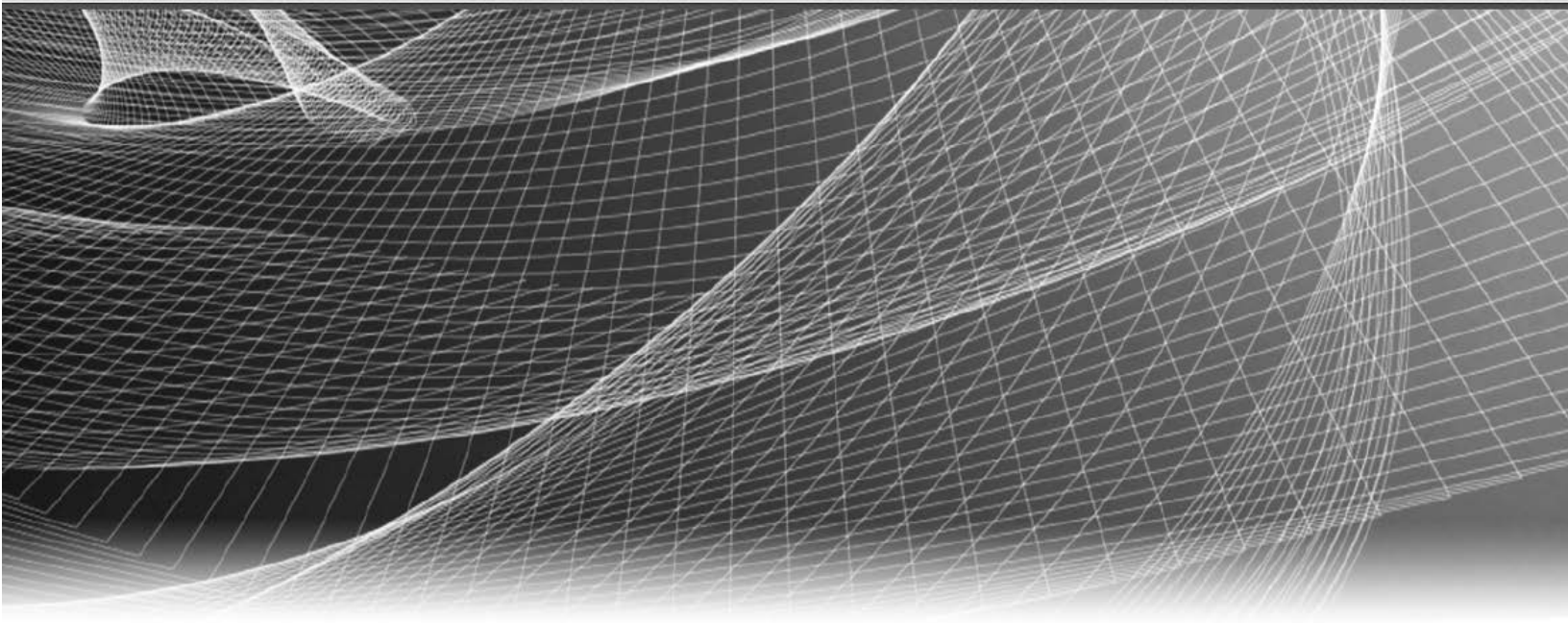


RSA Security Analytics

Konfigurationsleitfaden für Incident Management

für Version 10.6

RSA

EMC²

Marken

Lizenzvereinbarung

Drittanbieterlizenzen

Hinweis zu Verschlüsselungstechnologien

Verteilung

Inhalt

Konfigurationsleitfaden für Incident Management

Dieser Leitfaden bietet eine Übersicht über Incident Management, eine detaillierte Anleitung zur Konfiguration von Incident Management in Ihrem Netzwerk, zusätzliche Verfahren, die zu anderen Zeitpunkten verwendet werden und Referenzmaterial, das die Benutzeroberfläche für die Konfiguration von Incident Management in Ihrem Netzwerk erklärt.

