RSA NETWITNESS® SUITE

RSA Archerとの統 合 ガイド

バージョン 11.0

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/EMC-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、本使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

2月 2018

目次

RSA Archerとの統合

管理者はRSA NetWitness SuiteとRSA NetWitness SecOps(Security Operations) Managerを統合し、インシデントの管理と改善を目的に、アラートとインシデントをNetWitness SuiteからArcherに送信することができます。このガイドでは、この統合を構成するためのワークフロー概要について説明します。

NetWitness SecOps Managerバージョン1.3.1.2で提供されるNetWitness Suite 11.0の統合オプションを次の表にリストします。

NetWitness SecOps Managerのバージョン	NetWitness Suite 11.0統合	参考情報
1.3.1.2	ESA(Event Stream Analysis)	詳細については、「Configure Event Stream Analysis for Integration with Archer SecOps」セクションを参照してください。
1.3.1.2	RE(Reporting Engine)	詳細については、「Configure Reporting Engine for Integration with Archer SecOps」セクションを参照してください。
1.3.1.2	Respond	詳細については、「Configure Respond for Integration with Archer SecOps 1.3.1.2」セクションを参照してください。
1.3.1.2	Archer Feed	詳細については、「RSA Archer Feed」セクションを参照してください。

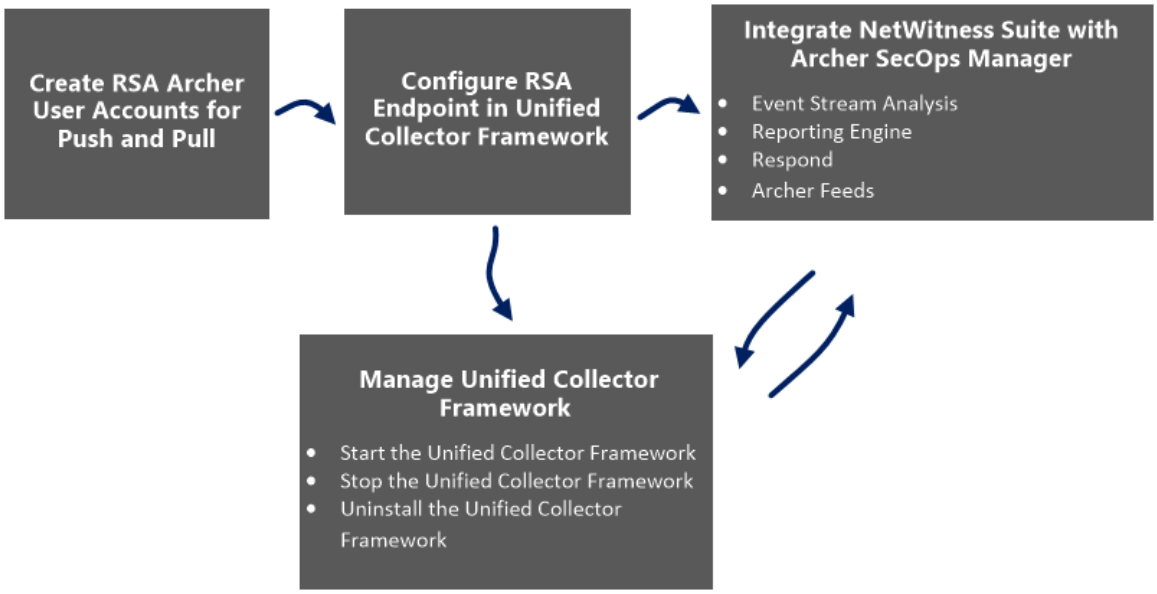
Archerと連携するNetWitnessの構成

RSA NetWitness SecOps Managerソリューションを活用すると、すべての対応可能なセキュリティアラートを集約し、インシデント対応およびSOC管理をより効率的かつプロアクティブに、対象を絞って実施できます。RSA NetWitness SecOps機能の詳細については、RSA Archer CommunityまたはRSA Archer Exchange CommunityにあるRSA Archerのドキュメントを参照してください。

RSA Archerのバージョンによって、NetWitness Suiteの統合方法が異なります。サポートされるArcherプラットフォームについては、「*SecOps Installation Guide*」を参照してください。

NetWitness SecOps Manager 1.3.1.2とNetWitness Suiteの統合には、RSA UCF (Unified Collector Framework) を使用します。これはSecurity Anlaytics IM(Incident Management) 統合サービスとSecOps Watchdogサービスで構成されています。

この図は、NetWitness Suite 11.0とNetWitness SecOps Manager 1.3.1.2との統合の流れを表しています。



プッシュ用とプル用のRSA Archerユーザアカウントを作成する

RSA Archer GRC Platformにデータを転送するWebサービスクライアントのユーザアカウントを作成する必要があります。

RSA NetWitness Suiteからデータを送受信するときに競合を回避するには、RSA Archerユーザアカウントが2つ必要です。

プッシュとプル用のユーザアカウントを作成するには、次の手順に実行します。

1. RSA ArcherのUIで、[**管理**]＞[**アクセス制御**]＞[**ユーザ**]＞[**新規追加**]の順にクリックします。
2. [**名**]フィールドと[**姓**]フィールドに、RSA Archer GRCにデータをプッシュするためにUCFがこのアカウントを使用することを示す名前を入力します。たとえば、「UCF User」および「Push」と入力します。

