RSA NETWITNESS® SUITE

Systemkonfigurationsleitfaden

für Version 11.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

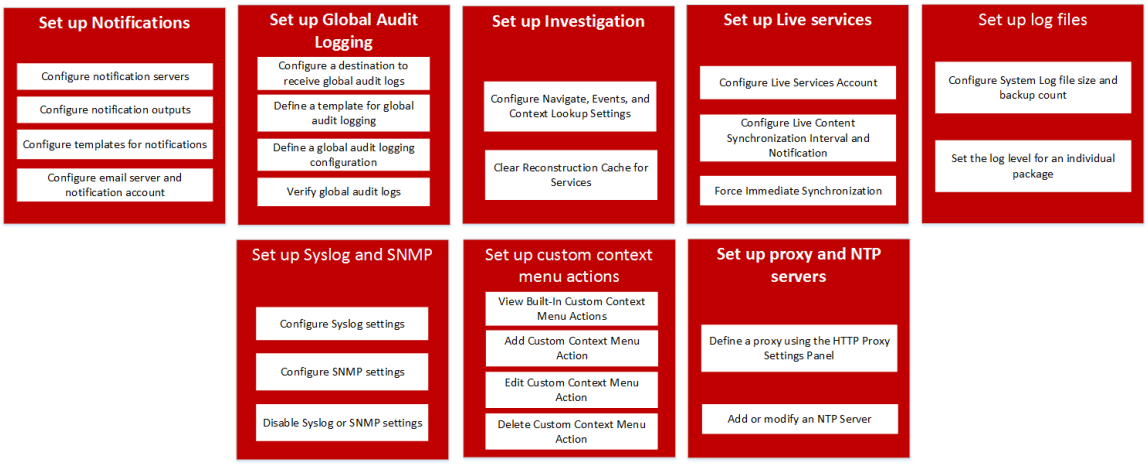
EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2018

Inhalt

Systemkonfiguration – Übersicht

In der Ansicht „Administration > System“ können Administratoren bestimmte Systemeinstellungen konfigurieren, um optimale Performance für NetWitness Suite zu erzielen. Dieses Diagramm zeigt die verfügbaren Konfigurationsoptionen an.



Die Standardverfahren in diesem Leitfaden bieten Anweisungen für Administratoren, die Einstellungen, die quer durch das System in NetWitness Suite angewendet werden, anpassen möchten. Obwohl einige dieser Einstellungen Standardwerte haben, müssen Administratoren alle Standardwerte anzeigen und evaluieren.

Die zusätzlichen Verfahren sind für die Einrichtung von NetWitness Suite nicht grundlegend erforderlich, sie umfassen bestimmte Anpassungsoptionen, die über die übliche Einrichtung hinausgehen; beispielsweise das Hinzufügen von benutzerdefinierten Kontextmenüs oder die Proxy-Einrichtung.

Darüber hinaus enthalten die Referenz- und Troubleshootingthemen ausführliche Informationen über die Benutzeroberfläche und Vorschläge zur Behebung möglicher Probleme.

Die folgenden Abschnitte beschreiben die Systemkonfiguration:

- Standardverfahren bietet Anweisungen für Administratoren, die Einstellungen, die quer durch das System in NetWitness Suite angewendet werden, anpassen möchten.
- Zusätzliche Verfahren enthält Anweisungen für die Einrichtung von Anpassungsoptionen, die über die übliche Systemkonfiguration hinausgehen.

Standardverfahren

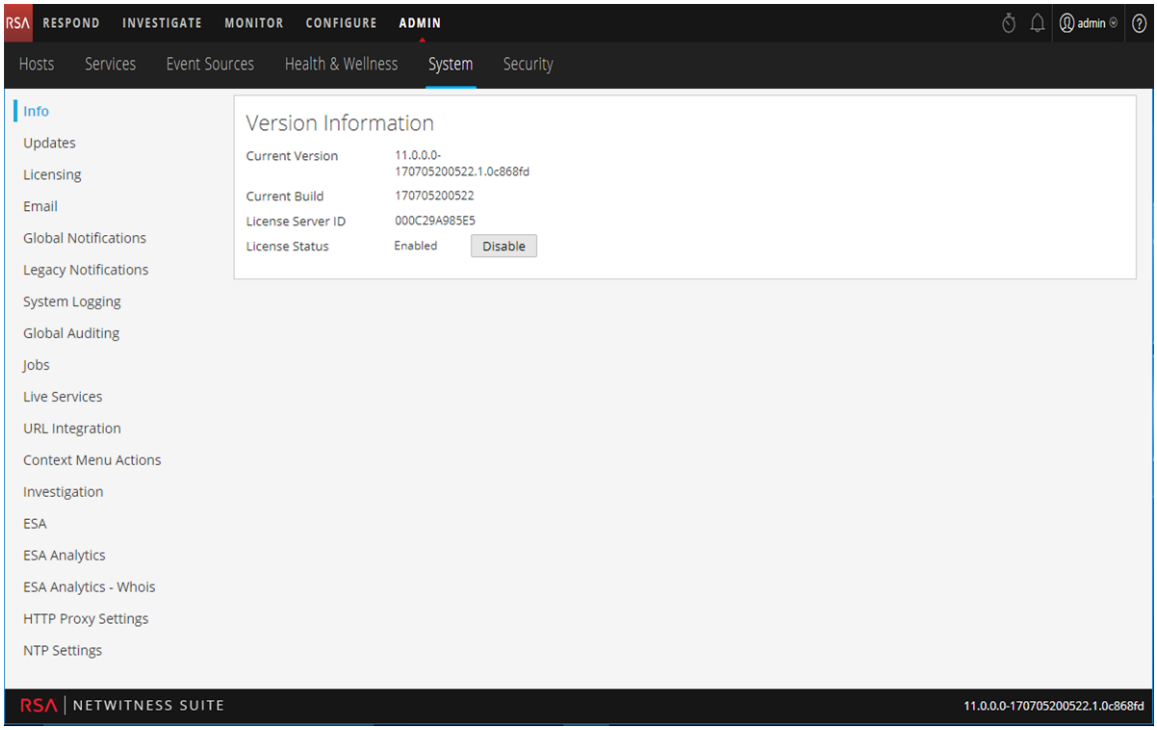
Die Themen in diesem Abschnitt enthalten Anweisungen für Administratoren, die Einstellungen, welche quer durch das System in NetWitness Suite angewendet werden, anpassen möchten. Obwohl einige dieser Einstellungen Standardwerte haben, müssen Administratoren alle Standardwerte anzeigen und evaluieren. Die Verfahren können in beliebiger Reihenfolge durchgeführt werden und sind in alphabetischer Reihenfolge aufgeführt.

Zugriff auf Systemeinstellungen

Dieses Thema ist eine Einführung in die Funktionen von NetWitness Suite für die Systemkonfiguration in der Ansicht „Administration > System“. Administratoren können Benachrichtigungen,E-Mail-Benachrichtigungen, die globale Auditprotokollierung, Protokollierungseinstellungen, die Verbindung zu Live-Services und die URL-Integration in NetWitness Suite konfigurieren.

So greifen Sie auf die Systemeinstellungen zu:

Navigieren Sie zu **ADMIN > System**.
Die Ansicht Administration > System wird angezeigt.



Auf der linken Seite der Ansicht „Administration > System“ befindet sich ein Optionsbereich, in dem alle für die Konfiguration verfügbaren System-Nodes aufgelistet sind. Wenn Sie einen Node auswählen, wird der zugehörige Inhalt im rechten Bereich angezeigt.

Konfigurieren von Benachrichtigungsservern

Dieses Thema bietet Anweisungen zur Konfiguration der Benachrichtigungsserver. Für ESA sind Benachrichtigungsserver erforderlich, um eine ESA-Regel zu definieren. Ein Benachrichtigungsserver ist auch erforderlich, um globale Auditprotokollierung zu konfigurieren.

In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Manamegement, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert. Benachrichtigungsserver definieren die Server, von denen Sie Systembenachrichtigungen empfangen möchten. Definieren Sie für globale Auditprotokollierung Log Decoders als Syslog-Benachrichtigungsserver.

Sie können einen Benachrichtigungsserver in NetWitness Suite definieren, löschen, bearbeiten, importieren und exportieren. Die relevanten Verfahren werden in gesonderten Themen beschrieben. Weitere Informationen über die Konfiguration von ESA-Warnmeldungen erhalten Sie unter „Benachrichtigungsmethoden“ im Handbuch **Versenden von Warnmeldungen mit ESA**. Sie können Benachrichtigungsausgaben und Benachrichtigungsserver auf die gleiche Weise löschen, bearbeiten, importieren und exportieren wie Vorlagen. Sie können Benachrichtigungsserver nicht deaktivieren oder löschen, die mit globalen Auditprotokollierungskonfigurationen verbunden sind.

Übersicht über Benachrichtigungsserver

Dieses Thema enthält eine Übersicht über Benachrichtigungsserver. Sie konfigurieren Benachrichtigungsserver in der Administrationsansicht des Systems (Administration > System > Benachrichtigungen > Registerkarte „Server“).

Globale Benachrichtigungen werden von einer Vielzahl an Komponenten in NetWitness Suite verwendet, wie z. B. Event Stream Analysis (ESA),Reagieren, Integrität und Zustand, Ereignisquellenmanagement (Event Source Manamegement, ESM) und globale Auditprotokollierung. Die Benachrichtigungseinstellungen werden als **Benachrichtigungsserver** bezeichnet.

Event Stream Analysis sendet Benachrichtigungen über verschiedene Systemereignisse per E-Mail, SNMP oder Syslog an die Benutzer. In ESA werden diese Einstellungen für Benachrichtigungen als Benachrichtigungsserver bezeichnet. Sie können mehrere Benachrichtigungsserver konfigurieren und sie beim Definieren von ESA-Regeln verwenden. Zum Beispiel können Sie mehrere E-Mail- oder Syslog-Server konfigurieren und die Einstellungen beim Definieren einer ESA-Regel verwenden.

Sie können folgende Benachrichtigungsserver konfigurieren:

- E-Mail
- SNMP

- Syslog
- Skript

Mit E-Mail-Benachrichtigungsservern können Sie E-Mail-Servereinstellungen konfigurieren, um Warnmeldungsbenachrichtigungen zu senden. SNMP-Benachrichtigungsservern ermöglichen die Konfiguration von SNMP-Trap-Hosteinstellungen als Benachrichtigungsserver, um Warnmeldungsbenachrichtigungen zu senden.

Mit Syslog-Benachrichtigungsservern können Sie Syslog-Einstellungen als Benachrichtigungsserver zum Senden von Benachrichtigungen konfigurieren. Wenn diese Funktion aktiviert ist, wird das Auditing von Syslog über das Syslog-Protokoll RFC 5424 bereitgestellt. Da es für Syslog zahlreiche systemeigene und Open-Source-Tools für das Reporting und Analysen gibt, hat sich Syslog als effektives Format zur Konsolidierung von Protokollen erwiesen. Für die globale Auditprotokollierung können Sie nur Syslog-Benachrichtigungsserver verwenden.

Mit Skriptbenachrichtigungsservern können Sie Skript als Benachrichtigungsserver konfigurieren.

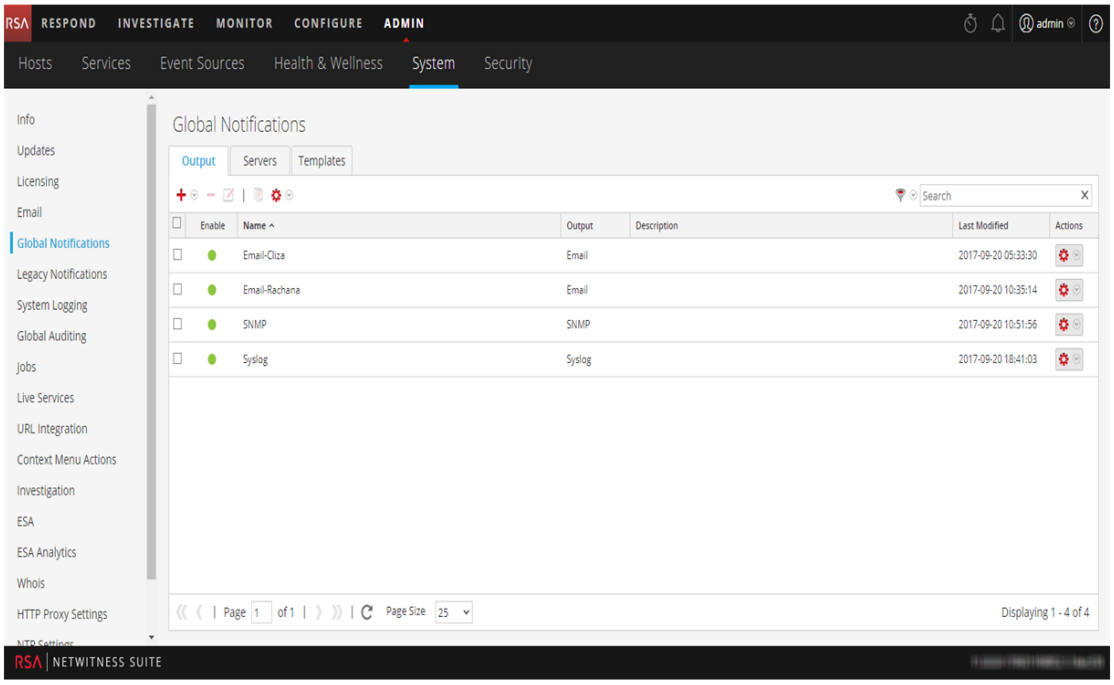
Detaillierte Informationen über die Konfiguration der verschiedenen Benachrichtigungsserver sowie über die Parameter und Beschreibungen finden Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver

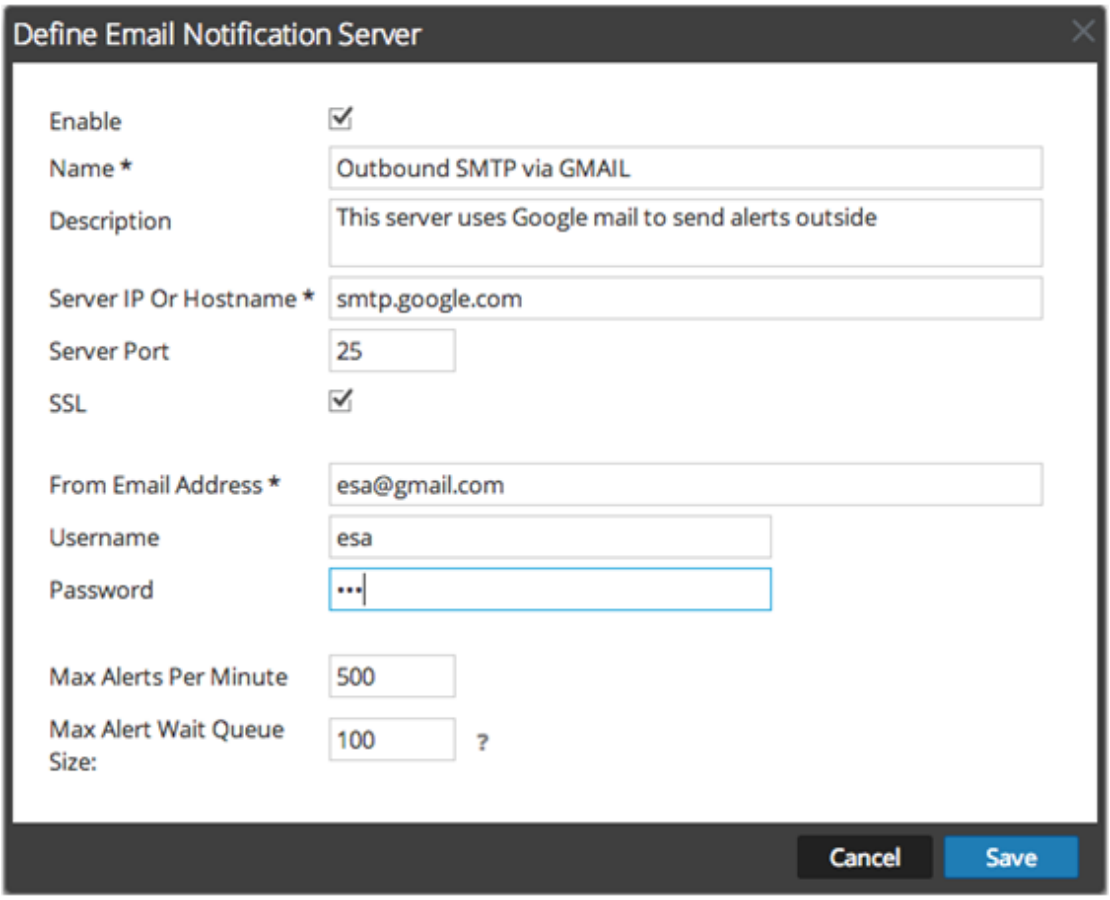
So konfigurieren Sie E-Mail-Servereinstellungen als einen Benachrichtigungsserver zum Senden von Warnmeldungsbenachrichtigungen:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
   Der Konfigurationsbereich **Benachrichtigungen** wird mit geöffneter Registerkarte **Ausgabe** angezeigt.

3. Klicken Sie auf die Registerkarte **Server**.



4. Wählen Sie aus dem Drop-down-Menü + die Option **E-Mail** aus.



5. Geben Sie im Dialogfeld **E-Mail-Benachrichtigungsserver definieren** die erforderlichen Informationen ein und klicken Sie auf **Speichern**.

Hinweis: Für die ESM/SMS- und ESA-Benachrichtigungen müssen Sie nur den Hostnamen/vollständig qualifizierten Domainnamen im Feld „IP-Adresse oder Hostname des Servers“ angeben.

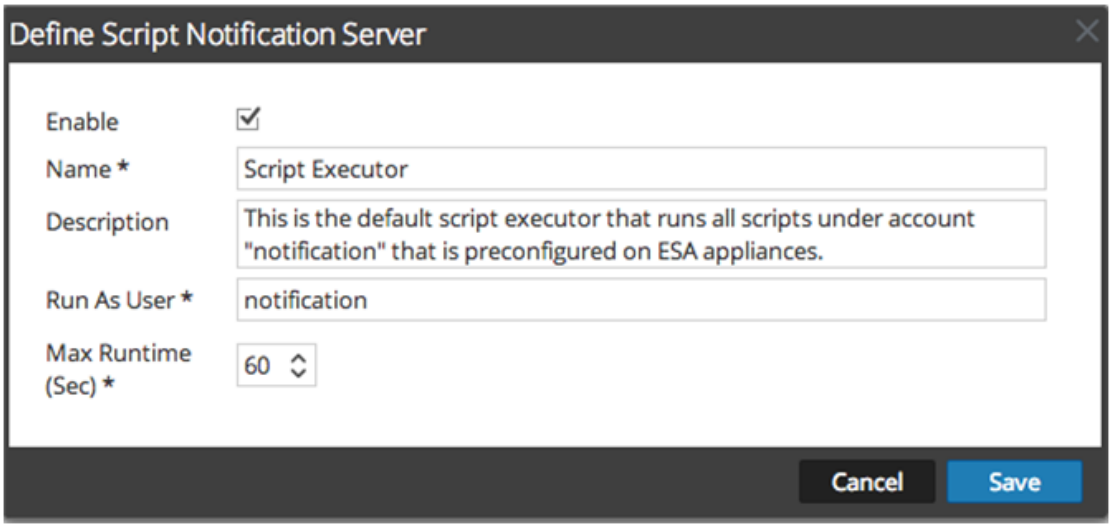
Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren eines Skripts als Benachrichtigungsserver

ESA ermöglicht Ihnen, Skripte als Reaktion auf ESA-Warnmeldungen auszuführen. Zunächst müssen Sie aber die Benutzeridentität und andere Details konfigurieren, die zur Ausführung der Skripte benötigt werden.

So konfigurieren Sie ein Skript als Benachrichtigungsserver:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich **Optionen** die Option **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Server**.
4. Wählen Sie aus dem Drop-down-Menü  die Option **Skript** aus.



5. Geben Sie im Dialogfeld **Skriptbenachrichtigungsserver definieren** die erforderlichen Informationen an und klicken Sie auf **Speichern**.

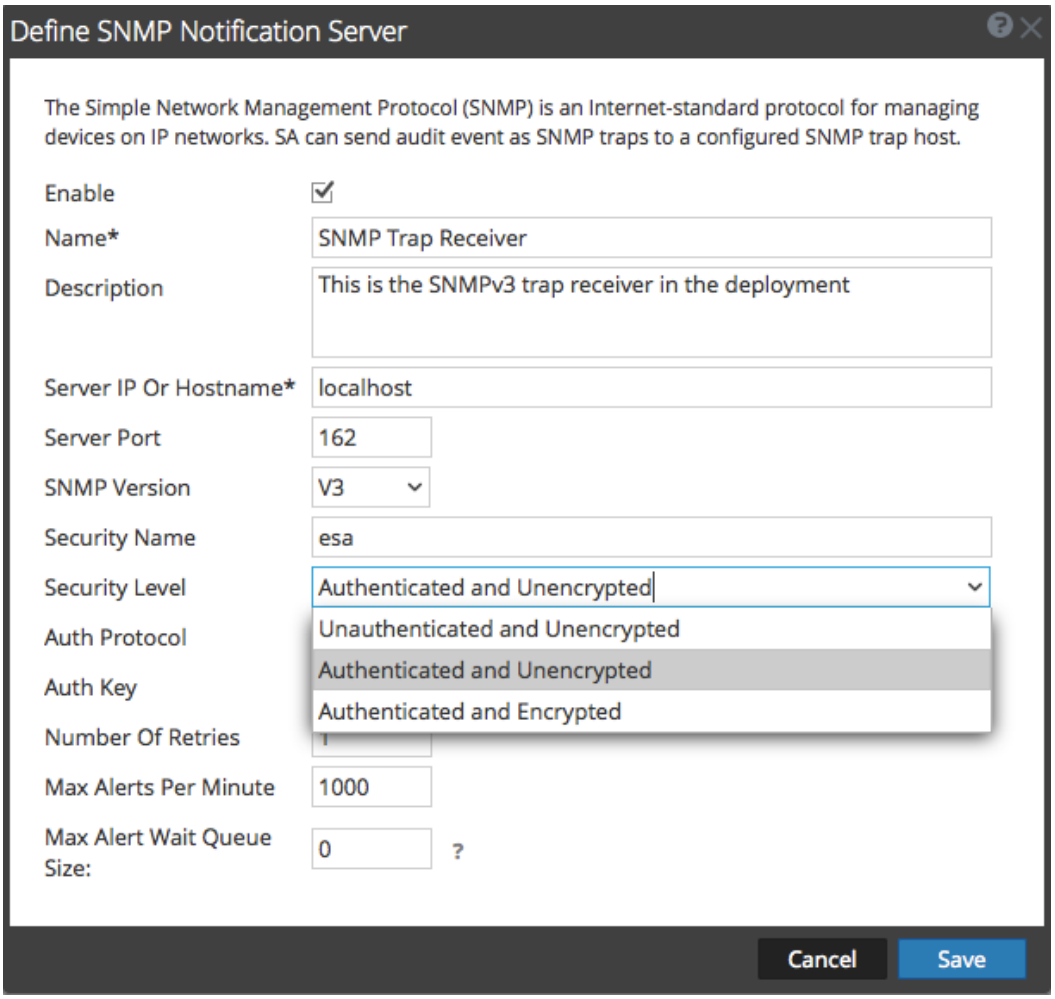
Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren der SNMP-Einstellungen als Benachrichtigungsserver

So konfigurieren Sie die SNMP-Trap-Hosteinstellungen als Benachrichtigungsserver zum Senden von Warnmeldungen:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Server**.

4. Wählen Sie aus dem Drop-down-Menü + die Option **SNMP** aus.



5. Geben Sie im Dialogfeld **SNMP-Benachrichtigungsserver definieren** die erforderlichen Informationen an und klicken Sie auf **Speichern**.

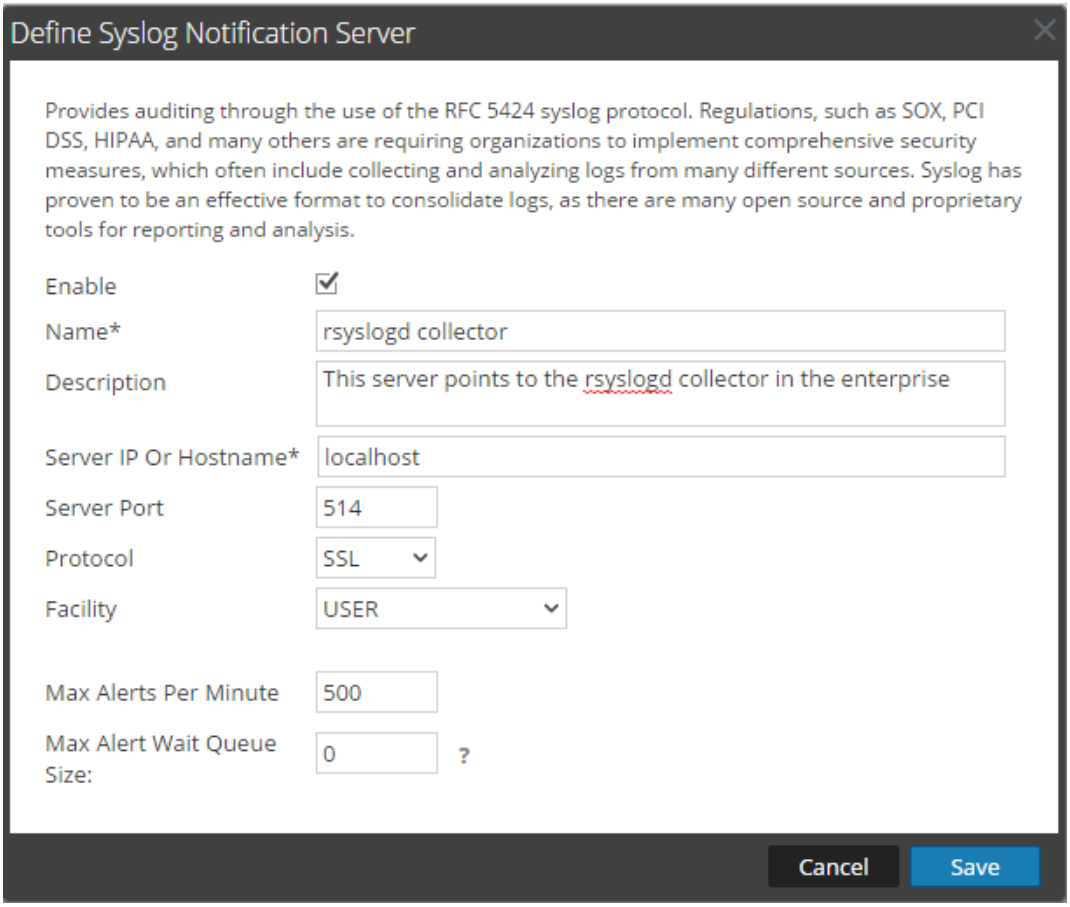
Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren Sie einen Syslog-Benachrichtigungsserver.

Dieses Thema bietet Anweisungen zum Konfigurieren eines Syslog-Benachrichtigungsservers. Wenn diese Funktion aktiviert ist, wird das Auditing von Syslog über das Syslog-Protokoll RFC 5424 bereitgestellt. Da es für Syslog zahlreiche systemeigene und Open-Source-Tools für das Reporting und Analysen gibt, hat sich Syslog als effektives Format zur Konsolidierung von Protokollen erwiesen.

So konfigurieren Sie Syslog als Benachrichtigungsserver:

1. Navigieren Sie zu **ADMINISTRATION > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Server**.
4. Wählen Sie im Drop-down-Menü **die Option** Syslog



   aus.

5. Geben Sie im Dialogfeld **Syslog-Benachrichtigungsserver definieren** die erforderlichen Informationen ein und klicken Sie auf **Speichern**.

Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren von Benachrichtigungsausgaben

Dieses Thema enthält Anweisungen zur Konfiguration von Benachrichtigungsausgaben. Diese Benachrichtigungsausgaben sind zur Definition einer ESA-Regel erforderlich.

In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Manamegement, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert.

Die Registerkarte „Ausgabe“ für die globale Auditprotokollierung muss nicht konfiguriert werden.

In den Konfigurationen für die Benachrichtigungsausgabe werden E-Mail-Adressen und Betreffzeilen, SNMP-Trap-OID-Einstellungen, Syslog-Ausgabeeinstellungen und Skriptcode definiert.

Sie könnenBenachrichtigungsausgaben in NetWitness Suite definieren, löschen, bearbeiten, importieren und exportieren. Die relevanten Verfahren werden in gesonderten Themen beschrieben. Weitere Informationen über die Konfiguration von ESA-Warnmeldungen erhalten Sie unter „Benachrichtigungsmethoden“. Sie können Benachrichtigungsausgaben auf die gleiche Weise löschen, bearbeiten, importieren und exportieren wie Vorlagen. Wenn Sie versuchen, eine Benachrichtigungsausgabe zu löschen, die von Warnmeldungen verwendet wird, wird eine Bestätigungsmeldung mit einer Warnung angezeigt, dass die diese Benachrichtigung verwendenden Warnmeldungen nicht mehr ordnungsgemäß funktionieren werden. In der Meldung wird die Anzahl der betroffenen Warnmeldungen angezeigt.

Benachrichtigungsausgaben – Übersicht

Dieses Thema bietet eine Übersicht über Benachrichtigungsausgaben. Diese Benachrichtigungsausgaben sind zur Definition einer ESA-Regel erforderlich. Benachrichtigungsausgaben werden in der Ansicht „Administration-System“ (Administration > System > Benachrichtigungen > Registerkarte „Ausgabe“) konfiguriert.

In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Manamegement, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert.

Hinweis: Sie müssen Benachrichtigungsausgaben (Registerkarte Ausgabe) nicht für die globale Auditprotokollierung konfigurieren.

Benachrichtigungsausgaben stellen im Wesentlichen die Ziele für das Versenden von Benachrichtigungen dar. Bei ESA können Sie mithilfe von Benachrichtigungsausgaben definieren, wie Sie ESA-Warnmeldungen empfangen möchten. Im Folgenden sind die verschiedenen Benachrichtigungsausgaben aufgeführt, die von NetWitness Suite unterstützt werden:

- E-Mail
- SNMP
- Syslog
- Skript

Mit den E-Mail-Benachrichtigungseinstellungen können Sie Ziel-E-Mail-Adressen definieren, an die die ESA-Warnmeldungen gesendet werden. Sie können auch mehrere Ziel-E-Mail-Adressen angeben. Darüber hinaus können Sie im Betreff der E-Mail eine benutzerdefinierte Beschreibung hinzufügen.

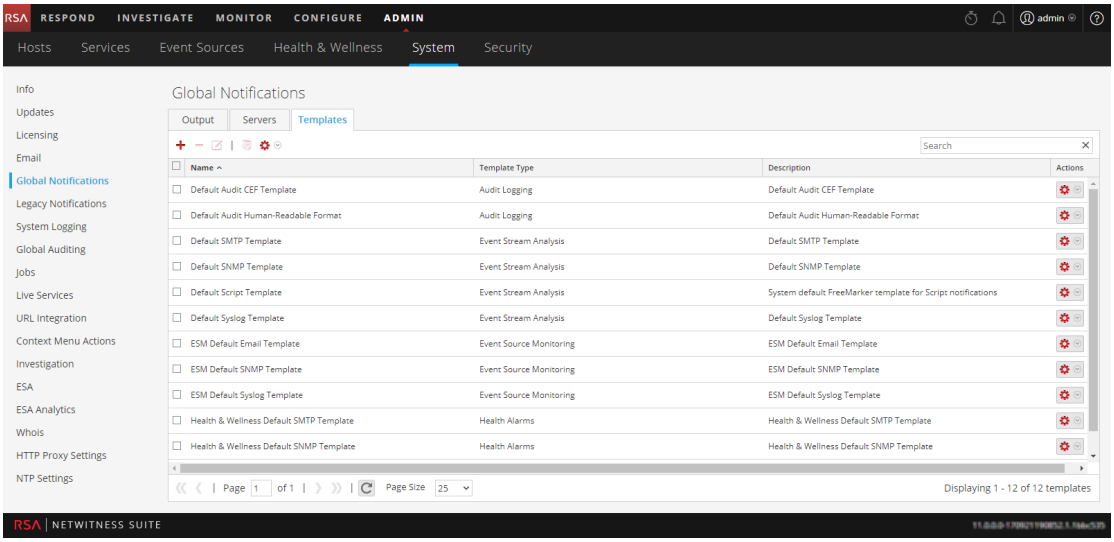
Mit SNMP-Benachrichtigungseinstellungen definieren Sie die SNMP-Einstellungen zum Senden von Warnmeldungsbenachrichtigungen. Syslog-Benachrichtigungen ermöglichen die Defintion der Syslog-Einstellungen zum Senden von Warnmeldungsbenachrichtigungen. Mit Skriptbenachrichtigungen können Sie das Skript definieren, das als Reaktion auf die Warnmeldung ausgeführt wird.

Detaillierte Informationen über die Benachrichtigungskonfigurationen sowie über die Parameter und Beschreibungen finden Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

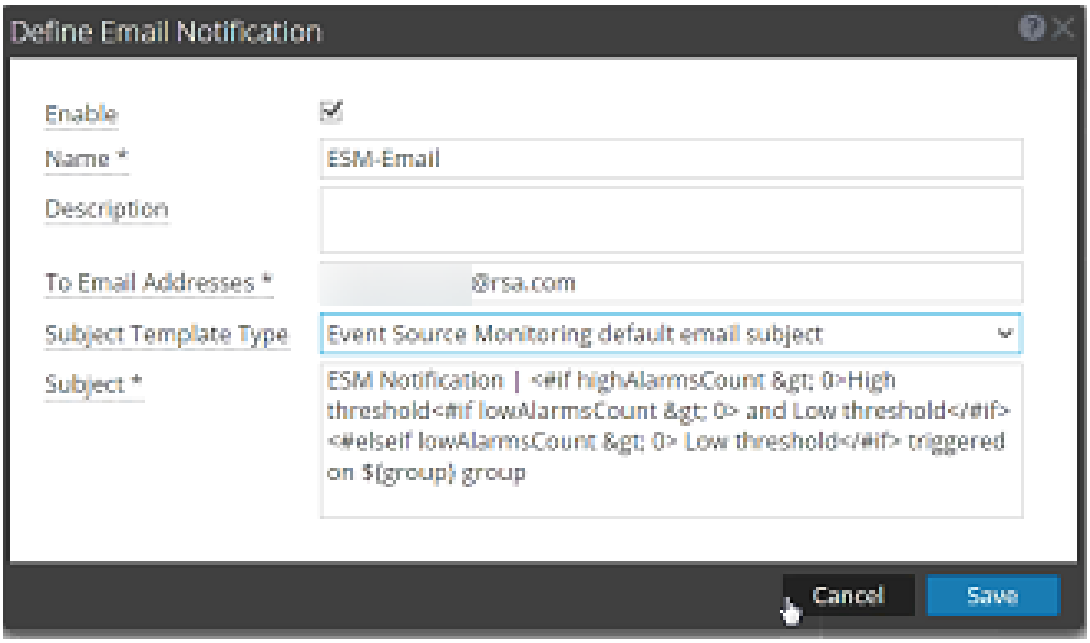
Konfigurieren von E-Mail als Benachrichtigung

So konfigurieren Sie E-Mail als Benachrichtigung:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.



3. Wählen Sie auf der Registerkarte **Ausgabe** im Drop-down-Menü die Option **E-Mail** aus.



4. Machen Sie im Dialogfeld **E-Mail-Benachrichtigung definieren** die erforderlichen Angaben und klicken Sie auf **Speichern**.

Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

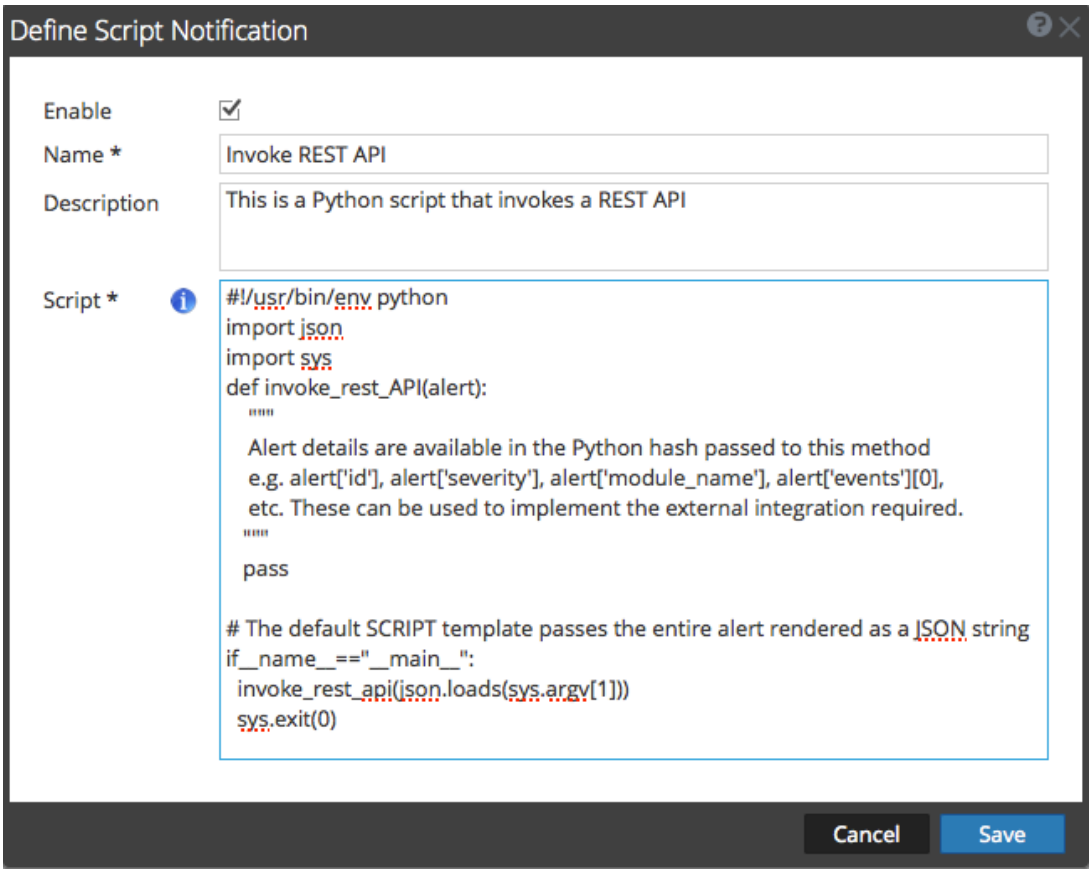
Konfigurieren von Skript als Benachrichtigung

In diesem Thema wird erläutert, wie Sie ein Skript definieren und es als Benachrichtigungsausgabe konfigurieren. ESA ermöglicht Ihnen, Skripte als Reaktion auf ESA-Warnmeldungen auszuführen. Sie müssen das Skript über die Registerkarte „ADMIN > System > Benachrichtigungen > Ausgabe“ definieren. Sie können ein beliebiges Skript für ESA-Benachrichtigungen angeben.