Themen

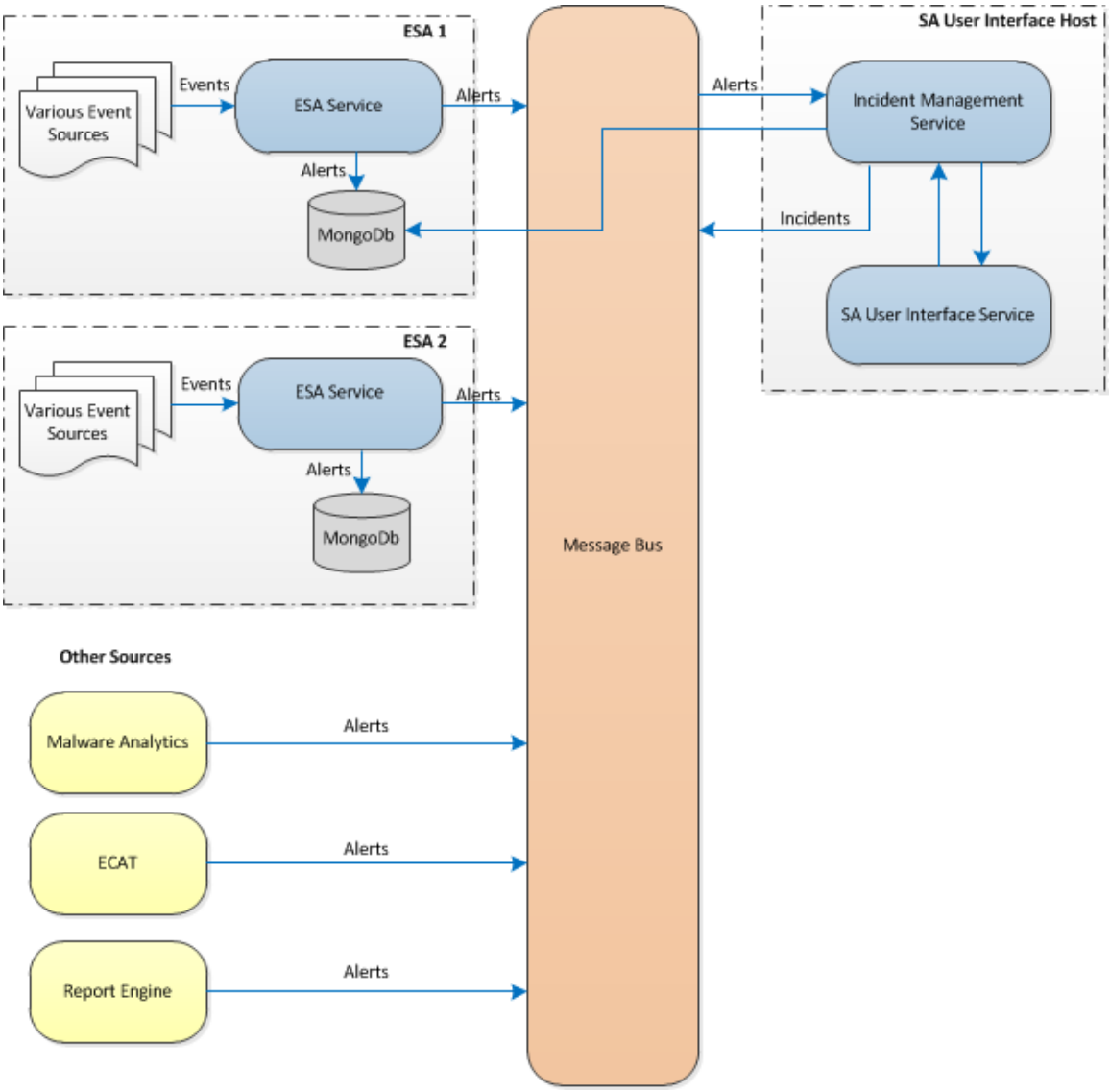
Übersicht über Incident Management

Security Analytics Incident Management verarbeitet Warnmeldungsdaten von verschiedenen Quellen über den Nachrichtenbus und zeigt diese Warnmeldungen auf der Security Analytics-Benutzeroberfläche an. Der Incident Management-Service erlaubt Ihnen, die Warnmeldungen logisch zu gruppieren und einen Workflow für die Reaktion auf den Incident zu starten, um die aufgetretenen Sicherheitsprobleme zu untersuchen und zu beheben.

Der Incident Management-Service verarbeitet Warnmeldungen vom Nachrichtenbus und normalisiert die Daten in ein gemeinsames Format (unter Beibehaltung der Originaldaten), um eine einfachere Regelverarbeitung zu ermöglichen. Er führt regelmäßig Regeln aus, um mehrere Warnmeldungen in einem Incident zu aggregieren und einige Attribute des Incident einzustellen (zum Beispiel Schwere, Kategorie usw.). Die Incidents werden vom Incident Management-Service dauerhaft in MongoDb abgelegt. Incidents werden im Nachrichtenbus auch zur Verarbeitung durch andere Systeme gepostet (zum Beispiel zur Integration in Archer).

Hinweis: Warnmeldungen werden vom Incident Management-Service dauerhaft in MongoDb abgelegt. In Security Analytics 10.4 und höher ist die Instanz von MongoDb auf einem der ESA-Hosts installiert. ESA ist eine erforderliche Komponente für Incident Management.