   注:プル用のアカウントを構成する場合は、RSA Archer GRCからデータをプルするためにUCFがこのアカウントを使用することを示す名前を入力します。たとえば、「UCF User」および「Pull」と入力します。
3. (オプション) この新しいユーザアカウントのユーザ名を入力します。

   注:ユーザ名を指定しない場合、RSA Archer GRC Platformでは、新しいユーザアカウントを保存する時に名と姓からユーザ名が作成されます。
4. [**連絡先**]セクションの[**メール**]フィールドに、この新しいユーザアカウントに関連付けるメールアドレスを入力します。
5. [**ローカリゼーション**]セクションで、タイムゾーンをUTC(協定世界時)に変更します。

   注:UCFでは、時間関連のすべての計算を標準化するためにUTC時間が使用されます。
6. [**アカウントのメンテナンス**]セクションに、新しいユーザアカウントの新しいパスワードを入力して確認します。

   注:新しいユーザアカウントのユーザ名とパスワードをメモしてください。UCFの設定で、Webサービスクライアントを介してRSA Archer GRC Platformと通信するときに、これらの認証情報を入力する必要があります。
7. [**次のログイン**時に強制的なパスワードの変更を行う]オプションをクリアします。
8. [**セキュリティパラメータ**]フィールドで、このユーザに対して使用するセキュリティパラメータを選択します。

   注:デフォルトのセキュリティパラメータでは、パスワードの変更間隔が90日に設定されているため、SA IM Integration Serviceに格納されたユーザアカウントパスワードも90日ごとに更新する必要があります。この操作を回避するには、SA IM Integration Serviceユーザアカウン用に新しいセキュリティパラメータを作成し、パスワード変更間隔を企業ポリシーで許可される最大値に設定します。
9. [**グループ**]タグをクリックし、次の手順を実行します。

a. [**グループ**]セクションで、[**ルックアップ**]をクリックします。

b. [**使用可能なグループ**]ウィンドウで、[グループ]を展開します。

c. 下にスクロールして[SOC:ソリューション管理者およびEM:読み取り専用]を選択します。

d. [**OK**]をクリックします。

10. [**適用**]をクリックしてから、[**保存**]をクリックします。

11. RSA Archer GRCシステムの言語および地域設定が「英語-米国」以外に設定されている場合は、次の手順を実行します。

a. 作成したユーザアカウントを開き、[**ローカリゼーション**]セクションの[ロケール]フィールドで[**英語(米国)**]を選択し、[**保存**]をクリックします。

b. RSA Archer GRC Platformをホストしているwindowsシステムで、IIS(Internet Information Services) Managerを開きます。

c. RSA Archer GRCサイトを展開し、[**.NETグローバリゼーション**]をクリックし、[**カルチャ**]フィールドと[**UIカルチャ**]フィールドの両方で[**英語(米国)**]を選択して、[**適用**]をクリックします。

d. RSA Archer GRCサイトを再起動します。

12. ステップ1～11を繰り返し、RSA Archer GRCからデータをプルするためにUCFの2番目のユーザアカウントを作成します。

RSA Unified Collector Frameworkのエンドポイントを構成する

エンドポイントは、UCFがRSA NetWitness SuiteおよびRSA Archer GRCシステムに到達するために必要な接続の詳細を提供します。

注:さまざまな統合を使用するには、いくつかのエンドポイントが必須になります。次のリストは、必須のエンドポイントを示しています。

必須のエンドポイント

- Archer Pushエンドポイント
- Archer Pullエンドポイント
- モードの選択:SecOpsまたは非SecOpsモード

注:
• 非SecOpsモードを選択した場合、インシデントは、RSA Archer Security Operations Managementではなく、NetWitness Suite Respondで管理されます。
• プロトコル(TCP、UDP、セキュアなTCP) に応じてポートを構成する必要があります。
• RSA Archer GRCサーバの証明書のサブジェクト名がホスト名に一致していることを確認します。

処理手順

1. UCFシステムで、次の手順を実行して、Connection Managerを開きます。
   a. コマンド プロンプトを開きます。
   b. ディレクトリを<install_dir>\SA IM integration service\data-collectorに変更します
   c. 次のコマンドを実行します。
      runConnectionManager.bat
2. **Connection Manager**で、エンドポイントを追加するため、「**1**」を入力します。
3. 次の手順を実行して、RSA Archer Security Operations Managementにデータをプッシュするためのエンドポイントを追加します。
   a. Archer の数を入力します。