So konfigurieren Sie das Skript als eine Benachrichtigung:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Globale Benachrichtigungen** aus.

3. Wählen Sie auf der Registerkarte „Ausgabe“ im Drop-down-Menü  die Option **Skript** aus.



4. Geben Sie im Dialogfeld **Skriptbenachrichtigung definieren** die erforderlichen Informationen an und klicken Sie auf **Speichern**.

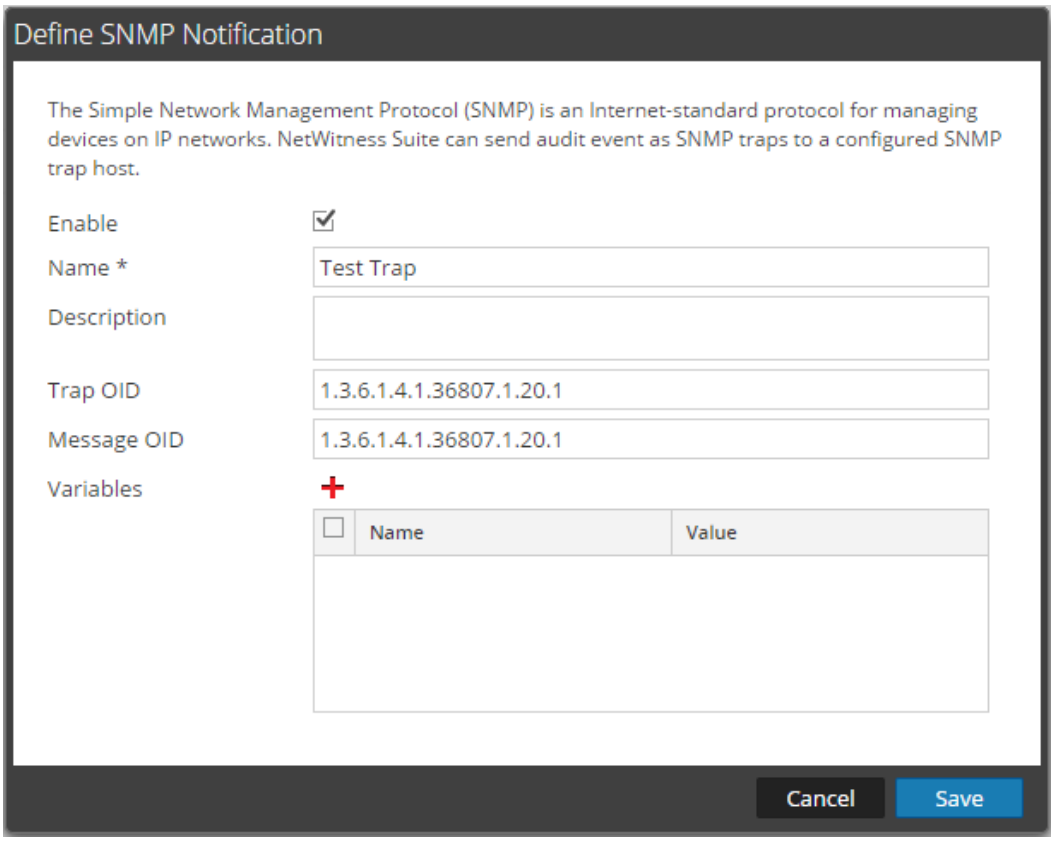
Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren von SNMP als Benachrichtigung

So konfigurieren Sie SNMP als eine Benachrichtigungsausgabe zum Senden von Warnmeldungsbenachrichtigungen:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich **Optionen** die Option **Globale Benachrichtigungen** aus.

3. Wählen Sie auf der Registerkarte „Ausgabe“ im Drop-down-Menü + die Option **SNMP** aus.



4. Geben Sie im Dialogfeld „SNMP-Benachrichtigung“ die erforderlichen Informationen an und klicken Sie auf **Speichern**.

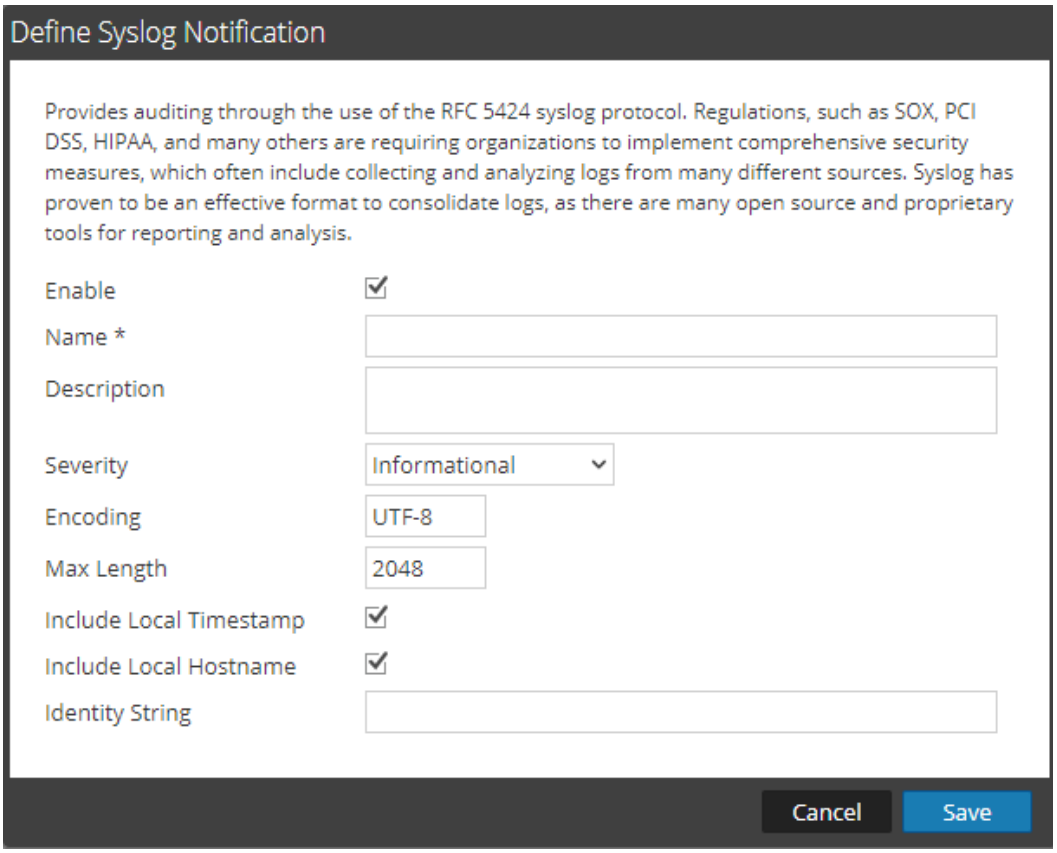
Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren von Syslog als Benachrichtigung

So konfigurieren Sie Syslog als Benachrichtigungsausgabe zum Senden von Warnmeldungsbenachrichtigungen:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.

3. Wählen Sie auf der Registerkarte „Ausgabe“ im Drop-down-Menü + die Option **Syslog** aus.



4. Geben Sie im Dialogfeld **Syslog-Benachrichtigungen definieren** die erforderlichen Informationen an und klicken Sie auf **Speichern**.

Weitere Informationen und Beschreibungen der Parameter erhalten Sie unter Dialogfelder zum Definieren der Benachrichtigungsserver.

Konfigurieren von Vorlagen für Benachrichtigungen

Sie konfigurieren Benachrichtigungsvorlagen in der Ansicht „Administration-System“ (Administration > System > Benachrichtigungen > Registerkarte „Vorlagen“). Eine Benachrichtigungsvorlage definiert das Format und die Nachrichtenfelder von Benachrichtigungen. Sie können unterschiedliche Vorlagentypen für Benachrichtigungen konfigurieren:

- Auditprotokollierung
- Event Stream Analysis
- Ereignisquellenüberwachung
- Integritätsalarme

Sie können Standardvorlagen verwenden oder je nach Vorlagentyp Ihre eigenen Vorlagen für E-Mail, SNMP, Syslog und Skript konfigurieren.

Die gobale Auditprotokollierung sendet Auditprotokolle in dem in der Vorlage für die Auditprotokollierung angegebenen Format. Sie können die Standardvorlagen für die Auditprotokollierung verwenden oder eigene Auditprotokollierungsvorlagen verwenden. Weitere Informationen zur Definition einer Vorlage für die Auditprotokollierung finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung.

Event Stream Analysis (ESA) sendet Benachrichtigungen in dem in den Vorlagen für Event Stream Analysis angegebenen Format. Die Event Stream Analysis-Standardvorlagen für E-Mail, SNMP und Syslog sind bei der Installation verfügbar. Sie können diese Vorlagen anpassen sowie neue Vorlagen erstellen, die Sie für die Benachrichtigungen verwenden können. Weitere Informationen zur Definition von ESA-Vorlagen finden Sie unter Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen.

Weitere Informationen über die Konfiguration von ESA-Warnmeldungen finden Sie unter „Benachrichtigungsmethoden“ im Handbuch **Versenden von Warnmeldungen mit ESA**. Sie können keine Vorlagen löschen, die mit globalen Auditprotokollinformationen verknüpft sind.

Hinweis: Beim Upgrade von NetWitness Suite 10.4 werden alle vorhandenen Vorlagen auf den Event Stream Analysis-Vorlagentyp migriert.

Informationen über das Definieren, Löschen, Bearbeiten, Duplizieren, Importieren und Exportieren einer Vorlage für Benachrichtigungen in NetWitness Suite finden Sie unter:

Konfigurieren von Vorlagen für globale Benachrichtigungen

Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen

Importieren und Exportieren einer Vorlage für globale Benachrichtigungen

Konfigurieren von Vorlagen für globale Benachrichtigungen

Dieses Thema enthält Anweisungen zum Hinzufügen, Bearbeiten, Duplizieren und Löschen von Vorlagen für globale Benachrichtigungen.

Sie können Standardvorlagen verwenden oder je nach Vorlagentyp Ihre eigenen Vorlagen für E-Mail, SNMP, Syslog und Skript konfigurieren.

Die gobale Auditprotokollierung sendet Auditprotokolle in dem in der Vorlage für die Auditprotokollierung angegebenen Format. Sie können die Standardvorlagen für die Auditprotokollierung verwenden oder eigene Auditprotokollierungsvorlagen verwenden. Weitere Informationen über die Definition einer Vorlage für die Auditprotokollierung finden Sie unter „Definieren einer Vorlage für die globale Auditprotokollierung“.

Event Stream Analysis (ESA) sendet Benachrichtigungen in dem in den Vorlagen für Event Stream Analysis angegebenen Format. Die Event Stream Analysis-Standardvorlagen für E-Mail, SNMP und Syslog sind bei der Installation verfügbar. Sie können diese Vorlagen anpassen sowie neue Vorlagen erstellen, die Sie für die Benachrichtigungen verwenden können. Weitere Informationen zur Definition von ESA-Vorlagen finden Sie unter Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen.

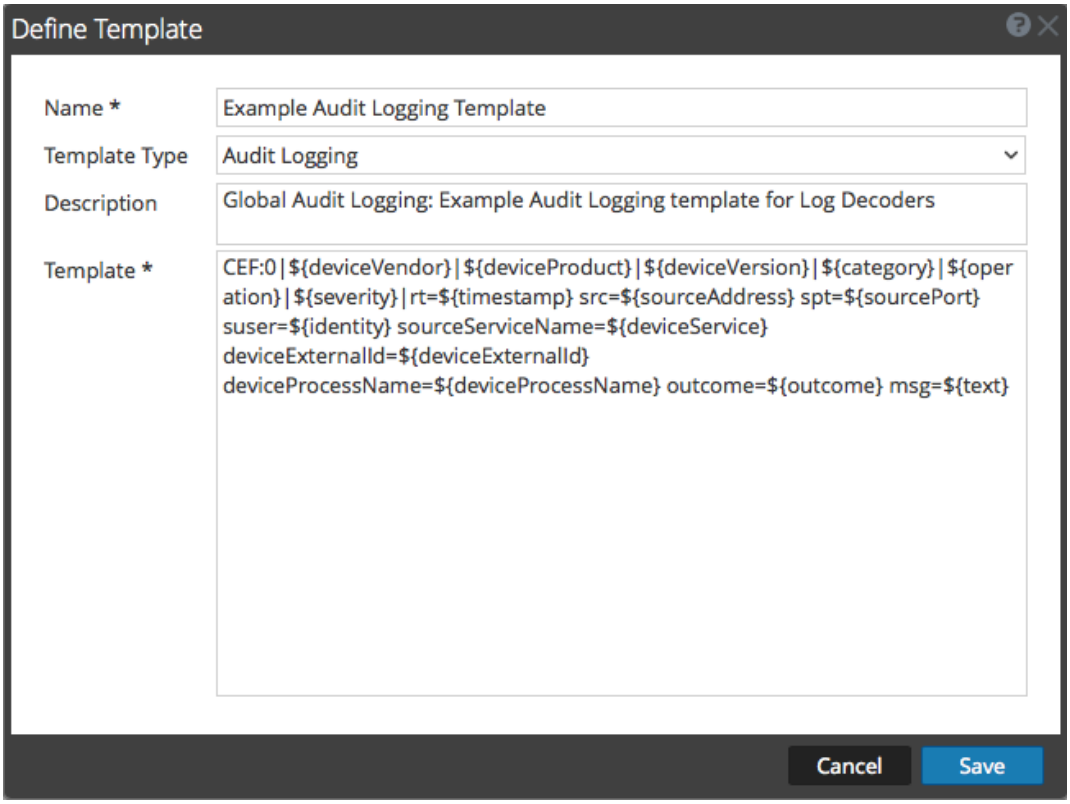
Beim Upgrade von NetWitness Suite 10.4 werden alle vorhandenen Vorlagen auf den Event Stream Analysis-Vorlagentyp migriert.

Hinzufügen einer Vorlage

Sie können die bereitgestellten Standardvorlagen verwenden oder eigene Vorlagen konfigurieren. So konfigurieren Sie Ihre eigene Vorlage:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Klicken Sie auf  , um eine Vorlage zu konfigurieren.
5. Geben Sie im Dialogfeld **Vorlage definieren** folgende Informationen ein:
   a. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
   b. Wählen Sie im Feld **Vorlagentyp** den Typ der Vorlage aus, die Sie erstellen möchten: Beispiel: Wenn Sie eine Vorlage für die globale Auditprotokollierung erstellen möchten, wählen Sie den Vorlagentyp Auditprotokollierung aus.
   c. Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung der Vorlage ein.
   d. Geben Sie im Feld **Vorlage** das Format für die Vorlage an.

e. Klicken Sie auf **Speichern**, um die Vorlage zu speichern.



Duplizieren einer Vorlage

Sie können eine vorhandene Standardvorlage oder eine benutzerdefinierte Vorlage kopieren. So duplizieren Sie eine Vorlage:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Wählen Sie die Vorlage, die Sie duplizieren möchten, und klicken Sie auf .

   Das Dialogfeld „Warnmeldungsvorlage duplizieren“ wird angezeigt.

5. Geben Sie den Namen der duplizierten Vorlage ein.
6. Klicken Sie auf **OK**.

Sie können eine Standardvorlage oder eine benutzerdefinierte Vorlage ändern. Wenn Sie eine Vorlage bearbeiten, werden die Änderungen erst sichtbar, wenn die Warnmeldung ausgelöst wird.

Bearbeiten von Vorlagen

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Wählen Sie eine Vorlage aus und klicken Sie auf  .
5. Ändern Sie im Dialogfeld **Vorlage definieren** nach Bedarf die Felder **Name**, **Vorlagentyp**, **Beschreibung** und **Vorlage**.
6. Klicken Sie auf **Speichern**, um die Vorlage zu speichern.

Löschen einer Vorlage

Sie können eine benutzerdefinierte Vorlage löschen. Wenn Sie eine Vorlage löschen, die in einer ESA-Regel verwendet wird, wird die Standardvorlage Event Stream Analysis für Warnmeldungen verwendet. Sie können keine Vorlagen löschen, die globalen Auditprotokollierungskonfigurationen zugeordnet sind.

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Wählen Sie eine oder mehrere Vorlagen aus und klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **Yes**.
   Die ausgewählte Vorlage wird gelöscht.

Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen

In diesem Thema wird beschrieben, wie Sie eine Vorlage für Warnmeldungsbenachrichtigungen festlegen können. Mit ESA (Event Stream Analysis) können Sie nützliche Vorlagen für Warnmeldungen erstellen. Um eine Vorlage erstellen zu können, sollten Sie mit FreeMarker und dem ESA-Datenmodell vertraut sein. Weitere Informationen zu FreeMarker können Sie dem Leitfaden zum Verfassen von Vorlagen in FreeMarker entnehmen.

ESA-Datenmodell

Nachstehend ist eine Regel für eine ESA-Warnmeldung aufgeführt:

```
@Name('module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert')
@Description('Brute Force Login To Same Destination')
@RSAAlert(oneInSeconds=0, identifiers={"ip_dst"})
SELECT* FROMEvent (ec_activity = 'Logon',ec_theme = 'Authentication',ec
outcome = 'Failure',ip_dst IS NOT NULL)
.std:groupwin(ip_dst)
.win:time_length_batch(60 seconds, 2)
GROUPBYip_dst HAVING COUNT(*) = 2;
```

Wenn eine Regel wie die oben stehende ausgelöst wird, besteht die erzeugte Warnmeldung aus zwei Ereigniskomponenten, die jeweils einer NextGen-Sitzung mit mehreren Metawerten ähneln. Das als Warnmeldung an den Freemarker-Vorlagenevaluator versandte Datenobjekt lautet wie folgt:

```
(root)
  |
  +- id = "4e67012f-9c53-4f0b-ac44-753e2c982b79"                    // Unique identifier for
each alert
  |
  +- severity = 1                                                    // The severity of the
alert
  +- time = 2013-12-31T11:02Z                                        // The alert time (needs a
?datetime for proper rendering)
  |  +- moduleType = "ootb"                                          // The module type
  |
  +- moduleName = "Brute Force Login To Same Destination"            // A description of the
module
  |
  +- statement = "module_144d43f5_f0b4_4cd0_8c6c_5ce65c37e624_Alert" // The name of the EPL
statement
  |  +- events                                                       // The constituent events -
as a sequence of event maps
       |   +- [0]                                                   // offset 0 (i.e. the first
constituent event)
       |   |       |   |
       |   +- event_cat_name = "User.Activity.Failed Logins"
       |   +- device_class = "Firewall"                             // event meta (accessible
as ${events[0].device_class}$)
       |   |       |   +- event_source_id = "uttam:50002:1703395"   // Investigation URI to the
individual session (used by SA)
       |   |
       |   +- ...                                                   // Other meta
       |   |
       |   +- sessionid = 1703395                                   // NextGen sessionid
       |   |
       |   +- time = 1388487764                                     // event/session time at
NextGen source (as a long Unix timestamp)
       |   |
       |   +- user_dst = "user5"
       |
       +- [1]                                                       // offset 1 (i.e. the
second consituent event)
           |
           +- device_class = "Firewall"
           |
           +- event_cat_name = "User.Activity.Failed Logins"
           |
```

```
+- event_source_id = "uttam:50002:1703405"
|
+- ...
|
+- sessionid = 1703405
|
+- time = 1388487766
|
+- user_dst = "user5"
```

Das Datenmodell hält zwei Typen von Vorlagenvariablen bereit:

- **Warnmeldungsmetadaten:** Diese enthalten Details zur Warnmeldungsebene, darunter Anweisungsname, Modulname, Warnmeldungs-ID, Warnmeldungszeit, Schweregrad usw. In der FreeMarker-Terminologie sind dies Variablen der obersten Ebene, die der Warnmeldungsinstanz selbst zugeordnet sind und einfach über ihren Namen referenziert werden können, z. B. `${moduleName}`. Dem Metawert `time` kommt eine besondere Stellung zu, da er vom Typ `Date` ist mit einem Suffix `?datetime` versehen sein muss, um korrekt wiedergegeben zu werden.

- **Metadaten der beteiligten Ereignisse**: Dazu zählen die Sitzungs-Metafelder der einzelnen Ereignisse, die in die Warnmeldung eingehen. Eine Warnmeldung kann mehrere beteiligte Ereignisse enthalten, weshalb in ein und derselben Warnmeldung mehr als eine derartige Zuordnung vorhanden sein kann. Diese sind für den FreeMarker-Vorlagenevaluator als Abfolge von Hashes erkennbar und müssen referenziert werden. Beispielsweise enthält die Warnmeldung zwei beteiligte Ereignisse, von denen die event_source_id für das erste als `${events[0].event_source_id}` und die gleiche für das zweite Ereignis als ${events[1].event_source_id} verfügbar ist. Sie müssen außerdem darauf achten, welche Metadatenfelder mehrwertig sind, da diese als Sequenzen behandelt werden müssen, z. B. ist ${events[0].alias_host} nicht möglich, da es eine Sequenz darstellt.

Hinweis: Die in den beteiligten Ereignissen verfügbaren Metadaten für eine bestimmte Warnmeldung ergeben sich aus der EPL SELECT-Klausel. Beispiel: Warnmeldungen aus `SELECT sessionid, time FROM ...` haben nur zwei verfügbare Metadatenwerte (sessionid, time). Die beteiligten Ereignisse in `SELECT * FROM Event ...` enthalten alle Metadatenfelder aus dem Typ `Event` mit Werten **ungleich null**.

Wenn in Ihren Vorlagen Metaschlüssel verwendet werden, die nicht in allen ausgegebenen Warnmeldungen vorhanden sind, sollten Sie möglichst die von FreeMarker bereitgestellten Standardwerte verwenden.

Beispiel: Wenn eine Vorlage mit TextId=${id},ec_outcome=${ec_outcome} füreine Warnmeldung bewertet wird, die den Metadatenschlüssel `ec_outcome` nicht enthält, schlägt die Vorlagenbewertung fehl. Verwenden Sie in solchen Fällen den Platzhalter für fehlende Werte `${ec_outcome!"default"}`.

Importieren und Exportieren einer Vorlage für globale Benachrichtigungen

Dieses Thema enthält Anweisungen zum Importieren und Exportieren einer Vorlage für Benachrichtigungen.

- Sie können standardmäßige oder benutzerdefinierte Vorlagen exportieren.
- Sie können eine Vorlage importieren, die von einer NetWitness Suite-Instanz exportiert wurde. Wenn Sie eine Vorlage mit demselben Namen wie eine vorhandene Vorlage importieren, dann wird die vorhandene Vorlage überschrieben.

Importieren von Vorlagen

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Wählen Sie in der Symbolleiste die Optionen > **Importieren** aus.
   Das Dialogfeld **Importieren** wird angezeigt.
5. Geben Sie im Feld **Dateiname:** den Dateinamen ein, oder klicken Sie auf **Durchsuchen** und wählen Sie die zu importierende Datei aus.
6. Klicken Sie auf **Import**.

Exportieren einer Vorlage

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Wählen Sie die Vorlage aus, die Sie exportieren möchten.

   Hinweis: Über die Optionen > **Alle exportieren** können Sie alle Vorlagen exportieren.

5. Wählen Sie in der Spalte **Aktionen** die Option > **Exportieren** aus.
   Das Dialogfeld **Exportieren** wird angezeigt.

6. Geben Sie im Feld **Dateiname eingeben** den Dateinamen ein.
7. Klicken Sie auf **Speichern**.

Konfigurieren von E-Mail-Servern und Benachrichtigungskonten

Dieses Thema enthält Anweisungen zum Konfigurieren von E-Mail, damit Benutzer Benachrichtigungen in NetWitness Suite erhalten können. RSA NetWitness® Suite kann Benachrichtigungen über verschiedene Systemereignisse per E-Mail an Benutzer senden. Damit diese E-Mail-Benachrichtigungen konfiguriert werden können, müssen Sie zuerst den SMTP-E-Mailserver konfigurieren. Der Bereich „E-Mail-Konfiguration“ bietet eine Möglichkeit zur:

- Konfiguration des E-Mailservers.
- Richten Sie ein E-Mail-Konto für den Erhalt von Benachrichtigungen ein.
- Anzeige von Statistiken zu E-Mail-Vorgängen.

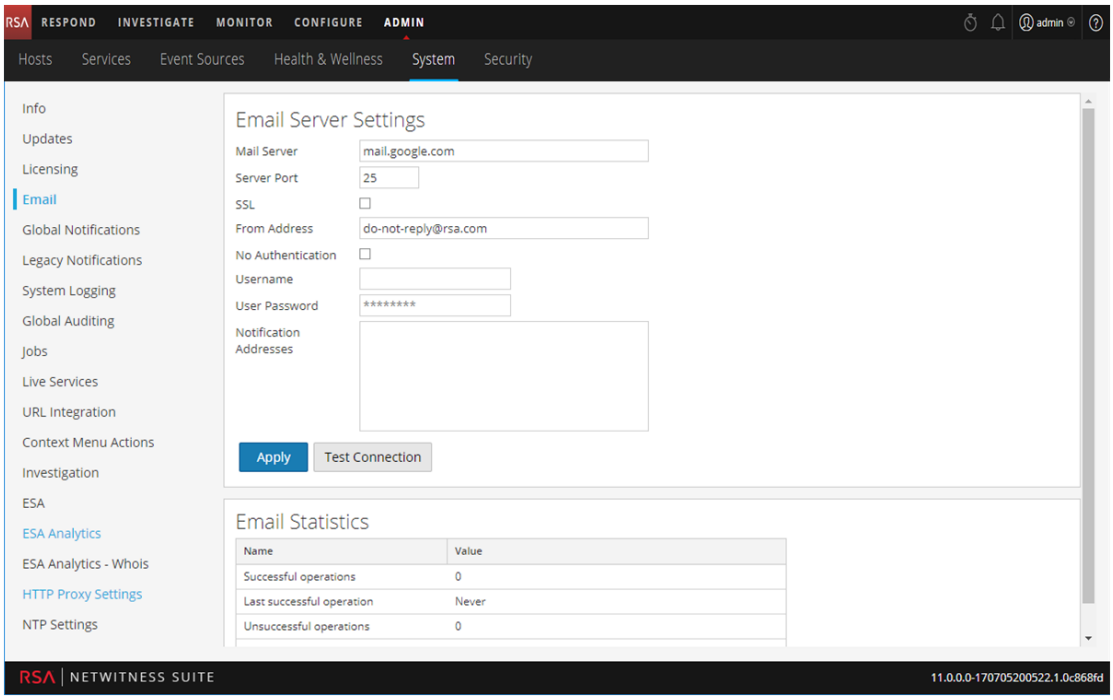
NetWitness Suite benötigt Zugriff auf einen SMTP-E-Mailserver, um Berichte an Benutzer senden zu können. Jedes Benutzerkonto kann für den Empfang von Berichten per E-Mail konfiguriert werden. Diese Berichte können manuell über die Benutzeroberfläche oder automatisch über das Auditsystem erzeugt werden. Es gelten die folgenden Richtlinien:

- Zum Senden von E-Mail-Nachrichten kann ein beliebiger SMTP-E-Mail-Host verwendet werden, wobei jeder Host eine andere Konfiguration erfordert. Der SMTP-Provider stellt die Einstellungen für die Konfiguration bereit.
- Einige SMTP-Server erfordern eine Benutzerauthentifizierung, um E-Mail-Nachrichten erfolgreich übermitteln zu können. Normalerweise ist dies der Benutzername und das Passwort für das E-Mail-Konto.
- Als Best Practice sollte für NetWitness Suite-Berichte ein neues, dediziertes E-Mail-Konto auf dem SMTP-E-Mailserver erstellt werden.

So konfigurieren Sie E-Mail-Benachrichtigungen für NetWitness Suite:

1. Navigieren Sie zu **ADMIN > System**.
   Die Ansicht Administration > System wird angezeigt.

2. Wählen Sie im Bereich „Optionen“ die Option **E-Mail** aus.



3. Wenn Sie den Standard-E-Mailserver ändern möchten, geben Sie den Namen des **E-Mailservers** und den **Serverport** an.
4. Wenn der E-Mailserver über SSL mit NetWitness Suite kommuniziert, aktivieren Sie das Kontrollkästchen neben **SSL verwenden**.
5. Geben Sie im Feld **Absenderadresse** den Namen des E-Mail-Kontos ein, über das die NetWitness Suite-E-Mail-Benachrichtigungen gesendet werden.
6. Wenn der SMTP-Server zur erfolgreichen Übermittlung von E-Mail-Benachrichtigungen eine Benutzerauthentifizierung benötigt, geben Sie den **Benutzernamen** und das **Benutzerpasswort** zur Anmeldung beim E-Mail-Konto an.
7. Klicken Sie zum Übernehmen der Einstellungen auf **Anwenden**.
   Sie können nun die NetWitness Suite-Module für den Empfang verschiedener Benachrichtigungen per E-Mail konfigurieren.

Konfigurieren der globalen Auditprotokollierung

Globale Auditprotokollierung bietet NetWitness Suite-Prüfern konsolidierte Einsichten in Benutzeraktivitäten innerhalb von NetWitness Suite in Echtzeit an zentraler Stelle. Diese Einsichten umfassen vom NetWitness Suite-System erfasste Auditprotokolle und die verschiedenen Services in der gesamten NetWitness Suite-Infrastruktur.

NetWitness Suite-Auditprotokolle werden in einem zentralen System gesammelt, das sie in das erforderliche Format konvertiert und an ein externes Syslog-System weiterleitet. Bei dem externen Syslog-System kann es sich um einen Syslog-Server eines Drittanbieters oder einen Log Decoder handeln.

Sie konfigurieren die globale Auditprotokollierung im Bereich „Globale Auditprotokollierungskonfigurationen“. Eine Auditprotokollierungsvorlage definiert das Format und die Meldungsfelder der Auditprotokolleinträge. Die Konfiguration des Syslog-Benachrichtigungsservers definiert das Ziel, an das die Auditprotokolle gesendet werden. Wenn Sie Auditprotokolle an einen Log Decoder weiterleiten möchten, konfigurieren Sie einen Syslog-Benachrichtigungsservertyp für den Log Decoder.

Nachfolgend sind einige Benutzeraktionen aufgeführt, die von NetWitness Suite protokolliert werden:

- Erfolgreiche Benutzeranmeldung
- User login failure
- Benutzerabmeldungen
- Maximale Anzahl fehlgeschlagener Anmeldeversuche überschritten
- Alle aufgerufenen Seiten der Benutzeroberfläche
- Gespeicherte Konfigurationsänderungen (einschließlich Änderung des eigenen Benutzerpassworts)
- Vom Benutzer durchgeführte Abfragen
- Verweigerte Benutzerzugriffe
- Datenexportvorgänge

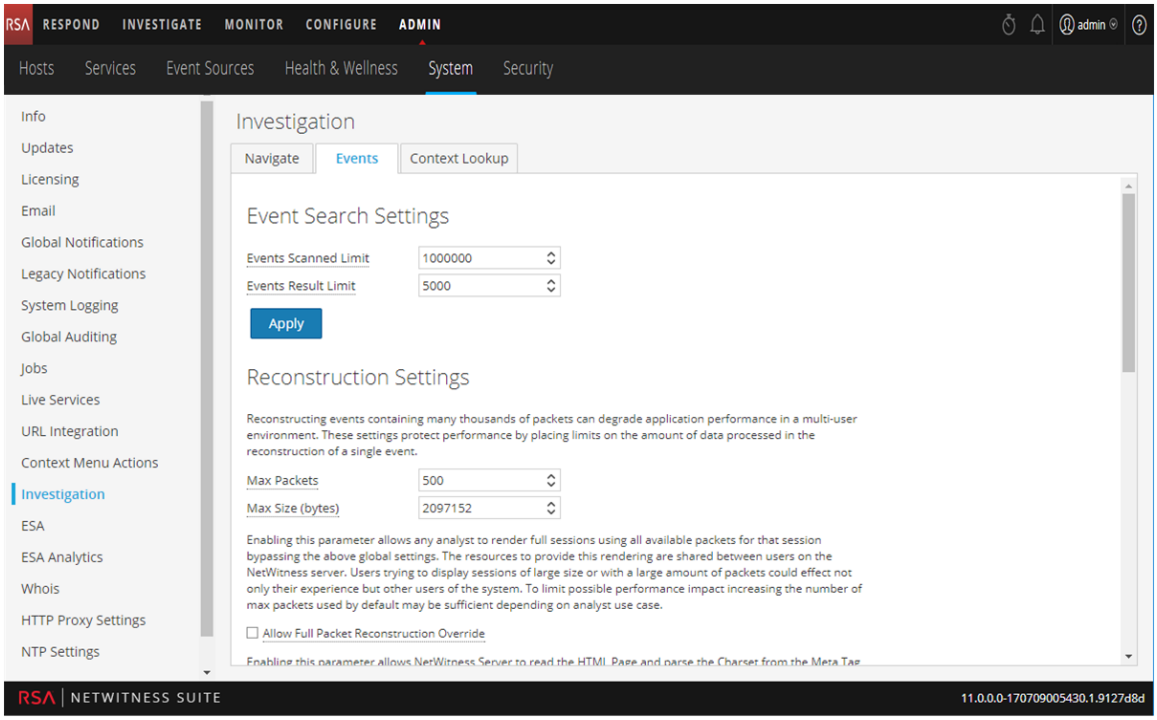
Nachdem Sie eine globale Auditprotokollierungskonfiguration erstellt haben, gehen Auditprotokolle, die diese Benutzeraktionen enthalten, automatisch in das externe Syslog-System ein. Dabei wird das Format verwendet, das in der ausgewählten Auditprotokollierungsvorlage angegeben wurde. Sie können mehrere globale Auditprotokollierungskonfigurationen für verschiedene Ziele erstellen, die verschiedene Vorlagen verwenden. So können Sie zum Beispiel eine globale Auditprotokollierungskonfiguration für einen externen Syslog-Server erstellen, mit einer Vorlage, die alle verfügbaren Metaschlüssel enthält, und eine andere Konfiguration für einen Log Decoder mit einer Vorlage, die ausgewählte Metaschlüssel enthält.

Für Log Decoder verwenden Sie die Audit-CEF-Standardvorlage. Sie können Felder zu der CEF (Common Event Format)-Vorlage hinzufügen oder aus ihr entfernen, wenn Sie spezielle Anforderungen haben. Entsprechende Anweisungen finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. Die verfügbaren Variablen werden im Abschnitt Unterstützte CEF-Metaschlüssel beschrieben.

Für Syslog-Server von Drittanbietern können Sie eine Standard-Auditprotokollierungsvorlage verwenden oder Ihr eigenes Format (CEF oder nicht CEF) definieren. Entsprechende Anweisungen finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. Die verfügbaren Variablen werden im Abschnitt Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung beschrieben.

Prüfer können die Auditprotokolle auf dem ausgewählten Log Decoder oder einem Syslog-Server eines Drittanbieters anzeigen. Wenn sie einen Log Decoder verwenden, können Prüfer die Auditprotokolle mithilfe von NetWitness Suite Investigation oder Reporting anzeigen.

Die folgende Abbildung zeigt globale Auditprotokolle in Investigation (Investigation > Ereignisse).



Beispiele einiger der protokollierten Benutzeraktionen finden Sie in Dialogfeld „Neue Konfiguration hinzufügen“. Eine Liste der Meldungstypen, die von den verschiedenen Komponenten von NetWitness Suite protokolliert werden, finden Sie in der Referenz der globalen Auditprotokollierungsvorgänge.

Globale Auditprotokollierung – übergeordnetes Verfahren

Die globale Auditprotokollierung wird im Bereich „Globale Auditprotokollierungskonfigurationen“ konfiguriert, der über Ansicht „Administration-System“ > Globales Auditing aufgerufen wird. Vor dem Konfigurieren der globalen Auditprotokollierung müssen ein Syslog-Benachrichtigungsserver und eine Auditprotokollierungsvorlage konfiguriert werden. Ein Syslog-Benachrichtigungsserver definiert das Ziel, an das die Auditprotokolle gesendet werden. Eine Auditprotokollierungsvorlage definiert das Format und die Meldungsfelder des Auditprotokolleintrags.

Im Bereich „Globale Auditprotokollierungskonfigurationen“ befindet sich der Link **Einstellungen anzeigen**, über den Sie zum Bereich „Globale Benachrichtigungen“ gelangen (Ansicht „Administrationssystem > Globale Benachrichtigungen“). Dort können Sie den Syslog-Benachrichtigungsserver und die Auditprotokollierungsvorlage konfigurieren.