Die folgende Abbildung illustriert ein allgemeines Datenflussdiagramm:



Sie müssen verschiedene Quellen konfigurieren, von denen die Warnmeldungen durch den Incident Management-Service gesammelt und aggregiert werden.

Konfigurieren von Incident Management

Dieses Thema enthält die erforderlichen übergeordneten Aufgaben, um den Incident Management-Service zu konfigurieren. Der Administrator muss die folgenden Schritte in der angegebenen Reihenfolge abschließen.

Themen

Schritt 1. Hinzufügen eines Incident Management-Services

In diesem Thema erfahren Sie, wie Sie den Incident Management-Service auf einem Host hinzufügen.

Voraussetzungen

Vergewissern Sie sich, dass Sie einen Host installiert haben, auf dem Sie den Incident Management-Service ausführen möchten. Informationen zum Verfahren für das Hinzufügen eines Hosts erhalten Sie unter **Schritt 1: Hinzufügen oder Aktualisieren eines Hosts** im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Verfahren

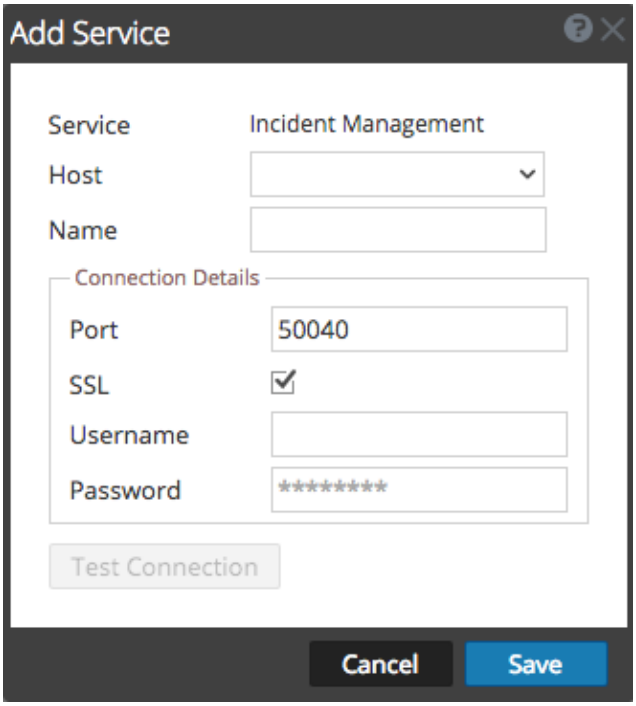
So fügen Sie den Incident Management-Service hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.

   Die Ansicht „Services“ wird angezeigt.

2. Wählen Sie im Bereich „Services“ die Optionen + **> Incident Management** aus.

   Das Dialogfeld **Service hinzufügen** wird angezeigt.



3. Stellen Sie folgende Informationen zur Verfügung:

Feld	Beschreibung
Host	Wählen Sie den Host aus, auf dem der IM-Server installiert ist.
Name	Geben Sie einen Namen für den Service ein.
Port	Der Standardport ist 50040.
SSL	Wählen Sie **SSL** aus, wenn Security Analytics über Secure Socket Layer mit dem Host kommunizieren soll. Die Sicherheit der Datenübertragung wird durch Verschlüsselung von Informationen und die Bereitstellung von Verfahren zur Authentifizierung mit SSL-Zertifikaten erzielt. Dies ist standardmäßig erforderlich. **Hinweis:** Wenn Sie SSL auswählen, stellen Sie sicher, dass SSL im Bereich Systemkonfiguration aktiviert ist.
Benutzername	Geben Sie den Benutzernamen des Hosts ein.
Password	Geben Sie das Passwort des Hosts ein.

4. Klicken Sie auf **Verbindung testen**, um festzustellen, ob Security Analytics sich mit dem Service verbindet.
5. Wenn das Ergebnis positiv ist, klicken Sie auf **Speichern**.

   Der hinzugefügte Service wird jetzt im Bereich „Services“ angezeigt.

Hinweis: Wenn der Test nicht erfolgreich ist, bearbeiten Sie die Serviceinformationen und versuchen Sie es erneut.

Schritt 2. Konfigurieren einer Datenbank für den Incident Management-Service

Sie müssen die Datenbank für den Incident Management-Service konfigurieren, damit sie verwendet werden kann. Die ESA-Installation erstellt und sichert eine Datenbankinstanz für den Incident Management-Service. Sie müssen einen der ESA-Server auswählen, der als Datenbankhost für den Incident Management-Service fungieren soll.

Überlegungen bei der Auswahl des Hosts für die ESA-Datenbank

Dieses Thema ist relevant, wenn Sie die siteübergreifende Korrelation in ESA aktivieren.