      注: RSA Archerのエンドポイントを追加するには、SSLを有効にする必要があります。

   b. エンドポイント名には、「**push**」と入力します。
   c. RSA Archer GRCシステムのURLを入力します。
   d. RSA Archer GRCシステムのインスタンス名を入力します。
   e. RSA Archer GRCシステムにデータをプッシュするために作成したユーザ アカウントのユーザ名を入力します。
   f. RSA Archer GRCシステムにデータをプッシュするために作成したユーザ アカウントのパスワードを入力し、パスワードを確認します。
   g. データをプルするためにこのアカウントを使用するかどうかを確認するメッセージが表示されたら、「**False**」と入力します。
4. 次の手順を実行して、RSA Archer Security Operations Managementからデータをプルするためのエンドポイントを追加します。

a. Archer の数を入力します。

注：RSA Archerのエンドポイントを追加するには、SSLを有効にする必要があります。

b. エンドポイント名には、「**pull**」と入力します。

c. RSA Archer GRCシステムのURLを入力します。

d. RSA Archer GRCシステムのインスタンス名を入力します。

e. RSA Archer GRCシステムからデータをプルするために作成したユーザアカウントのユーザ名を入力します。

f. RSA Archer GRCシステムからデータをプルするために作成したユーザアカウントのパスワードを入力し、パスワードを確認します。

g. データをプルするためにこのアカウントを使用するかどうかを確認するメッセージが表示されたら、「**True**」と入力します。

5. RSA NetWitness Suiteのエンドポイントを追加します。

- 対応の場合

a. Security Analytics IMの番号を入力します。

b. エンドポイント名を入力します。

c. SAホストのIPアドレスを入力します。

d. ［SAメッセージング ポート］に**5671**と入力します。

e. 改善タスクのターゲット キューを入力します。「All」を選択すると、RSA Archer Integration(GRC) とIT Helpdesk(Operations) の両方が選択されます。

f. NetWitness Suiteトラスト ストアに証明書を自動的に追加するには、次の手順を実行します。

i. 「**yes**」と入力します。

ii. NetWitness Suiteホストのユーザ名とパスワードを入力します。

注：CAトラスト ストアの設定に失敗したというエラーを受信した場合は、「RSA Archer統合のトラブルシューティング」を参照してください。

g. 次の手順を実行して、UCF Connection Managerでモードを選択します。

i. モード選択の番号を入力します。

ii. 以下のいずれかのオプションを選択します。

- RSA NetWitness Suiteでインシデント ワークフローを管理。
- RSA Archer Security Operations Managementでのみインシデント ワークフローを管理

- Reporting EngineおよびEvent Stream Analysisの場合

a. サード パーティ統合を使用するには、次の手順を実行して、Syslogサーバのエンドポイントを追加します。

i. 番号を入力して、「Syslog Server Endpoint」を選択します。

ii. 次の情報を入力します。

- ユーザ定義名
- SSLを構成したTCPポート番号

注 : デフォルトは1515。Syslogサーバをこのモードでホストしない場合は、「**0**」を入力します。

- TCPポート番号 : Syslogクライアントが Syslogメッセージを TCPモードで送信する場合は、TCPポートを入力します。

注 : デフォルトは1514。Syslogサーバをこのモードでホストしない場合は、「**0**」を入力します。

- UDPポート番号 : Syslogクライアントが Syslogメッセージを UDPモードで送信する場合は、UDPポートを入力します。

注 : デフォルトは514。Syslogサーバをこのモードでホストしない場合は、「**0**」を入力します。

デフォルトでは、「**0**」を入力して無効にしない限り、Syslogサーバは上記の3つのモードで動作します。

b. Syslogクライアントをテストするには、「Test Syslog Client」の番号を入力します。`<install_dir>\SA IM integration service\config\mapping\test-files\`からファイルを使用してTest Syslog Clientを使用します。

6. Connection Managerで、「**5**」を入力して、各エンドポイントをテストします。

NetWitness SuiteとArcher SecOps Managerの統合

RSA NetWitness SecOps Managerでインシデント ワークフローを管理するために、システム統合設定を構成する必要があります。

RSA Archer Security Operationsでインシデント ワークフローを管理するためにシステム統合設定を構成する方法については、「*NetWitness Respondガイド*」の「RSA Archer Security Operationsでインシデントを管理するための統合設定」を参照してください。

RSA UCF(Unified Collector Framework)

RSA NetWitness SuiteとRSA Archer SecOps Manager 1.3.1.2の統合には、RSA UCF(Unified Collector Framework) を使用します。RSA UCF(Unified Collector Framework) は、サポートするすべてのSIEMツールと、RSA NetWitness SecOps Managerソリューションを統合しています。RSA NetWitness Suite Respondを統合すると、インシデント ワークフローをNetWitness Suite Respondで管理でき、また改善タスクや未完了のデータ侵害をRSA Archer Security Operations Managementソリューションでの管理や改善のためにアナリストがエスカレーションできるようになります。また、Unified Collector Frameworkは、改善タスク(発見事項として作成される) 、データ侵害、またはこれらの両方を転送します。

注:
• RSA NetWitness SuiteとUnified Collector Frameworkの両方で同じオプションを構成する必要があります。
• RSA NetWitness RespondモジュールをReporting EngineまたはEvent Stream Analysisと統合すると、RSA Archer SecOps Managerにイベントおよびインシデントが重複して作成されます。