Führen Sie zum Konfigurieren der globalen Auditprotokollierung die folgenden Verfahren in der angegebenen Reihenfolge aus.

Methoden	Referenz/Anweisungen
1. Konfigurieren Sie einen Syslog-Benachrichtigungsserver.	Konfigurieren Sie einen Syslog-Benachrichtigungsserver für die globale Auditprotokollierung. Sie können einen Drittanbieter-Syslog-Server oder einen Log Decoder als Ziel für die Auditprotokolle definieren. Konfigurieren eines Ziels zum Empfang globaler Auditprotokolle. Globale Auditprotokollierungskonfigurationen erfordern den Servertyp Syslog-Benachrichtigungsserver. Wenn Sie globale Auditprotokolle an einen Log Decoder weiterleiten möchten, erstellen Sie einen Benachrichtigungsserver vom Syslog-Typ.

Methoden	Referenz/Anweisungen
2. Wählen Sie die zu verwendende Auditprotokollierungsvorlage aus oder konfigurieren Sie eine neue.	Wählen Sie eine Auditprotokollierungsvorlage für den Syslog-Benachrichtigungsserver aus. Sie können eine Standard-Auditprotokollierungsvorlage verwenden oder eine eigene Vorlage definieren. Globale Auditprotokollierungskonfigurationen erfordern den Vorlagentyp „Auditprotokollierung“ und den Servertyp „Syslog-Benachrichtigungsserver“. Weitere Informationen hierzu finden Sie unter Konfigurieren von Vorlagen für Benachrichtigungen. Für Log Decoder verwenden Sie die **Audit-CEF-Standardvorlage**. Wenn bestimmte Anforderungen vorliegen, können Sie Felder zur CEF-Vorlage (Common Event Format) hinzufügen oder aus ihr entfernen. Im Abschnitt „Definieren einer Vorlage für globale Auditprotokollierung“ finden Sie weitere Erläuterungen. Für Syslog-Server von Drittanbietern können Sie eine Standard-Auditprotokollierungsvorlage verwenden oder Ihr eigenes Format (CEF oder nicht CEF) definieren. Entsprechende Anweisungen finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. Die verfügbaren Variablen werden im Abschnitt „Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung“ beschrieben.

Methoden	Referenz/Anweisungen
3. (Optional – nur bei Verwendung eines Log Decoder) Implementieren Sie von Live aus den Common Event Format-Parser in Ihrem Log Decoder.	Vergewissern Sie sich, dass Sie den neuesten Common Event Format-Parser von Live implementiert und aktiviert haben. Anweisungen hierzu finden Sie unter Suchen und Bereitstellen von Live-Ressourcen und Aktivieren und Deaktivieren von Protokollparsern.
4. Definieren Sie eine globale Auditprotokollierungskonfiguration, in der festgelegt ist, wie die globalen Auditprotokolle an externe Syslog-Systeme weitergeleitet werden.	Anweisungen hierzu enthält der Abschnitt Definieren einer globalen Auditprotokollierungskonfiguration. Nachdem Sie eine globale Auditprotokollierungskonfiguration hinzugefügt haben, werden Auditprotokolle an den in der Konfiguration angegebenen Benachrichtigungsserver weitergeleitet.
5. Vergewissern Sie sich, dass die Auditereignisse in den globalen Auditprotokollen angezeigt werden.	Testen Sie Ihre Auditprotokolle, um sicherzustellen, dass darin alle Auditereignisse aufgeführt werden, die in Ihrer Auditprotokollierungsvorlage definiert sind. Entsprechende Anweisungen finden Sie unter Überprüfen von globalen Auditprotokollen.

Konfigurieren eines Ziels zum Empfang globaler Auditprotokolle

In der globalen Auditprotokollierung sind Syslog-Benachrichtigungsserver die Konfigurationen, die definieren, welche Ziele globale Auditprotokolle empfangen sollen. Sie müssen einen Syslog-Benachrichtigungsserver konfigurieren, um globale Auditprotokollierung zu verwenden. Sie können einen Drittanbieter-Syslog-Server oder einen Log Decoder als Ziel für die Auditprotokolle definieren.

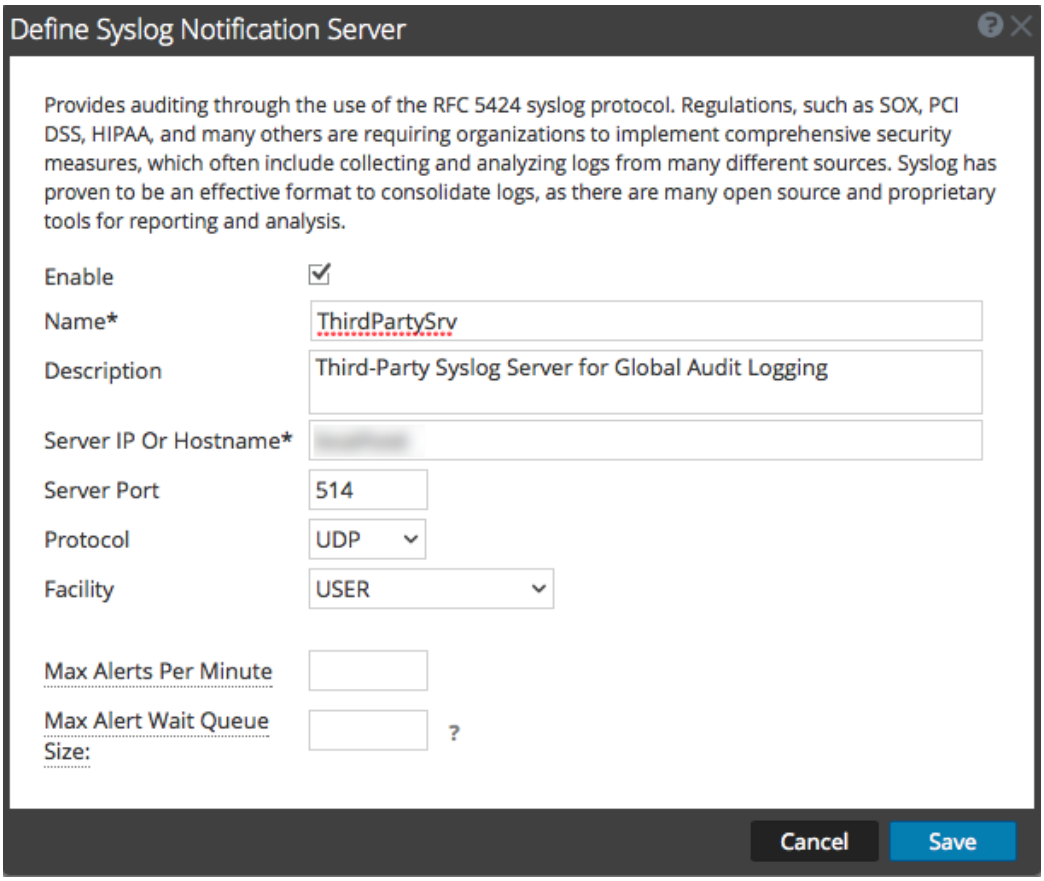
Konfigurieren eines Syslog-Benachrichtigungsservers für einen Drittanbieter-Syslog-Server

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Server**.

Hinweis: Die Registerkarte „Ausgabe“ für die globale Auditprotokollierung muss nicht konfiguriert werden.

4. Wählen Sie im Drop-down-Menü + die Option **Syslog** aus.

   Das Dialogfeld **Syslog-Benachrichtigungsserver definieren** wird angezeigt.



5. Konfigurieren Sie den Syslog-Benachrichtigungsserver wie in der folgenden Tabelle beschrieben.

Feld	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Drittanbieter-Benachrichtigungsservers
Beschreibung	(Optional) Eine kurze Beschreibung des Benachrichtigungsservers

Feld	Beschreibung
IP-Adresse oder Hostname des Servers	Der Hostname oder die IP-Adresse des Drittanbieter-Syslog-Servers
Serverport	Die Nummer des Ports, den der Ziel-Syslog-Prozess überwacht
Protokoll	Das Protokoll, das zur Übertragung formatierter Auditprotokolle an den Drittanbieter-Syslog-Server verwendet wird
Facility	Die Syslog-Facility, die verwendet wird, wenn formatierte Auditprotokolle auf den Drittanbieter-Syslog-Server geschrieben werden

Die Felder **Max. Warnmeldungen pro Minute** und **Max. Größe von Warnmeldungen in der Warteschlange** werden für die globale Auditprotokollierung nicht verwendet.

6. Klicken Sie auf **Speichern**.

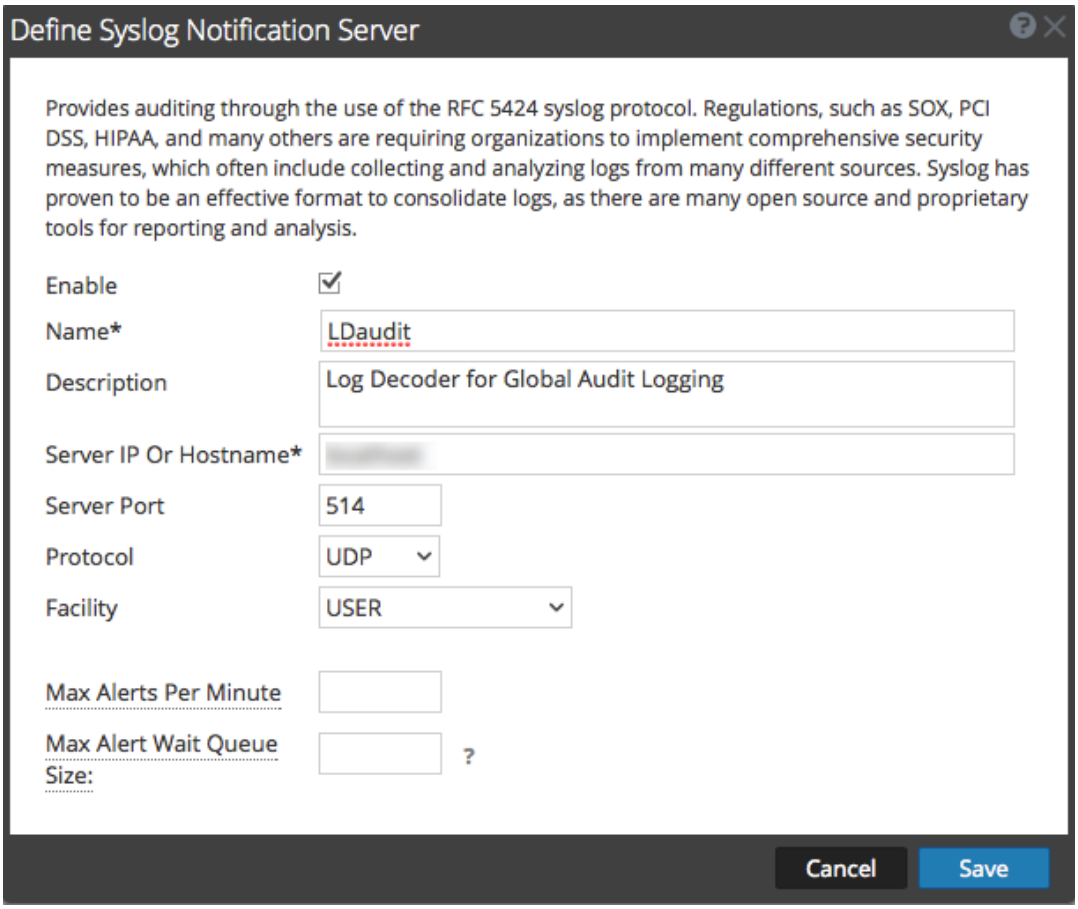
Konfigurieren eines Syslog-Benachrichtigungsservers für einen Log Decoder

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Server**.

   Hinweis: Die Registerkarte „Ausgabe“ für die globale Auditprotokollierung muss nicht konfiguriert werden.

4. Wählen Sie im Drop-down-Menü  die Option **Syslog** aus.

   Das Dialogfeld **Syslog-Benachrichtigungsserver definieren** wird angezeigt.



5. Konfigurieren Sie den Syslog-Benachrichtigungsserver wie in der folgenden Tabelle beschrieben.

Feld	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Log Decoder-Syslog-Benachrichtigungsservers
Beschreibung	(Optional) Eine kurze Beschreibung des Benachrichtigungsservers
IP-Adresse oder Hostname des Servers	Der Hostname oder die IP-Adresse des Log Decoder
Serverport	Die Nummer des Ports, den der Ziel-Syslog-Prozess überwacht

Feld	Beschreibung
Protokoll	Das Protokoll, das zur Übertragung formatierter Auditprotokolle an den Log Decoder verwendet wird
Facility	Die Syslog-Facility, die verwendet wird, wenn formatierte Auditprotokolle auf den Log Decoder geschrieben werden

Die Felder **Max. Warnmeldungen pro Minute** und **Max. Größe von Warnmeldungen in der Warteschlange** werden für die globale Auditprotokollierung nicht verwendet.

6. Klicken Sie auf **Speichern**.

Nächste Schritte

Wählen Sie eine standardmäßige Auditprotokollierungsvorlage für die Verwendung bei der globalen Auditprotokollierung aus. Sofern erforderlich, können Sie eine angepasste Vorlage definieren. Weitere Informationen erhalten Sie unter Definieren einer Vorlage für die globale Auditprotokollierung.

Definieren einer Vorlage für die globale Auditprotokollierung

Dieses Thema enthält Informationen zum Definieren einer Auditprotokollierungsvorlage für die globale Auditprotokollierung. Konfigurieren Sie vor der Konfiguration der globalen Auditprotokollierung zunächst einen Syslog-Benachrichtigungsserver und wählen Sie eine Auditprotokollierungsvorlage aus. Sie können eine standardmäßige Auditprotokollierungsvorlage auswählen oder Ihre eigene Vorlage definieren.

NetWitness Suite enthält zwei standardmäßige Auditprotokollierungsvorlagen:

- **Audit-CEF-Standardvorlage**: Sie können diese Vorlage für Log Decoders und Syslog-Server von Drittanbietern verwenden.
- **Audit-Standardvorlage Menschenlesbares Format**: Sie können diese Vorlage nur für Syslog-Server von Drittanbietern verwenden. Leiten Sie Meldungen von dieser Vorlage nicht an einen Log Decoder weiter.

Das erste Verfahren enthält Anweisungen zum Definieren einer Auditprotokollierungsvorlage für einen Log Decoder. Die Auditprotokollierungsvorlage definiert das Format und die Meldungsfelder der Auditprotokolle, die an den Log Decoder oder Syslog-Server eines Drittanbieters gesendet werden.

Globale Auditprotokollierungsvorlagen, die Sie für einen Log Decoder definieren, verwenden CEF (Common Event Format) und müssen die folgenden spezifischen Standardanforderungen erfüllen:

- Die CEF-Header müssen in der Vorlage enthalten sein.
- Verwenden Sie nur die Erweiterungen (Schlüssel=Wert), die in der Tabelle Unterstützte CEF-Metaschlüssel aufgeführt sind.
- Vergewissern Sie sich, dass die Erweiterungen im Format `key=${string}<space>key=${string}` sind.

Das zweite Verfahren bietet Anweisungen zum Definieren einer benutzerdefinierten globalen Auditprotokollierungsvorlage im für Menschen lesbaren Format für einen Syslog-Server eines Drittanbieters. Für Syslog-Server von Drittanbietern können Sie Ihr eigenes Format (CEF oder Nicht-CEF) definieren.

Definieren einer globalen Auditprotokollierungsvorlage für einen Log Decoder

Sie können die **Audit-CEF-Standardvorlage** verwenden, um globale Auditprotokolle an einen Log Decoder zu senden. So definieren Sie eigene Vorlagen:

1. Navigieren Sie zu **ADMINISTRATION > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Klicken Sie auf +, um eine Vorlage zu konfigurieren.
5. Geben Sie im Dialogfeld **Vorlage definieren** folgende Informationen ein:
   a. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
   b. Wählen Sie im Feld **Vorlagentyp** den Vorlagentyp **Auditprotokollierung** aus.
   c. Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung der Vorlage ein.
   d. Geben Sie im Feld **Vorlage** das Format für die Auditprotokollierungsvorlage an.
   Das folgende Format ist ein Beispiel für eine benutzerdefinierte Vorlage. Es unterscheidet sich von der Standard-CEF-Vorlage.

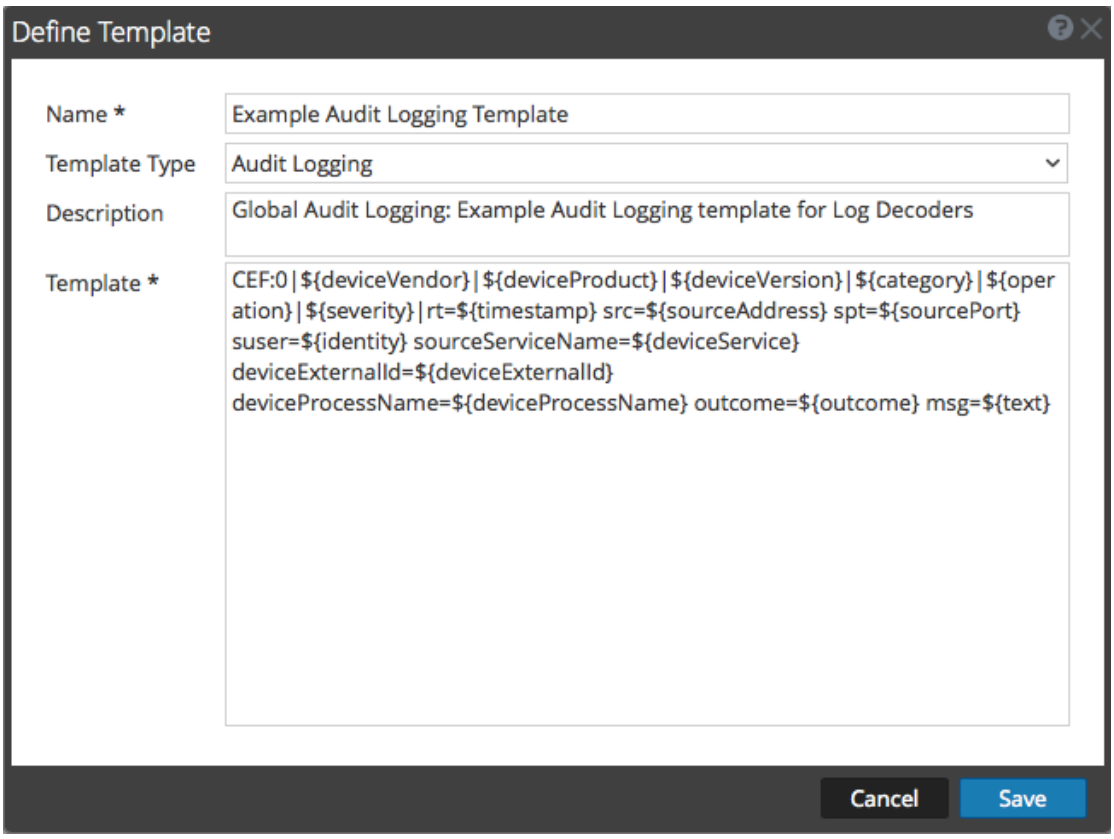
```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome}
msg=${text}
```

Der hervorgehobene CEF-Syslog-Header dient der Erfüllung der Anforderungen des

CEF-Standards und ist für den CEF-Parser im Log Decoder erforderlich. Die anderen Schlüssel sind optional und können konfiguriert werden. Alle unterstützten Metaschlüssel, die vom CEF-Parser im Log Decoder unterstützt werden, sind in der Tabelle Unterstützte CEF-Metaschlüssel aufgeführt.

> **Hinweis:** Verwenden Sie alle Erweiterungen im folgenden Format:
> `deviceProcessName=${deviceProcessName} outcome=${outcome}`
> Fügen Sie ein `<space>` zwischen jedem key=${string}-Paar im Erweiterungsschlüssel-Abschnitt ein.

6. Klicken Sie auf **Speichern**.



Vergewissern Sie sich nach dem Definieren der CEF-Auditprotokollierungsvorlage, dass Sie den neuesten CEF-Parser (Common Event Format) von Live bereitgestellt und aktiviert haben. Anweisungen hierzu finden Sie unter „Suchen und Bereitstellen von Live-Ressourcen“ und „Aktivieren und Deaktivieren von Protokollparsern“.

Hinweis: Wenn Sie einen bestimmten Metaschlüssel für Investigation und Reporting benötigen, vergewissern Sie sich, dass die von Ihnen ausgewählten Metaschlüssel in der Datei **table-map.xml** auf dem Log Decoder indexiert sind. Wenn sie nicht indexiert sind, gehen Sie gemäß dem Thema „Pflege der Tabellenzuordnungsdateien“ im *Leitfaden zur Host- und Servicekonfiguration* vor, um die Tabellenzuordnungen zu aktualisieren. Stellen Sie sicher, dass die Metaschlüssel in der Datei **index-concentrator.xml** auf dem Concentrator ebenfalls indexiert sind. Unter dem Thema „Bearbeiten einer Serviceindexdatei im *Leitfaden zur Host- und Servicekonfiguration* finden Sie weitere Informationen.

Definieren einer benutzerdefinierten globalen Auditprotokollierungsvorlage

Für Drittanbieter-Syslog-Server können Sie Ihr eigenes Vorlagenformat definieren (CEF oder kein CEF). Sie können die **Audit-Standardvorlage Menschenlesbares Format** verwenden, um globale Auditprotokolle an einen Drittanbieter-Syslog-Server in einem Format zu senden, das leichter zu lesen ist als das CEF-Format. Wenn Sie Ihre eigene Vorlage in einem für Menschen lesbaren Format definieren möchten, gehen Sie folgendermaßen vor.

Für Log Decoder müssen Sie eine CEF-Vorlage mit einigen speziellen Anforderungen verwenden. Das Verfahren *Definieren einer Auditprotokollierungsvorlage für einen Log Decoder* oben enthält Anweisungen zur Erstellung einer Vorlage im CEF-Format.

So definieren Sie eine benutzerdefinierte globale Auditprotokollierungsvorlage im für Menschen lesbaren Format:

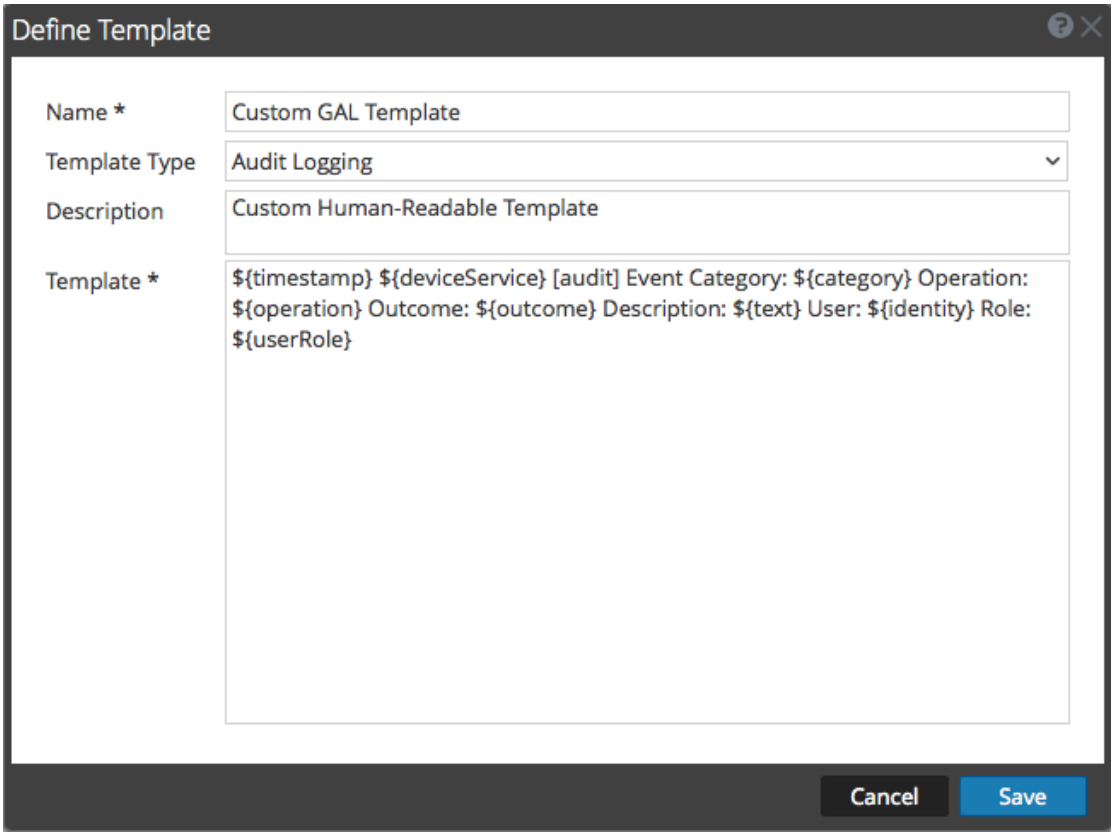
1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im linken Navigationsbereich **Benachrichtigungen** aus.
3. Klicken Sie auf die Registerkarte **Vorlagen**.
4. Klicken Sie auf  , um eine Vorlage zu konfigurieren.
5. Geben Sie im Dialogfeld **Vorlage definieren** folgende Informationen ein:
   a. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
   b. Wählen Sie im Feld **Vorlagentyp** den Vorlagentyp **Auditprotokollierung** aus.
   c. Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung der Vorlage ein.
   d. Geben Sie im Feld **Vorlage** das Format für die Auditprotokollierungsvorlage an. Das folgende Beispiel ist im für Menschen lesbaren Format mit ausgewählten Metaschlüsselvariablen dargestellt.

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
Operation: ${operation} Outcome: ${outcome} Description: ${text}
User: ${identity} Role: ${userRole}
```

Sie können alle Metaschlüsselvariablen verwenden, die von der globalen

Auditprotokollierung unterstützt werden. Diese sind in der Tabelle Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung aufgeführt.

6. Klicken Sie auf **Speichern**.



Das folgende Beispiel zeigt globale Auditprotokolle im für Menschen lesbaren Format zu dieser Vorlage an:

```
06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY

Apr 06 2015 14:16:04 NW_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

Nächster Schritt

Unter Definieren einer globalen Auditprotokollierungskonfiguration finden Sie Anweisungen zur Definition einer globalen Auditprotokollierungskonfiguration für NetWitness Suite.

Definieren einer globalen Auditprotokollierungskonfiguration

Dieses Thema enthält Anweisungen für Administratoren zum Definieren einer globalen Auditprotokollierungskonfiguration. Dieses Verfahren muss nur durchgeführt werden, wenn Sie in Ihrer Umgebung eine zentralisierte Auditprotokollierung einrichten möchten. In den globalen Auditprotokollierungskonfigurationen wird festgelegt, wie die globalen Auditprotokolle an externe Syslog-Systeme oder Log Decoder weitergeleitet werden. Die Auditprotokolle werden an die ausgewählten Benachrichtigungsserver gesendet.

Voraussetzungen

Bevor Sie beginnen, konfigurieren Sie zunächst die folgenden Komponenten für die Verwendung der globalen Auditprotokollierung:

- Syslog-Benachrichtigungsserver
- Auditprotokollierungsvorlage

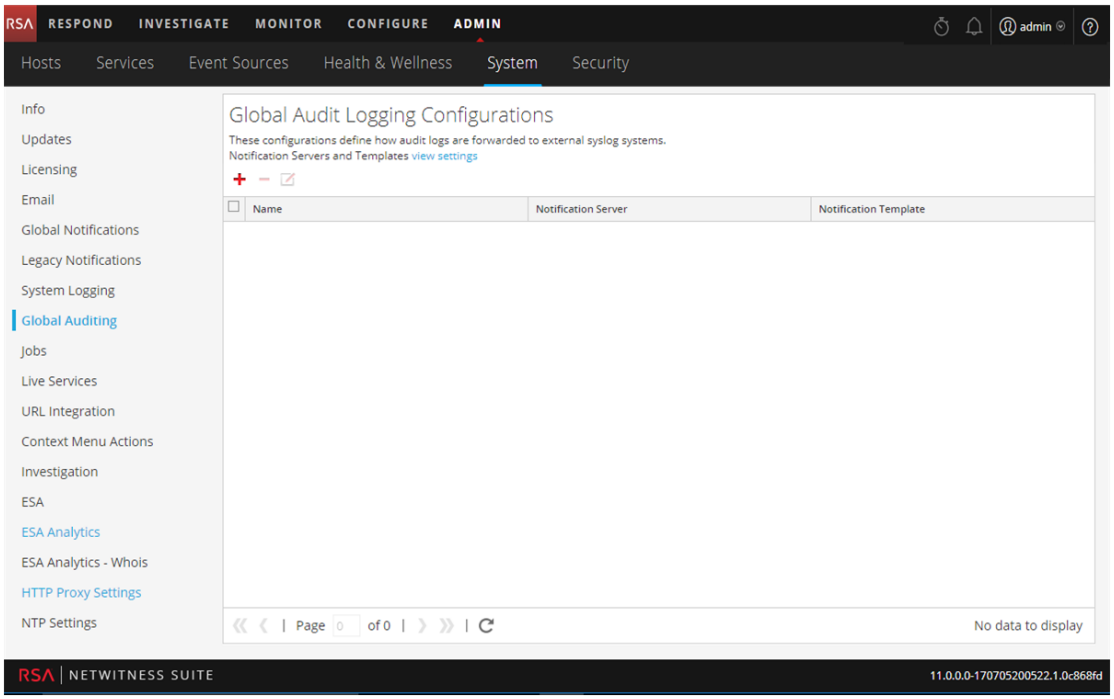
Die Konfiguration des Benachrichtigungsservers und der Vorlage erfolgt im Bereich „Globale Benachrichtigungen“. Den Bereich Globale Benachrichtigungen können Sie aufrufen, indem Sie im Bereich Globale Auditprotokollierungskonfigurationen auf den Link **Einstellungen anzeigen** klicken. Für die globale Auditprotokollierung können nur Benachrichtigungsserver des Typs Syslog definiert werden. Verwenden Sie für Log Decoders einen Benachrichtigungsserver des Typs Syslog sowie eine Auditprotokollierungsvorlage im Common Event Format (CEF). Sie können eine Standard-Auditprotokollierungsvorlage verwenden oder Ihre eigene Vorlage definieren. Es ist auch möglich, mehrere Auditprotokollierungsvorlagen und Syslog-Benachrichtigungsserver für Ihre globalen Auditprotokollierungskonfigurationen zu erstellen.

Wenn Ihre globalen Auditprotokolle an einen Log Decoder weitergeleitet werden, implementieren Sie von Live aus den Common Event Format-Parser in Ihrem Log Decoder.

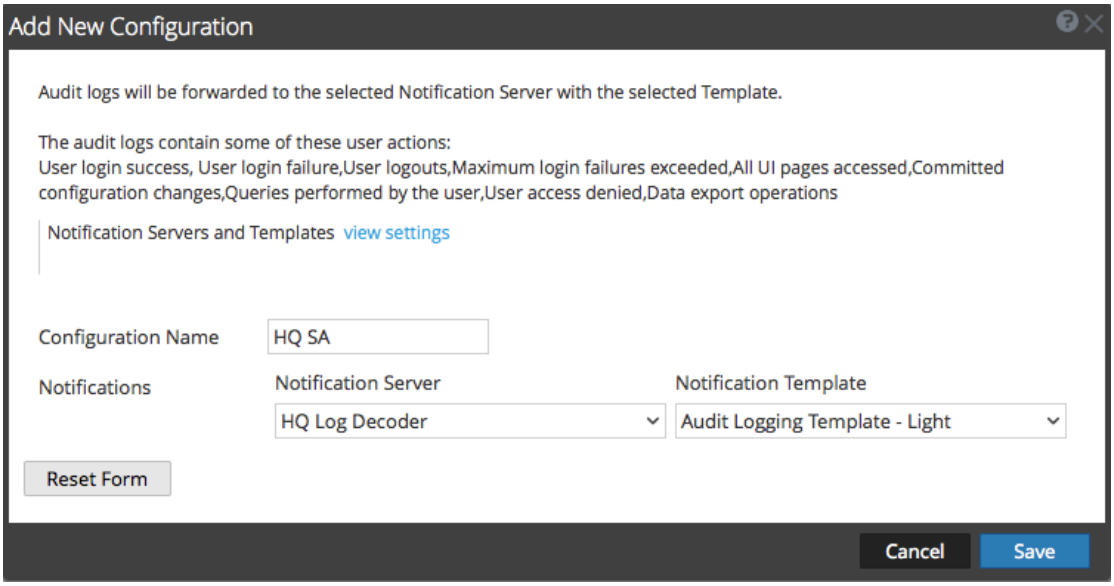
Hinzufügen einer globalen Auditprotokollierungskonfiguration

1. Navigieren Sie zu **ADMIN > System**.

2. Wählen Sie im Bereich „Optionen“ die Option **Globales Auditing** aus.
   Der Bereich **Globale Auditprotokollierungskonfigurationen** wird angezeigt.



3. Klicken Sie auf +, um eine globale Auditprotokollierungskonfiguration hinzuzufügen.
   Das Dialogfeld **Neue Konfiguration hinzufügen** wird angezeigt.



4. Geben Sie im Feld **Konfigurationsname** einen eindeutigen Namen für die globale Auditprotokollierungskonfiguration ein. Beispielsweise können Sie eine globale

Auditprotokollierungskonfiguration für einen bestimmten Zweck erstellen, wie etwa HQ NW für eine NetWitness Suite-Konfiguration für den Unternehmenshauptsitz.

5. Wählen Sie im Bereich **Benachrichtigungen** den Syslog-**Benachrichtigungsserver** aus, der in dieser Konfiguration verwendet werden soll. Der Benachrichtigungsserver ist das Ziel, an das die globalen Auditprotokolle gesendet werden.
6. Wählen Sie die **Benachrichtigungsvorlage** für die Auditprotokollierung aus, die in dieser Konfiguration verwendet werden soll. In der Auditprotokollierungsvorlage sind das Format und die Meldungsfelder des zu versendenden Auditprotokolls festgelegt.
7. Klicken Sie auf **Speichern**.

Im Abschnitt Dialogfeld "Neue Konfiguration hinzufügen" finden Sie weitere Informationen und Beispiele für die protokollierten Benutzeraktionen. Eine Liste der Meldungstypen, die von den verschiedenen Komponenten von NetWitness Suite protokolliert werden, finden Sie unter Bereich „Globale Auditprotokollierungskonfigurationen“.

Bearbeiten einer globalen Auditprotokollierungskonfiguration

Dieses Thema enthält Anweisungen zur Bearbeitung einer globalen Auditprotokollierungskonfiguration. Sie können eine globale Auditprotokollierungskonfiguration bearbeiten, um das Ziel der globalen Auditprotokolle für Ihre Benutzeraudits zu ändern, indem Sie einen anderen Benachrichtigungsserver auswählen. Sie können auch die Felder für Format und Meldung der globalen Auditprotokolleinträge ändern, indem Sie eine andere Benachrichtigungsvorlage auswählen. Änderungen am Benachrichtigungsserver oder an der Vorlage nehmen Sie im Bereich „Globale Benachrichtigungen“ vor. Den Bereich Globale Benachrichtigungen können Sie aufrufen, indem Sie im Bereich Globale Auditprotokollierungskonfigurationen auf den Link **Einstellungen anzeigen** klicken.

Sie können nicht ändern, welche NetWitness Suite-Benutzeraktionen protokolliert und in den globalen Auditprotokollen versendet werden.

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Globales Auditing** aus.
3. Wählen Sie im Bereich **Globale Auditprotokollierungskonfigurationen** eine zu bearbeitende Konfiguration aus und klicken Sie auf  .
4. Ändern Sie im Dialogfeld **Neue Konfiguration hinzufügen** die globale Auditprotokollierungskonfiguration wie erforderlich. Sie können den **Namen der Konfiguration** ändern und einen anderen **Benachrichtigungsserver** oder eine andere **Vorlage** auswählen.
5. Klicken Sie auf **Speichern**.

Löschen einer globalen Auditprotokollierungskonfiguration

Durch das Löschen einer globalen Auditprotokollierungskonfiguration werden die zugehörigen Benachrichtigungsserver- und Vorlagen nicht gelöscht. Nachdem Sie eine globale Auditprotokollierungskonfiguration gelöscht haben, wird die in dieser Konfiguration angegebene Weiterleitung der globalen Auditprotokolle eingestellt.

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Globales Auditing** aus.
3. Wählen Sie im Bereich **Globale Auditprotokollierungskonfigurationen** eine zu löschende Konfiguration aus und klicken Sie auf .

   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.

   Die ausgewählte Konfiguration wird gelöscht.