Die siteübergreifende Korrelation in ESA ermöglicht Ihnen das Erstellen einer Bereitstellung, die einen Regelsatz und mehrere ESA-Services umfasst. Die wichtigsten Merkmale einer Bereitstellung mit siteübergreifender Korrelation sind:

1. Es gibt einen zentralen ESA-Service.
2. Wenn Sie Regeln bereitstellen, leiten ESA-Services relevante Ereignisse an den zentralen ESA-Service weiter.
3. Der zentrale ESA-Service führt die Regeln aus und erzeugt Warnmeldungen.

Wenn Sie die siteübergreifende Korrelation aktivieren, müssen Sie bei der Auswahl des ESA-Services für Incident Management einige wichtige Faktoren berücksichtigen:

- Wählen Sie einen ESA-Service aus, der sich auf dem Security Analytics-Server befindet, um die Latenz beim Zugriff auf die MongoDB zu reduzieren.
- Wählen Sie den ESA-Service aus, der den geringsten Datenverkehr aufweist.

Hinweis: Wählen Sie nicht den zentralen ESA-Service, da dieser seinen eigen Datenverkehr aufnimmt und die weitergeleiteten Ereignisse von anderen ESA-Services empfängt.

Standardmäßig ist die siteübergreifende Korrelation deaktiviert. Wenn Sie die siteübergreifende Korrelation aktivieren möchten, müssen Sie sich mit RSA Professional Services in Verbindung setzen, um am Versuchsprogramm zur siteübergreifenden Korrelation teilnehmen zu können.

Voraussetzungen

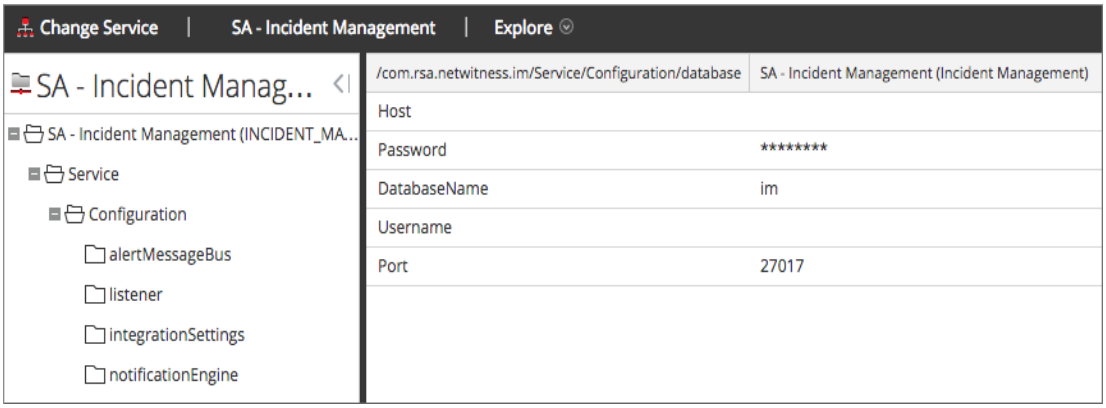
Vergewissern Sie sich, dass ein ESA-Host installiert und konfiguriert ist.

Verfahren

So konfigurieren Sie eine Datenbank für den Incident Management-Service:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie im Bereich „Services“ den Incident Management-Service und  **>Ansicht > Durchsuchen** aus.
   Die Serviceübersicht wird angezeigt.
3. Wählen Sie im Bereich „Optionen“ die Optionen **Service > Konfiguration > Datenbank** aus.

   Die Datenbankansicht wird im rechten Bereich angezeigt.



4. Stellen Sie folgende Informationen bereit:
   - **Host**: Der Hostname oder die IP-Adresse des ESA-Hosts, der als Datenbank ausgewählt wurde
   - **DatabaseName**: im (Standardwert)
   - **Port**: 27017 (Standardwert)
   - **Benutzername**: Der Benutzername für das Benutzerkonto der IM-Datenbank (ESA erstellt einen IM-Benutzer mit den entsprechenden Berechtigungen.)
   - **Passwort**: Das für den IM-Benutzer ausgewählte Passwort
5. Starten Sie den Incident Management-Service mit dem folgenden Befehl neu:

   ```
   service rsa-im restart
   ```

Hinweis: Der Neustart des Incident Management-Services ist wichtig, damit die Datenbankkonfiguration abgeschlossen werden kann.