UCFは、NetWitness Suite Reporting Engine、HP ArcSight、NetWitness Suite Respondなど、複数のSIEMツールとの同時接続をサポートします。ただし、2つのNetWitness Suiteサーバを同じUCFに接続するなど、同じSIEMツールの複数のインスタンスとの同時接続はサポートされません。

前提条件

- RSA_Archer_Security_Operations_Managementパッケージをインストールします。RSA Archerのドキュメントである「RSA Archer Community」、または https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchangeの[コンテンツ]タブを参照してください。
- NetWitness SecOps Managerをインストールします。
- NetWitness SecOps Manager 1.3.1.2と互換性のあるNetWitness Suite 11.0を必ず使用してください。
- RSAでRespondが構成されていることを確認します。NetWitness Suite

RSA UCF(Unified Collector Framework) を使用すると、RSA Archer Security Operations Managementと以下を統合できます。

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

Archer SecOpsとの統合のためのRespondの構成

Archer SecOpsとの統合のためにRespondを構成するには、NetWitness Suiteで以下の手順を実行します。

ステップ1. NetWitness Suite Respondのモードの選択

1. [**管理**]＞[**サービス**]＞[**Respond**]＞[**エクスプローラ**]の順に選択します。
2. `Respond/Aggregation/export`に移動します。
3. `archer-secops-integration-enabled`フィールドを**true**にして有効にします。
4. Respondサービスを再起動します。

ステップ2.UCFにアラートを転送するようにNetWitness Suite Respondを構成する

1. Secopsミドルウェア ボックスで`C:\Program Files\RSA\SA IM integration service\cert-tool\certs`に移動します。
2. `keystore.cert.pem`と`rootcastore.cert.pem`の両方をcertsフォルダからコピーします(NWサーバのフォルダをインポートする) 。
   ```
   cp rootcastore.crt.pem /etc/pki/nw/trust/import

   cp keystore.crt.pem /etc/pki/nw/trust/import
   ```
3. SSHでNWサーバ ボックスに接続します。
   a. update-admin-nodeコマンドを実行します。
      ```
      orchestration-cli-client --update-admin-node
      ```
   b. RabbitMQサービスを再起動します。
      ```
      service rabbitmq-server restart
      ```
   c. ユーザarcherを作成し、仮想ホスト「`/rsa/system`」に対する権限を設定します。
      ```
      rabbitmqctl add_user archer archer

      rabbitmqctl clear_password archer

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

ステップ3. NetWitness Suite Respondにアラートを転送する

- **NetWitness Suite Event Stream AnalysisアラートをNetWitness Respondに転送するには、次の手順を実行します。**
  a. **[管理]**>**[サービス]**>**[ESA]**サービスを選択します。
  b. Event Stream Analysisサービスを選択し、>**[表示]**>**[構成]**を選択します。
  c. **[詳細]**タブをクリックします。
  d. **[メッセージ バスでアラートを転送]**チェックボックスがデフォルトでオンになっていることを確認します。オンになっていない場合は、**[メッセージ バスでアラートを転送]**チェックボックスをオンにして、**[適用]**をクリックします。
- **NetWitness Suite Reporting EngineアラートをNetWitness Respondに転送するには、次の手順を実行します。**
  a. **[管理]**>**[サービス]**>**[Reporting Engine]**サービスを選択します。
  b. Reporting Engineサービスの>**[表示]**>**[構成]**をクリックします。
  c. **[全般]**タブをクリックします。
  d. **[システム構成]**セクションで、**[Respondへのアラート転送]**チェックボックスをオンにし、**[適用]**をクリックします。
- **NetWitness Suite Malware AnalysisアラートをNetWitness Respondに転送するには、次の手順を実行します。**
  a. **[管理]**>**[サービス]**>**[Malware Analysis]**サービスを選択します。
  b. Malware Analysisサービスの>**[表示]**>**[構成]**をクリックします。
  c. **[監査]**タブをクリックします。
  d. **[対応アラート]**セクションで、**[有効な構成値]**チェックボックスがオンになっていることを確認します。チェックボックスがオンになっていない場合は、チェックボックスをオンにし、**[適用]**をクリックします。

ステップ4.EndPointアラートをNetWitness Suite Respondに転送する

RSA Endpointアラートは、NetWitness Respondを使用してRSA Archer GRCに送信できます。メッセージ バスを使用してNetWitness Endpointアラートを構成する方法の詳細については、「*NetWitness Endpoint統合ガイド*」の「メッセージ バス経由のNetWitness EndPointアラートの構成」のトピックを参照してください。

ステップ 5.アラートをインシデントに統合する

NetWitness Respondに着信したアラートを、インシデントに自動的に統合し、RSA Archer Security Operations Managementに転送することができます。統合ルールが1分ごとに自動的に実行され、選択した一致条件とグループ化オプションに基づいて、アラートがインシデントに統合されます。アラートの統合の詳細については、「*NetWitness Respond構成ガイド*」の「Respondにアラートを表示するためのアラート ソースの構成」トピックを参照してください。

