 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
   - https://ucf_hostname_or_ip:port/archer/sa/feed

   où *http(s):ucf_hostname_or_ip:port* correspond à l'adresse de votre service d'intégration Security Analytics Incident Management. Utilisez le mode https si vous avez activé la communication SSL avec RSA Security Analytics. Par exemple : http://10.10.10.10:9090 ou https://10.10.10.10:8443.

   Remarque : Si Incident Management 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 Security Analytics en vue d'utiliser les fichiers d'accès du service d'intégration Security Analytics Incident Management.
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 Index 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 Archer SecOps 1.3.

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 Security Analytics Incident Management plus tôt que prévu.
3. Sélectionnez RSA Unified Collector Framework.
4. Cliquez sur **Stop**.

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 1.2 ou d'Archer SecOps 1.3 avec Security Analytics Incident Management.

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

Problème : Après avoir ajouté le point de terminaison de Security Analytics Incident Management, le magasin d'approbations de l'autorité de certification n'est pas configuré.

Solution :

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

Copier manuellement des certificats Enterprise Management

Si les certificats n'ont pas été copiés automatiquement, vous pouvez les copier manuellement.

1. Copiez keystore-em.crt du certificat à partir de la machine UCF à l'emplacement suivant : <install_dir>\SA IM integration service\cert-tool\certs to the Security Analytics server at /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security.
2. Connectez-vous à la machine où est installé RSA Security Analytics.
3. Accédez à l'emplacement où le certificat du magasin d'approbations SA est copié :
   ```
   cd /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security
   ```
4. Exécutez la commande suivante :
   ```
   keytool -import -alias ucfcert -keystore cacerts -filekeystore-em.crt.der
   ```

Remarque : Si vous avez copié les certificats parce que l'ajout du point de terminaison Enterprise Management a échoué, vous devez ajouter de nouveau le point de terminaison sans copier automatiquement les certificats. Voir **Configurer les points de terminaison dans RSA Unified Collector Framework** Configurer Security Analytics pour une utilisation avec Archer.

Certificats Security Analytics Incident Management

Si des certificats ne sont pas copiés automatiquement, vous pouvez les copier manuellement.

1. Copiez keystore.crt.pem du certificat à partir de la machine UCF à l'emplacement <rép_ installation>\SA IM integration service\cert-tool\certs vers le serveur Security Analytics : path/tmp.
2. Connectez-vous à la machine où est installé RSA Security Analytics.
3. Accédez à /tmp.
4. Pour ajouter le certificat UCF à Security Analytics RabbitMQ, saisissez ce qui suit :
   ```
   cat keystore.crt.pem >>
   /etc/puppet/modules/rabbitmq/files/truststore.pem
   ```
5. Fournissez les informations suivantes (en anglais) :
   ```
   >puppet agent -t
   ```
6. Lorsque l'agent termine, quittez Connection Manager.
7. Redémarrez le service RSA Unified Collector Framework à partir de services.msc.
8. Exécutez de nouveau Connection Manager.

Incidents dans la solution RSA Archer Security Operations Management

Problème : Les conclusions et incidents de sécurité n'apparaissent pas dans la solution RSA Archer Security Operations Management.

Solution :

1. Confirmez que les heures de votre système middleware et de la plate-forme RSA Archer sont synchronisées ou présentent une différence maximale d'une seconde.
2. Vérifiez que le point de terminaison est correctement configuré.
3. Confirmez qu'UCF est configuré sur le mode approprié.
   - Pour les conclusions, vous devez choisir de gérer le workflow d'incidents dans RSA Security Analytics.
   - Pour les incidents de sécurité, vous devez choisir de gérer le workflow d'incidents dans RSA Archer Security Operations Management.
4. Connectez-vous via SSH à l'hôte du serveur Web SA et saisissez la commande suivante pour vérifier que la file d'incidents RSA Archer (im.archer_incident_queue) est créée :
   ```
   curl -k -u guest:guest
   ```

```
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_incident_queue --
silent --stderr - | grep -o '"name"\:.*
```

Remarque : Si la file d'attente est créée, le résultat sera le suivant :

```
"name":"im.archer_incident_
queue","vhost":"/rsa/im/integration","durable
":true,"auto_delete":false,"arguments":
{},"node":"sa@localhost"}
```

5. Connectez-vous via SSH à l'hôte du serveur Web SA et saisissez la commande suivante pour vérifier que la file d'attente de tickets RSA Archer (im.archer_incident_queue) est créée :

```
curl -k -u guest:guest
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_tickets_queue --
silent --stderr - | grep -o '"name"\:.*'
```

Remarque : Si la file d'attente est créée, le résultat sera le suivant :

```
"name":"im.archer_tickets_
queue","vhost":"/rsa/im/integration","durable
":true,"auto_delete":false,"arguments":
{},"node":"sa@localhost"}
```

6. Connectez-vous via SSH à l'hôte du serveur Web SA et saisissez la commande suivante pour vérifier le nombre de messages dans la file d'attente :

```
curl -k -u guest:guest
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_incident_queue -- silent --stderr -
| grep -o '"messages"\:[0-
9]*'
```

Remarque : Si la file d'attente est créée, le résultat sera le suivant : `"messages" : 5`

7. Confirmez que les files d'attente ci-dessus sont renseignées par des messages provenant d'UCF.

Tâches de remédiation dans RSA Archer Security Operations Management

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 Security Analytics Incident Management.
4. Assurez-vous que la file d'attente est configurée sur Tous ou Opérations.

Erreurs entre RSA Security Analytics et RSA Unified Collector Framework

Problème : Dans *<rép_install>*\SA IM integration service\logs\collector.log, il existe des erreurs SSL entre RSA Security Analytics et RSA Unified Collector Framework.

Solution :

1. Vérifiez que les certificats SSL sont valides.

   Remarque : Les certificats Security Analytics Incident Management sont valides 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 *<rép_installation>*\SA IM integration service\data-collector.
2. Saisissez : `runConnectionManager.bat`
3. Saisissez le chiffre correspondant à une nouvelle génération de certificat du service d'intégration Security Analytics Incident Management.
4. Dans le point de terminaison Security Analytics Incident Management de Connection Manager, saisissez le chiffre correspondant à la modification du point de terminaison.

5. Saisissez Oui pour copier automatiquement les certificats dans la zone de stockage fiable Security Analytics.

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