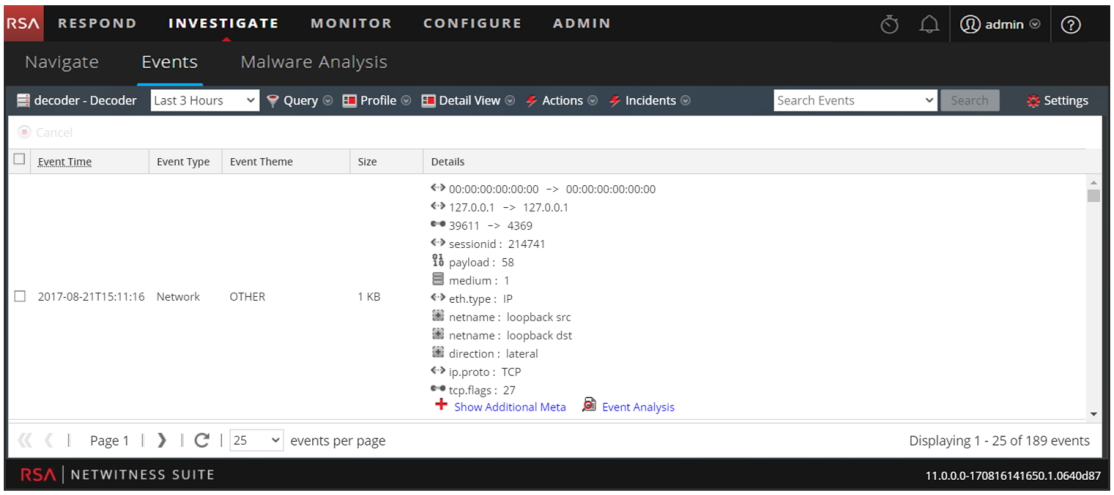
Überprüfen von globalen Auditprotokollen

Dieses Thema enthält Anleitungen zum Überprüfen von globalen Auditprotokollen. Nach dem Konfigurieren der globalen Auditprotokollierung sollten Sie Ihre globalen Auditprotokolle testen, um sich zu vergewissern, dass die Auditereignisse entsprechend der Definition in Ihrer globalen Auditprotokollierungsvorlage aufgeführt werden.

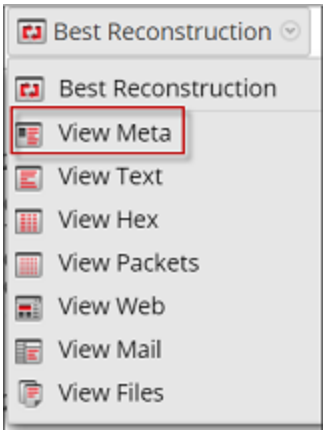
Bevor Sie mit dieser Aufgabe beginnen, führen Sie die unter Konfigurieren der globalen Auditprotokollierung beschriebenen Schritte aus.

So zeigen Sie die globalen Auditprotokolle an und überprüfen sie, wenn Sie einen Log Decoder verwenden:

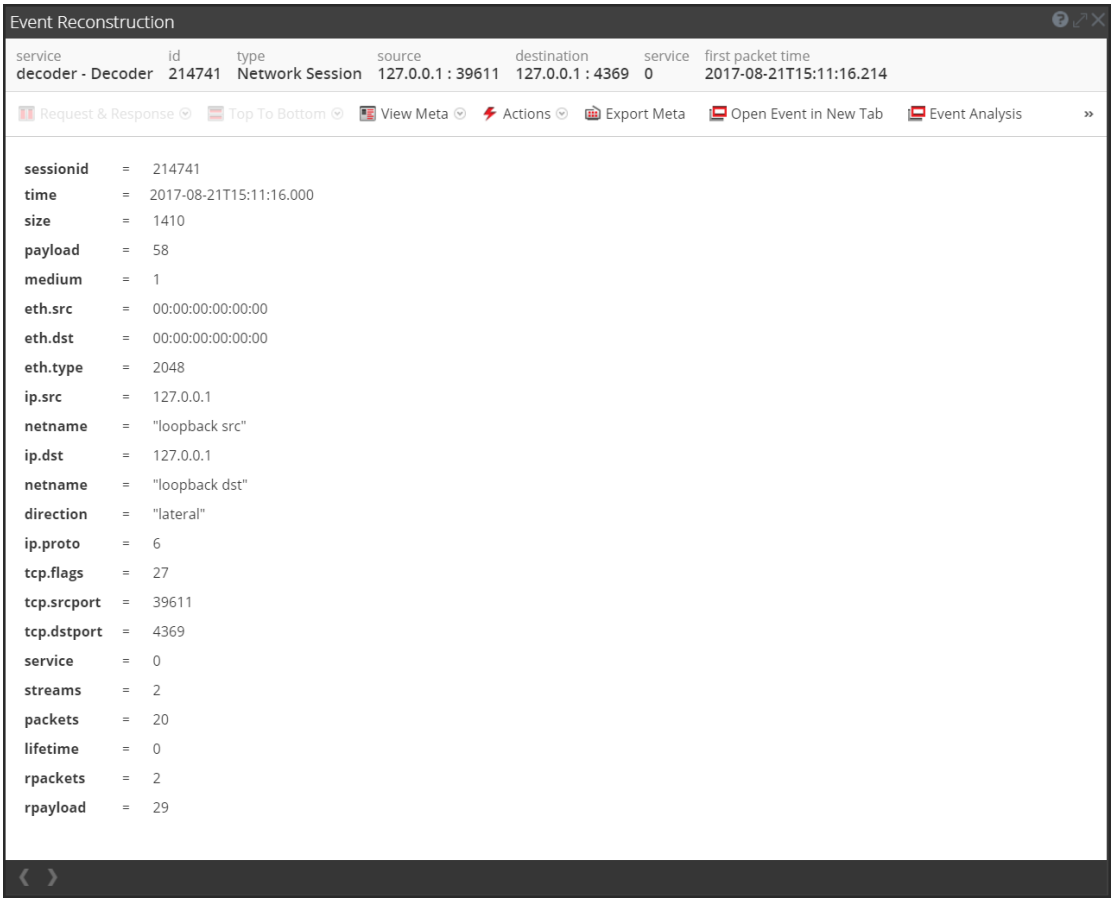
1. Navigieren Sie zu **Untersuchen > Ereignisse**.
2. Wählen Sie aus der Navigationsansicht heraus den Log Decoder aus und klicken Sie auf **Navigieren**.



3. Vergleichen Sie die Felder in den globalen Auditprotokollen mit den Feldern, die in der Vorlage für die globale Auditprotokollierung definiert wurden, die Sie in Ihrer globalen Auditprotokollierungskonfiguration verwendet haben.
4. Doppelklicken Sie auf ein Protokoll und wählen Sie im Dialogfeld „Ereignisrekonstruktion“ die Option **Metadaten anzeigen** aus.



5. Überprüfen Sie, ob die Metadaten, die Sie prüfen möchten, korrekt sind.



Beispiel für CEF-Ausgabe

Das folgende Beispiel zeigt globale Auditprotokolle für eine CEF (Common Event Format)-Vorlage für Auditprotokolle.

Vorlage:

```
CEF:0|${deviceVendor}|${deviceProduct}|${deviceVersion}|${category}|${oper
ation}|${severity}| rt=${timestamp} src=${sourceAddress}
spt=${sourcePort}
suser=${identity} sourceServiceName=${deviceService}
deviceExternalId=${deviceExternalId} dst=${destinationAddress}
dpt=${destinationPort} dvcpid=${deviceProcessId}
deviceProcessName=${deviceProcessName} outcome=${outcome} msg=${text}
```

Beispielprotokolle:

```
2017-04-09T18:45:46.313096+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|login|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=51366 suser=admin sourceServiceName=LOG_DECODER
deviceExternalId=96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
2017-04-09T18:45:46.322132+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.204.33 spt=47690 suser=admin sourceServiceName=BROKER
deviceExternalId= 314fb8c8-afe4-4249-9468-a36035008a52 outcome=success
2017-04-09T18:45:46.325792+00:00 <hostname> CEF:0|RSA|Security Analytics
Audit|11.0.0.0|AUTHENTICATION|logoff|6|rt=Apr 09 2017 18:45:46
src=10.20.252.197 spt=59495 suser=admin sourceServiceName=CONCENTRATOR
deviceExternalId= 96b08193-a9d0-4a79-b362-87b56851f411 outcome=success
```

Wobei `<hostname>` der Syslog-Header-Hostname (alias.host) ist.

Für CEF-Vorlagen gilt, wenn ein Auditereignis für ein Feld in einer Vorlage keinen Wert hat, dann wird das entsprechende Ereignis, das auf einem Syslog-Server oder Log Decoder eines Drittanbieters eingeht, dazu führen, dass das Feld entfernt wird.

Beispiel für Ausgabe in für Menschen lesbarem Format

Das folgende Beispiel zeigt globale Auditprotokolle für eine Auditprotokollvorlage in für Menschen lesbarem Format auf einem Drittanbieter-Syslog-Server an.

Vorlage:

```
${timestamp} ${deviceService} [audit] Event Category: ${category}
```

Operation: ${operation} Outcome: ${outcome} Description: ${text}

User: ${identity} Role: ${userRole}

Beispielprotokolle:

```
06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category: CONFIGURATION
Operation: Set Outcome: null Description: null User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY
```

```
Apr 06 2017 14:16:04 REPORTING_ENGINE [audit] Event Category:
CONFIGURATION Operation: IPDBConfig Outcome: SUCCESS Description: Config
update event occurred User: admin Role:
Administrators+Administrators+PRIVILEGED_CONNECTION_AUTHORITY
```

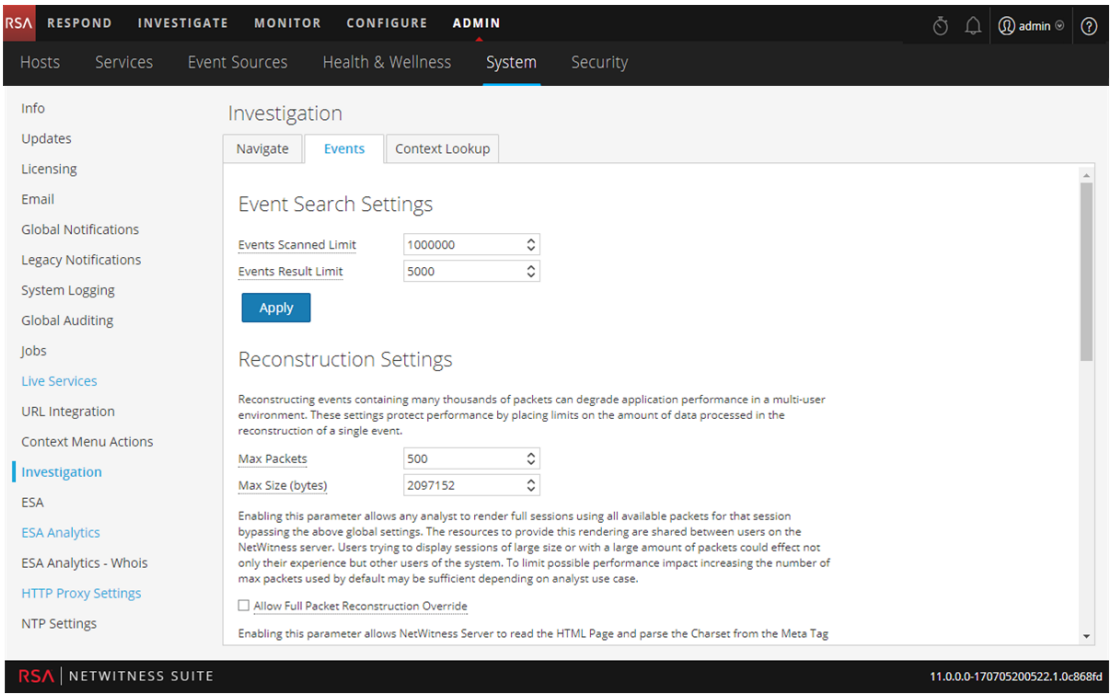
```
Apr 06 2017 14:16:04 SA_SERVER [audit] Event Category: DATA_ACCESS
Operation: /admin/1/config Outcome: Success Description: null User:
admin Role: Administrators+Administrators+PRIVILEGED_CONNECTION_
AUTHORITY
```

Konfigurieren von Ermittlungseinstellungen

Dieses Thema enthält Anweisungen für Administratoren, die die Einstellungen konfigurieren, die für alle Ermittlungen auf der konfigurierten NetWitness Suite-Instanz gelten. Die Einstellungen zum Konfigurieren und Optimieren des Verhaltens von NetWitness Suite Investigation werden in der Ansicht „System“ > Bereich „Investigation“ angezeigt. Diese Einstellungen gelten für alle Ermittlungen und Rekonstruktionen auf der aktuellen Instanz von NetWitness Suite.

Konfigurieren der Einstellungen für Navigation, Ereignisse und Kontextabfrage

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich Optionen die Option **Investigation** aus. Der Bereich „Investigation-Konfiguration“ wird angezeigt.



3. Wählen Sie auf der Registerkarte **Navigieren** im Feld **Render-Threadeinstellung** die maximale Anzahl von gleichzeitigen Metaschlüsselwerten aus, die von einem Benutzer in der Navigationsansicht geladen werden. Klicken Sie auf **Anwenden**.
4. Legen Sie auf der Registerkarte **Navigieren** im Abschnitt **Einstellungen zu Parallelkoordinaten** die maximalen Grenzwerte für gescannte Metawerte und Metawertergebnisse fest, die in einer Parallelkoordinatenvisualisierung enthalten sein können. Für eine bessere Performance werden folgende Einstellungen empfohlen: Scangrenzwert für Metawerte: 100.000 und Ergebnisgrenzwert für Metawerte: 1.000 bis 10.000

   Klicken Sie auf **Anwenden**.
5. Legen Sie auf der Registerkarte **Ereignisse** im Abschnitt **Sucheinstellungen für Ereignisse** die maximale Anzahl von gescannten Ereignissen und Ereignisergebnissen fest, die in der Ereignisansicht angezeigt werden, wenn ein Analyst eine Ereignissuche durchführt. Klicken Sie auf **Anwenden**.
6. Legen Sie auf der Registerkarte **Ereignisse** im Abschnitt **Rekonstruktionseinstellungen** die Grenzwerte für die Menge der in der Rekonstruktion eines einzelnen Ereignisses verarbeiteten Daten fest. Die Standardwerte sind maximal 100 Pakete und 2.097.152 Byte. Wenn Analysten bei der Rekonstruktion von Sitzungen in Investigation eine langsame Performance feststellen, müssen die Rekonstruktionseinstellungen möglicherweise angepasst werden. Klicken Sie auf **Anwenden**.

Achtung: Das Einstellen eines höheren Werts beeinträchtigt durch die längere Dauer und den erhöhten Arbeitsspeicherverbrauch zur Rekonstruktion eines Ereignisses die Performance des NetWitness-Server. Das Einstellen des Werts auf Null deaktiviert jede Begrenzung und kann möglicherweise zu einem Ausfall von NetWitness-Server führen.

7. (Optional) Aktivieren Sie auf der Registerkarte **Ereignisse** im Abschnitt **Einstellungen für Rekonstruktion der Webansicht** die Verwendung von Begleitdateien in einer Rekonstruktion der Webansicht und konfigurieren Sie die zusätzlichen Einstellungen zum Kalibrieren der Webansichtsrekonstruktionen. Hierzu gehört der Zeitraum (in Sekunden), in dem verknüpfte Ereignisse gescannt werden, die maximale Anzahl von zu scannenden verknüpften Ereignissen und Außerkraftsetzen der Rekonstruktionseinstellungen, die für Webansichtsrekonstruktionen verwendet werden. Klicken Sie auf **Anwenden**.
8. Verwalten Sie auf der Registerkarte **Kontextabfrage** die Zuordnung der Context Hub-Metadatentypen mit Metaschlüsseln in Investigation. Sie können Metaschlüssel zur Liste der in Investigation von Context Hub unterstützten Metadatentypen hinzufügen oder entfernen. Verfahren im Zusammenhang mit dieser Registerkarte finden Sie unter „Managen der Metadatentyp- und Metaschlüsselzuordnung“ im *Leitfaden Investigation und Malware Analysis*.

Löschen des Rekonstruktionscaches für Services

Unter Rekonstruktionscacheeinstellungen können Administratoren den Cache für einen oder mehrere Services löschen. Der Administrator kann z. B. den Cache für einen einzigen Broker, einen Broker und Decoder oder für alle verbundenen Services löschen. Im Folgenden finden Sie Beispiele dafür, warum in einer Rekonstruktion ein veralteter Cache verwendet wird.

- Die Sitzungen von Downstreamservices können ungültig gemacht worden sein oder die Daten von Downstreamservices wurden zurückgesetzt. Beispiel: Wenn Investigation einen Broker durchsucht und bei einem Downstream-Concentrator oder -Decoder die Daten zurückgesetzt wurden, stimmen die Meta- und Sitzungsdaten für den ermittelnden Service (Broker) nicht mit dem Inhalt überein, wenn der Downstreamservice zurückgesetzt und neu aufgefüllt wurde. Die Rekonstruktion in Investigation zeigt Inhalt aus dem Cache an, der nicht mit dem tatsächlichen Inhalt übereinstimmt. Sogar wenn der Decoder offline ist, wird der Inhalt weiterhin in der Broker-Rekonstruktion angezeigt. Das Löschen des Caches auf dem Broker führt zu einem Zugriffsversuch von NetWitness Suite auf den Decoder. Da der Decoder offline ist, wird ein Fehler zurückgegeben.
- Der Cache kann auch veraltet sein, wenn eine Service-ID für einen Downstreamservice geändert wird. Dies kann vorkommen, wenn Sie Services aus NetWitness Suite exportieren

oder Services importieren, löschen oder hinzufügen, da NetWitness Suite Service-IDs wiederverwenden kann. In dieser Situation führt das Löschen des Caches auf dem Broker dazu, dass NetWitness Suite Daten von den Services anfordert.

Führen Sie einen der folgenden Schritte aus, um den Rekonstruktionscache zu leeren:

1. Um den Cache für einen oder mehrere Services zu leeren, wählen Sie die Services aus und klicken Sie auf **Cache für ausgewählte Services leeren**.
2. Klicken Sie zum Leeren des Caches für alle aufgeführten Services auf **Cache für alle Services leeren**
   . Der Rekonstruktionscache für die ausgewählten Services wird gelöscht. NetWitness Suite sendet eine Datenanforderung an die Services.

Konfigurieren der Einstellungen von Live-Services

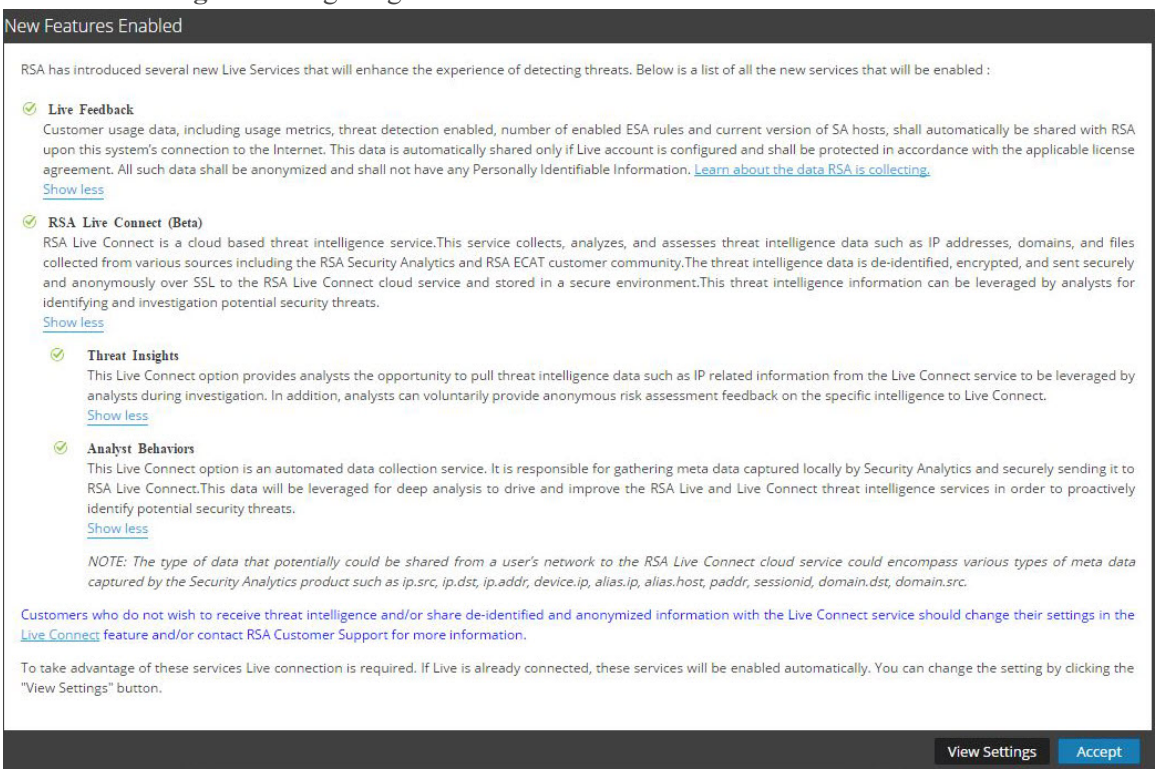
Die Optionen für die Konfiguration von Live-Services befinden sich in der Ansicht „System“ > Bereich „Konfiguration der Live-Services“. Im Bereich „Live-Konfiguration“ können Sie Folgendes konfigurieren:

- das Live-Konto
- die Planung für die Aktualisierung von Live-Inhalten und Einstellungen für die Benachrichtigung von Aktualisierungen
- Teilnahme an Live-Services Feedback.
- Freigabe von Live Content-Nutzung
- RSA Live Connect (Betaversion)

Voraussetzung

Bitte wenden Sie sich an den RSA Kundendienst, um Ihr Live-Konto für NetWitness Suite zu aktivieren. Wenn Sie eine Bestätigung erhalten, dass Ihr Live-Konto eingerichtet wurde, können Sie die CMS-Serververbindung konfigurieren und testen.

Wenn Sie sich zum ersten Mal bei NetWitness Suite anmelden, wird das Dialogfeld **Neue Funktionen eingeführt** angezeigt.



Durch Klicken auf **Akzeptieren** stimmen Sie automatisch Folgendem zu:

- Teilnahme an Live Feedback
- Verwenden von Connect-Funktionen, um Threat Intelligence-Daten zu erhalten.
- NetWitness Suite erlauben, anonyme, technische Daten zu Ihrer Umgebung an RSA zu senden.

Wenn Sie auf **Einstellungen anzeigen** klicken, werden Sie zur Live-Services-Benutzeroberfläche umgeleitet, um die Einstellungen für Live Feedback und Live Connect Threat Data Sharing anzuzeigen. Wenn Sie das Live-Konto nicht konfiguriert haben, wird ein maskierter Bildschirm angezeigt.

Weitere Informationen über Analystenverhalten und Datenfreigabe finden Sie im Thema **NetWitness-Feedback und Datenfreigabe** im *Handbuch Live Services Management*.

Informationen über die Teilnahme an Live Feedback

Wenn Sie an Live Feedback teilnehmen, werden relevante Informationen zur weiteren Verbesserung erfasst. Weitere Informationen über Live Feedback finden Sie unter Übersicht über Live Feedback.

Bei der Installation von NetWitness Suite werden Sie aufgefordert, an Live Feedback teilzunehmen. Informationen finden Sie unter Konfigurieren der Einstellungen von Live-Services.

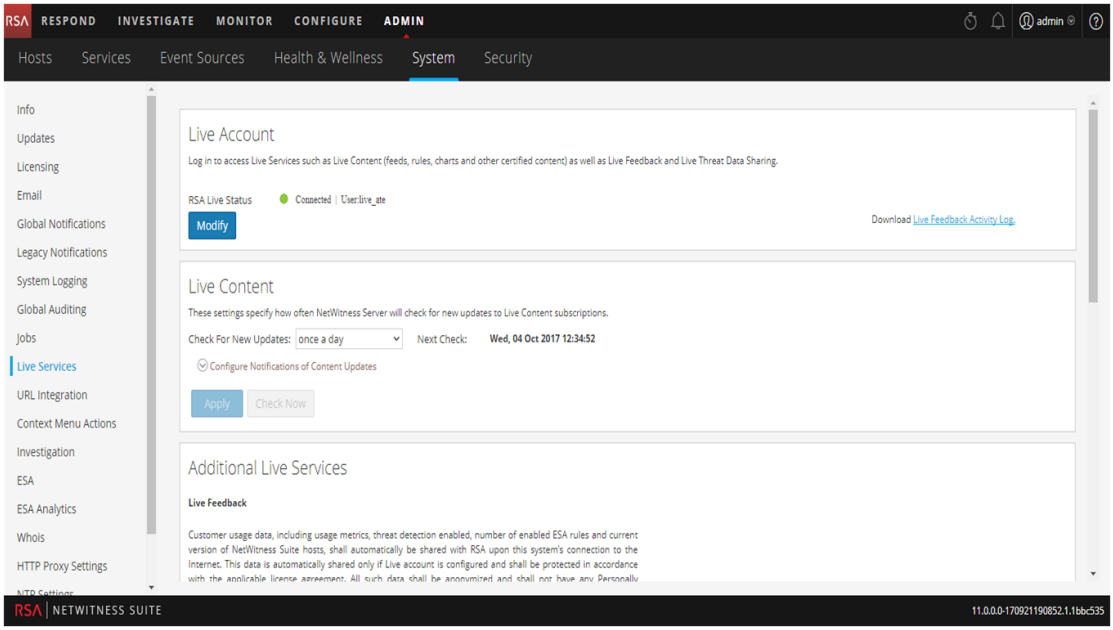
Bei Bedarf können Sie manuell Nutzungsverlaufsdaten herunterladen und diese in RSA freigeben. Informationen zum Herunterladen der Nutzungsverlaufsdaten und zum Freigeben der Daten in RSA finden Sie unter Hochladen von Daten in RSA für Live Feedback.

Dieses Kapitel enthält die folgenden Themen:

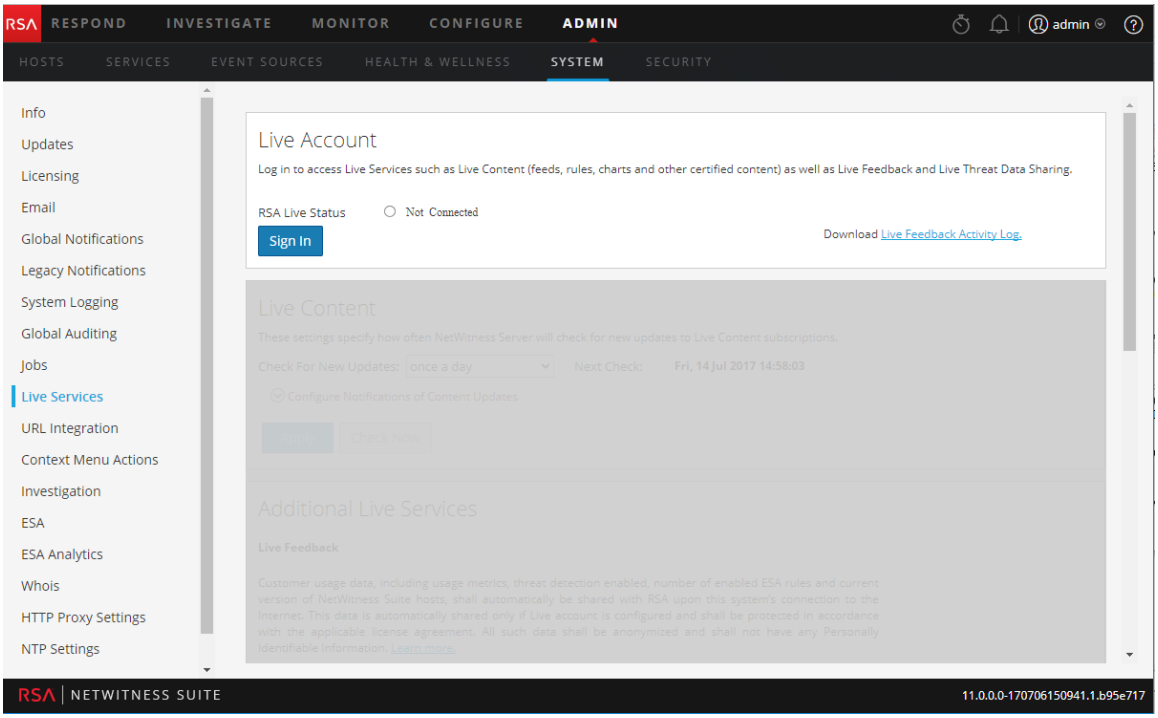
- Zugriff auf den Bereich „Live-Services-Konfiguration“
- Konfigurieren des Live-Kontos
- Konfigurieren des Synchroniationsintervalls und der Synchronisationsbenachrichtigung für Live-Inhalte
- Erzwingen einer sofortigen Synchronisation
- Verwenden von RSA Live Connect (Betaversion)

Zugriff auf den Bereich „Live-Services-Konfiguration“

1. Navigieren Sie zu **ADMIN > SYSTEM**.
2. Wählen Sie im linken Navigationsbereich **Live-Services** aus.



Hinweis: Wenn Sie sich nicht mit Ihren Anmeldedaten für das Live-Konto angemeldet haben, wird ein maskierter Bildschirm angezeigt.



Konfigurieren des Live-Kontos

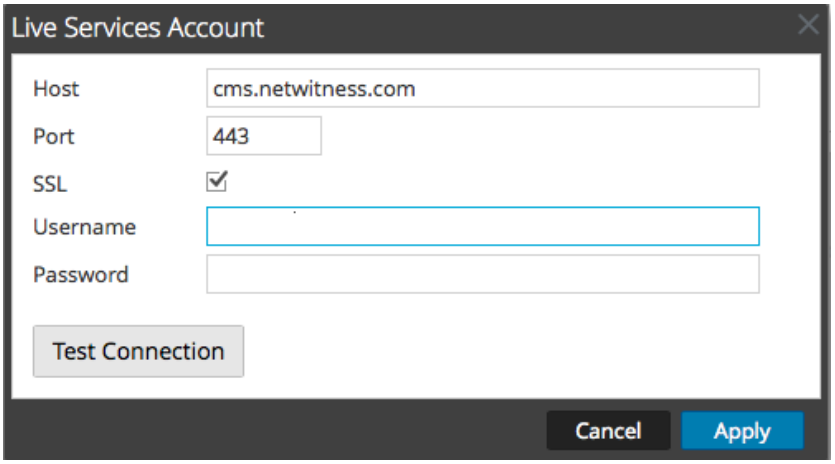
Im Abschnitt **Live-Konto** müssen Sie das Live-Konto des Benutzers einrichten. Die zum Einrichten des Live-Kontos für den Benutzer erforderlichen Informationen sind der Benutzername, dass Passwort und die Live-URL für das Contentmanagement-System. Diese Information wird von Customer Care bereitgestellt.

So konfigurieren Sie ein Live-Konto:

1. Klicken Sie im Abschnitt **Live-Konto** auf **Anmelden**.

   Hinweis: Die Schaltfläche **Ändern** zeigt an, dass das Live-Konto konfiguriert ist. Klicken Sie auf **Ändern**, um den Benutzer zu ändern, der auf Live-Services zugreift.

2. Geben Sie im Dialogfeld „Live-Services-Konto“ den Host (in der Regel **cms.netwitness.com**) und anschließend Benutzername und Kennwort ein.

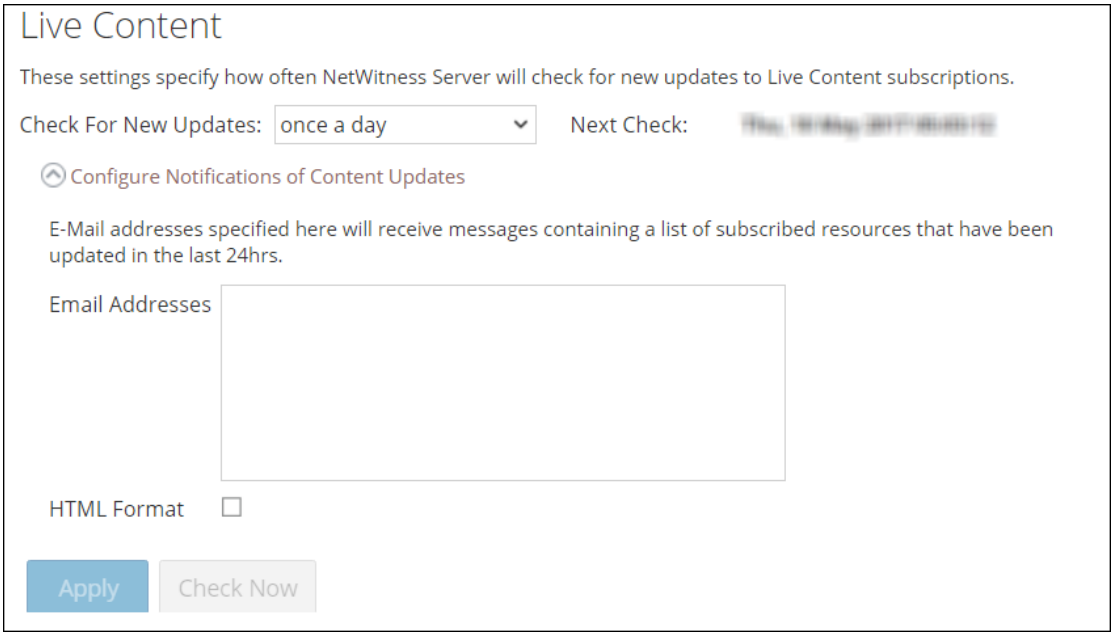


3. (Optional) Wenn Sie ein anderes CMS verwenden, geben Sie die Host-URL für das Contentmanagement-System ein. Der Standardwert verweist auf das CMS unter **cms.netwitness.com**.
4. (Optional) Wenn Sie ein anderes CMS verwenden, geben Sie den Kommunikationsport an, über den Live Anforderungen an das Contentmanagement-System senden soll. Der Standardwert für dieses Feld ist **443**, das ist der Kommunikationsport auf dem Contentmanagement-System.
5. (Optional) Wenn Sie SSL nicht verwenden möchten, deaktivieren Sie die Option **SSL**. (SSL ist standardmäßig aktiviert.)
6. Klicken Sie auf **Verbindung testen**, um die CMS-Verbindung zu testen.
7. Um die Konfiguration zu speichern und anzuwenden, klicken Sie auf **Anwenden**.

Konfigurieren des Synchroniationsintervalls und der Synchronisationsbenachrichtigung für Live-Inhalte

Sie können das Intervall ändern, in dem NetWitness Suite nach neuen Aktualisierungen für Live-Inhalte sucht:

1. Verwenden Sie das Feld **Auf neue Aktualisierungen prüfen**, um das Intervall zu ändern. Wählen Sie ein Intervall aus der Drop-down-Liste aus. Der Standardwert für diese Einstellung ist **Einmal am Tag**.



2. Wenn SieLive-Services so konfigurieren möchten, dass an mindestens eine Person Aktualisierungsberichte gesendet werden, geben Sie im Feld **E-Mail-Adressen** die E-Mail-Adressen in einer durch Kommas getrennten Liste ein, z. B. **john@company.com,ted@company.com,brian@company.com**
3. (Optional) Wählen Sie **HTML-Format** aus, um Nachrichten im HTML-Format statt im Textformat zu erhalten.
4. Klicken Sie zum Speichern und Anwenden auf **Anwenden**.

   Die Uhrzeit und das Datum der nächsten geplanten Live-Synchronisation wird basierend auf dem für die Überprüfung konfigurierten Intervall angezeigt.

Erzwingen einer sofortigen Synchronisation

Anstatt auf den nächsten geplanten Ressourcenzyklus zu warten, zwingt diese Option Live dazu, sofort mit der Synchronisation der abonnierten Ressourcen in dieser Instanz von NetWitness Suite zu beginnen. Damit können unter anderem die unmittelbaren Auswirkungen einer Konfigurationsänderung angezeigt werden, wenn z. B. ein neuer Service hinzugefügt wurde oder neue Ressourcen auf die automatische Bereitstellung umgestellt wurden. Die geplante Synchronisation kann auch Stunden später stattfinden, wenn Live-Services für eine mehrmals täglich stattfindende Synchronisation eingerichtet wurde.

Achtung: Wenn ein FlexParser im Aktualisierungszyklus bereitgestellt ist, kann die Synchronisation einen erneuten Ladevorgang des Parsers auslösen. Dies ist ein- oder zweimal täglich akzeptabel, aber ständige erneute Ladevorgänge des Parsers können zu Paketverlusten beim Decoder führen. Wenn dies das anfängliche Setup ist und Sie keine Live-Ressourcenabonnements konfiguriert haben, führen Sie nicht Jetzt Synchronisieren aus. Warten Sie, bis Sie Abonnements konfiguriert haben.

Um Synchronisation sofort zu erzwingen, klicken Sie auf **Jetzt prüfen**. NetWitness Suite sucht in den abonnierten Ressourcen nach Aktualisierungen.

Verwenden von RSA Live Connect (Betaversion)

Bei RSA Live Connect handelt es sich um einen cloudbasierten Bedrohungsinformationsservice. Dieser Service erfasst, analysiert und bewertet Intelligence-Daten zu Bedrohungen wie beispielsweise IP-Adressen, Domains und Dateien, die aus verschiedenen Quellen erfasst werden, unter anderem aus der Kunden-Community von RSA NetWitness® Suite und RSA NetWitness® Endpoint. RSA Live Connect besteht aus den folgenden Funktionen:

- Bedrohungseinblicke
- Analystenverhalten

Bedrohungseinblicke

Bedrohungseinblicke ermöglicht Analysten das Abrufen von Intelligence-Daten zu Bedrohungen (z. B. IP-bezogene Informationen) vom Live Connect-Service, um sie bei Ermittlungen zu nutzen.

Bedrohungseinblicke ist im Abschnitt **Weitere Live-Services** standardmäßig aktiviert. Wenn Context-Hub-Service konfiguriert wurde, wird Live Connect automatisch als Datenquelle für Context Hub hinzugefügt. Weitere Informationen finden Sie im Thema **Konfigurieren von Live Connect-Datenquellen für Context Hub** im *Context Hub-Konfigurationsleitfaden*.