Schritt 3. Konfigurieren von Warnmeldungsquellen für das Anzeigen von Warnmeldungen in Incident Management

Dieses Verfahren ist erforderlich, damit Warnmeldungen von den Warnmeldungsquellen in Incident Management angezeigt werden. Sie können die Option, die Warnmeldungen in der Ansicht „Incident Management“ anzuzeigen, aktivieren oder deaktivieren. Standardmäßig ist diese Option in Reporting Engine, Malware Analytics und ECAT deaktiviert und nur in Event Stream Analysis aktiviert. Wenn Sie also den Service „Incident Management“ installieren, müssen Sie diese Option in Reporting Engine, Malware Analytics, und ECAT aktivieren, damit die entsprechenden Warnmeldungen in der Ansicht „Incident Management“ angezeigt werden.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Der Incident Management-Service ist auf Security Analytics installiert und wird ausgeführt.
- Eine Datenbank wird für den Incident Management-Service konfiguriert.
- ECAT ist installiert und wird ausgeführt.

Konfigurieren von Reporting Engine zur Anzeige von durch Reporting Engine ausgelösten Warnmeldungen in der Ansicht „Incident Management“

Die Anzeige der Reporting Engine-Warnmeldungen in der Ansicht „Incident Management“ ist standardmäßig deaktiviert. Um die Reporting Engine-Warnmeldungen anzuzeigen, müssen Sie die Incident Management-Warnmeldungen in der Servicekonfigurationsansicht > Registerkarte „Allgemein“ für die Reporting Engine aktivieren.

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie einen Reporting Engine-Service und dann  > **Ansicht > Konfiguration** aus.
   Die Servicekonfigurationsansicht wird mit geöffneter Registerkarte Reporting Engine Allgemein angezeigt.
3. Wählen Sie **Systemkonfiguration** aus.
4. Aktivieren Sie das Kontrollkästchen für **Warnmeldungen an IM weiterleiten**.
   Die Reporting Engine leitet nun die Warnmeldungen an Incident Management weiter.

Informationen zu Parametern auf der Registerkarte „Allgemein“ finden Sie im Thema **Reporting Engine-Registerkarte „Allgemein“** im *Reporting Engine-Konfigurationsleitfaden*.

Konfigurieren von Malware Analytics zur Anzeige von durch Malware Analytics ausgelösten Warnmeldungen in der Ansicht „Incident Management“

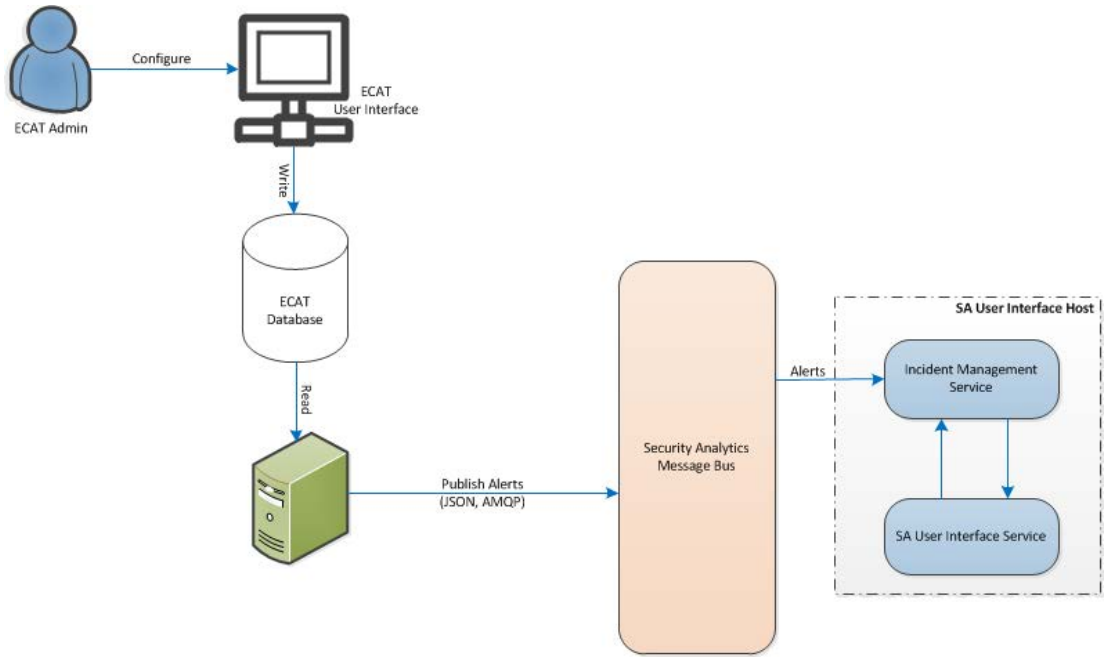
Die Anzeige von Warnmeldungen aus Incident Management ist eine Auditing-Funktion in Malware Analysis. Eine Beschreibung des Verfahrens zum Aktivieren von Warnmeldungen aus Incident Management finden Sie im Thema **(Optional) Konfigurieren des Auditing auf dem Malware Analysis-Host** im *Malware Analysis-Konfigurationsleitfaden*.