アラートの統合を構成するには、次の手順を実行します。

1. **構成**＞[**インシデントのルール**]を選択します。
2. 標準提供のルールを有効にするには、次の手順を実行します。
   a. ルールをダブル クリックします。
   b. [**有効**]を選択します。
   c. [**保存**]をクリックします。
   d. ルールごとにステップa～cを繰り返します。
3. 新しいルールを追加するには、次の手順を実行します。
   a. ＋をクリックします。
   b. [**有効**]を選択します。
   c. 以下の各フィールドに入力します。
      - ルール名
      - アクション
      - 一致条件
      - グループ化オプション
      - インシデント オプション
      - 優先度
      - 通知
4. [**保存**]をクリックします。

NetWitness SecOps Managerと統合するためのReporting Engineの構成

Reporting EngineのためのSyslog出力アクションを構成するには、次の手順を実行します。

1. [**管理**]＞[**サービス**]を選択します。
2. Reporting Engineサービスを選択し、[**表示**]＞[**構成**]をクリックします。
3. [**出力アクション**]タブをクリックします。

4. [**NetWitness Suiteの構成**]セクションの[**ホスト名**]フィールドに、Reporting Engineサーバのホスト名とIPアドレスを入力します。
5. [**Syslog構成**]セクションで、次のようにSyslog構成を追加します。
   a. [**サーバ名**]フィールドに、UCFのホスト名を入力します。
   b. [**サーバ ポート**]フィールドに、UCF Syslog構成で選択したポートを入力します。
   c. [**プロトコル**]フィールドで、転送プロトコルを選択します。

   注:セキュアなTCPを選択した場合は、SSLを構成する必要があります。
6. [**保存**]をクリックします。

セキュアなSyslogサーバ用にNetWitness Suite Reporting Engine SSLを構成するには、次の手順を実行します。

Syslogサーバがセキュアなで構成されている場合は、SSLを構成します。

1. 証明書`keystore.crt.der`をUCFマシンから`/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-2.b11.el7_3.x86_64/jre/lib/security`にあるNetWitness Suiteサーバボックスにコピーします。
2. 次のコマンドを実行します。

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

   注:上記のコードをコピー&ペーストしないでください。エラーを回避するために、手でコマンドを入力してください。
3. **ServerCertificateValidationEnabled**を**true**に設定します。
   - [**管理**]>[**サービス**]に移動します。
   - Reporting Engineサービスの>[**表示**]>[**エクスプローラ**]をクリックします。
   - [**com.rsa.soc.re**]>[**構成**]>[**SSLContextConfiguration**]を展開します。
   - **sslContextConfiguration**を展開し、**ServerCertificateValidationEnabled**を**true**に設定します。
4. Reporting Engineサービスを再起動します。

NetWitness Suiteでルールを構成するには、次の手順を実行します。

1. [**監視**]>[**レポート**]>[**管理**]をクリックします。
   [管理]タブが表示されます。
2. [**ルール グループ**]パネルで、**+**をクリックします。

3. 新しいグループの名前を入力します。
4. 作成したグループを選択し、[ルール]ツールバーで✚をクリックします。
5. [**ルールタイプ**]フィールドで、[NetWitness DB]を選択します。
6. ルールの名前を入力します。
7. 作成するルールに応じて、[**選択**]フィールドと[**条件**]フィールドに値を入力します。

   注:上記で設定したSyslog名を使用して、Syslog構成を追加します。

8. [**保存**]をクリックします。

注:Reporting EngineとRSA Archer GRCに同じ数のアラートを表示するには、[Syslog]タブと[レコード]タブの両方で、[実行]を1回に設定する必要があります。

NetWitness SuiteにReporting Engineのアラートテンプレートを追加するには、次の手順を実行します。

UCFシステムログの構成が不要のアラートテンプレートsyslog出力アクションに関するアラートを作成するときに使用できる付属します。これらのテンプレートは、RSA Archer GRC Platformでのインシデントにアラートの集計に使用する基準を定義します。

サンプルのテンプレートは、UCFシステムの次の場所にあります。

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

1. [**監視**]>[**レポート**]>[**管理**]>[**アラート**]をクリックします。
2. [**テンプレート**]タブをクリックします。
3. ✚をクリックします。
4. [**名前**]フィールドに、アラートテンプレートの名前を入力します。
5. [**メッセージ**]フィールドに、アラートメッセージを入力します。
6. [**作成**]をクリックします。
7. 追加するアラートテンプレートごとにステップ3～6を繰り返します。

NetWitness Suiteでアラートを構成するには、次の手順を実行します。

RSA NetWitness Suite Reporting Engineのアラート機能では、ベースとなるルールを継続的に実行し、さまざまな方法で通知を行うことができます。

1. [**監視**]>[**レポート**]>[**管理**]>[**アラート**]をクリックします。
2. ✚をクリックします。
3. [**有効化**]を選択します。

4. 作成したルールを選択します。
5. [**Decoderへのプッシュ**]を選択します。

   注:このフィールドに値を入力しない場合、RSA Archer Security Alertsアプリケーション内のリンクからRSA NetWitness Suiteに戻ることはできません。
6. [データソース]リストからデータソースを選択します。
7. [**通知**]セクションで、[**Syslog**]を選択します。
8. ＋をクリックします。
9. Syslog構成のフィールドに入力します。
10. [**本文テンプレート**]フィールドで、Syslogアラートに使用するテンプレートを選択します。
11. [**保存**]をクリックします。