Mit Live Connect als Datenquelle für Context Hub können Sie die Option „Kontextabfrage“ in der Ansicht „Investigation > Navigieren“ oder der Ansicht „Investigation > Ereignisse“ verwenden, um kontextbezogene Informationen abzurufen. Anweisungen dazu finden Sie im Thema **Anzeigen von zusätzlichem Kontext für einen Datenpunkt** im *Leitfaden Investigation und Malware Analysis*.

Analystenverhalten

Analystenverhalten ist eine Funktion, bei der Analysten am Teilen von Daten mit der RSA-Community teilnehmen. Dies ist ein automatisierter Datensammlungsservice. Sein Ziel ist es, Informationen über potenzielle Bedrohungen im RSA Live Connect-Cloudservice für Analysezwecke zu teilen. Bei den Daten, die möglicherweise aus Ihren Netzwerk mit RSA Live Connect geteilt werden, kann es sich um verschiedene, von NetWitness Suite erfasste Metadatentypen wie ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst oder domain.src handeln. Weitere Informationen über Analystenverhalten und Datenfreigabe finden Sie im Thema **NetWitness-Feedback und Datenfreigabe** im *Handbuch Live Services Management*.

Übersicht über Live Feedback

Dieses Thema bietet eine Einführung in Live Feedback. Live Feedback erfasst relevante Informationen wie die Lizenznutzungsdaten für PacketDecoder, Log Decoder und Malware Analysis, aktivierter oder deaktivierter Status der Bedrohungserkennung, Anzahl der aktivierten ESA-Regeln sowie die Versionsnummerdetails aller Services von NetWitness Suite. Weitere Informationen über die Lizenznutzungsdaten für Packer Decoder, Log Decoder und Malware Analysis finden Sie unter **Registerkarte „Messungsbasierte Lizenzen“** im *Lizenzierungsleitfaden*. Die Informationen werden gesammelt, um zukünftige Versionen von NetWitness Suite zu verbessern. Sie werden automatisch auf Live Feedback angemeldet und Sie können diese Option nicht deaktivieren.

Zusätzlich können Informationen über die Nutzung von Live-Inhalten auch für RSA freigegeben werden. Live-Inhalte-Nutzungsmetriken für Ressourcentypen aus **KONFIGURIEREN > LIVE-INHALTE > Suchkriterien**, wie die Gesamtanzahl für RSA-Anwendungsregeln, RSA-Korrelationsregel usw., können für RSA freigegeben werden. Die gesammelten Informationen werden verwendet, um die Verwendung von Live-Inhalt zu verbessern. Weitere Informationen zur Freigabe der Konfiguration von Live-Inhalt finden Sie im Bereich „Konfiguration der Live-Services“.

Informationen über die Teilnahme an Live Feedback

Wenn Sie an Live Feedback teilnehmen, werden relevante Informationen zur weiteren Verbesserung erfasst. Weitere Informationen über Live Feedback finden Sie unter Übersicht über Live Feedback.

Bei der Installation von NetWitness Suite werden Sie aufgefordert, an Live Feedback teilzunehmen. Informationen finden Sie unter Konfigurieren der Einstellungen von Live-Services.

Bei Bedarf können Sie manuell Nutzungsverlaufsdaten herunterladen und diese in RSA freigeben. Informationen zum Herunterladen der Nutzungsverlaufsdaten und zum Freigeben der Daten in RSA finden Sie unter Hochladen von Daten in RSA für Live Feedback.

Hinweis: Live Feedback ist nur aktiviert, wenn Sie Ihr Live-Konto konfiguriert haben.

Die Live Feedback-Daten weisen das JSON-Format auf, wie unten beschrieben. Wenn Sie sich mit Ihren Anmeldedaten des Live-Kontos anmelden, wird täglich eine einzelne verschlüsselte JSON-Datei automatisch auf die RSA-Server hochgeladen.

JSON-Datei

Die JSON-Datei besteht aus Nutzungsdateninformationen für eine Komponente oder eine Reihe von Komponenten. Im Falle einer Reihe von Komponenten mit derselben Lizenz-ID werden die Nutzungsdaten für alle Komponenten zusammengefasst und als eine Komponente namens „Anspruch“ dargestellt. Allerdings, auch wenn nur eine einzige Komponente, z. B. ein Log Decoder oder Decoder, vorhanden ist, wird eine Komponente „Anspruch“ erzeugt und die Nutzungsdaten für eine einzige Komponente anzeigen. Diese Zusammenfassung ist für Komponenten, insbesondere Log Decoders, Decoders oder Malware Analysis.

Hinweis: Die Version des Anspruchs ist immer null, da sie die Zusammenfassung von Lizenzdaten ist.

Beispiel: Es sind drei Decoders mit derselben Lizenz-ID „xxx“ mit den folgenden Nutzungsdaten vorhanden:
Decoder1 = 150 MB
Decoder2 = 250 MB
Decoder3 = 100 MB
Die aggregierten Nutzungsdaten von 500 MB werden angezeigt.

Diese JSON-Datei wird in den folgenden Abschnitten beschrieben.

- Komponenten
- Metriken
- Andere Produktinformationen
- Beispiel

Komponenten

Informationen über jeden Service in Ihrer NetWitness Suite-Bereitstellung. Dies wird als Komponente dargestellt. Für jede Komponente werden die folgenden Informationen angezeigt.

Komponente	Beschreibung
Version	Versionsnummer der Komponente in der NetWitness Suite-Bereitstellung. Zum Beispiel: 11.0.0.0.x.x.x.x.
ID	Dies ist die eindeutige Komponenten-ID, die für den Host steht und für die Zuordnung zu den erzeugten Kennzahlen verwendet wird.
Eigenschaften	• **Name**: Dies ist der Name der Eigenschaft für diese Komponente. Zum Beispiel: Malware Analysis, ESA, Log Decoder usw. • **Wert**: Dies ist der eindeutige Wert zur Identifikation der Komponente.

Metriken

Kennzahlen der Komponenten (Hosts), insbesondere Log Decoder, Decoder und Malware Analysis. Die Lizenznutzungsdaten für jeden Host werden freigegeben. Für Live-Inhalte-Nutzungsmetriken werden Ressourcentypen aus **Live > Suche**, wie die Gesamtanzahl für RSA-Anwendungsregeln, RSA-Korrelationsregel usw., freigegeben.

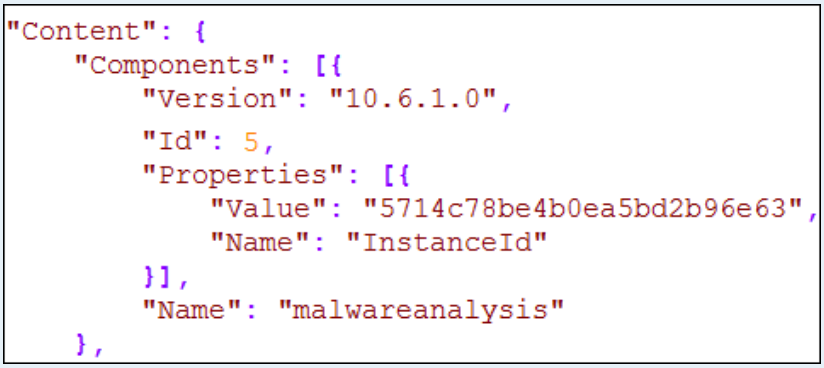
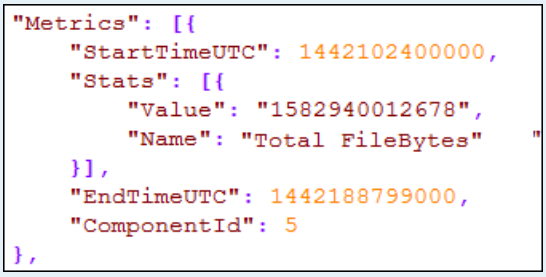
Komponente	Beschreibung
StartTimeUTC	Dies ist der Zeitraum, in dem die Kennzahlen erfasst werden (im Format EPOCH).
Stats	• **Wert**: Dies ist der Wert, der für die spezifische Komponenten-ID für jede Komponente erzeugt wird. • **Name**: Dies ist der Name der Statistik, für die die Kennzahl erfasst wird. Zum Beispiel: Bytes gesamt erfasst.
EndTimeUTC	Dies ist der Zeitpunkt, zu dem die Erfassung der Kennzahlen abgeschlossen ist (im Format EPOCH).
Komponenten-ID	Dies ist die ID der Komponente, für die der Wert aufgezeichnet wird.

Andere Produktinformationen

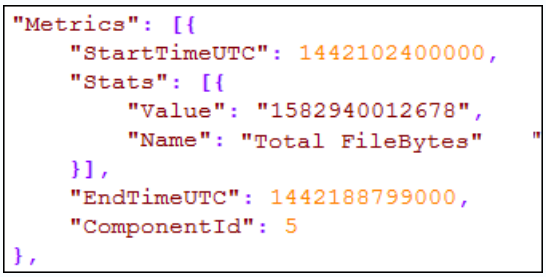
- **Produkttyp**: Dies ist der Name des Produkts. In diesem Beispiel lautet der Produkttyp NetWitness Suite.
- **Version**: Dies ist die Version der JSON-Datei, die die Änderungen nachverfolgt, die an dem Dateiformat vorgenommen werden.
- **Produktinstanz**: Dies ist die Lizenzserver-ID.
- **Prüfsumme**: Dies ist die Informationen, die für Integritätsprüfungen verwendet wird.

In der folgenden Tabelle werden Details der JSON-Datei mit Beispielen beschrieben.

Metriken	Beschreibung
Content	Zeigt den Inhalt, der alle Komponenten, Kennzahlen, Produkttyp- und Produktinstanzdaten enthält, außer der Prüfsumme.

Metriken	Beschreibung
Komponenten	Die Details aller Services in NetWitness Suite werden als Komponente dargestellt. Die Details der Komponente, z. B. die Versionsnummer der Komponente, der Name und der Wert, werden wie nachfolgend dargestellt angezeigt:  **Version**: Zeigt die Version dieses NetWitness Suite-Services an. Beispiel: 11.0.0.0. **ID**: Zeigt eine eindeutige ID, die für den NetWitness Suite-Service erzeugt wird und mit der die Kennzahlen für diese bestimmte Komponente verknüpft werden. In diesem Beispiel ist die ID für Malware Analysis 5 und die Kennzahl für die Komponenten-ID 5 wird in Byte angezeigt, wie unten dargestellt:  **Eigenschaften**: Zeigt die Eigenschaften der Komponente an, z. B. Name und Wert, wie in der obigen Abbildung dargestellt. **Wert**: Zeigt den Wert der Eigenschaft, die eine interne UUID für eine Komponente ist, wie in der obigen Abbildung dargestellt. Diese wird von NetWitness Suite erzeugt. Beispiel: Für Malware Analysis wird der Wert angezeigt als `"55f7a0b30e502231c42d063f"`. **Name: Instanz-ID**: Zeigt den Namen der Eigenschaft an, wie in der Abbildung oben dargestellt.

Metriken	Beschreibung
	Name: „malwareanalysis“: Zeigt den Namen der Komponente an, der ein Servicename ist wie Log Decoder, Decoder oder Malware Analysis.

Metriken	Zeigt die Liste der Kennzahlen mit die Nutzungsdaten für Komponenten an, insbesondere Log Decoder, Decoder und Malware Analysis.
	In diesem Beispiel wird die Kennzahl für Komponenten-ID 5 in Byte angezeigt, wie unten dargestellt.
	 
	"Metrics": [{
	"StartTimeUTC": 1442102400000,
	"Stats": [{
	"Value": "1582940012678",
	"Name": "Total FileBytes"
	}],
	"EndTimeUTC": 1442188799000,
	"ComponentId": 5
	},

	StartTimeUTC: Zeigt die Zeit an, zu der die Metriken erfasst werden, im Format EPOCH.
	Stats: Zeigt Nutzungswert und Nutzungstypstatistik der Komponente an.
	Wert: Gibt den Wert der Statistiken an. Beispiel: „Wert“: „1582940012678“, wie in der obigen Abbildung dargestellt.
	Name: Zeigt den Namen der Statistiken an. Beispiel: Bytes gesamt erfasst oder Dateibytes gesamt.
	EndTimeUTC: Zeigt den Zeitpunkt an, zu dem die Erfassung von Kennzahlen abgeschlossen ist, im Format EPOCH.
	ComponentId: Zeigt die ID der Komponente, für die die Messwerte erfasst werden. Dies ist dasselbe wie „ID“ im Abschnitt „Komponenten“.
Inhalt	Zeigt den Inhalt, der alle Komponenten, Kennzahlen, Produkttyp- und Produktinstanzdaten enthält, außer der Prüfsumme.

Metriken	Beschreibung
Komponenten	Die Details aller Services in NetWitness Suite werden als Komponente dargestellt. Die Details der Komponente, z. B. die Versionsnummer der Komponente, der Name und der Wert, werden wie nachfolgend dargestellt angezeigt:


```
"Content": {
    "Components": [{
        "Version": "10.6.2.0",
        "Id": 6,
        "Properties": [{
            "Value": "57444ddde4b0dd618093064d",
            "Name": "InstanceId"
        }],
        "Name": "reportingengine"
    },
```


Version: Zeigt die Version dieses NetWitness Suite-Services an. Beispiel: 11.0.0.0

ID: Zeigt eine eindeutige ID, die für den NetWitness Suite-Service erzeugt wird und mit der die Kennzahlen für diese bestimmte Komponente verknüpft werden. In diesem Beispiel ist die ID für Reporting Engine 6 und die Kennzahl wird für die ComponentID 6 in Byte angezeigt, wie unten dargestellt:


```
"Metrics": [{
    "StartTimeUTC": 1473292800000,
    "Stats": [{
        "Value": "10",
        "Name": "Number of RE Report"
    },
    {
        "Value": "2",
        "Name": "Number of RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of RE Chart"
    },
    {
        "Value": "14",
        "Name": "Number of RE Rule"
    },
    {
        "Value": "2",
        "Name": "Number of Enabled RE Alert"
    },
    {
        "Value": "1",
        "Name": "Number of Enabled RE Chart"
    }],
    "EndTimeUTC": 1473379199000,
    "ComponentId": 6
},
```

Metriken	Beschreibung
	Eigenschaften: Zeigt die Eigenschaften der Komponente an, z. B. Name und Wert, wie in der obigen Abbildung dargestellt.
	Wert: Zeigt den Wert der Eigenschaft, die eine interne UUID für eine Komponente ist, wie in der obigen Abbildung dargestellt. Diese wird von NetWitness Suite erzeugt. Beispiel: Für Reporting Engine wird der Wert als „`57444ddde4b0dd618093064d`“ angezeigt.
	Name: „**InstanceId**“: Zeigt den Namen der Eigenschaft an, wie in der Abbildung oben dargestellt.
	Name: „**reportingengine**“: Zeigt den Namen der Komponente an, der ein Servicename ist wie Log Decoder, Decoder oder ReportingEngine.
	Name: Zeigt die Liste der Kennzahlen mit den Nutzungsdaten für Komponenten an, insbesondere Log Decoder, Decoder und ReportingEngine. In diesem Beispiel wird die Kennzahl fürComponentID 6 in Byte angezeigt, wie unten dargestellt. `"Metrics": [{ "StartTimeUTC": 1473292800000, "Stats": [{ "Value": "10", "Name": "Number of RE Report" }, { "Value": "2", "Name": "Number of RE Alert" }, { "Value": "1", "Name": "Number of RE Chart" }, { "Value": "14", "Name": "Number of RE Rule" }, { "Value": "2", "Name": "Number of Enabled RE Alert" }, { "Value": "1", "Name": "Number of Enabled RE Chart" }], "EndTimeUTC": 1473379199000, "ComponentId": 6 },`
	StartTimeUTC: Zeigt die Zeit an, zu der die Metriken erfasst werden, im Format EPOCH.

Metriken	Beschreibung
	Stats: Zeigt Nutzungswert und Nutzungstypstatistik der Komponente an.
	Wert: Gibt den Wert der Statistiken an. Beispiel: Anzahl der RE-Berichte ist 10, Anzahl der RE-Warnmeldungen ist 2, Anzahl der RE-Diagramm ist 1 usw., wie in der obigen Abbildung dargestellt.
	Name: Zeigt den Namen der Statistiken an. Beispiel: Anzahl der RE-Berichte, Anzahl der RE-Warnmeldungen, Anzahl der RE-Diagramme, Anzahl der RE-Regeln, Anzahl der aktivierten RE-Warnmeldungen, Anzahl der aktivierten RE-Diagramme.
	EndTimeUTC: Zeigt den Zeitpunkt an, zu dem die Erfassung von Kennzahlen abgeschlossen ist, im Format EPOCH.
	ComponentId: Zeigt die ID der Komponente, für die die Messwerte erfasst werden. Dies ist dasselbe wie „ID“ im Abschnitt „Komponenten“.
productType	Zeigt den Typ des Produkts an, das die Datei erzeugt. Zum Beispiel: `"ProductType": "NetWitness Suite"`
ProductInstance	Zeigt die Lizenzserver-ID an und ist pro NetWitness Suite eindeutig. Zum Beispiel: `"ProductInstance": "00-0C-29-6C-66-E3"`
Checksum	Zeigt die Prüfsumme für den Abschnitt „Inhalt“ in der Datei an. Wird von RSA für die Integritätsprüfung verwendet. Zum Beispiel: `"Checksum": "883DACF97E4BCD9F590A1461A4DD0A312B5883A6CF82E0518E77AAB6A6DDB654"`

Beispiel

Hier ist eine JSON-Beispieldatei.


```
{
    "Content": {
        "Components": [{
            "Version": "10.6.1.0",
            "Id": 7,
            "Properties": [{
                "Value": "57470c96e4b0cf62c7bfbd53",
                "Name": "InstanceId"
            }],
            "Name": "esa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 4,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e69",
                "Name": "InstanceId"
            }],
            "Name": "incidentmanagement"
        },
        {
            "Version": "10.6.1.0",
            "Id": 2,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e65",
                "Name": "InstanceId"
            }],
            "Name": "sa"
        },
        {
            "Version": "10.6.1.0",
            "Id": 1,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e63",
                "Name": "InstanceId"
            }],
            "Name": "malwareanalysis"
        },
        {
            "Version": "10.6.1.0",
            "Id": 3,
            "Properties": [{
                "Value": "5714c78be4b0ea5bd2b96e67",
                "Name": "InstanceId"
            }],
            "Name": "reportingengine"
        }],
        "Metrics": [{
            "StartTimeUTC": 1464480000000,
            "Stats": [{
                "Value": "Disabled",
                "Name": "Threat Detection"
            },
            {
                "Value": "3.0",
                "Name": "Number Of Enabled ESA Rules"
            }],
            "EndTimeUTC": 1464566399000,
            "ComponentId": 7
        }],
        "EndTime": 1464566399000,
        "Version": "1.0",
        "StartTime": 1464479999000,
        "ProductType": "Security Analytics",
        "ProductInstance": "00-0C-29-A2-57-B4"
    },
    "Checksum": "6445C704D3F9E67D24DBA8F11EB6C003CBCC0E199576342E6E6D2545524F583F"
}
```

Hochladen von Daten in RSA für Live Feedback

Dieses Thema enthält Anweisungen für einen NetWitness Suite-Administrator zum Exportieren der Kennzahlen in NetWitness Suite für Live Feedback.

Wenn das Live-Konto nicht konfiguriert ist,können Sie Nutzungsdaten manuell in RSA hochladen. Weitere Informationen finden Sie unter Bereich „Konfiguration der Live-Services“.

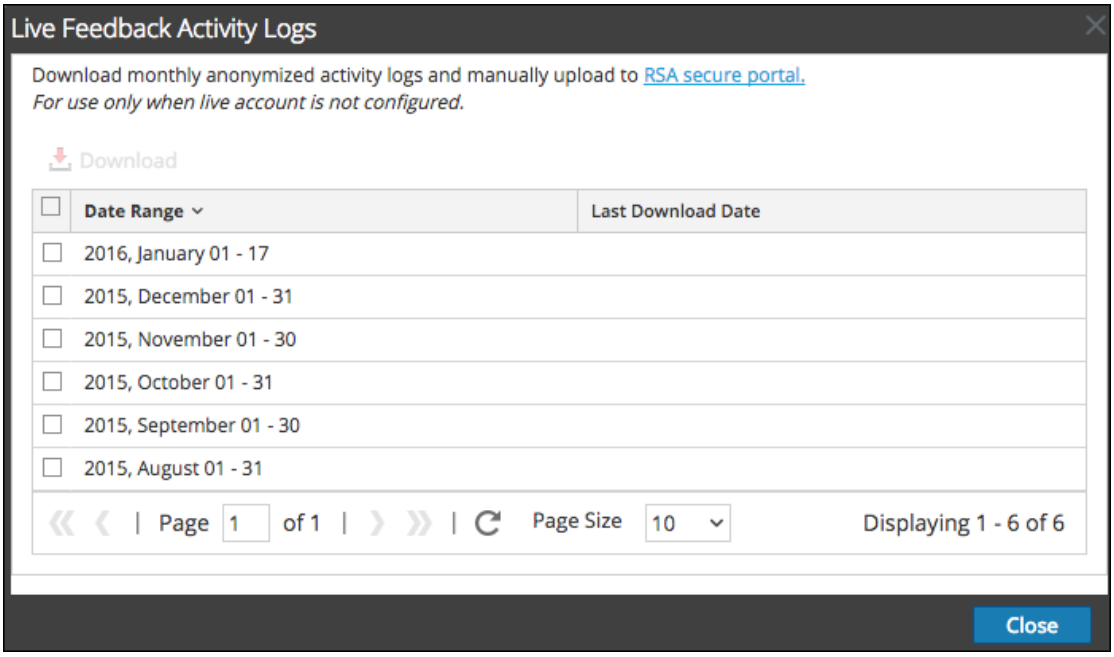
Der Abschnitt „Live-Konto“ verfügt über ein Live Feedback-Aktivitätsprotokoll, mit dem Sie die erforderlichen Nutzungsdaten für Live Feedback herunterladen können. Dies ist unabhängig von der Live-Konto-Konfiguration aktiv.

Sie können zunächst die Live Feedback-Verlaufsdaten herunterladen und danach hochladen, um sie mit RSA zu teilen.

Herunterladen von Live Feedback-Verlaufsdaten

So laden Sie Live Feedback-Verlaufsdaten herunter:

1. Navigieren Sie zu **ADMIN** > **System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Live-Services** aus.
   Der Bildschirm **Live-Konto** wird angezeigt, auf dem der **RSA Live-Status** angezeigt wird und das **Live Feedback-Aktivitätsprotokoll** heruntergeladen werden kann.
3. Klicken Sie auf **Live Feedback-Aktivitätsprotokoll herunterladen**.
   Das Fenster **Live Feedback-Aktivitätsprotokoll herunterladen** wird geöffnet, in dem der NetWitness Suite-Benutzer die erforderlichen Live Feedback-Verlaufsdaten herunterladen kann.



4. Wählen Sie einen oder mehrere Einträge aus, indem Sie die Kontrollkästchen aktivieren, und

klicken Sie auf **Herunterladen**.

Hinweis: Wenn Sie mehrere Einträge in der Verlaufstabelle auswählen, besteht die heruntergeladene ZIP-Datei aus einer einzelnen JSON-Datei für jeden Monat.

Die heruntergeladenen Live Feedback-Daten haben das JSON-Format und sind in einer ZIP-Datei gepackt. Weitere Informationen finden Sie unter Übersicht über Live Feedback.

Freigabe von Daten mit RSA

Nachdem Sie die Live Feedback-Daten heruntergeladen haben, können Sie sie mithilfe des folgenden Verfahrens hochladen.

So geben Sie die Daten für RSA frei:

1. Klicken Sie auf das **sichere RSA-Portal**, das im Fenster **Live Feedback-Aktivitätsprotokolle** verfügbar ist.
   Der RSA NetWitness® Suite Live Feedback-Anmeldebildschirm wird angezeigt.
2. Melden Sie sich beim Portal zum Hochladen der Live Feedback-Aktivitätsprotokolle mit Ihren Live-ID-Anmeldeinformationen an.
3. Klicken Sie auf **Datei auswählen**, und wählen Sie die heruntergeladene Datei aus.
4. Klicken Sie auf **Hochladen**.

Konfigurieren von Protokolldateieinstellungen

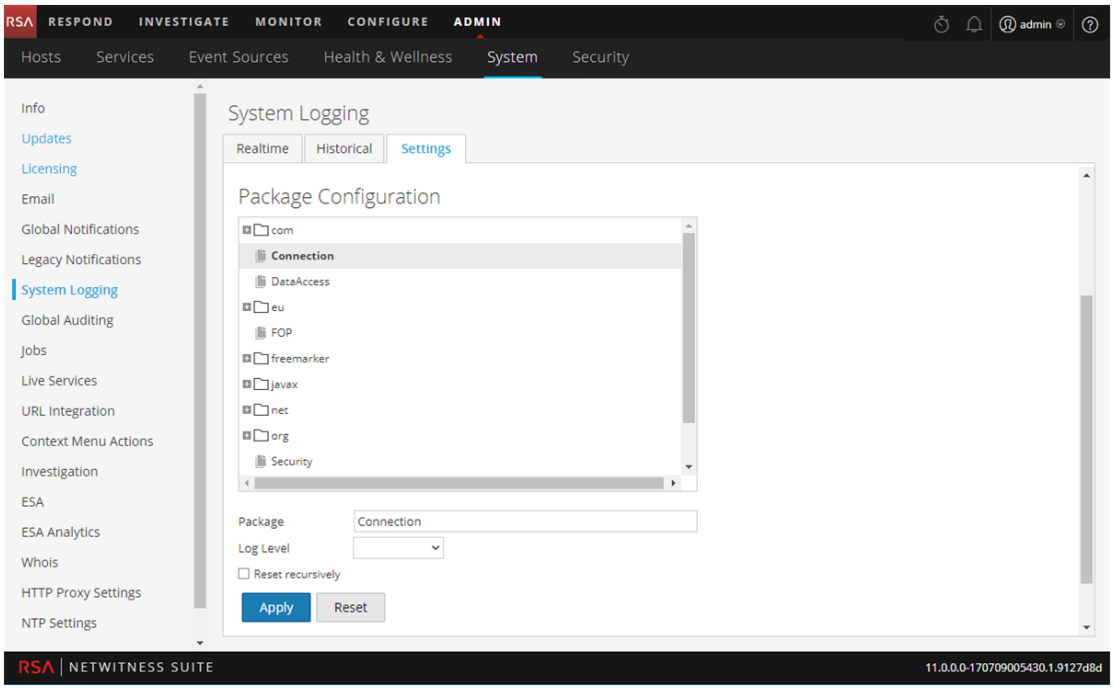
In RSA NetWitness® Suite können Sie die Größe der Protokolldateien, die Anzahl der aufbewahrten Backupprotokolldateien sowie die standardmäßigen Protokollierungsebenen für die Pakete in NetWitness Suite konfigurieren.

Konfigurieren der Systemprotokolldateigröße und der aufbewahrten Backupdateien

Die Protokolldateigröße und die Anzahl der Backupdateien sind mit Standardwerten konfiguriert. Wenn Sie die Standardwerte für die Protokolldateigröße und die Anzahl der Backups ändern möchten, gehen Sie wie folgt vor:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **System Protokollierung** aus.
   Der Bereich „Systemprotokollierungskonfiguration“ wird standardmäßig mit angezeigter Registerkarte „Echtzeit“ geöffnet.

3. Klicken Sie auf die Registerkarte **Einstellungen**.

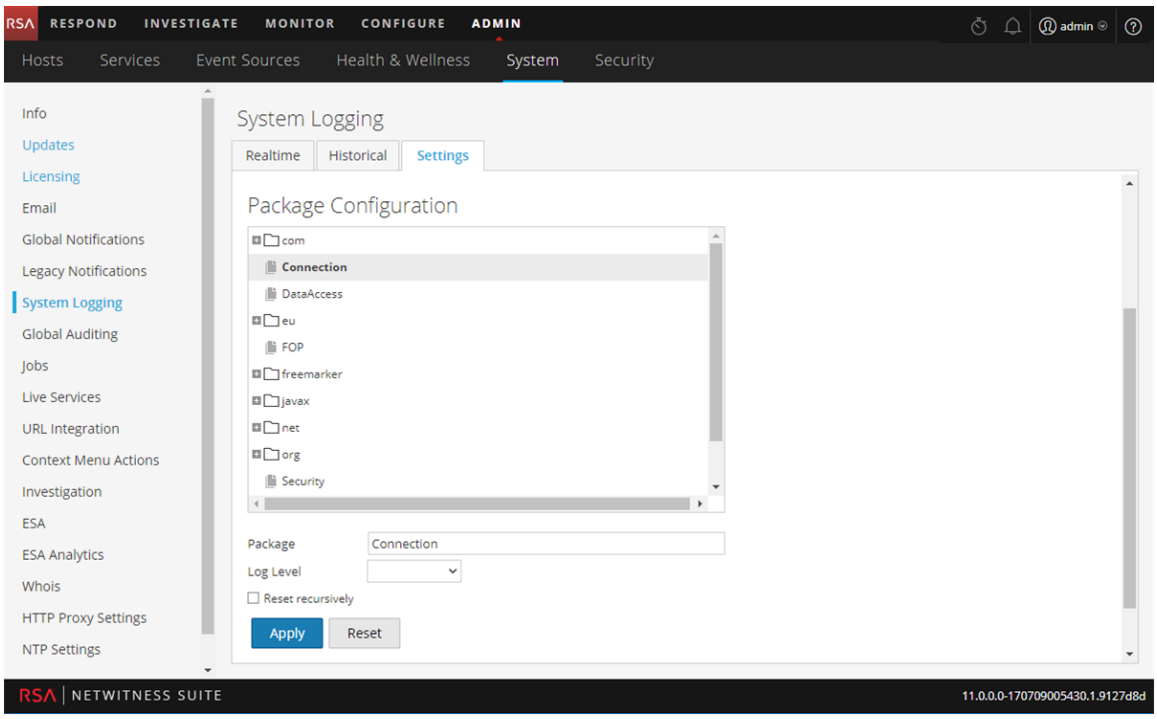


4. Geben Sie im Feld **Max. Protokollgröße** die maximale Größe in Byte ein. Der Mindestwert für diese Einstellung beträgt **4096**.
5. Geben Sie in das Feld **Max. Anzahl Backupdateien** die maximale Anzahl an Backupdateien ein, die aufbewahrt werden sollen. Der Mindestwert für diese Einstellung beträgt **0**. Wenn die maximale Anzahl von Protokolldateien erreicht ist und eine neue Backupdatei erstellt wird, wird das älteste Backup gelöscht.
6. Klicken Sie auf **Anwenden**.
   Die Änderungen treten sofort in Kraft.

Festlegen der Protokollebene für ein einzelnes Paket

Der Abschnitt „Paketkonfiguration“ zeigt die RSA NetWitness Packets in einer Baumstruktur an. Die Struktur enthält alle innerhalb von NetWitness Suite verwendete Pakete. Sie können einen Drill-down in die Struktur durchführen, um die Protokollebenen eines jeden Pakets anzuzeigen. Die Protokollierungsebene für alle Pakete, für die keine Angabe gemacht wird, ist die **root**-Ebene. So legen Sie die Protokollebene für ein Paket fest:

1. Wählen Sie das Paket in der **Paketstruktur** aus.
   Der Name des Pakets wird im Feld **Paket** angezeigt. Wenn für das Paket bereits eine Protokollebene festgelegt ist, wird diese Ebene angezeigt.



2. Wählen Sie die **Protokollebene** in der Drop-down-Liste aus.
3. Klicken Sie auf **Anwenden**.
   Die neue Protokollebene wird sofort wirksam.
4. (Optional) Wenn Sie die standardmäßige **root**-Protokollebene wiederherstellen möchten, klicken Sie auf **Zurücksetzen**.

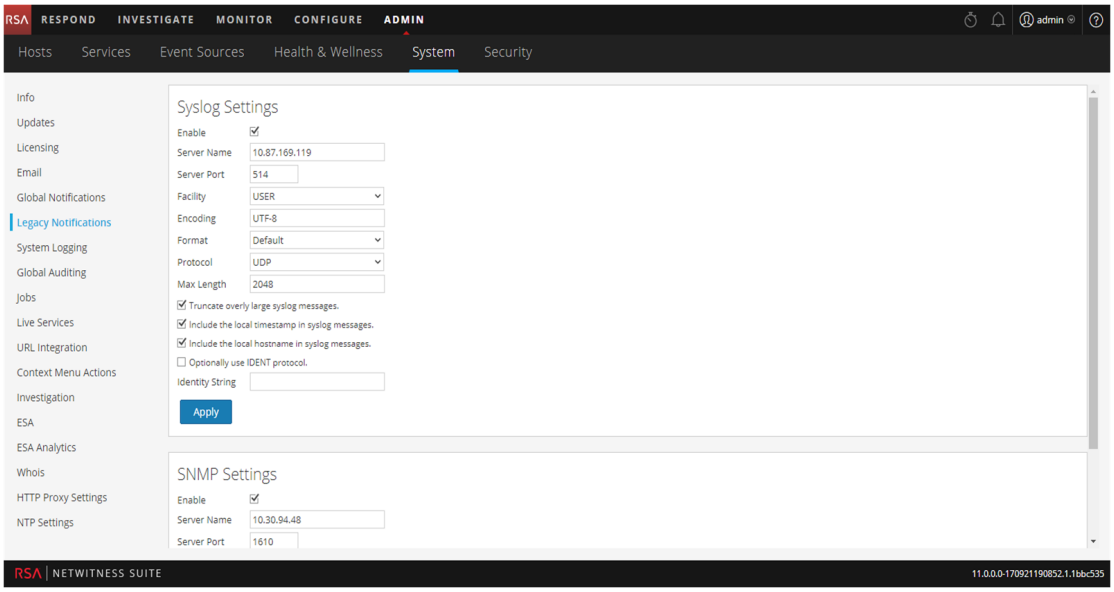
Konfigurieren von Syslog- und SNMP-Einstellungen

Im Bereich „Alte Benachrichtigungen“ können Sie Syslog-und SNMP-Benachrichtigungseinstellungen konfigurieren. Diese Konfigurationen werden für Berechtigungen, altes Ereignisquellenmanagement (Event Source Manamegement, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung verwendet.

Konfigurieren und Aktivieren der Syslog-Einstellungen

1. Navigieren Sie zu **ADMIN > System**.

2. Wählen Sie im Bereich „Optionen“ die Option **Alte Benachrichtigungen** aus.
   Der Konfigurationsbereich „Alte Benachrichtigungen“ wird angezeigt.

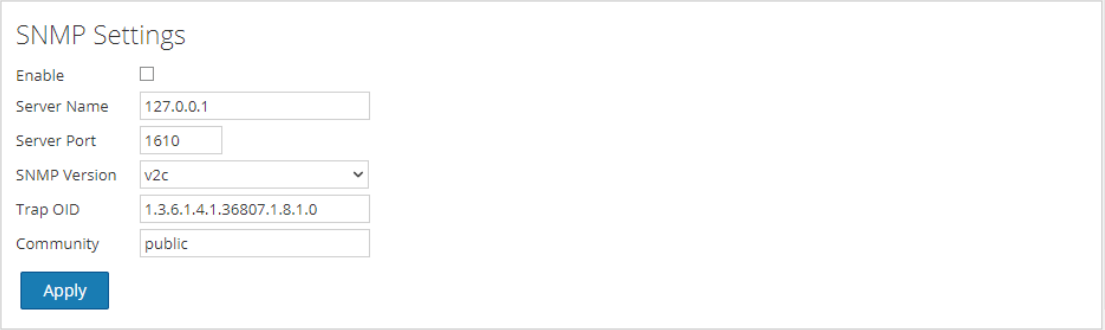


3. Geben Sie unter **Syslog-Einstellungen** in den Feldern **Servername** und **Serverport** den Namen des Hosts ein, auf dem der Syslog-Zielprozess ausgeführt wird, sowie den Port, den der Syslog-Zielprozess überwacht.
4. Spezifizieren Sie in den Feldern **Gerät**, **Codierung**, **Format** und **Max. Länge** das Syslog-Gerät, die Codierung des Nachrichtentexts, das Nachrichtenformat sowie die maximale Länge der Nachricht.
5. Wählen Sie im Feld **Protokoll** UDP oder TCP aus.
6. (Optional) Wählen Sie über die Optionen aus, was die Nachrichten beinhalten sollen. **Zu lange Syslog-Meldungen kürzen**, **Lokalen Zeitstempel in Syslog-Meldungen einfügen** und **Den lokalen Hostnamen zu Syslog-Nachrichten hinzufügen**.
7. (Optional) Konfigurieren Sie Syslog, jeder Syslog-Warnmeldung eine Identitätszeichenfolge voranzustellen.
8. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
9. Klicken Sie auf **Anwenden**.
   Syslog-Benachrichtigungen werden sofort aktiviert.

Detaillierte Informationen zu diesen Einstellungen erhalten Sie im Bereich „Konfiguration alter Benachrichtigungen“.

Konfigurieren und Aktivieren der SNMP-Einstellungen

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Alte Benachrichtigungen** aus.
   Der Konfigurationsbereich „Alte Benachrichtigungen“ wird angezeigt, wobei sich SNMP-Einstellungen am unteren Rand des Bereichs befinden.



3. Geben Sie unter **SNMP-Einstellungen** in den Feldern **Servername** und **Serverport** den Hostnamen und den Überwachungsport des SNMP-Trap-Hosts an.
4. Wählen Sie im Drop-down-Menü die **SNMP-Version** aus: **v1** oder **v2c**.
5. Geben Sie im Feld **Trap-OID** die Objekt-ID für den SNMP-Trap auf dem Trap-Host an, der das Auditereignis empfängt. Der Standardwert ist **0.0.0.0.0.1**.
6. Geben Sie im Feld **Community** die zur Authentifizierung auf dem SNMP-Trap-Host verwendete Community-Zeichenfolge an. Der Standardwert lautet **öffentlich**.
7. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
8. Klicken Sie auf **Anwenden**.
   SNMP-Benachrichtigungen werden sofort aktiviert.