Konfigurieren von ECAT zur Anzeige von durch ECAT ausgelösten Warnmeldungen in der Ansicht „Incident Management“

Dieses Verfahren ist für die Integration von ECAT in Security Analytics erforderlich, damit die ECAT-Warnmeldungen von der Incident Management-Komponente von Security Analytics erkannt und in der Ansicht **Incident > Warnmeldungen** angezeigt werden.

Hinweis: Das Thema **RSA ECAT-Integration** im *RSA ECAT-Integrationsleitfaden* bietet eine Übersicht über ECAT-Integrationsfunktionen in Security Analytics sowie detaillierte Verfahren zur Konfiguration der Integration von ECAT in Security Analytics über den Nachrichtenbus.

Das Diagramm unten stellt den Fluss von ECAT-Warnmeldungen zur Incident Management-Warteschlange von Security Analytics und seine Anzeige in der Ansicht **Incident > Warnmeldungen** dar.



Konfigurieren von ECAT zur Anzeige von ECAT-Warnmeldungen

So konfigurieren Sie ECAT, damit ECAT-Warnmeldungen in der Security Analytics-Benutzeroberfläche angezeigt werden:

1. Klicken Sie in der ECAT-Benutzeroberfläche auf **Konfiguration > Überwachung und externe Komponenten**.

   Das Dialogfeld **Überwachung und externe Komponenten** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste an einer beliebigen Stelle in das Dialogfeld und wählen Sie **Komponente hinzufügen** aus.

   Das Dialogfeld **Komponente hinzufügen** wird angezeigt.

3. Stellen Sie folgende Informationen bereit:

   - Wählen Sie in den Drop-down-Optionen als **Komponententyp** den IM-Broker aus.
   - Geben Sie einen Benutzernamen zur Identifizierung des IM-Broker ein.
   - Geben Sie den **Hostnamen oder die IP-Adresse** des IM-Broker ein.
   - Geben Sie die **Portnummer** ein. Der Standardport ist 5671.

4. Klicken Sie auf **Speichern und Schließen**, um alle Dialogfelder zu schließen.

5. Um SSL für IM-Warnmeldungen einzurichten, führen Sie folgende Schritte auf ECAT aus, um die SSL-Kommunikation einzurichten:

   a. Exportieren Sie auf dem primären ECAT-Konsolenserver das ECAT CA-Zertifikat im cer-Format (Base-64-verschlüsselt X.509) aus dem persönlichen Zertifikat-Store des lokalen Computers (ohne den privaten Schlüssel auszuwählen).

   b. Erzeugen Sie auf dem primären ECAT-Konsolenserver mithilfe des ECAT CA-Zertifikats ein Clientzertifikat für ECAT. (Der CN-Name muss auf „ecat“ festgelegt werden.)

   ```
   makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
   sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "EcatCA" -is MY -ir
   LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
   cy end -sy 12 client.cer
   ```

   c. Notieren Sie sich auf dem primären ECAT-Konsolenserver den Thumbprint des in Schritt b generierten Clientzertifikats. Geben Sie den Thumbprint-Wert des Clientzertifikats im Abschnitt IMBrokerClientCertificateThumbprint der ConsoleServer.Exe.Config-Datei ein (siehe Abbildung).

   ```
   <add key="IMBrokerClientCertificateThumbprint"
   value="?896df0efacf0c976d955d5300ba0073383c83abc"/>
   ```

d. Hängen Sie auf dem SA-Server den Inhalt der ECAT CA-Zertifikatdatei im CER-Format (aus Schritt a) an die Datei `/etc/puppet/modules/rabbitmq/files/truststore.pem` an.

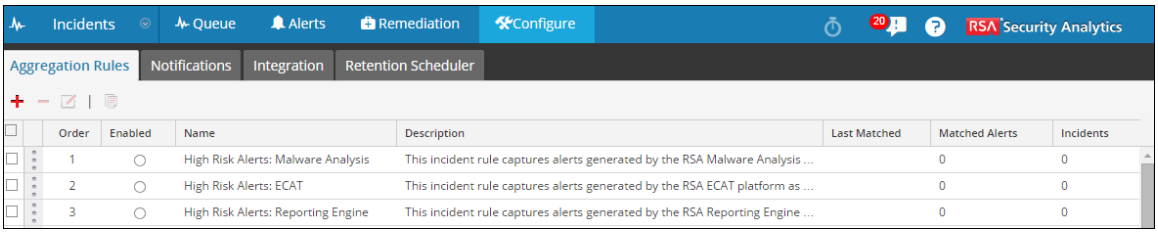
e. Führen Sie auf dem SA-Server den Puppet Agent wie dargestellt aus (oder warten Sie 30 Minuten, bis der SA-Server ausgeführt wird).

```
puppet agent -t
```

f. Importieren Sie auf dem primären ECAT-Konsolenserver die Datei `/var/lib/puppet/ssl/certs/ca.pem` vom Security Analytics-Server in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen. Dadurch wird sichergestellt, dass der ECAT als Client dem Zertifikat des IM-Servers vertrauen kann.