Archer SecOpsとの統合のためのEvent Stream Analysisの構成

NetWitness SuiteでEvent Stream AnalysisのSyslog通知設定を構成するには、次の手順を実行します。

1. [**管理**]＞[**システム**]＞[**グローバル通知**]をクリックします。
2. [**出力**]タブをクリックします。
3. Event Stream AnalysisのSyslog通知を定義して有効化します。
4. [**サーバ**]タブをクリックします。
5. Syslog通知サーバを定義して、有効にします。
6. [Syslogサーバ構成]セクションで、次のように入力します。

   フィールドの説明:

   - [名前]:カスタムの名前を指定します。
   - [サーバIP(ホスト名)]:UCFをインストールしたシステムのホスト名またはIPアドレスを指定します。
   - [ポート]:UCFがリスンするポート番号を指定します。
   - [ファシリティ]:Syslogファシリティを指定します。
   - [プロトコル]:プロトコルを選択します。
7. [**保存**]をクリックします。

セキュアなSyslogサーバ用にNetWitness Suite Event Stream Analysis SSLを構成するには、次の手順を実行します。

Syslogサーバがセキュアなで構成されている場合は、SSLを構成します。

1. **[管理]＞[サービス]**を選択します。
2. [Event Stream Analysis]サービスを選択します。**[エクスプローラ]＞[構成]＞[SSL]**をクリックします。
3. **ServerCertificateValidationEnabled**を**true**に設定します。
4. `rootcastore.cert.pem` をUCFマシンからEvent Stream Analysisサーバの `/etc/pki/ca-trust/source/anchors`にコピーします。
5. 次のコマンドを実行します。

   ```
   update-ca-trust
   ```

6. Event Stream Analysisサーバを再起動します。

Event Stream Analysisのアラート テンプレートを追加するには、次の手順を実行します。

UCF システムログの構成が不要のアラート テンプレート syslog 出力アクションに関するアラートを作成するときに使用できる付属します。これらのテンプレートは、RSA Archer GRC Platform でのインシデントにアラートの集計に使用する基準を定義します。

サンプルのテンプレートは、UCFシステムの次の場所にあります。

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

`Templates\SecOps_SA_ESA_templates.txt`

1. **[管理]＞[システム]＞[グローバル通知]**を選択します。
2. [**テンプレート**]タブをクリックします。
3. ＋をクリックします。
4. [**テンプレート タイプ**]フィールドで、[Event Stream Analysis]を選択します。
5. [**名前**]フィールドに、テンプレートの名前を入力します。
6. (オプション) [**説明**]フィールドに、テンプレートの簡単な説明を入力します。
7. [**テンプレート**]フィールドに、アラート メッセージを入力します。
8. [**保存**]をクリックします。
9. 追加するアラート テンプレートごとにステップ3～8を繰り返します。

Event Stream Analysisのルールを作成するには、次の手順を実行します。

1. [**構成**]＞[**ESAルール**]をクリックします。
2. [**ルール ライブラリ**]で、＋をクリックします。

3. [**ルールビルダ**]を選択します。
4. [**ルール名**]フィールドに、ルールの名前を入力します。
5. [**説明**]フィールドに、ルールの説明を入力します。
6. [**重大度**]を選択します。
7. [**条件**]セクションで、次の手順を実行します。
   a. ステートメントをビルドするために、**+**をクリックします。
   b. 名前を入力し、条件タイプを選択し、ステートメントのメタデータとメタ値のペアを追加します。
   c. [**保存**]をクリックします。
   d. ルールのステートメントがすべてビルドされるまで、ステップa～cを繰り返します。
8. [**通知**]セクションで、[**Syslog**]を選択します。
9. 前に作成した通知、Syslogサーバ、テンプレートを選択します。
10. [**保存**]と[**閉じる**]をクリックします。
11. [**構成**]＞[**導入**]をクリックします。
12. Event Stream Analysisサービスのセクションの**+**をクリックします。
13. [Event Stream Analysis]サービスを選択します。
14. [**今すぐ導入**]をクリックします。
15. [**Event Stream Analysisルール**]セクションで、[**+**]をクリックして作成するEvent Stream Analysisのルールを選択し、[**今すぐ導入**]をクリックします。

RSA Archer Feed

デフォルトでは、SA IM Integration Serviceによって、RSA Archerデバイスアプリケーションの[IPアドレス]フィールドと[重要度評価]フィールドのみがRSA NetWitness Suiteにフィードされます。デバイスアプリケーションが相互参照する[ビジネスユニット]フィールドと[施設]フィールドをFeedに含めるように、Enterprise Managementプラグインをカスタマイズすることができます。詳細については、https://community.emc.com/community/connect/grc_ecosystem/rsa archerまたはhttps://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchangeにあるArcherのドキュメントを参照してください。

注：RSA Archer GRC Platformからビジネスユニットおよび施設の情報をLiveにフィードすることを計画している場合は、これらのフィールドのキーをindex-concentrator-custom.xmlファイルに追加する必要があります。