Detaillierte Informationen zu diesen Einstellungen erhalten Sie im Bereich „Konfiguration alter Benachrichtigungen“.

Deaktivieren der Syslog- oder SNMP-Einstellungen

So deaktivieren Sie die Syslog- oder SNMP-Einstellungen auf dieser NetWitness Suite-Instanz:

1. Deaktivieren Sie das entsprechende Kontrollkästchen **Aktivieren**.
2. Klicken Sie auf **Anwenden**.
   Die ausgewählten Einstellungen werden sofort deaktiviert.

Zusätzliche Verfahren

Die zusätzlichen Verfahren sind für die Einrichtung von NetWitness Suite nicht grundlegend erforderlich, sie umfassen bestimmte Anpassungsoptionen, die über die übliche Einrichtung hinausgehen; beispielsweise das Hinzufügen von benutzerdefinierten Kontextmenüs oder die Proxy-Einrichtung.

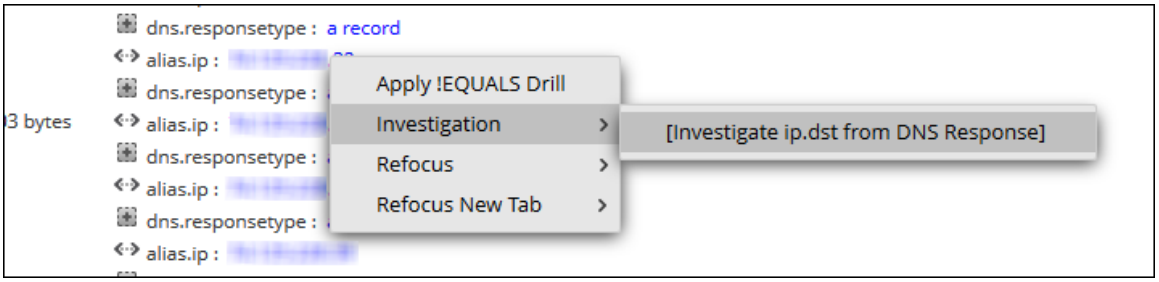
Hinzufügen benutzerdefinierter Kontextmenüaktionen

Im Bereich „Kontextmenüaktionen“ können Administratoren Kontextmenüaktionen für die aktuelle Instanz von NetWitness Suite anzeigen, hinzufügen und bearbeiten. Jede Kontextmenüaktion gilt für einen bestimmten Kontext in der NetWitness Suite-Benutzeroberfläche und wird als Option angezeigt, wenn Sie bei einer bestimmten Position in der Benutzeroberfläche mit der rechten Maustaste klicken.

Einige Kontextmenüaktionen sind in NetWitness Suite integriert. Sie können die Standard-Kontextmenüaktionen nicht bearbeiten oder löschen. Sie können benutzerdefinierte Kontextmenüaktionen erstellen und bearbeiten. Wenn Sie eine benutzerdefinierte Variante einer integrierten Kontextmenüaktion erstellen möchten, können Sie die Konfiguration in eine neue Kontextmenüaktion kopieren und die benutzerdefinierte Kontextmenüaktion ändern. Eine Kontextmenüaktion wird in CSS-Code (Cascading Stylesheet) festgelegt, der Folgendes definiert:

- Den Titel der Option im Kontextmenü.
- DasNetWitness SuiteModul, in dem das Kontextmenü verfügbar ist.
- Die Inhalte, für die die Aktion gilt.

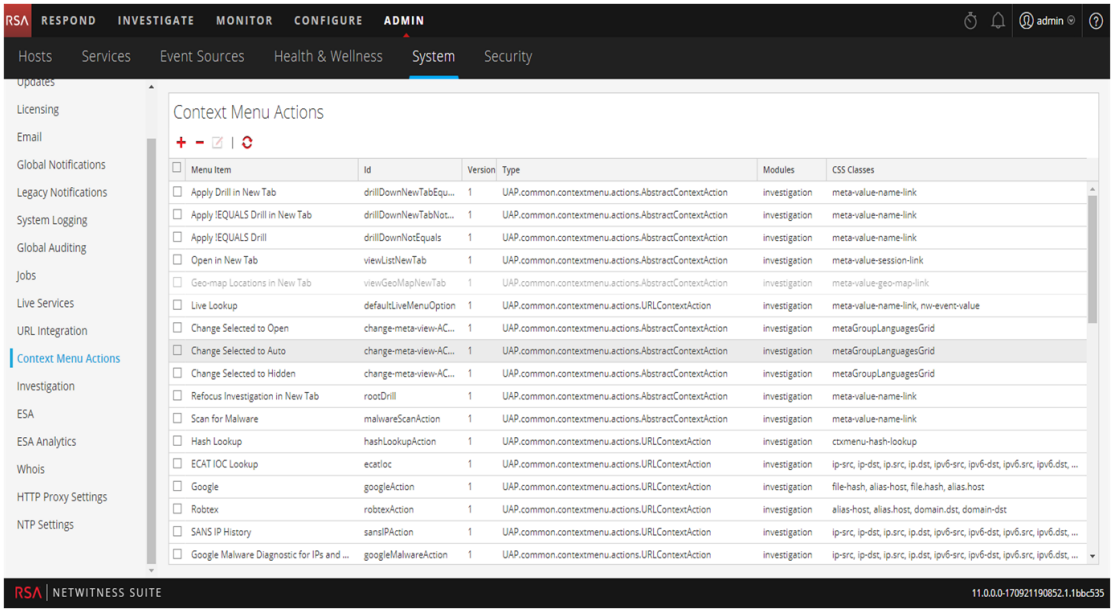
Dies ist ein Beispiel für eine benutzerdefinierte Kontextmenüaktion. Als ein Beispielverfahren werden unten die Schritte und der CSS-Code zum Erstellen dieses Beispiels bereitgestellt.



Anzeigen von Kontextmenüaktionen in NetWitness Suite

So zeigen Sie sowohl standardmäßige als auch benutzerdefinierte Kontextaktionen in NetWitness Suite an:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Kontextmenüaktionen** aus.



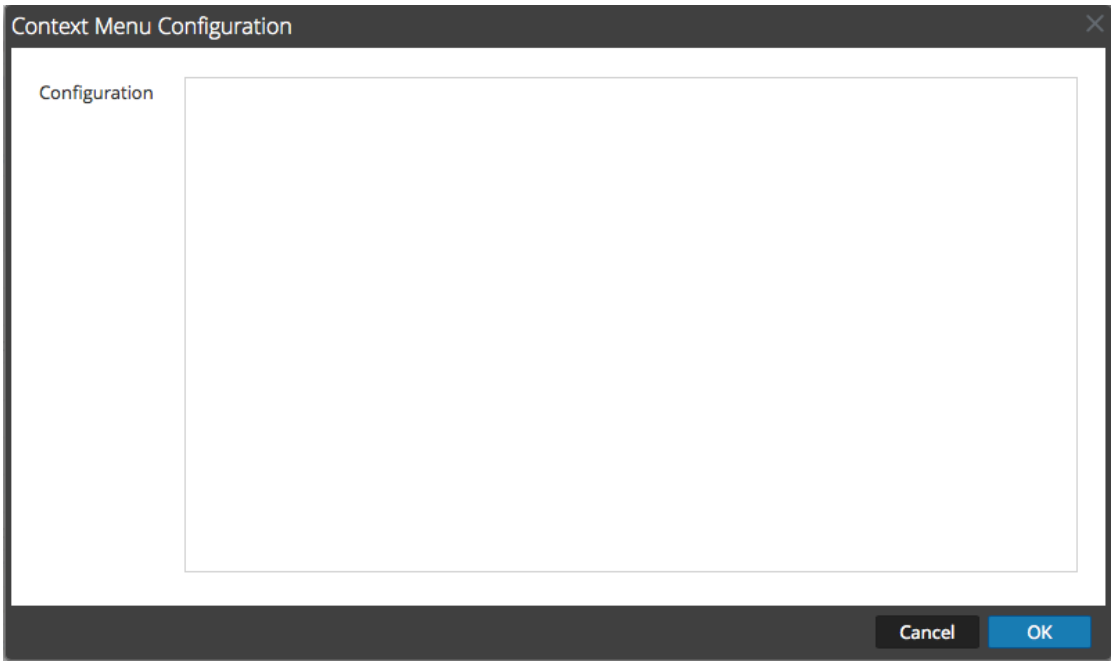
Details zu den Informationen im Bereich Kontextmenüaktion finden Sie unter Bereich Kontextmenüaktionen

Hinzufügen einer Kontextmenüaktion

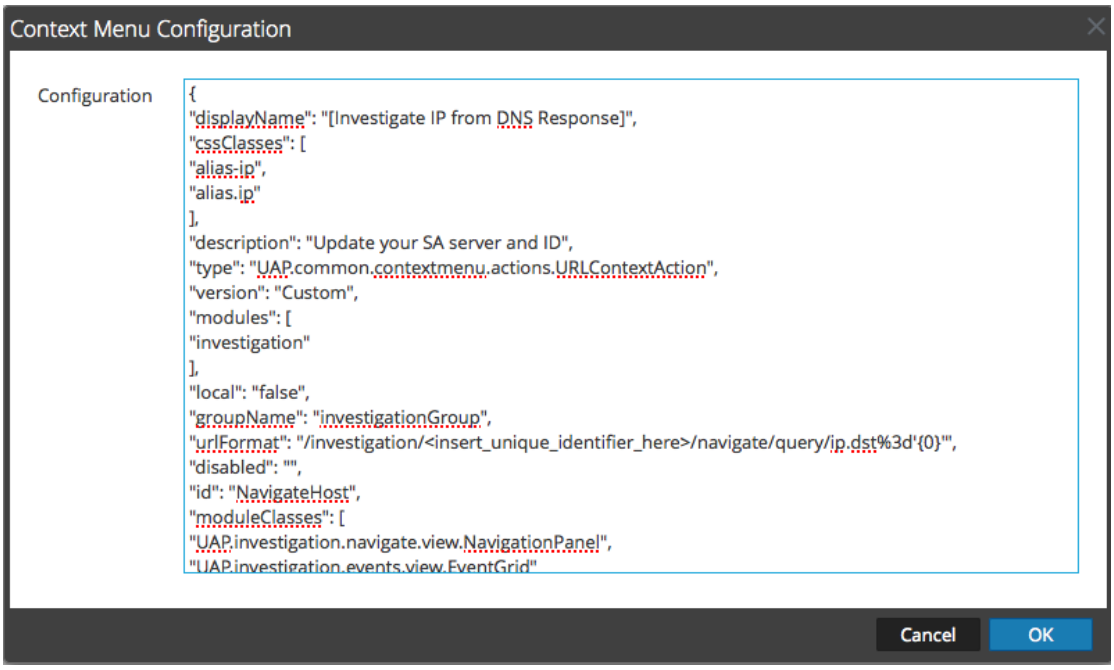
So fügen Sie eine Kontextmenüaktion in NetWitness Suite hinzu:

1. Klicken Sie in der Symbolleiste auf +.

   Das Dialogfeld „Kontextmenü-Konfiguration“ wird angezeigt.



2. Geben Sie den CSS-Code ein, mit dem die Kontextmenüaktion definiert wird. Das Beispielverfahren am Ende dieses Themas bietet eine schrittweise Anleitung, die Sie verwenden können, um eine nützliche Kontextmenüaktion zu erstellen.



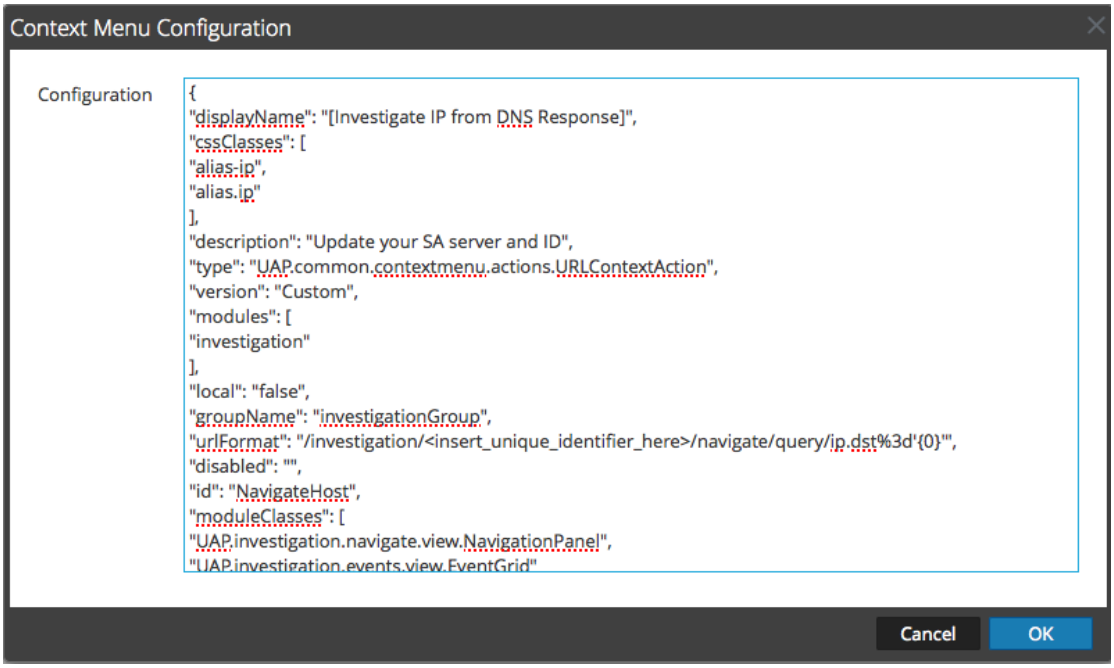
3. Klicken Sie auf **OK**
.Die neue Kontextmenüaktion wird erstellt und am Ende der Liste der Kontextmenüaktionen hinzugefügt.

4. Um die neue Kontextmenüaktion zu aktivieren, starten Sie den Browser neu.
   Das Kontextmenüaktion wird am konfigurierten Speicherort verfügbar.

Bearbeiten einer Kontextaktion

So bearbeiten Sie eine Kontextaktion:

1. Wählen Sie die Zeile im Raster aus und **doppelklicken** Sie dann entweder auf die Zeile oder klicken Sie auf .
   Das Dialogfeld **Kontextmenü-Konfiguration** wird angezeigt.



2. Bearbeiten Sie die **Konfiguration**.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.
4. Um die aktualisierte Aktion zu verwenden, starten Sie den Browser neu.

Löschen einer Kontextaktion

So entfernen Sie eine Kontextaktion vollständig aus NetWitness Suite:

1. Wählen Sie die Aktion aus.
2. Klicken Sie auf .
   Ein Dialogfeld fordert Sie auf, zu bestätigen, dass Sie die Kontextmenüaktion löschen möchten.
3. Klicken Sie auf **Yes**.
   Die Option wird aus dem Bereich Kontextmenüaktionen entfernt.

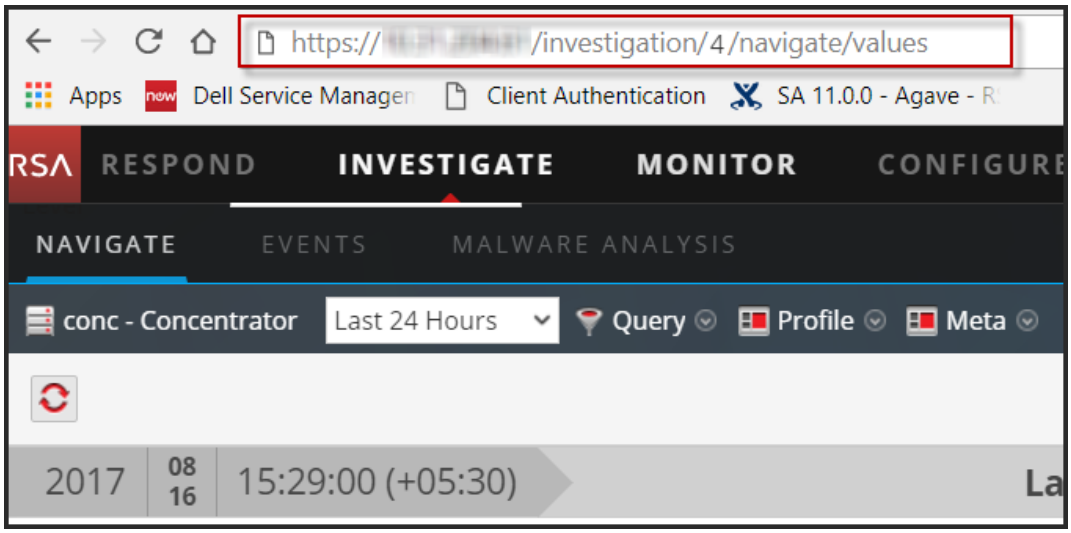
4. Starten Sie den Browser neu, um die Aktion aus den Kontextmenüs zu entfernen, in denen sie enthalten war.

Beispiel für die Vorgehensweise: Kontextmenüaktion zum Untersuchen von ip.dst aus alias.ip

In diesem Beispiel wird eine Kontextmenüaktion hinzugefügt, mit der Analysten aus den `alias.ip`-Werten (die von einer DNS-Anforderung zurückgegebenen IP-Adressen) Werte der `ip.dst`-Metaschlüssel pivotieren können. Analysten können damit jeden Datenverkehr an die IP-Adresse erkennen, die bei einer DNS-Abfrage zurückgegeben wurde.

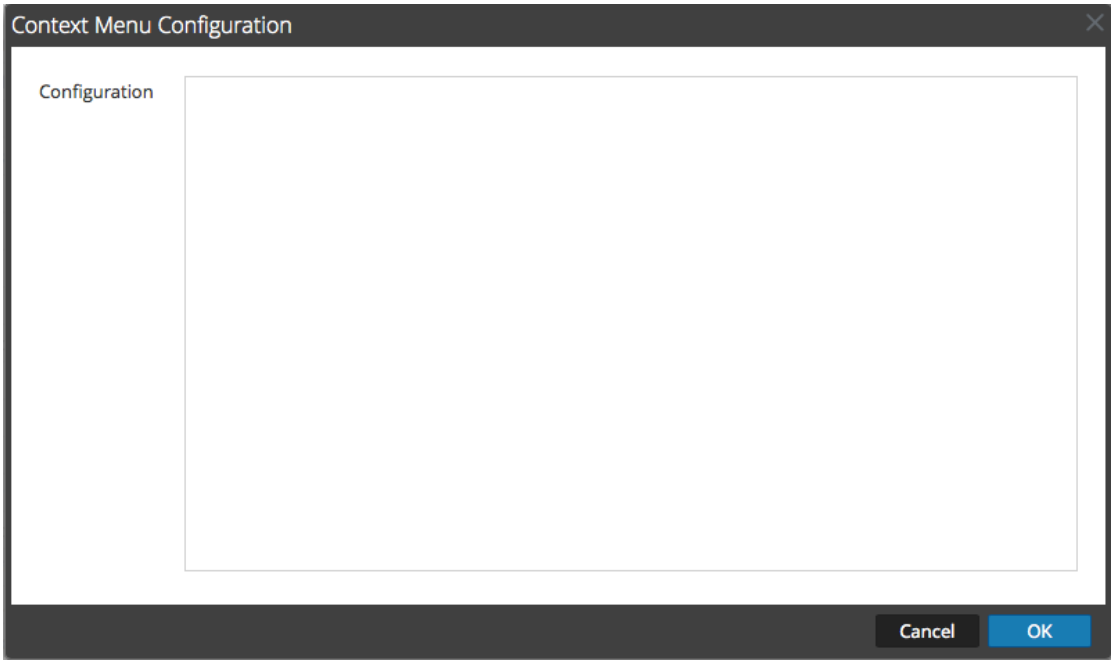
So implementieren Sie die Kontextmenüaktion:

1. Bestimmen Sie die eindeutige Kennung für Ihren NetWitness-Server wie folgt:
   a. Melden Sie sich bei NetWitness Suite an, wählen Sie im Hauptmenü die Option **Investigation > Navigieren** aus, wählen Sie einen zu untersuchenden Service (z. B. einen Concentrator) aus und warten Sie, bis die Werte geladen wurden.
   b. Suchen Sie die URL und die Zahl nach `investigation`. In diesem Beispiel lautet die eindeutige Kennung für die Aktion 4. Sie benötigen diese eindeutige ID, um die Kontextmenüaktion hinzuzufügen.



2. Klicken Sie in der Symbolleiste auf .

   Das Dialogfeld „Kontextmenü-Konfiguration“ wird angezeigt.

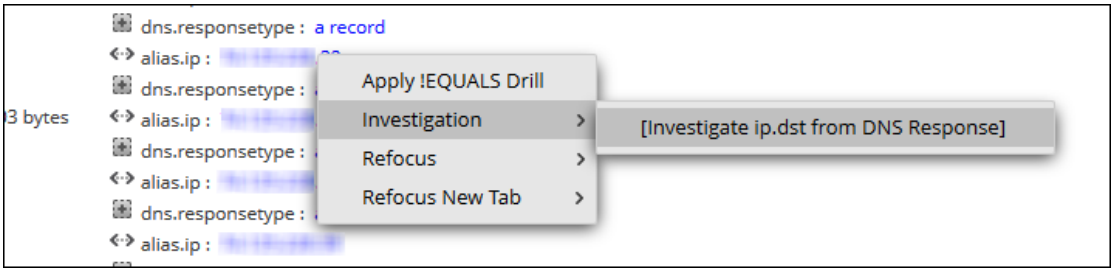


3. Kopieren Sie den gesamten Beispiel-Codeblock unten und fügen Sie ihn in das Fenster ein.

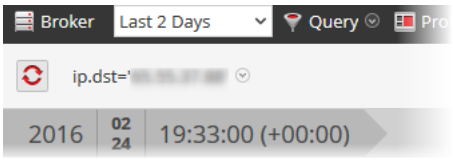
```
{
    "displayName": "[Investigate IP from DNS Response]",
    "cssClasses": [
        "alias-ip",
        "alias.ip"
    ],
    "description": "Update your NW server and ID",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "Custom",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "investigationGroup",
    "urlFormat": "/investigation/<insert_unique_identifier_
here>/navigate/query/ip.dst%3d'{0}'",
    "disabled": "",
    "id": "NavigateHost",
    "moduleClasses": [
```

```
            "UAP.investigation.navigate.view.NavigationPanel",
            "UAP.investigation.events.view.EventGrid"
        ],
        "openInNewTab": "true"
    }
```

4. Ersetzen Sie in der Zeile **urlFormat** den Eintrag **<insert-unique_identifier_here>** durch den eindeutigen Bezeichner.
   Die URL sollte wie folgt aussehen:
   `"/investigation/4/navigate/query/ip.dst%3d'{0}'"`
5. Klicken Sie auf **OK**, und starten Sie Ihren Browser neu.
6. Öffnen Sie, um die Aktion zu testen, eine Ermittlung in der Navigationsansicht und klicken mit der rechten Maustaste auf den Metaschlüssel `alias.ip`.
   Die Ermittlungsoption im Kontextmenü sollte der folgenden Abbildung ähneln.



7. Sollte einen Pivot erzeugen, der diesem gleicht.



8. Wenn Sie dieses Beispiel zur Ermittlung des DNS-Datenverkehrs verwenden, sollten Sie in Betracht ziehen, eine spezifische Metagruppe für DNS-Datenverkehr zu erstellen, wie in „Managen von benutzerdefinierten Metagruppen im *Leitfaden Investigation und Malware Analysis* beschrieben.

Konfigurieren von NTP-Servern

Dieses Thema enthält Anweisungen zum Konfigurieren von NTP-Servern (Network Time Protocol). NTP ist ein Protokoll zum Sychronisieren der Uhrzeiten von Hostcomputern über ein Netzwerk. Weitere Informationen über NTP finden Sie auf der Startseite (http://www.ntp.org/).

Hinweis: NW-Core-Hosts müssen mit dem NW-Host über UDP-Port123 kommunizieren können, um die NTP-Zeitsynchronisation durchzuführen.

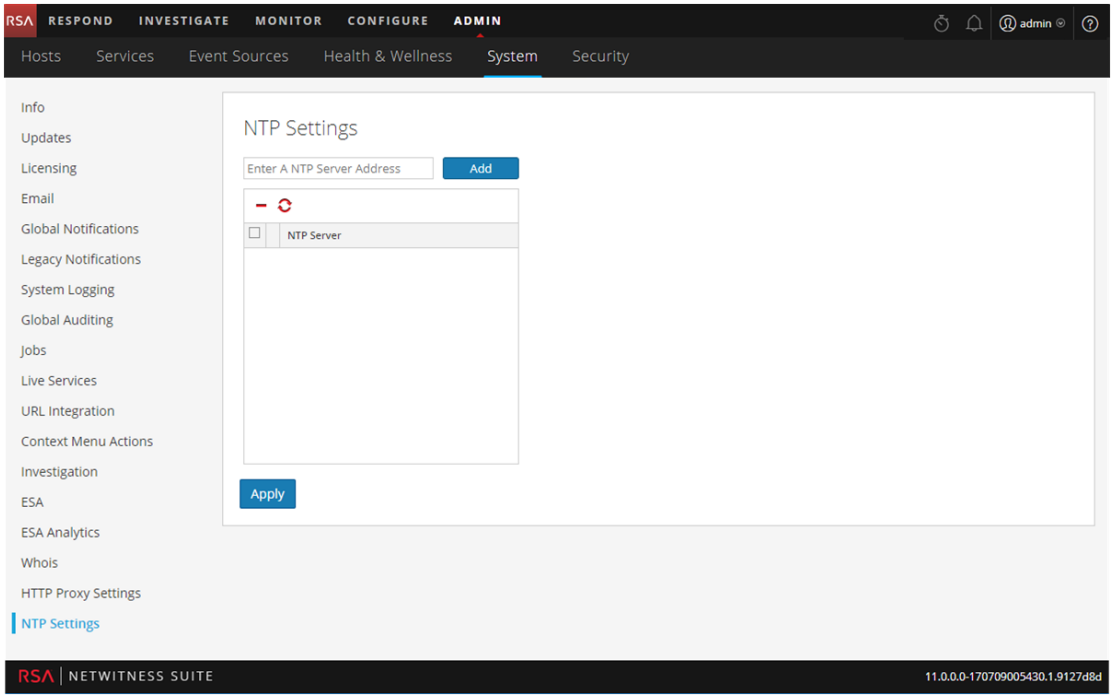
Sie können in der Ansicht **Administration** > **System** > **NTP-Einstellungen** einen oder mehrere NTP-Server konfigurieren. Nach der Konfiguration eines NTP-Servers verwendet NetWitness Suite NTP zum Synchronisieren der Uhrzeiten der Hostcomputer. Sie konfigurieren mehrere NTP-Server zwecks Failover. Dieses Kapitel enthält die folgenden Themen:

- Hinzufügen von NTP-Servern
- Ändern von NTP-Servern

Hinzufügen von NTP-Servern

So fügen Sie einen NTP-Server hinzu:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **NTP-Einstellungen** aus.
   Der Bereich „NTP-Einstellungen“ wird angezeigt, in dem Sie zur Eingabe des Hostnamens (d. h. der IP-Adresse oder des vollständig qualifizierten Domainnamens) eines NTP-Servers aufgefordert werden.



3. Geben Sie die IP-Adresse oder den vollständig qualifizierten Domainnamen eines NTP-Servers ein.
   Wenn die Syntax des Hostnamens ungültig ist, deaktiviert NetWitness Suite die

Schaltflächen **Hinzufügen** und **Anwenden** und die Meldung wird angezeigt, dass Sie **einen ungültigen Hostnamen eingegeben haben**.

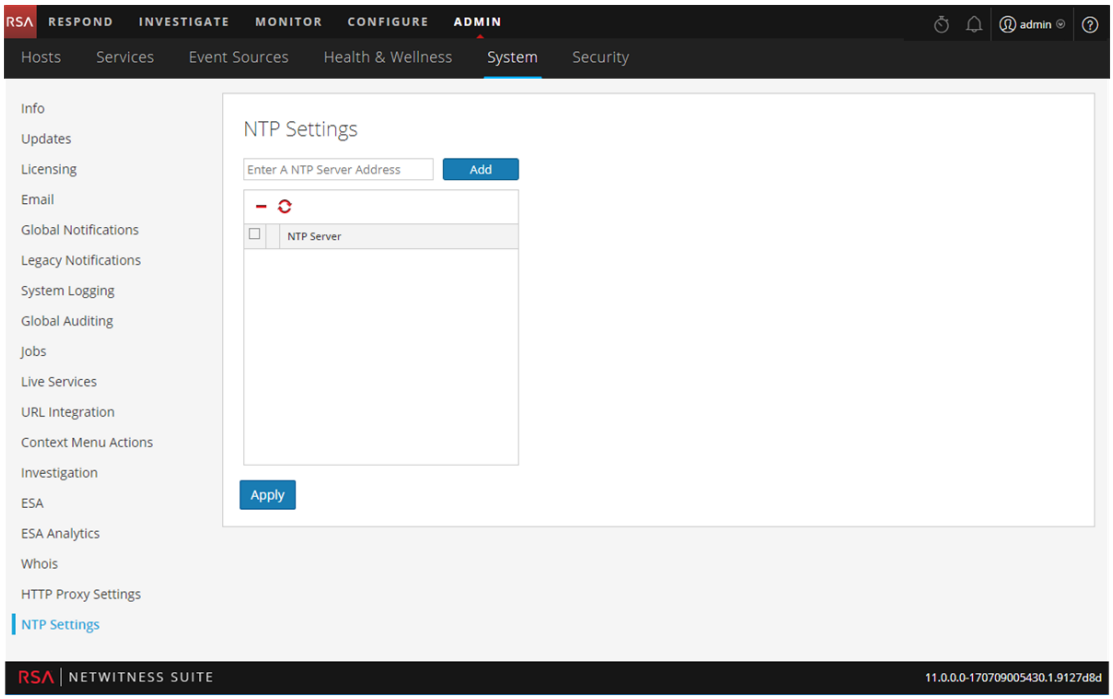
4. Klicken Sie auf **Add**.
   - Wenn die Syntax des Hostnamens gültig ist und NetWitness Suite den Server erreichen kann, wird die Meldung **Validieren** angezeigt.
   - Wenn die Syntax des Hostnamens gültig ist und NetWitness Suite einen Server nicht erreichen kann, wird die folgende Meldung angezeigt, wobei ***Hostname*** für den Hostnamen steht, den Sie hinzufügen wollten: **Der NTP-Server *Hostname* ist nicht erreichbar. Überprüfen Sie die Adresse und die Firewalleinstellungen.**
5. Klicken Sie auf **Anwenden**.
   Ein Dialogfeld zeigt die Benachrichtigung an, dass die Einstellungen gespeichert wurden, und fordert Ihre Bestätigung an, dass Sie die Einstellungen jetzt anwenden möchten.
6. Klicken Sie auf **Yes**.
   Der angegebene NTP-Server stellt nun sicher, dass die Uhrzeiten Ihres Hostcomputers synchronisiert sind. Wenn Sie mehrere NTP-Server konfigurieren möchten und ein Server ausgefallen ist, erfolgt in NetWitness Suite ein Failover zum nächsten konfigurierten Server.

Weitere Informationen über Parameter und ihre Beschreibungen erhalten Sie unter Bereich „NTP-Einstellungen“.

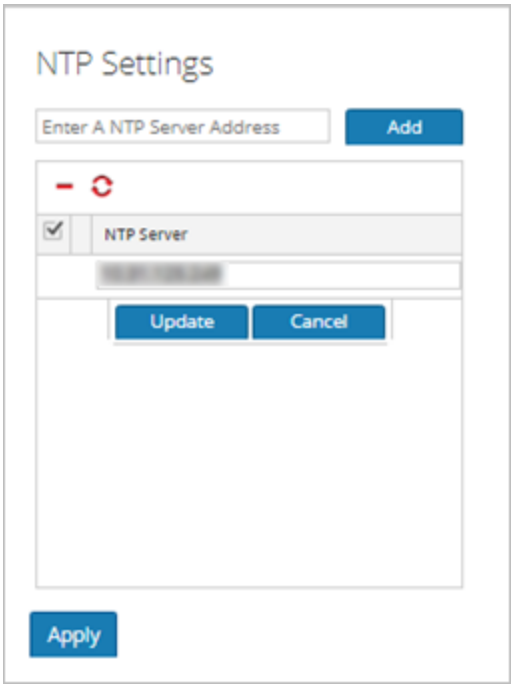
Ändern von NTP-Servern

So ändern Sie einen vorhandenen NTP-Server:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **NTP-Einstellungen** aus.
   Der Bereich „NTP-Einstellungen“ wird angezeigt.



3. Doppelklicken Sie auf den Hostnamen **NTP-Server**, den Sie ändern möchten.
   Das Textfeld „NTP-Server“ kann nun bearbeitet werden und die Schaltflächen „Aktualisieren“ und „Abbrechen“ werden angezeigt.



4. Bearbeiten Sie den Hostnamen, klicken Sie auf **Aktualisieren** und dann auf **Anwenden**. (Klicken Sie auf **Abbrechen**, bevor Sie auf **Anwenden** klicken, um die Bearbeitung abzubrechen.)
   NetWitness Suite ändert den Hostnamen entsprechend Ihren Bearbeitungen.

Dialogfeld „Neue Konfiguration hinzufügen“

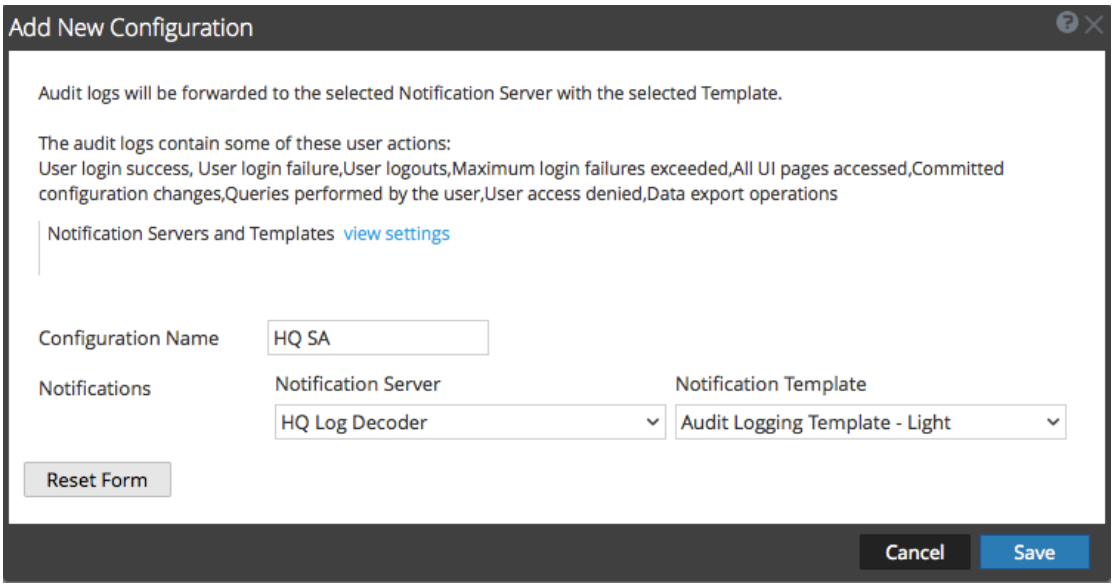
Im Bereich „Globale Auditprotokollierungskonfigurationen“ der Ansicht „Administration“ > „System“ von RSA NetWitness® Suite können mehrere globale Auditprotokollierungskonfigurationen erstellt werden. Diese Konfigurationen dienen dazu, bei der Durchführung von Benutzeraudits die globalen Auditprotokolle an einen zentralen Speicherort weiterzuleiten.

Beschreibungen zu Verfahren im Zusammenhang mit der globalen Auditprotokollierung finden Sie unter Konfigurieren der globalen Auditprotokollierung.

So rufen Sie das Dialogfeld **Neue Konfiguration hinzufügen** auf:

1. Wählen Sie in Hauptmenü **Admin > System** aus.
2. Wählen Sie im Bereich „Optionen“ die Option **Globales Auditing** aus.
3. Klicken Sie im Bereich **Globale Auditprotokollierungskonfigurationen** auf +.

   Das **Dialogfeld „Neue Konfiguration hinzufügen“** wird angezeigt.



Im Bereich Benachrichtigungen können Sie einen Syslog-Benachrichtigungsserver für die globale Auditprotokollierungskonfiguration sowie eine Vorlage für die globalen Auditprotokolle auswählen. In der Vorlage sind die Details der globalen Auditprotokolleinträge definiert.

Funktionen

In der folgenden Tabelle werden die Komponenten in den Dialogfeldern Neue Konfiguration hinzufügen und Konfiguration bearbeiten beschrieben.

Funktion	Beschreibung
Link **Einstellungen anzeigen** für Benachrichtigungsserver und Vorlagen	Hierüber gelangen Sie in den Bereich „Globale Benachrichtigungen“, in dem Sie die Einstellungen zum Benachrichtigungsserver und zu den Vorlagen ansehen und ändern können. Ein Syslog-Benachrichtigungsserver und eine Auditprotokollierungsvorlage müssen vorhanden sein, um eine globale Auditkonfiguration erstellen zu können.
Konfigurationsname	Gibt den eindeutigen Namen an, der zur Identifizierung der globalen Auditprotokollierungskonfiguration verwendet wird.
Benachrichtigungsserver	Gibt den Syslog-Benachrichtigungsserver zum Senden der ausgewählten Auditprotokollinformationen an. Unter Konfigurieren eines Ziels zum Empfang globaler Auditprotokolle finden Sie Anweisungen zum Erstellen eines Syslog-Benachrichtigungsservers für die globale Auditprotokollierung.