Einstellen des Zählers für abgestimmte Warnmeldungen und Incidents

Dieses Verfahren ist optional. Administratoren können damit ändern, wann der Zähler für abgestimmte Warnmeldungen auf 0 zurückgesetzt wird. Auf der Registerkarte „Aggregationsregeln“ werden diese Zähler in Spalten auf der rechten Seite angezeigt.



Diese Spalten bieten die folgenden Informationen für eine Regel:

- Die Spalte **Zuletzt abgestimmt** zeigt die Uhrzeit an, zu der die Regel zuletzt Warnmeldungen abgestimmt hat.
- Die Spalte **Abgestimmte Warnmeldungen** zeigt die Anzahl der abgestimmten Warnmeldungen für die Regel an.
- Die Spalte **Incidents** zeigt die Anzahl der von der Regel erstellten Incidents an.

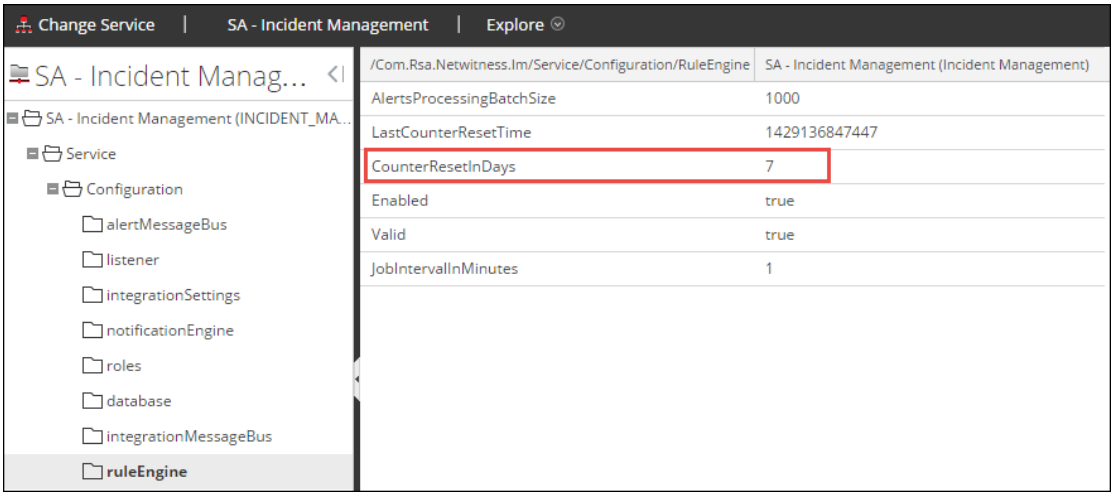
Standardmäßig werden diese Werte alle 7 Tage auf Null zurückgesetzt. Je nachdem, wie lange die Zählungen fortgesetzt werden sollen, können Sie die Standardanzahl der Tage ändern.

Hinweis: Wenn der Zähler auf Null zurückgesetzt wird, wechseln nur die Zahlen in den drei Spalten auf Null. Es werden keine Warnmeldungen oder Incidents gelöscht.

So stellen Sie einen Zähler für abgestimmte Warnmeldungen und Incidents ein:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration** > **Services** aus.
2. Wählen Sie einen Incident Management-Service aus und wählen Sie dann > **Ansicht** > **Durchsuchen** aus.

3. Wählen Sie in der Ansicht „Durchsuchen“ auf der linken Seite **Service > Konfiguration > ruleEngine** aus.



4. Geben Sie im rechten Bereich die Anzahl der Tage in das Feld **CounterResetInDays** ein.
5. Starten Sie den Service neu, damit die Änderungen wirksam werden:
   a. Wählen Sie **Services** aus.
   b. Wählen Sie den Service aus und klicken Sie auf  **> Neustart**.