ConcentratorおよびDecoderサービスを更新する

NetWitness SecOps ManagerのSA IM Integration Serviceは、カスタムFeed用のファイルを管理し、これらのファイルをEnterprise Managementエンドポイントを構成するときに指定したローカルフォルダに配置します。RSA NetWitness SuiteのLiveモジュールは、このフォルダからFeedファイルを受け取ります。その後、LiveはDecoderにFeedをプッシュします。Decoderは、収集したネットワークトラッフィクとFeed定義に基づいて、メタデータの作成を開始します。各Concentratorが、Decoderによって作成された新しいメタデータを認識できるようにするには、`index-concentrator-custom.xml`、`index-logdecoder-custom.xml`、`index-decoder-custom.xml files`を編集する必要があります。

1. **[管理]＞[サービス]**を選択します。
2. Concentratorを選択し、  **＞[表示]＞[構成]**を選択します。
3. [**ファイル**]タブをクリックします。
4. ドロップダウンリストから[index-concentrator-custom.xml]を選択します。次のいずれかの操作を実行します。
   - ファイルにコンテンツがすでに存在する場合は、次のように、新しいメタデータ要素のキーを追加します。

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

     注：コードをコピー＆ペーストしないでください。エラーを回避するために、手でコマンドを入力してください。
   - ファイルが空の場合は、次の内容を追加します。

     ```
     <?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. [**適用**]をクリックします。
6. 複数のデバイスに追加するには、次の手順を実行します。
   a. [**プッシュ**]をクリックします。
   b. このファイルのプッシュ先のデバイスを選択します。
   c. [**OK**]をクリックします。
7. index-logdecoder-custom.xmlとindex-decoder-custom.xmlを使用して、Log DecoderおよびIndex Decoderに対してステップ1～7を繰り返します。
8. ConcentratorサービスとDecoderサービスを再起動します。

UCFでRSA Archer Enterprise Managementエンドポイントを追加する

1. 次の手順を実行して、UCF Connection Managerでモードを選択します。
   a. モード選択の番号を入力します。
   b. 以下のいずれかのオプションを選択します。
      - RSA NetWitness Suiteでインシデント ワークフローを管理。
      - RSA Archer Security Operations Managementでのみインシデント ワークフローを管理。
2. 次の手順を実行して、RSA Archer Enterprise Managementエンドポイントを追加します。
   a. Enterprise Managementの番号を入力します。
   b. 次の表に示したフィールドに入力します。

フィールド	説明
エンドポイント名	オプションのエンドポイント名。
Webサーバのポート	デフォルトは9090。WebサーバのURLを構成します。NetWitness SuiteのLive Feedでポート番号を含むURLを、http://hostname:port/archer/sa/feedのように指定する必要があります。
重要度	RSA Archer GRCからPullする資産の重要度を指定します。 **false**の場合、あらゆる重要度の資産をPullします。 **true**の場合、重要度が「高」の資産のみをPullします。 これを手動で編集する場合は、collector-configプロパティファイルのem.criticalityプロパティを編集して、次のように重要度をカンマ区切りで指定します。LOW, MEDIUM, HIGH.
Feedディレクトリ	RSA Archer GRCから取得した資産CSVファイルを保存するディレクトリ。 **注**：既存のディレクトリパスを指定する必要があります。
Webサーバのユーザ名	EM Webサーバへの認証を行うためのユーザ名。 **注**：これは、NetWitness Suite live feedの構成時に提供されます。

フィールド	説明
Webサーバのパスワード	EM Webサーバへの認証を行うためのパスワード。 **注**：これは、NetWitness Suite live feedの構成時に提供されます。
SSLモード	デフォルト値はNo。 **No**の場合、URLは`http mode: http://hostname:port/archer/sa/feed`を使用します。 ホスト ファイルを更新していない場合は、「RSA NetWitness Suiteのホスト ファイルの更新」セクションを参照してください。 **注**：NetWitness Suiteでは、Archerの繰り返しFeedをSSLモードで現在サポートしていません。

RSA NetWitness Suiteのホスト ファイルを更新する

1. 次の場所にあるNetWitness Suiteサーバのホスト ファイルを編集します(vi /etc/hosts) 。
2. UCFホストのIPアドレスとして、次のアドレスを入力します。

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

3. 次のコマンドを実行してNetWitness Suiteサーバを再起動します。

   ```
   service jetty restart
   ```

4. NetWitness Suite Live Feedを構成するときに、次のように、URLにはIPアドレスの代わりにホスト名と、UCFでEnterprise Managementエンドポイントに構成したポート番号を入力します。

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

5. 接続が動作することを確認します。

繰り返しFeedタスクを作成する

RSA NetWitness SuiteでNetWitness Respond Integration ServiceからFeedファイルをダウンロードし、DecoderにFeedをプッシュするには、繰り返しFeedタスクを作成し、Feed設定を定義する必要があります。