Funktion	Beschreibung
Benachrichtigungsvorlage	Gibt die Vorlage an, die für die globale Auditprotokollierungskonfiguration verwendet werden soll. Die Vorlage muss eine Auditprotokollierungsvorlage sein. Für Log Decoder verwenden Sie die **Audit-CEF-Standardvorlage**. Wenn bestimmte Anforderungen vorliegen, können Sie Felder zur CEF-Vorlage (Common Event Format) hinzufügen oder aus ihr entfernen. Im Abschnitt Definieren einer Vorlage für die globale Auditprotokollierung finden Sie weitere Erläuterungen. Für Syslog-Server von Drittanbietern können Sie eine Standard-Auditprotokollierungsvorlage verwenden oder Ihr eigenes Format (CEF oder nicht CEF) definieren. Entsprechende Anweisungen finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. Die verfügbaren Variablen werden im Abschnitt Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung beschrieben.
Schaltfläche **Formular zurücksetzen**	Löscht die Konfigurationseinstellungen im Dialogfeld.

Protokollierte Benutzeraktionen

Die folgende Tabelle enthält einige Beispiele für Benutzeraktionen, die von NetWitness Suite protokolliert werden. Mindestens diese Benutzeraktionen werden gegebenenfalls protokolliert.

Benutzeraktion	Beispiel
Erfolgreiche Benutzeranmeldung	Ein Benutzer meldet sich mit gültigen Anmeldeinformationen an.
User login failure	Ein Benutzer versucht, sich mit ungültigen Anmeldeinformationen anzumelden.

Benutzeraktion	Beispiel
Benutzerabmeldungen	Ein Benutzer meldet sich von NetWitness Suite ab („Administration“ „Abmelden“) oder wird wegen Überschreitung der maximalen Sitzungszeit abgemeldet.
Max. Anmeldungsfehler überschritten	Ein Benutzer hat fünfmal versucht, sich mit ungültigen Anmeldeinformationen anzumelden. Die Zahl 5 ist unter Max. Anmeldungsfehler auf der Registerkarte Einstellungen der Ansicht Administration > Sicherheit definiert (Administration > Sicherheit > Einstellungen).
Alle aufgerufenen Seiten der Benutzeroberfläche	Wenn ein Benutzer das Reporting-Modul aufruft („Administration“ > „Berichte“), wird dies als `[REP] Reports` protokolliert. Ruft ein Benutzer die Ansicht „System“ des Moduls Administration auf („Administration“ > „System“), wird dies als `[ADM] System` protokolliert.
Gespeicherte Konfigurationsänderungen	Ein Benutzer ändert sein Passwort und/oder eine andere Sicherheitseinstellung (Registerkarte Administration > Sicherheit > Einstellungen).
Vom Benutzer durchgeführte Abfragen	Ein Benutzer führt eine Investigation-Abfrage durch.
Verweigerte Benutzerzugriffe	Ein Benutzer versucht, auf ein Modul zuzugreifen, besitzt jedoch nicht die erforderlichen Berechtigungen.
Datenexportvorgänge	Ein Benutzer exportiert von der Ansicht Ereignisse aus Daten (Investigation > Ereignisse > Aktionen > Exportieren).

Listen der Meldungstypen, die von den verschiedenen NetWitness Suite-Komponenten protokolliert werden, finden Sie in der Referenz der globalen Auditprotokollierungsvorgänge.

Unterstützte CEF-Metaschlüssel

In diesem Thema werden die CEF (Common Event Format)-Metaschlüssel beschrieben, die NetWitness Suite globale Auditprotokollierung unterstützt.

Globale Auditprotokollierungsvorlagen, die Sie für einen Log Decoder definieren, verwenden CEF (Common Event Format) und müssen die folgenden spezifischen Standardanforderungen erfüllen:

- Die CEF-Header müssen in der Vorlage enthalten sein.
- Es dürfen nur die Erweiterungen und angepassten Erweiterungen in einem (Schlüssel=Wert)-Format aus der untenstehenden Metaschlüsseltabelle verwendet werden.
- Es muss sichergestellt werden, dass die Erweiterungen und benutzerdefinierten Erweiterungen das Format `key=${string}<space>key=${string}` haben.

Für Syslog-Server von Drittanbietern können Sie Ihr eigenes Format (CEF oder Nicht-CEF) definieren.

Beschreibungen zu Verfahren im Zusammenhang mit dieser Tabelle finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung und Konfigurieren der globalen Auditprotokollierung.

Unterstützte CEF-Metaschlüssel

In der folgenden Tabelle werden die CEF-Syslog-Metaschlüssel beschrieben, die von der globalen Auditprotokollierung von NetWitness Suite unterstützt werden. Die Felder „Datum/Uhrzeit“ und „Hostname“ im Syslog-Präfix sind nicht konfigurierbar und in der Vorlage nicht enthalten, aber sie stehen standardmäßig am Anfang jeder Protokollmeldung. Der CEF-Header ist erforderlich, um den CEF-Standard zu erfüllen, und auch jeder CEF-Parser erfordert den CEF-Header. Die Erweiterungen und benutzerdefinierten Erweiterungen sind optional. Die Audit-CEF-Standardvorlage enthält viele der Felder in dieser Tabelle. Sie können jede der aufgeführten Erweiterungen und angepassten Erweiterungen der globalen Auditprotokollierungsvorlage, die Sie definieren, hinzufügen.

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
Syslog-Präfix				

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
Datum/Uhrzeit	Nicht konfigurierbar	Syslog-Header Datum/Uhrzeit	event.time.str	Vorübergehend
Hostname	Nicht konfigurierbar	Syslog-Header Hostname	alias.host	Keiner
CEF-Header		Die Felder im CEF-Header sind erforderlich, um dem CEF-Standard zu entsprechen, und auch jeder CEF-Parser erfordert sie.		
CEF:Version	CEF:0	CEF-Header	--STATISCH--	-
DeviceVendor	${deviceVendor}	Der Anbieter des Produkts, RSA	-	-
DeviceProduct	${deviceProduct}	Die Produktreihe. Dies ist immer NetWitness Suite Audit.	Produkt	Vorübergehend
DeviceVersion	${deviceVersion}	Host-/Service-Version	version	Vorübergehend

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
Signatur-ID	${category}	Kennung des Auditereignisses. Sie spezifiziert die Kategorie des Auditereignisses.	event.type	Keiner
Name	${operation}	Beschreibung des Ereignisses	event.desc	Keiner
Schweregrad	${severity}	Schweregrad des Auditereignisses	severity	Vorübergehend
Erweiterungen				
deviceExternalId	${deviceExternalId}	Eindeutige ID des Hosts oder Services, der das Auditereignis erzeugt	hardware.id	Vorübergehend
deviceFacility	${deviceFacility}	Die Syslog-Facility, die verwendet wird, wenn das Ereignis auf den Syslog-Daemon geschrieben wird. Beispiel: authpriv.	cs.devfacility	Custom

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
deviceProcessName	${deviceProcessName}	Name der ausführbaren Datei, die dvcpid entspricht	process	Keiner
dpt	${destinationPort}	Zielport	ip.dstport	Keiner
dst	${destinationAddress}	Ziel-IP-Adresse	ip.dst	Keiner
dvcpid	${deviceProcessId}	ID des Prozesses, der das Ereignis erzeugt, d. h. die Prozess-ID des NetWitness Suite-Services	process.id	Vorübergehend
msg	${text}	Freier Text, zusätzliche Information oder tatsächliche Beschreibung des Ereignisses	msg	Vorübergehend
outcome	${outcome}	Ergebnis der durchgeführten Operation, die dem Auditereignis entspricht	result	Vorübergehend

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
proto	${transportProtocol}	Verwendetes Netzwerkprotokoll	protocol	Vorübergehend
requestClientApplication	${userAgent}	Browserinformationen zum Benutzer, der auf die Seite zugreift	user.agent	Vorübergehend
rt	${timestamp}	Zeitpunkt, zu dem das Ereignis berichtet wird	event.time	Keiner
sourceServiceName	${sourceService}	Der Service, der für die Erzeugung dieses Ereignisses verantwortlich ist	service.name	Vorübergehend
spt	${sourcePort}	Quellport	ip.srcport	Vorübergehend

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
spriv	${userRole}	Benutzerrollen-Berechtigungszuordnung. Zum Beispiel: admin.owner, appliance.manage, connections.manage, everyone, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	Berechtigung	Vorübergehend
src	${sourceAddress}	Quell-IP-Adresse	ip.src	Keiner
suser	${Identity}	Identität des angemeldeten Benutzers, der für die Erzeugung des Auditereignisses verantwortlich ist	user.dst	Keiner
Benutzerdefinierte Erweiterungen				

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
deviceService	${deviceService}	Service, der für die Erzeugung des Ereignisses verantwortlich ist	cs.devservice	Custom
Parameter	${parameters}	API- und Operationsparameter, die spezifische Parameter über eine Frage erfassen	Index	Vorübergehend
paramKey	${key}	Ein Configuration-Item-Schlüssel. Das ist der Konfigurationsparameter, für den das Auditereignis erfasst wird. Beispiel: /sys/config/stat.interval	cs.key	Custom
paramValue	${value}	Ein Konfigurationswert. Das ist der während der Aktualisierung erfasste Wert.	cs.value	Custom

CEF-Feld	Zeichenfolge	Beschreibung	NW-Metaschlüssel	Index in Log Decoder
userGroup	${userGroup}	Rollenzuweisung. Beispiel: Administratoren, Analysten, MalwareAnalysten, Malware_ Analysten, Operatoren, PRIVILEGED_ CONNECTION_ AUTHORITY, SOC_Manager	Gruppe	Keiner
referrerURL	${referrerUrl}	Die übergeordnete URL, die sich auf die aktuelle URL bezieht	URL	Vorübergehend
sessionId	${sessionId}	Sitzungs- oder Verbindungskennung	log.session.id	Vorübergehend

Hinweis: Verwenden Sie alle Erweiterungen im folgenden Format:
`deviceProcessName=${deviceProcessName} outcome=${outcome}`
Verwenden Sie ein `<space>` zwischen einem Wert und einem Tagnamen.

Standardmäßig werden keine Metaschlüssel indiziert. In der obigen Tabelle zeigt die Spalte **Index in Log Decoder** den Zustand des Schlüsselworts `flags` („Vorübergehend“, „Keine“ und „Benutzerdefiniert“). Wenn ein Schlüssel auf `Transient` eingestellt ist, wird er geparst, aber nicht in der Datenbank gespeichert. Wenn er auf `None` eingestellt ist, wird er indiziert und in der Datenbank gespeichert. Ein Schlüssel, der als „Benutzerdefiniert“ aufgeführt ist, existiert nicht in der Datei table-map.xml und wird daher gar nicht gespeichert oder geparst.

Anweisungen zum Überprüfen und Aktualisieren der Tabellenzuordnungen finden Sie unter „Pflegen der Tabellenzuordnungsdateien“. Informationen zum Aktualisieren der angepassten Indexdatei auf dem Concentrator finden Sie unter „Bearbeiten einer Serviceindexdatei“.

Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung

In diesem Thema werden die Metaschlüsselvariablen beschrieben, die von der globalen Auditprotokollierung von NetWitness Suite unterstützt werden.

NetWitness Suite stellt vordefinierte Vorlagen für die globale Auditprotokollierung bereit, die Sie für die Konfiguration Ihrer globalen Auditprotokollierung verwenden können. Für Syslog-Server von Drittanbietern können Sie mithilfe von unterstützten Metaschlüsselvariablen Ihr eigenes Vorlagenformat (CEF oder nicht CEF) definieren.

Beschreibungen zu Verfahren im Zusammenhang mit dieser Tabelle finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung und Konfigurieren der globalen Auditprotokollierung.

Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung

Die folgende Tabelle beschreibt die Metaschlüsselvariablen, die die globale Auditprotokollierung von NetWitness Suite unterstützt. Verwenden Sie diese Werte, um eine angepasste Vorlage für die Auditprotokollierung für einen Syslog-Server eines Drittanbieters zu erstellen.

Variable	Beschreibung
${category}	Kennung des Auditereignisses. Sie spezifiziert die Kategorie des Auditereignisses.
${destinationAddress}	Ziel-IP-Adresse
${destinationPort}	Zielport
${deviceExternalId}	Eindeutige ID des Services, der das Auditereignis erzeugt
${deviceFacility}	Die Syslog-Facility, die verwendet wird, wenn das Ereignis auf den Syslog-Daemon geschrieben wird. Beispiel: authpriv.
${deviceProcessId}	ID des Prozesses, der das Ereignis erzeugt, d. h. die Prozess-ID des NetWitness Suite-Services
${deviceProcessName}	Name der ausführbaren Datei, die dvcpid entspricht
${deviceProduct}	Die Produktreihe. Dies ist immer NetWitness Suite Audit.

Variable	Beschreibung
${deviceService}	Service, der für die Erzeugung des Ereignisses verantwortlich ist
${deviceVendor}	Der Anbieter des Produkts, RSA
${deviceVersion}	Host-/Service-Version
${identity}	Identität des angemeldeten Benutzers, der für die Erzeugung des Auditereignisses verantwortlich ist
${key}	Ein Configuration-Item-Schlüssel. Das ist der Konfigurationsparameter, für den das Auditereignis erfasst wird.
${operation}	Beschreibung des Ereignisses
${outcome}	Ergebnis der durchgeführten Operation, die dem Auditereignis entspricht
${parameters}	API- und Operationsparameter, die spezifische Parameter über eine Frage erfassen
${referrerUrl}	Die übergeordnete URL, die sich auf die aktuelle URL bezieht
${Sitzungs-ID},	Sitzungs- oder Verbindungskennung
${severity}	Schweregrad des Auditereignisses
${sourceAddress}	Quell-IP-Adresse
${sourcePort}	Quellport
${sourceService}	Der Service, der für die Erzeugung dieses Ereignisses verantwortlich ist
${text}	Freier Text, zusätzliche Information oder tatsächliche Beschreibung des Ereignisses
${timestamp}	Zeitpunkt, zu dem das Ereignis berichtet wird
${transportProtocol}	Verwendetes Netzwerkprotokoll

Variable	Beschreibung
${userAgent}	Browserinformationen zum Benutzer, der auf die Seite zugreift
${userGroup}	Rollenzuweisung
${userRole}	Benutzerrollen-Berechtigungszuordnung
${value}	Ein Konfigurationswert. Das ist der während der Aktualisierung erfasste Wert

Referenz der globalen Auditprotokollierungsvorgänge

In diesem Thema werden die Meldungstypen aufgelistet, die von den verschiedenen NetWitness Suite-Komponenten protokolliert werden. Die meisten Meldungen geben einfach den protokollierten Vorgang an, gegebenenfalls wird auch die Bedeutung der Meldung erläutert.

Nachdem Sie eine globale Auditprotokollierungskonfiguration erstellt haben, gehen Auditprotokolle automatisch in das externe Syslog-System ein. Dabei wird das Format verwendet, das in der ausgewählten Auditprotokollierungsvorlage angegeben wurde. Die Meldungstypen, die von den verschiedenen NetWitness Suite-Komponenten protokolliert werden, sind in den folgenden Tabellen aufgeführt.

CARLOS

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von CARLOS protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	SetProviderConfiguration	Ein neuer Benachrichtigungsserver (z. B. SMTP-Server) wurde hinzugefügt oder aktualisiert.
2	SetInstanceConfiguration	Ein neuer Benachrichtigungstyp (z. B E-Mail-Ziel) wurde hinzugefügt oder aktualisiert.
3	SetTemplateDefinition	Eine neue Vorlage wurde hinzugefügt oder aktualisiert.
4	RemoveProviderConfiguration	Ein Benachrichtigungsserver wurde entfernt.
5	RemoveInstanceConfiguration	Ein Benachrichtigungstyp wurde entfernt.
6	RemoveTemplateDefinition	Eine Vorlagendefinition wurde entfernt.

Seriennummer	Vorgangsname	Bedeutung
7	Commit	Die Änderung eines Konfigurations-Bean wurde festgeschrieben.
8	Einstellen	Ein JMX-Eigenschaftswert wurde über die NetWitness Suite-Ansicht „Durchsuchen“ festgelegt.

ESA

In der folgenden Tabelle sind die Vorgänge aufgelistet, die von Event Stream Analysis (ESA) protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
9	SetSourceRequest	Ein Concentrator wurde ESA als Quelle hinzugefügt oder aktualisiert.
10	RemoveSourceRequest	Ein Concentrator wurde als Quelle aus ESA entfernt.
11	SetEplModule	Ein EPL-Modul wurde in ESA bereitgestellt oder aktualisiert.
12	RemoveEplModule	Ein EPL-Modul wurde aus ESA entfernt.
13	SetEnrichmentSourceRequest	Eine ESA-Erweiterungsquelle wurde hinzugefügt/aktualisiert.
14	RemoveEnrichmentSourceRequest	Eine ESA-Erweiterungsquelle wurde entfernt.

Seriennummer	Vorgangsname	Bedeutung
15	SetDatabaseReference	Ein Erweiterungsdatenbankverweis auf ESA wurde vorgenommen.
16	UpdateEnrichmentData	Datenzeilen wurden einer ESA-Erweiterungsquelle hinzugefügt.
17	SetEnrichmentConnection	Zwischen einem EPL-Modul und einer Erweiterungsquelle wurde eine Verbindung hergestellt.
18	RemoveEnrichmentConnection	Eine Verbindung zwischen einem EPL-Modul und einer Erweiterungsquelle wurde entfernt.
19	DisableTrialModule	ESA-Testregeln wurden deaktiviert.

Investigation

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von Investigations protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	VisualizePreferences	Vorgänge in Bezug auf die Informer-Visualisierungsanforderung
2	ParallelCoordinates	Vorgänge in Bezug auf das Laden von Navigation in der Koordinationsansicht
3	TimeLine	Vorgänge in Bezug auf das Laden der Navigation in der Zeitachsenansicht

Seriennummer	Vorgangsname	Bedeutung
4	ExternalQuery	Vorgang, wenn eine Direktabfrage über URL ausgelöst wird
5	PrintView	Vorgänge zum Öffnen von Investigation in der Druckansicht
6	submitExtractFiles	Vorgang zum Senden einer Anforderung zum Extrahieren von Dateien aus Sitzungen
7	submitExtractLogs	Vorgang zum Senden einer Anforderung zum Extrahieren von Protokollen aus Sitzungen
8	submitExtractPcap	Vorgang zum Senden einer Anforderung zum Extrahieren von Sitzungen aus -Sitzungen
9	DataScienceDrill	Vorgang zum Untersuchen eines Data Science-Berichts
10	breadCrumbs	Vorgang zum Zugreifen auf die Abfrage-Breadcrumbs
11	Create	Vorgang, wenn eine neue Investigation-Abfrage als -Prädikat für die Verwendung zur URL-Integration gespeichert wird
12	userPredicates	Vorgang zum Zugreifen auf zuletzt verwendete Abfragen eines Benutzers

Seriennummer	Vorgangsname	Bedeutung
13	chartDefaultMetas	Vorgang zum Zugreifen auf zuletzt verwendete Metadaten für die Erzeugung des -Koordinatendiagramms
14	defaultDevice	Vorgang zum Zugreifen auf das Standard-Investigation-Gerät
15	deleteDefaultDevice	Vorgang zum Löschen des Standard-Investigation-Geräts
16	chartPreferences	Vorgang zum Bearbeiten eines Investigation-Navigationsdiagrammparameters , z. B. „Höhe“
17	devicePreferences	Vorgang, zum Speichern der Einstellungen zum Investigation-Gerät, z. B. „Zeitbereich“, „Profil“, „Metagruppen“ usw.
18	topValues	Vorgang zum Abrufen der Top-Werte für Metadaten. In der Regel über das Dashlet „Top-Werte“ aufgerufen
19	MetaLanguages	Vorgang zum Lesen der Metasprachen von einem Gerät
20	MetaGroups	Vorgänge in Bezug auf Investigation-Metagruppen
21	DefaultMetaKeys	Vorgänge in Bezug auf Investigation-Standardmetaschlüssel

Seriennummer	Vorgangsname	Bedeutung
22	UpdateDefaultMetaKeys	Vorgänge zur Aktualisierung von Investigation-Standardmetaschlüsseln
23	UpdateMetaGroup	Vorgänge zur Aktualisierung von Investigation-Metagruppen
24	ApplyMetaGroup	Vorgänge zur Verwendung von Investigation-Metagruppen
25	DeactivateMetaGroup	Vorgänge zum Zurücksetzen von Investigation-Metagruppen in der Benutzeroberfläche
26	DeleteMetaGroup	Vorgänge zum Entfernen einer Investigation-Metagruppe
27	DeleteMetaGroups	Vorgänge zum Entfernen mehrerer Investigation-Metagruppen
28	ImportMetaGroups	Vorgänge zum Importieren von Investigation-Metagruppen
29	ExportMetaGroup	Vorgänge zum Exportieren mehrerer Investigation-Metagruppen
30	GeoMap	Vorgang zum Zugreifen auf die Geomap-Ansicht von Investigation
31	deleteEndpointCache	Vorgang zum Löschen des Rekonstruktionscaches eines Geräts
32	delete	Vorgang zum Löschen von Warnmeldungsvorlagen

Seriennummer	Vorgangsname	Bedeutung
33	CustomColumnGroup	Vorgang zum Anwenden oder Lesen einer benutzerdefinierten Spaltengruppe
34	Import	Vorgänge in Bezug auf das Importieren von Spaltengruppen oder Profilen
35	Export	Vorgänge in Bezug auf das Exportieren von Spaltengruppen oder Profilen
36	SaveProfile	Vorgang zum Speichern eines Investigation-Profils
37	ApplyProfile	Vorgang zum Anwenden eines Investigation-Profils
38	DeactivateProfile	Vorgang zum Deaktivieren eines Investigation-Profils
39	DeleteProfile	Vorgang zum Löschen eines Investigation-Profils
40	DeleteProfiles	Vorgang zum Löschen mehrerer Investigation-Profile

Reporting Engine

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von der Reporting Engine protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	TEMPLATE	Für alle Vorgänge in Bezug auf eine Vorlage

Seriennummer	Vorgangsname	Bedeutung
2	CHART	Für alle Vorgänge in Bezug auf ein Diagramm
3	REPORT	Für alle Vorgänge in Bezug auf einen Bericht
4	RULE	Für alle Vorgänge in Bezug auf eine Regel
5	IMAGE	Für alle Vorgänge in Bezug auf die in Berichten verwendeten Logobilder
6	LIST	Für alle Vorgänge in Bezug auf eine Liste
7	ALERT	Für alle Vorgänge in Bezug auf eine Warnmeldung
8	CONFIG	Für alle Vorgänge in Bezug auf eine Konfigurationsänderung
9	SCHEDULE	Für alle Vorgänge in Bezug auf eine Planung
10	ROLE	Für alle Vorgänge in Bezug auf eine Rolle/Autorisierung
11	BATCH_JOB	Für alle Vorgänge in Bezug auf Batchjobs
12	SCHEDULER	Für alle Vorgänge in Bezug auf einen Planer
13	QUERYPROCESSOR	Für alle Vorgänge in Bezug auf einen Abfrageprozessor

Seriennummer	Vorgangsname	Bedeutung
14	FORMATTER	Für alle Vorgänge in Bezug auf einen Formatierer
15	OUTPUTACTION	Für alle Vorgänge in Bezug auf eine Ausgabeaktion
16	STATUSMANAGER	Für alle Vorgänge in Bezug auf einen Statusmanager
17	BATCH_RUNDEF	Für alle Vorgänge in Bezug auf eine Batchausführungsdefinition
18	CHARTGROUP	Für alle Vorgänge in Bezug auf eine Diagrammgruppe
19	REPORTGROUP	Für alle Vorgänge in Bezug auf eine Berichtgruppe
20	RULEGROUP	Für alle Vorgänge in Bezug auf eine Regelgruppe
21	LISTGROUP	Für alle Vorgänge in Bezug auf eine Listengruppe
22	DISKSPACE	Für alle Vorgänge in Bezug auf Speicherplatz

Warehouse Connector

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von Warehouse Connector protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	LockBox Password Create	Vorgang zum Erstellen des LockBox-Passworts

Seriennummer	Vorgangsname	Bedeutung
2	LockBox Password Update	Vorgang zum Aktualisieren des LockBox-Passworts
3	LockBox Password Refresh	Vorgang zum Aktualisieren des LockBox-Passworts
4	Adding Stream	Vorgang zum Hinzufügen eines Streams
5	Adding Source	Vorgang zum Hinzufügen einer Quelle
6	Adding Destination	Vorgang zum Hinzufügen eines Ziels
7	Removing	Vorgang zum Entfernen einer Quelle, eines Streams oder eines Ziels
8	Changing Password	Vorgang zum Ändern des Passworts
9	Updating Source	Vorgang zum Aktualisieren der Quelle
10	Adding Source to Stream	Vorgang zum Hinzufügen einer Quelle zu einem Stream
11	Deleting Source from Stream	Vorgang zum Löschen einer Quelle aus einem Stream
12	Setting Destination to Stream	Vorgang zum Festlegen eines Ziels auf einen Stream

Seriennummer	Vorgangsname	Bedeutung
13	Finalizing Stream	Vorgang zum Fertigstellen eines Streams und Initiieren der Aggregation
14	Stopping Stream	Vorgang zum Beenden eines Streams
15	Starting Stream	Vorgang zum Starten eines Streams
16	Reloading Stream	Vorgang zum Neuladen eines Streams

Integrität und Zustand

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von Integrität und Zustand protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	SavePolicyRequest	Vorgang beim Hinzufügen oder Ändern einer Policy
2	RemovePolicyRequest	Vorgang beim Entfernen einer Policy

NetWitness Suite Core-Services

In der folgenden Tabelle sind die Vorgänge aufgeführt, die von den NetWitness Suite Core-Services protokolliert werden.

Serial #	Vorgangsname	Bedeutung
1	FILE-Command	Vorgang zum Auflisten, Abrufen und Löschen von Dateien aus genehmigten Verzeichnissen auf diesem Gerät
2	SERVICE-Start	Service gestartet

Serial #	Vorgangsname	Bedeutung
3	SERVICE-Stop	Service beendet
4	REDIRECT-Syslog	Vorgang zur Syslog-Weiterleitung
5	ADD-Monitor	Ausgabe eines Vorgangs zur Dateisystemüberwachung
6	DELETE-Monitor	Ausgabe eines Löschvorgangs zur Dateisystemüberwachung
7	SHUTDOWN-Service/shutdown.service	Stoppen eines Appliance-Service
8	REBOOT-Service	Neustarten eines Appliance-Service
9	CONFIGURE-Network	Ausgabe einer Netzwerkkonfigurationsänderung
10	SET-NTP	Ausgabe eines Vorgangs zur NTP-Festlegung
11	STOP-NTP	Ausgabe eines Vorgangs zur NTP-Beendigung
12	NTP-Timesync	Ausgabe eines Vorgangs zur NTP-Zeitsynchronisierung
13	SET-SNMP	Ausgabe einer SNMP-Festlegung
14	UPGRADE/upgrade	Ausgabe eines Upgradevorgangs
15	create.collection	Vorgang zum Erstellen einer leeren Sammlung
16	restore	Ausgabe einer Wiederherstellung
17	session.aggregation	Ausgabe eines Aggregationsstarts/-stopps

Serial #	Vorgangsname	Bedeutung
18	add.device	Hinzufügen eines Geräts zur Aggregation
19	edit.device	Bearbeitung eines zur Aggregation verwendeten Geräts
20	delete.device	Löschung eines zur Aggregation verwendeten Geräts
21	capture.start	Start eines Erfassungsvorgangs
22	capture.stop	Stopp eines Erfassungsvorgangs
23	select.interface	Auswählen einer Erfassungsschnittstelle
24	export	Vorgang zum Exportieren von Paketen oder Sitzungen
25	reload	Ausgabe des erneute Ladevorgangs eines Parsers
26	schema	Ausgabe einer Schemaanforderung für geladene Parser
27	upload/file.upload	Ausgabe eines Dateiuploads
28	notify	Ausgabe einer Feedbenachrichtigung
29	delete	Ausgabe einer Dateilöschung
30	edit.config	Vorgang zur Konfigurationsänderung
31	parsers.transforms	Durchführung einer Sprachschlüsseltransformation
32	data.reset	Vorgang zur Datenzurücksetzung
33	timeout	REST-Anforderungs-Timeout
34	Abbrechen	Abbrechen einer laufenden Abfrage

Serial #	Vorgangsname	Bedeutung
35	timeroll	Vorgang zum Löschen der Datenbankdateien, die eine bestimmte Grenze überschreiten
36	dump	Vorgang zum Erstellen eines Speicherauszugs von Informationen aus der Datenbank in Dateien im NWD-Format
37	session.wipe	Ausgabe eines Vorgangs zum Sitzungs-Wipe
38	REPLACE-Rule	Ausgabe eines Vorgangs zur Regelersetzung
39	MERGE-Rule	Ausgabe eines Vorgangs zur Regelzusammenführung
40	ERASE-Rule	Ausgabe einer Löschung eines Satzes aller Regeln
41	ADD-Rule	Ausgabe eines Vorgangs zur Regelhinzufügung
42	DELETE-Rule	Ausgabe einer Löschung eines Regelsatzes
43	sdk.info	Ausgabe einer SDK-Zusammenfassungsinformation
44	sdk.session	Ausgabe einer SDK-Sitzungsinformation
45	sdk.language	Ausgabe einer SDK-Sprache
46	sdk.aliases	Ausgabe einer SDK-Aliasanforderung

Serial #	Vorgangsname	Bedeutung
47	sdk.transform	Ausgabe einer SDK-Transformationsanforderung
48	sdk.search	Ausgabe einer Suchanforderung für Sitzungsinhalt
49	sdk.cache	Vorgang in Bezug auf Sitzungsinhaltscache
50	sdk.content	Ausgabe einer Sitzungsinhaltsanforderung
51	check.authorization	Vorgang zum Überprüfen von Benutzerrollen auf Berechtigungen zum Ausführen eines Vorgangs
52	close.connection	Ausgabe eines Vorgangs zur Verbindungsschließung
53	handshake	Ausgabe eines SSL-Handshake
54	logon/login	Vorgang zum Anmelden bei anderen Services aus SA, hauptsächlich für privilegierte Benutzer
55	STOREDPROCOP	Ausgabe eines Abbruchs/Starts eines Dateiuploads
56	ADD-Task	Geplante Aufgabe hinzugefügt
57	DELETE-Task	Geplante Aufgabe gelöscht
58	logoff	Ausgabe eines Abmeldevorgangs
59	list.cacerts	Ausgabe eines Vorgangs zur Auflistung vertrauenswürdiger CA-Zertifikate

Serial #	Vorgangsname	Bedeutung
60	delete.cacerts	Ausgabe eines Vorgangs zur Löschung vertrauenswürdiger CA-Zertifikate
61	add.cacerts	Ausgabe eines Vorgangs zur Hinzufügung vertrauenswürdiger CA-Zertifikate
62	restart.command	Ausgabe einer Neustart-Befehlszeilenoption
63	delete.file/file.delete	Vorgang zum Löschen von Systemkonfigurationsdateien
64	update.file/file.update	Vorgang zum Aktualisieren der Systemkonfigurationsdatei
65	create.file	Ausgabe eines Vorgangs zur Dateierstellung
66	query	Ausgabe einer Datenbankabfrage
67	unlock	Ausgabe eines Vorgangs zur Entsperrung eines Benutzerkontos
68	user.add	Vorgang zum Erstellen von Benutzerkonten auf einzelnen Geräten
69	user.delete	Vorgang zum Löschen eines Benutzers auf einzelnen Geräten
70	group.create	Vorgang zum Hinzufügen einer neuen Gruppe zum System
71	user.remove	Entfernen eines Benutzerkontos aus einer Gruppe
72	group.delete	Löschen einer Gruppe aus der /Benutzer/Gruppen-Baumstruktur

Serial #	Vorgangsname	Bedeutung
73	add.user	Ausgabe eines Befehls, mit dem der Sammlung ein Benutzer hinzugefügt wird
74	delete.user	Ausgabe eines Befehls, mit dem ein Benutzer aus der Sammlung gelöscht wird
75	remove.user	Entfernen eines Benutzers aus einer Sammlung
76	collection.open	Ausgabe eines Öffnungsbefehls für eine Sammlung
77	collection.close	Ausgabe eines Schließbefehls für eine Sammlung
78	collection.delete	Ausgabe eines Befehls zum Löschen einer Sammlung
79	reingest.start	Vorgang zur erneuten Aufnahme von Paketdaten in der Sammlung
80	feed.notify	Ausgabe eines Befehls zur Feedbenachrichtigung
81	collect	Ausgabe eines Sammlungsbefehls
82	collect.start	Ausgabe eines Datensammlungsstarts
83	collection.global	Ausgabe eines Befehls zum Parserimport
84	parser.reload	Ausgabe eines Befehls zum erneuten Laden eines Parsers
85	reingest	Vorgang zur erneuten Aufnahme von Paketdaten in der Sammlung

Serial #	Vorgangsname	Bedeutung
86	collection.create	Ausgabe eines Befehls zum Erstellen einer Sammlung
87	collection.restore	Ausgabe eines Befehls zum Wiederherstellen einer Sammlung
88	collection.clone	Ausgabe eines Befehls zum Klonen einer Sammlung
89	parser.reload	Ausgabe eines Befehls zum erneuten Laden eines Parsers
90	sdk.query	Durchführung einer Abfrage der Metadatenbank
91	sdk.msearch	Suche nach Musterentsprechungen in zahlreichen Sitzungen oder Paketen
92	sdk.values	Durchführung einer Wertanzahlabfrage und Rückgabe der entsprechenden Werte für einen Bericht
93	sdk.timeline	Rückgabe der Anzahl der Sitzungen/Größe/Pakete in diskreten Zeitintervallen

Malware Analysis

In der folgenden Tabelle sind die Vorgänge aufgelistet, die von der Komponente Malware Analysis (MA) protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	GetDashBoardSummaryRequest	Dashboard-Analysestatistik abrufen

Seriennummer	Vorgangsname	Bedeutung
2	GetFileScoreSummaryRequest	Aggregierte Dateibewertungen nach Bewertungstyp und Risikoniveau abrufen
3	CountEventsAndFilesRequest	Anzahl der Ereignisse und Dateien in einem Zeitrahmen abrufen
4	GetAvVendorDetectionRequest	AV-Anbieteranalyseergebnisse abrufen
5	GetAVVendorsRequest	Liste der unterstützten AV-Anbieter abrufen
6	SetInstalledAVVendors	Aktualisierung der Liste der installierten AV-Anbieter in Konfiguration anfordern
7	CountEventByCriteriaRequest	Ereignisse nach Kriterien zählen
8	FindEventByIdRequest	Ereignis nach ID abrufen
9	FindEventByCriteriaRequest	Ereignis nach Kriterien abrufen
10	DeleteEventRequest	Ereignis löschen
11	CommentOnEventRequest	Kommentar zum Ereignis hinzufügen
12	ReSubmitEventRequest	Ereignis erneut zur Analyse absenden
13	FindEventScoreByIdRequest	Ereignisbewertung nach Ereignis-ID abrufen

Seriennummer	Vorgangsname	Bedeutung
14	FindEventScoreByCriteriaRequest	Ereignisbewertung nach Kriterien abrufen
15	FindMetaByIdRequest	Meta nach ID abrufen
16	FindMetaByCriteriaRequest	Meta nach Kriterien abrufen
17	FindMetaValueByCriteriaRequest	Metawert nach Kriterien abrufen
18	CountByDistinctMetaValueRequest	Spezifische Metawerte zählen
19	CountByMetaNameAndValueWithDate RangeIntervalRequest	Meta und Werte mit Intervall für Diagrammanzeige zählen
20	CountByValueAndAverageOverallScore Request	Meta zählen und Gesamtbewertungen für Ereignisse zuordnen
21	CountByValueAndAverageGroupScore Request	Meta zählen und Gruppenbewertungen für Ereignisse zuordnen
22	CountFileEntryByCriteriaRequest	Dateien nach Kriterien zählen
23	FindFileEntryByIdRequest	Datei nach ID abrufen
24	FindFileEntryByCriteriaRequest	Datei nach Kriterien abrufen
25	ReSubmitFileEntryRequest	Datei erneut zur Analyse senden
26	FileDownloadRequest	Datei aus Repository herunterladen
27	FileUploadRequest	Datei zur Analyse hochladen
28	FindFileScoreByIdRequest	Dateibewertung nach ID abrufen

Seriennummer	Vorgangsname	Bedeutung
29	FindFileScoreByCriteriaRequest	Dateibewertung nach Kriterien abrufen
30	FindHashValueByIdRequest	Whitelist/Blacklist-Hash-Wert nach ID abrufen
31	FindHashValueByCriteriaRequest	Whitelist/Blacklist-Hash-Wert nach Kriterien abrufen
32	AddHashValueRequest	Whitelist/Blacklist-Hash-Wert hinzufügen
33	UpdateHashValueRequest	Whitelist/Blacklist-Hash-Wert aktualisieren
34	DeleteHashValueRequest	Whitelist/Blacklist-Hash-Wert löschen
35	FindHashValueByMd5Request	Whitelist/Blacklist-Hash-Wert nach md5 abrufen
36	AddHashValueInFileRequest	Datei und Hash-Wert zu Repository hinzufügen
37	GetDefaultRulesRequest	Standard-IOC-Regelkonfiguration abrufen
38	ResetToDefaultRulesRequest	Standard-IOC-Regelkonfiguration auf Standard zurücksetzen
39	GetAllOverrideRulesRequest	Vom Benutzer erstellte überschreibende Konfiguration für IOC-Regeln abrufen
40	FindOverrideRuleByIdRequest	Überschreibende IOC-Regel nach ID suchen
41	AddOverrideRuleRequest	Überschreibende IOC-Regel hinzufügen

Seriennummer	Vorgangsname	Bedeutung
42	UpdateOverrideRuleRequest	Überschreibende IOC-Regel aktualisieren
43	DeleteOverrideRuleRequest	Überschreibende IOC-Regel löschen
44	SubmitOnDemandNextGenRequest	Neuen Ondemand-Scan der nächsten Generation absenden
45	FindOnDemandJobEntryByIdRequest	Ondemand-Jobentität nach ID abrufen
46	FindOnDemandJobEntryByCriteria Request	Ondemand-Jobentität nach Kriterien abrufen
47	GetOnDemandJobInfoRequest	Ondemand-Jobreferenzentität nach ID abrufen
48	GetOnDemandDefaultConfiguration	Abruf der Ondemand-Standardkonfiguration anfordern
49	CancelOnDemandJobRequest	Laufenden Ondemand-Job abbrechen
50	DeleteOnDemandJobRequest	Ondemand-Job löschen
51	ReSubmitOnDemandJobRequest	Ondemand-Job erneut absenden
52	SubscriptionRequest	MA-Cloud-Kommunikation abonnieren
53	UnSubscribeRequest	Abonnement der MA Cloud-Kommunikation stornieren
54	GetTopEventInfluencesRequest	Oberste N Ereignisbeeinflusser abrufen

Seriennummer	Vorgangsname	Bedeutung
55	GetServerInfoRequest	Serverinformationen, z. B. Serverzeit, abrufen
56	DataResetRequest	Datenbank zurücksetzen
57	OnDemandJobStatusNotification	Fortschritt bei Ondemand-Job an Abonnenten melden
58	LicenseStatusNotification	Lizenzstatus melden – Anzahl analysierte Proben
59	DataResetNotification	Melden, dass Daten zurückgesetzt wurden
60	GetIocSummaryRequest	IOC-Regeln aggregiert nach Ereignis-/Dateibewertungen abrufen
61	FindAlertTemplatesByCriteriaRequest	rabbitmq-Warnmeldungsvorlagen nach Kriterien abrufen
62	SaveAlertTemplateRequest	Warnmeldungsvorlage aktualisieren
63	DeleteAlertTemplateRequest	Warnmeldungsvorlage löschen
64	GetJobStatusRequest	Analysethreadstatus für laufenden Job abrufen
65	GetEventTypeCountSummaryRequest	Ereignisanalyseanzahl nach Datumsdiagramm abrufen
66	Logon	Bei MA-Service anmelden
67	Modified	Konfigurationsänderungen werden modifiziert

Seriennummer	Vorgangsname	Bedeutung
68	GetNextGenSummaryRequest	Dashboard-Zusammenfassungsstatistik der nächsten Generation abrufen

NetWitness Suite-Benutzeroberfläche

In der folgenden Tabelle sind die Vorgänge aufgelistet, die von der NetWitness Suite-Benutzeroberfläche protokolliert werden.