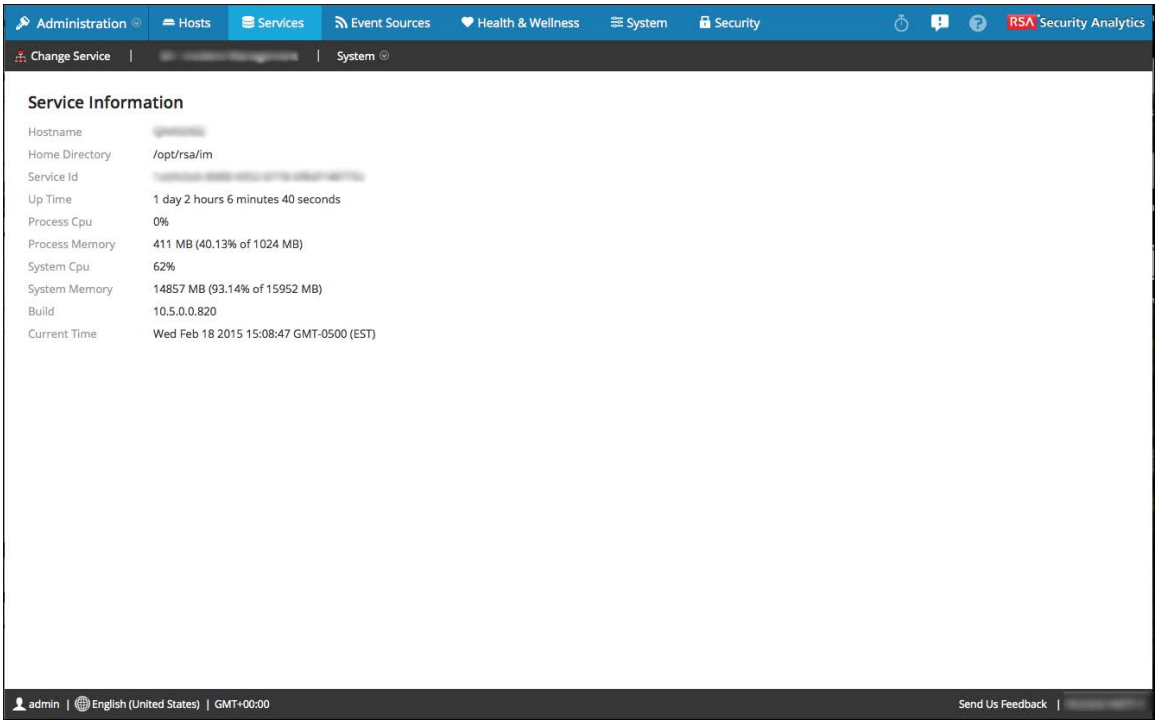
Ansicht „Services-System“ von Incident Management

In der Ansicht „Services-System“ können Sie Informationen über den Incident Management-Service anzeigen.

Zugriff auf die Ansicht

So greifen Sie auf diese Ansicht zu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Administration > Services** aus.
2. Wählen Sie im Raster **Services** einen Incident Management-Service und > **Ansicht** > **System** aus.
   Die Ansicht „Services-System“ von Incident Management wird angezeigt.



Serviceinformationen

Die Ansicht System enthält einen Bereich: den Bereich Serviceinformationen. Der Bereich „Serviceinformationen“ bietet eine Servicezusammenfassung, die sich leicht von der generischen Ansicht „Services > System“ unterscheidet. Diese Tabelle beschreibt die Serviceinformationen des Bereichs.

Feld	Beschreibung
Hostname	Zeigt den Namen des Hosts an. Beispiel: NWAPPLIANCE2682
Benutzerverzeichnis	Zeigt den Speicherort des Incident Management-Stamm-verzeichnisses an. Beispiel: /opt/rsa/im
Service-ID	Zeigt die Service-ID an. Beispiel: 1694b15c-42c7-410d-9ba3-a7c48ba4722d
Betriebszeit	Zeigt die Zeitdauer an, die seit dem Start des Hosts vergangen ist. Beispiel: 0 5 Stunden 33 Minuten 20 Sekunden
Prozess-CPU	Zeigt an, wie viel Prozent der CPU (Central Processing Unit) der Prozess belegt. Beispiel: %0
Prozess-Speicher	Zeigt den vom Prozess belegten Arbeitsspeicher an. Beispiel: 86285 KB (8,37 % von 1024 MB)
System-CPU	Zeigt an, wie viel Prozent der CPU das System belegt. Beispiel: %2
Systemspeicher	Zeigt den vom System belegten Arbeitsspeicher an. Beispiel: 30065 MB (31,05 % von 96831 MB)
Build	Zeigt die Versionsnummer von Security Analytics an. Beispiel: 10.6.0.0.1009
Aktuelle Zeit	Zeigt den aktuellen Tag der Woche, Datum und Uhrzeit an. Beispiel: Thu Jan 14 2016 11:15:23 GMT-0500 (EST)