注：RSA Archer SecOps 1.2の場合：RSA NetWitness SuiteでRCFマシンからFeedファイルをダウンロードし、DecoderにFeedをプッシュするには、繰り返しFeedタスクを作成し、Feed設定を定義する必要があります。手順は、少数の例外を除いて、RSA Archer SecOps 1.3の場合と類似しています。詳細については、「RSA Archer Exchange Community」のドキュメントを参照してください。

1. **[構成]** > **[カスタムFeed]**を選択します。
2. [Feed]ビューで、＋をクリックします。
3. [**カスタムFeed**]を選択し、[**次へ**]をクリックします。
4. [**繰り返し**]を選択します。
5. Feedの名前を入力します。
6. [URL]フィールドに、次のURLを入力します。

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

   ここで、*`http :ucf_hostname_or_ip:port`*は、NetWitness Respond Integration Serviceシステムのアドレスです。例：`http://10.10.10.10:9090`。

   注：RespondがSSLモードで実行されている場合は、URL内にホスト名を使用する必要があります。

7. [**認証情報**]を選択します。
8. [**ユーザ名**]フィールドと[**パスワード**]フィールドに、NetWitness Respond Integration Serviceシステムのファイルへのアクセスに使用するためにRSA NetWitness Suite用に作成したユーザアカウントの認証情報を入力します。
9. Feedの繰り返し間隔を定義します。
10. [**日付範囲**]セクションで、Feedの開始日と終了日を定義し、[**次へ**]をクリックします。
11. このFeedのプッシュ先の各Decoderを選択し、[**次へ**]をクリックします。
12. [**タイプ**]フィールドでIPが選択されていることを確認します。
13. [**インデックス列**]フィールドで、[1]を選択します。
14. 2番目の列で、キー値の重要度を設定し、[**次へ**]をクリックします。
15. Feed構成の詳細を確認して、[**完了**]をクリックします。

Unified Collector Frameworkの管理

このセクションでは、Archer SecOps 1.3.1.2と統合するためにRSA UCF(Unified Collector Framework) を構成および管理する追加タスクについて説明します。

RSA Unified Collector Frameworkを開始する

1. **[コントロール パネル] > [管理ツール] > [サービス]**をクリックします。
2. [RSA Unified Collector Framework]を選択します。
3. **開始**をクリックします。

RSA Unified Collector Frameworkを停止する

1. **[コントロール パネル] > [管理ツール] > [サービス]**をクリックします。
2. RSA SecOpsWatchDog Serviceを停止します。

   注 : Watchdog Serviceを停止しない場合、Watchdog ServiceはNetWitness Respondサービスを開始します。

3. [RSA Unified Collector Framework]を選択します。
4. [**停止**]をクリックします。

注 : サービスのシャットダウンに時間がかかりすぎる場合は、タスク マネージャーを使用して、RSASAIMDCServiceを停止します。

RSA Unified Collector Frameworkをアンインストールする

1. [**コントロール パネル**] > [**プログラムと機能**]をクリックします。
2. [**RSA Unified Collector Framework**]を選択します。
3. **Uninstall**をクリックします。

RSA Archer統合のトラブルシューティング

このセクションでは、NetWitness Suite RespondでArcher SecOps 1.3.1.2を構成する際に発生する可能性のある一般的な問題を解決する方法について説明します。

CAトラストストアの設定

問題:NetWitness Suite Respondのエンドポイントを追加した後、CAトラストストアの設定に失敗します。

解決方法:

1. NetWitness Suiteホストのssh認証情報が有効であることを確認します。
2. 認証情報は正しいが、エラーが引き続き発生する場合は、証明書を手動でコピーします。

RSA Archer Security Operations Managementの改善タスク

問題:UCFを介してオペレーション キューにプッシュされる改善タスクがRSA Archer Security Operations Managementに発見事項として表示されません。

解決方法:

1. Connection Managerを開きます。
   - コマンド プロンプトを開きます
   - ディレクトリを`<install_dir>\SA IM integration service\data-collector`に変更します。
   - `runConnectionManager.bat`と入力します。
2. 2を入力してエンドポイントを編集します。
3. NetWitness Suite Respondに3を入力します。
4. ターゲット キューが[All]または[Operations]に設定されていることを確認します。

RSA NetWitness SuiteとRSA Unified Collector Framework間のエラー

問題:`<install_dir>\SA IM integration service\logs\collector.log`で、RSA NetWitness SuiteとRSA Unified Collector Frameworkとの間にSSLエラーが発生します。

解決方法:

1. SSL証明書が有効であることを確認します。

   注:NetWitness Suite Respondの証明書の有効期間は2年間です。

2. 証明書が期限切れの場合は、期限が切れた証明書を再生成して、コピーします。

証明書を再生成およびコピーするには、次の手順を実行します。

1. コマンド プロンプトで、`<install_dir>\SA IM integration service\data-collector`に移動します。
2. 「`runConnectionManager.bat`」と入力します。
3. Regenerate SA IM Integration Service Certificateの番号を入力します。
4. NetWitness Suite Respondのエンドポイントで、接続マネージャにEdit Endpointの番号を入力します。
5. NetWitness Suiteトラスト ストアに証明書を自動的にコピーするには、「Yes」を入力します。

注: 証明書のコピーに失敗する場合は、証明書を手動でコピーします。