Serial #	Vorgangsname	Bedeutung
1	uploadTrialLicense	Testlizenz hochladen
2	LicenseEntitle	Lizenz berechtigen
3	LicenseDeactivation	Lizenz deaktivieren
4	ExpiredLicense	Lizenz abgelaufen
5	LicenseOutOfComplianceAcknowledgement	EULA-Bestätigung
6	resetLicense	Lizenz zurücksetzen
7	usageDateExport	Lizenzdatennutzung – csv/pdf
8	refreshLicense	LLS-Lizenz aktualisieren
9	LicenseOutOfCompliance	Ungültig
10	OOTBEntitlementOutOfCompliance	OOTB-Probelizenz ungültig
11	OOTBEntitlementFirstLoginTimeModified	OOTB-Zeit geändert
12	OOTBEntitlementFileDeleted	OOTB-Datei gelöscht
13	OOTBEntitlementDataTampering	OOTB-Daten manipuliert
14	uploadOfflineResponse	Offlineantwort hochladen

Serial #	Vorgangsname	Bedeutung
15	offlineDownloadCapRequest	Offlineanforderung herunterladen
16	movePerpetualToMetered	Servicebasierte Lizenz auf messungsbasierte Lizenz umstellen
17	moveMeteredToPerpetual	Messungsbasierte Lizenz auf servicebasierte Lizenz umstellen
18	mapServiceLicense	Service echter Lizenz zuordnen
19	delete	Vorgang zum Löschen von Warnmeldungsvorlagen
20	HttpRequest	Vorgang für die Auditprotokollierung der URL, auf die zugegriffen wird
21	Page Accessed	Vorgang für die Auditprotokollierung der Seite, auf die zugegriffen wird
22	Navigate	Vorgang zum Navigieren zu der Seite, auf die zugegriffen wird
23	Events	Vorgang zum Anzeigen der Seite des Ereignisses, auf das zugegriffen wird
24	Recon	Vorgang für die angeforderte Ereignisrekonstruktion
25	Services	Vorgang beim Lesen der Liste verfügbarer Geräten für Investigation.

Serial #	Vorgangsname	Bedeutung
26	Service	Vorgang für eine Liste von Geräten, deren Untersuchung angefordert wurde
27	Collections	Vorgang zum Anzeigen der Liste der angeforderten Sammlungen
28	Profiles	Vorgang zum Anwenden eines Profils
29	ColumnGroups	Vorgang zum Anwenden oder Lesen einer Spaltengruppe
30	ParallelCoordinates	Vorgänge in Bezug auf das Laden von Navigation in der Koordinationsansicht
31	Timeline	Vorgänge in Bezug auf das Laden der Navigation in der Zeitachsenansicht
32	PrintView	Vorgänge zum Öffnen von Investigation in der Druckansicht
33	Preferences	Vorgänge in Bezug auf eine Informer-Anforderung
34	import	Vorgänge in Bezug auf das Importieren von Spaltengruppen oder Profilen
35	export	Vorgänge in Bezug auf das Exportieren von Spaltengruppen oder Profilen

Serial #	Vorgangsname	Bedeutung
36	Predicate	Vorgänge in Bezug auf in Investigation verwendete Abfragen (Prädikate)
37	Languages	Vorgang für die von einem Gerät angeforderte Sprache
38	CancelLanguageLoad	Vorgang zum Abbrechen des Ladens der Sprache über die Seite „Navigieren“
39	summary	Vorgang für eine von einem Gerät angeforderte Zusammenfassung
40	languages	Vorgang für eine von einem Gerät angeforderte Sprache
41	aliases	Vorgang für von einem Gerät angeforderte Meta-Aliase
42	query	Vorgang für eine von einem Gerät angeforderte SDK-Abfrage
43	msearch	Vorgang für eine von einem Gerät angeforderte Metasuche
44	nodeListing	Node-Liste für einen Node von einem Gerät angefordert
45	content	SDK Content-Abruf von einem Gerät für das Herunterladen einer PCAP- oder Protokolldatei angefordert

Serial #	Vorgangsname	Bedeutung
46	Export Files	Dateiliste für eine Sitzung in der Dateiansicht oder „Extraktionsjobs“ angefordert
47	packets	Pakete für Sitzungen in der Paketansicht oder „Extraktionsjobs“ angefordert
48	deleteEndpointCache	Vorgang zum Löschen des Rekonstruktionscaches eines Geräts
49	Logon	Vorgang zum Anmelden eines Benutzers bei der NetWitness Suite-Benutzeroberfläche
50	Logoff	Vorgang zum Abmelden eines Benutzers bei der NetWitness Suite-Benutzeroberfläche
51	defaultDevice	Vorgang zum Zugreifen auf das Standard-SA-Benutzeroberflächengerät
52	deleteDefaultDevice	Vorgang zum Löschen des Standard-Investigation-Geräts
53	submitExtractFiles	Vorgang zum Senden einer Anforderung zum Extrahieren von Dateien aus Sitzungen
54	submitExtractLogs	Vorgang zum Senden einer Anforderung zum Extrahieren von Protokollen aus Sitzungen

Serial #	Vorgangsname	Bedeutung
55	submitExtractPcap	Vorgang zum Senden einer Anforderung zum Extrahieren von Sitzungen aus Sitzungen
56	MetaGroup	Vorgänge in Bezug auf SA-Benutzeroberflächen-Metagruppen
57	ExternalQuery	Vorgang, wenn eine Direktabfrage über URL ausgelöst wird
58	GeoMap	Vorgang zum Zugreifen auf die Geomap-Ansicht von Investigation
59	SaveProfile	Vorgang zum Speichern eines Investigation-Profils
60	ApplyProfile	Vorgang zum Anwenden eines Investigation-Profils
61	DeleteProfile	Vorgang zum Anwenden eines Investigation-Profils
62	DeactivateProfile	Vorgang zum Anwenden eines Investigation-Profils
63	VisualizePreferences	Vorgänge in Bezug auf die Informer-Visualisierungsanforderung

Serial #	Vorgangsname	Bedeutung
64	ExportMetaGroup	Vorgänge zum Exportieren mehrerer SA-Benutzeroberflächen-Metagruppen
65	userPredicates	Vorgänge zum Exportieren mehrerer SA-Benutzeroberflächen-Metagruppen
66	FileView	Vorgang für eine Rekonstruktionsanforderung für die Dateiansicht
67	resource.update	Vorgang, wenn der Status der Live-Abonnements geändert wird

Reagieren

In der folgenden Tabelle sind die Vorgänge aufgelistet, die von der Reagieren-Komponente protokolliert werden.

Seriennummer	Vorgangsname	Bedeutung
1	update	Aktualisieren der Benachrichtigungseinstellungen
2	update	Aktualisieren der Konfiguration von Integrationseinstellungen
3	delete	Löschen von Warnmeldungen
4	create	Erstellen eines neuen Incident
5	update	Aktualisieren von Incident-Details

Seriennummer	Vorgangsname	Bedeutung
6	read	Lesen von Incident-Details
7	delete	Löschen von Incidents
8	read	Lesen der Korrekturaufgaben
9	delete	Löschen von Korrekturaufgaben
10	update	Aktualisieren von Korrekturaufgaben
11	create	Erstellen einer neuen Regel
12	update	Aktualisieren der vorhandenen Warnmeldungsregel
13	reorder	Neuanordnen der Priorität von Warnmeldungsregeln

Lokale Speicherorte für Auditprotokolle

NetWitness Suite verfügt über globale Auditprotokollierungsfunktionen. Wenn Sie die globale Auditprotokollierung konfigurieren, werden die Auditprotokolle sämtlicher NetWitness Suite-Komponenten in einem zentralen System erfasst. Dieses konvertiert die Protokolle in das erforderliche Format und leitet sie an einen Syslog-Server eines Drittanbieters oder an einen Log Decoder weiter.

Wenn Sie die Auditprotokolle der einzelnen Services ansehen möchten, finden Sie sie in den lokalen Speicherorten der Auditprotokolle. Die folgende Tabelle enthält die lokalen Verzeichnispfade der Auditprotokolle für die NetWitness Suite-Benutzeroberfläche und die verschiedenen NetWitness Suite-Services.

Service/Modul	Details zum Auditprotokoll
NetWitness Suite-Benutzeroberfläche (NetWitness Suite Web Server)	Die NetWitness Suite-Benutzeroberfläche sendet Auditprotokolle an die folgenden Speicherorte: • **/var/lib/netwitness/uax/logs/audit/audit.log** (für Menschen lesbares Format) • Syslog, auf dem lokalen Host ausgeführt (JSON-Format) Die NetWitness Suite-Benutzeroberfläche verwendet das Syslog-Facility-Feld AUTH zum Schreiben von Auditprotokollen an Syslog. Sie können die Auditprotokolle nur im ersten Speicherort anzeigen (/var/lib/netwitness/uax/logs/audit/audit.log).
Core-Services (Decoder, Log Decoder, Concentrator, Broker und Archiver), Log Collector, Warehouse Connector, Workbench und IPDB Extractor	Die Core-Services und vergleichbare Services senden Auditprotokolle an Syslog, das auf dem lokalen Host ausgeführt wird. Pfad: **/var/log/secure** (JSON-Format) Die Core-Services verwenden das Syslog-Facility-Feld AUTHPRIV zum Schreiben von Auditprotokollen an Syslog.

Service/Modul	Details zum Auditprotokoll
Reporting Engine, Malware Analysis, Reagieren und Event Stream Analysis (ESA)	Diese Services senden Auditprotokolle an die folgenden Speicherorte: • **<Anwendungsstammverzeichnis>/logs/audit/audit.log** (für Menschen lesbares Format) • Syslog, auf dem lokalen Host ausgeführt (JSON-Format) Die Auditprotokolle dieser Services werden an folgenden Orten gespeichert: Reporting Engine: **/home/rsasoc/rsa/soc/reporting-engine/logs/audit/audit.log** Antwortserver /var/log/netwitness/respond-server/respond-server-audit.log Malware Analysis: **/var/lib/netwitness/rsamalware/spectrum/logs/audit/audit.log** Event Stream Analysis: **/opt/rsa/esa/logs/audit/audit.log** Diese Services verwenden das Syslog-Facility-Feld AUTH, um Auditprotokolle an Syslog zu schreiben. Sie können die Auditprotokolle nur im ersten Speicherort sehen (<Anwendungsstammverzeichnis>/logs/audit/audit.log).

Service/Modul	Details zum Auditprotokoll
Integrität und Zustand, Ereignisquellenmanagement (Event Source Management, ESM) und Appliance and Service Grouping (ASG)	Diese Services senden Auditprotokolle an die folgenden Speicherorte: • **/opt/rsa/sms/logs/audit/audit.log** (für Menschen lesbares Format) • Syslog, auf dem lokalen Host ausgeführt (JSON-Format) Diese Services verwenden das Syslog-Facility-Feld „AUTH“ zum Schreiben von Auditprotokollen an Syslog. Sie können die Auditprotokolle nur im ersten Speicherort anzeigen (/opt/rsa/sms/logs/audit/audit.log).

Troubleshooting der Systemkonfiguration

Die Themen in diesem Abschnitt bieten Informationen zum Troubleshooting für Administratoren, die Einstellungen konfigurieren, die systemübergreifend in NetWitness Suite angewendet werden.

Troubleshooting bei der globalen Auditprotokollierung

Troubleshooting von NTP-Serverkonfigurationen

Troubleshooting bei der globalen Auditprotokollierung

Dieses Thema enthält Informationen zu möglichen Problemen, mit denen NetWitness Suite-Benutzer bei der Implementierung der globalen Auditprotokollierung in NetWitness Suite konfrontiert werden können. In diesem Thema finden Sie Erklärungen und Lösungen.

Nach dem Konfigurieren der globalen Auditprotokollierung sollten Sie Ihre Auditprotokolle testen, um sich zu vergewissern, dass die Auditereignisse entsprechend der Definition in Ihrer Auditprotokollierungsvorlage aufgeführt werden. Wenn Sie die Auditprotokolle nicht auf Ihrem Syslog-Server oder Log Decoder eines Drittanbieters anzeigen können oder die Auditprotokolle nicht wie erwartet angezeigt werden, lesen Sie die grundlegenden Troubleshooting-Vorschläge im Folgenden. Wenn die Probleme dann immer noch bestehen, können Sie sich die erweiterten Troubleshooting-Vorschläge ansehen.

Grundlegendes Troubleshooting

Wenn Sie Auditprotokolle nicht auf einem Syslog-Server oder Log Decoder eines Drittanbieters anzeigen können:

- Vergewissern Sie sich, dass RabbitMQ einwandfrei funktioniert.
- Überprüfen Sie die Konfiguration des Syslog-Benachrichtigungsserver und vergewissern Sie sich, dass sie aktiviert ist.
  (Diese Konfiguration finden Sie unter „ADMINISTRATION“ > „System“ > „Globale Benachrichtigungen“. Wählen Sie nicht „Alte Benachrichtigungen“ aus.)
- Überprüfen Sie die globale Auditprotokollierungskonfiguration.

Anweisungen dazu erhalten Sie unter Konfigurieren der globalen Auditprotokollierung und Überprüfen von globalen Auditprotokollen. Wenn Sie Auditprotokolle an einen Log Decoder senden:

- Vergewissern Sie sich, dass der Log Decoder die Aggregation auf dem Concentrator auf demselben Host durchführt (ADMINISTRATION > Services > (Concentrator auswählen) >  >Ansicht > Konfiguration).

- Überprüfen Sie, ob der neueste CEF-Parser bereitgestellt und aktiviert ist.
- Überprüfen Sie die Benachrichtigungsvorlage für die Auditprotokollierung. Sie müssen eine CEF-Vorlage verwenden und alle Protokolle, die in den Log Decoder übertragen werden, müssen eine CEF-Vorlage verwenden.

Wenn Sie Auditprotokolle an einen Syslog-Server eines Drittanbieters senden:

- Vergewissern Sie sich, dass der für den Drittanbieter-Syslog-Server konfigurierte Zielport nicht von einer Firewall blockiert wird.

Erweitertes Troubleshooting

Um die globale Auditprotokollierung in Ihrem Netzwerk verwenden zu können, muss RabbitMQ ordnungsgemäß funktionieren.

Bei der zentralisierten Auditprotokollierung schreibt jeder der NetWitness Suite-Services Auditprotokolle an das rsyslog-Plug-in auf dem lokalen Host, das Port 50514 unter Verwendung von UDP überwacht. Das im Auditprotokollierungspaket enthaltene rsyslog-Plug-in fügt zusätzliche Informationen an und lädt diese Protokolle zu RabbitMQ hoch. Der auf dem NetWitness-Server-Host ausgeführte Logstash aggregiert die Auditprotokolle aller NetWitness Suite-Services, konvertiert Sie in das erforderliche Format und sendet Sie zur Untersuchung an einen Syslog-Server eines Drittanbieters oder an Log Decoder. Sie konfigurieren das Format der globalen Auditprotokolle und das vom Logstash verwendete Ziel über die NetWitness Suite-Benutzeroberfläche.

Anweisungen hierzu enthält der Abschnitt Definieren einer globalen Auditprotokollierungskonfiguration.

Überprüfen der Pakete und Services auf den Hosts

NetWitness Suite-Host

Die folgenden Pakete oder Services müssen auf dem NetWitness-Server-Host vorhanden sein:

- rsyslog-8.4.1
- rsa-audit-rt
- logstash-1.5.4-1
- rsa-audit-plugins
- rabbitmq server

Services auf einem anderen Host als dem NetWitness Suite-Host

Die folgenden Pakete oder Services müssen auf allen anderen NetWitness Suite-Hosts, die nicht der NetWitness-Server-Serverhost sind, vorhanden sein:

- rsyslog-8.4.1
- rsa-audit-rt
- rabbitmq server

Log Decoder

Wenn Sie globale Auditprotokolle an einen Log Decoder weiterleiten, müssen die folgenden Parser vorhanden und aktiviert sein:

- CEF

Mögliche Probleme

Was ist zu tun, wenn eine Aktion auf einem Service ausgeführt wird, die Auditprotokolle den konfigurierten Syslog-Server oder Log Decoder eines Drittanbieters aber nicht erreichen?

Dies kann eine oder alle der folgenden Ursachen haben:

- Ein Service protokolliert nicht auf den lokalen Syslog-Server.
- Auditprotokolle werden nicht vom lokalen Syslog-Server an RabbitMQ hochgeladen.
- Auditprotokolle werden nicht auf dem NetWitness-Server-Host aggregiert.
- Aggregierte Protokolle auf dem NetWitness-Server-Host werden nicht an den konfigurierten Syslog-Server eines Drittanbieters oder an Log Decoder weitergeleitet.
- Der Log Decoder ist nicht für das Empfangen globaler Auditprotokolle im CEF-Format konfiguriert:
  - Die Log Decoder-Erfassung ist nicht aktiviert.
  - Es ist kein CEF-Parser vorhanden.
  - Der CEF-Parser ist nicht aktiviert.

Mögliche Lösungen

Die folgende Tabelle enthält mögliche Lösungen für die Probleme.

Problem	Mögliche Lösungen

Ein Service protokolliert nicht auf den lokalen Syslog-Server.	• Vergewissern Sie sich, dass rsyslog ordnungsgemäß funktioniert.
	Dazu können Sie den folgenden Befehl verwenden:
	`service rsyslog status`
	• Vergewissern Sie sich, dass rsyslog den Port 50514 unter Verwendung von UDP überwacht.
	Dazu können Sie den folgenden Befehl verwenden:
	`netstat -tulnp|grep rsyslog`
	• Vergewissern Sie sich, dass die Anwendung oder Komponente Auditprotokolle an Port 50514 sendet. Führen Sie das Dienstprogramm tcpdump auf der lokalen Schnittstelle für Port 50514 aus.
	Dazu können Sie den folgenden Befehl verwenden:
	`sudo tcpdump -i lo -A udp and port 50514`
	
	Die Befehlsausgaben finden Sie unten unter *Lösungsbeispiele*.

Auditprotokolle werden nicht vom lokalen Syslog-Server an RabbitMQ hochgeladen.	• Vergewissern Sie sich, dass das rsyslog-Plug-in ordnungsgemäß funktioniert.
	Dazu können Sie den folgenden Befehl verwenden:
	`ps -ef|grep rsa_audit_onramp`
	• Vergewissern Sie sich, dass der RabbitMQ-Server ordnungsgemäß funktioniert.
	Dazu können Sie den folgenden Befehl verwenden:
	`service rabbitmq-server status`
	
	Die Befehlsausgaben finden Sie unter „Lösungsbeispiele“.

Problem	Mögliche Lösungen

Auditprotokolle werden nicht auf dem NetWitness-Server-Host aggregiert.	• Vergewissern Sie sich, dass Logstash ordnungsgemäß funktioniert.
	Dazu können Sie die folgenden Befehle verwenden:
	`ps -ef|grep logstash`
	`service logstash status`
	• Vergewissern Sie sich, dass der RabbitMQ-Server ordnungsgemäß funktioniert.
	Dazu können Sie den folgenden Befehl verwenden:
	`service rabbitmq-server status`
	• Vergewissern Sie sich, dass der RabbitMQ-Server Port 5672 überwacht.
	Dazu können Sie den folgenden Befehl verwenden:
	`netstat -tulnp|grep 5672`
	• Suchen Sie nach Fehlern, die auf der Logstash-Ebene entstehen.
	Sie können den folgenden Befehl verwenden, um den Speicherort der Protokolldateien zu suchen:
	`ls -l /var/log/logstash/logstash.*`
	Die Befehlsausgaben finden Sie unter „Lösungsbeispiele“.

Problem	Mögliche Lösungen

Aggregierte Protokolle auf dem NetWitness-Server-Host werden nicht an den konfigurierten Syslog-Server eines Drittanbieters oder an Log Decoder weitergeleitet.	• Vergewissern Sie sich, dass Logstash ordnungsgemäß funktioniert.
	Dazu können Sie die folgenden Befehle verwenden:
	`ps -ef|grep logstash`
	`service logstash status`
	• Suchen Sie nach Fehlern, die auf der Logstash-Ebene entstehen.
	Sie können den folgenden Befehl für den Speicherort der Protokolldateien verwenden:
	`ls -l /var/log/logstash/logstash.`
	Die Befehlsausgaben finden Sie unten unter „Lösungsbeispiele“.
	• Vergewissern Sie sich, dass der Zielservice ausgeführt wird.
	• Vergewissern Sie sich, dass der Zielservice den korrekten Port unter Verwendung des korrekten Protokolls überwacht.
	• Vergewissern Sie sich, dass der konfigurierte Port auf dem Zielhost nicht blockiert wird.

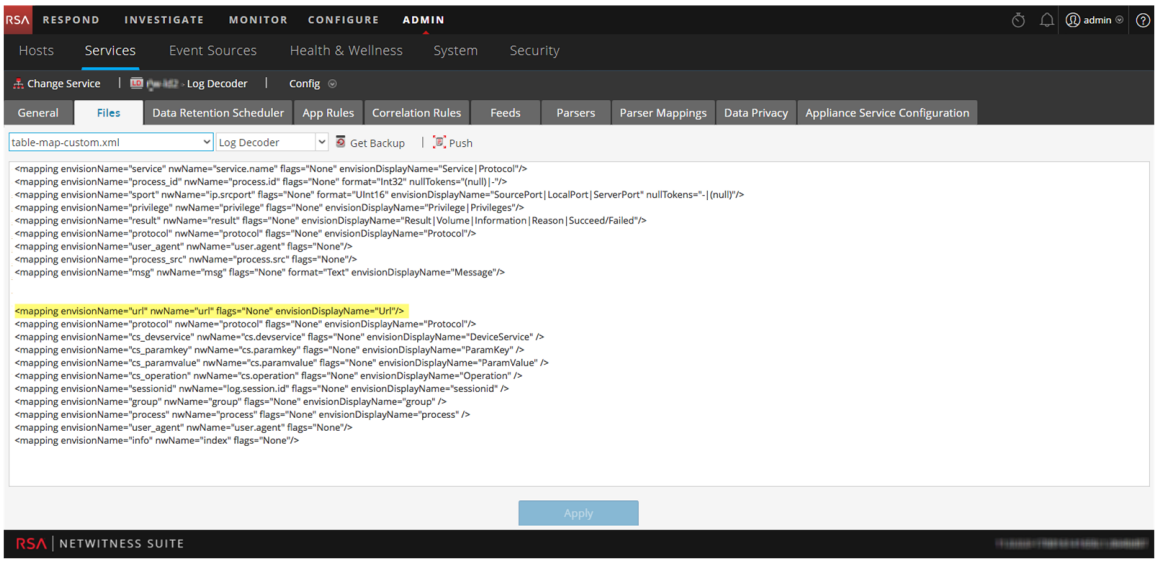
Problem	Mögliche Lösungen
Vom Logstash weitergeleitete Auditprotokolle führen zu Parserfehlern auf dem Log Decoder.	• Vergewissern Sie sich, dass Sie eine passende Benachrichtigungsvorlage verwenden. Von einem Log Decoder geparste Auditprotokolle müssen im CEF-Format vorliegen. Das Ziel, von dem Auditprotokolle direkt oder indirekt zum Log Decoder gelangen, muss ebenfalls eine CEF-Vorlage verwenden. • Die Benachrichtigungsvorlage muss dem CEF-Standard entsprechen. Befolgen Sie die Schritte in diesem Handbuch, um die standardmäßige CEF-Vorlage zu verwenden oder eine den strengen Richtlinien entsprechende benutzerdefinierte CEF-Vorlage zu erstellen. Weitere Informationen erhalten Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. • Überprüfen Sie die Logstash-Konfiguration.

Warum werden benutzerdefinierte Metadaten nicht in Investigation angezeigt?

Wenn Metadaten nicht in Investigation angezeigt werden, bedeutet das normalerweise, dass sie nicht indexiert sind. Wenn Sie benutzerdefinierte Metadaten für Investigation und Reporting verwenden möchten, vergewissern Sie sich, dass die ausgewählten Metaschlüssel in der Datei **table-map-custom.xml** auf dem Log Decoder indexiert sind. Befolgen Sie das Verfahren „Pflegen der Tabellenzuordnungsdateien“, um die Datei **table-map-custom.xml** auf dem Log Decoder zu bearbeiten.

Vergewissern Sie sich, dass die benutzerdefinierten Metaschlüssel auch in der Datei **index-concentrator-custom.xml** auf dem Concentrator indexiert sind. Weitere Informationen erhalten Sie unter „Bearbeiten einer Serviceindexdatei“.

Die folgende Abbildung zeigt ein Beispiel für die Datei **table-map-custom.xml** in NetWitness-Server (ADMINISTRATION > Services > (Log Decoder auswählen) >  > Ansicht > Konfiguration). Das Beispiel für den benutzerdefinierten Metawert `url` ist hervorgehoben.

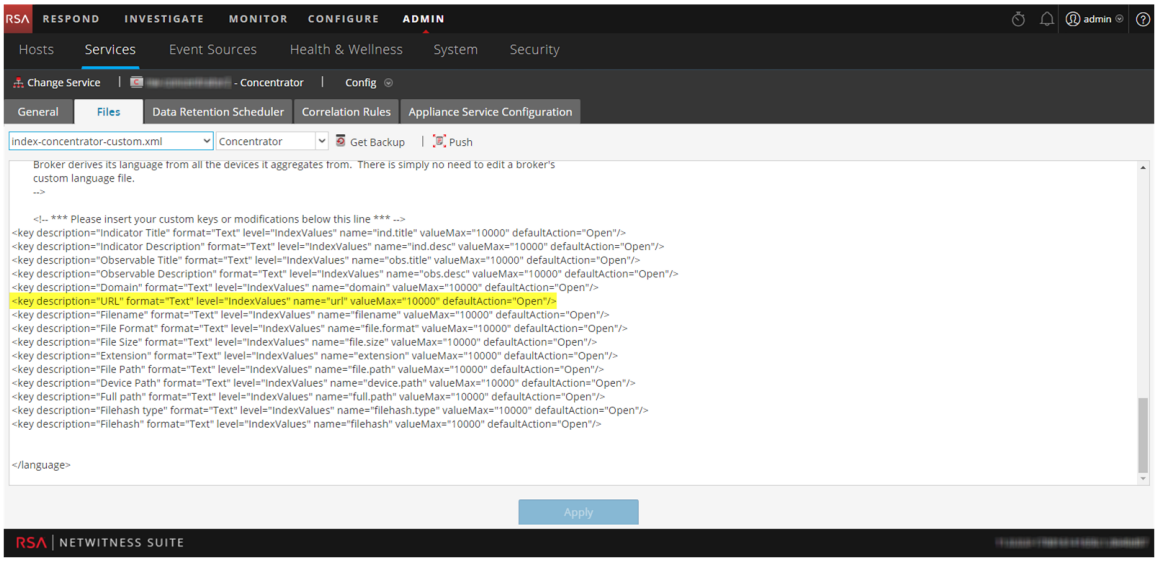


Im folgenden Codebeispiel aus der oben genannten Datei **table-map-custom.xml** ist der benutzerdefinierte Metawert `url` hervorgehoben:

<mapping envisionName="url" nwName="url" flags="None" envisionDisplayName="Url"/>

```
<mapping envisionName="protocol" nwName="protocol" flags="None"
envisionDisplayName="Protocol"/><mapping envisionName="cs_devservice"
nwName="cs.devservice" flags="None" envisionDisplayName="DeviceService"
/><mapping envisionName="cs_paramkey" nwName="cs.paramkey" flags="None"
envisionDisplayName="ParamKey" /><mapping envisionName="cs_paramvalue"
nwName="cs.paramvalue" flags="None" envisionDisplayName="ParamValue"
/><mapping envisionName="cs_operation" nwName="cs.operation"
flags="None" envisionDisplayName="Operation" /><mapping
envisionName="sessionid" nwName="log.session.id" flags="None"
envisionDisplayName="sessionid" /><mapping envisionName="group"
nwName="group" flags="None" envisionDisplayName="group" /><mapping
envisionName="process" nwName="process" flags="None"
envisionDisplayName="process" /><mapping envisionName="user_agent"
nwName="user.agent" flags="None"/><mapping envisionName="info"
nwName="index" flags="None"/>
```

Die folgende Abbildung zeigt ein Beispiel für die Datei **index-concentrator-custom.xml** in NetWitness-Server (ADMINISTRATION > Services > (Concentrator auswählen) > > Ansicht > Konfiguration). Das Beispiel für den benutzerdefinierten Metawert `url` ist hervorgehoben.



Im folgenden Codebeispiel aus der Datei **index-concentrator-custom.xml** oben ist der benutzerdefinierte Metawert `url` hervorgehoben:

```
<key description="Severity" level="IndexValues" name="severity"
valueMax="10000" format="Text"/><key description="Result"
level="IndexValues" name="result" format="Text"/><key
level="IndexValues"  name="ip.srcport" format="UInt16"
description="SourcePort"/><key description="Process" level="IndexValues"
name="process" format="Text"/><key description="Process ID"
level="IndexValues" name="process_id" format="Text"/><key
description="Protocol" level="IndexValues" name="protocol"
format="Text"/><key description="UserAgent" level="IndexValues"
name="user_agent" format="Text"/><key description="DestinationAddress"
level="IndexValues" name="ip.dst" format="IPv4"/><key
description="SourceProcessName" level="IndexValues" name="process.src"
format="Text"/><key description="Username" level="IndexValues"
name="username"  format="Text"/><key description="Info"
level="IndexValues" name="index"  format="Text"/><key
description="customdevservice" level="IndexValues" name="cs.devservice"
```

```
format="Text"/>
<key description="url" level="IndexValues" name="url"  format="Text"/>
<key description="Custom Key" level="IndexValues" name="cs.paramkey"
format="Text"/><key description="Custom Value" level="IndexValues"
name="cs.paramvalue"  format="Text"/><key description="Operation"
level="IndexValues" name="cs.operation"  format="Text"/><key
description="CS Device Service" level="IndexValues" name="cs.device"
format="Text" valueMax="10000" defaultAction="Closed"/>
```

Lösungsbeispiele

Die folgenden möglichen Lösungsbeispiele zeigen die Ausgaben der Beispielbefehle. Eine vollständige Liste aller Lösungen finden Sie in der Tabelle oben.

Vergewissern Sie sich, dass rsyslog ordnungsgemäß funktioniert.

Dazu können Sie den folgenden Befehl verwenden:

```
service rsyslog status
```

```
[root@NWAPPLIANCE22574 ~]# service rsyslog status
rsyslogd (pid  1293) is running...
[root@NWAPPLIANCE22574 ~]#
```

Vergewissern Sie sich, dass rsyslog den Port 50514 unter Verwendung von UDP überwacht.

Dazu können Sie den folgenden Befehl verwenden:

```
netstat -tulnp|grep rsyslog
```

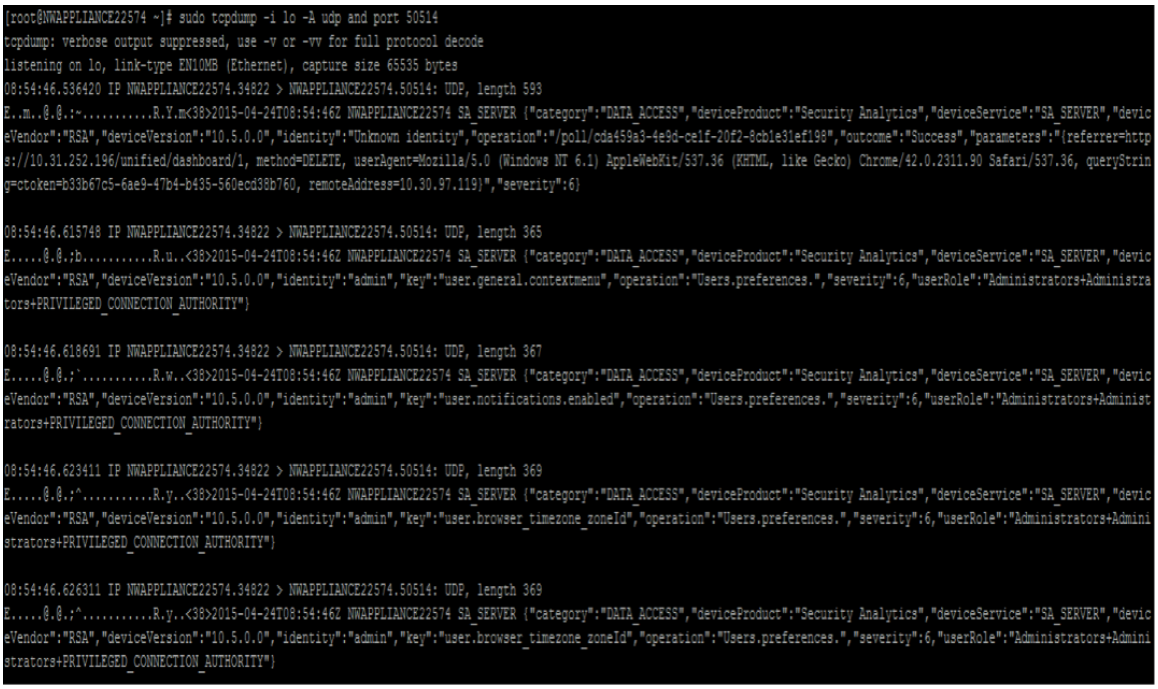
```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep rsyslog
udp        0      0 127.0.0.1:50514           0.0.0.0:*                           1293/rsyslogd
[root@NWAPPLIANCE22574 ~]#
```

Vergewissern Sie sich, dass die Anwendung oder Komponente Auditprotokolle an Port 50514 sendet.

Die folgende Abbildung zeigt die Ausgabe bei Ausführen des Dienstprogramms tcpdump auf der lokalen Schnittstelle für Port 50514.

Dazu können Sie den folgenden Befehl verwenden:

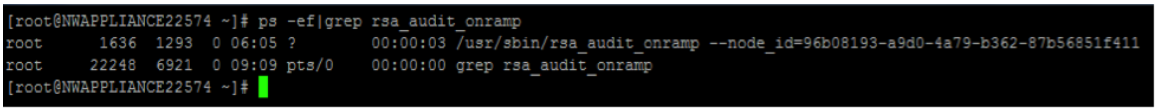
```
sudo tcpdump -i lo -A udp and port 50514
```



Vergewissern Sie sich, dass das rsyslog-Plug-in ordnungsgemäß funktioniert.

Dazu können Sie den folgenden Befehl verwenden:

```
ps -ef|grep rsa_audit_onramp
```



Vergewissern Sie sich, dass der RabbitMQ-Server ordnungsgemäß funktioniert.

Dazu können Sie den folgenden Befehl verwenden:

```
service rabbitmq-server status
```

```
[root@NWAPPLIANCE22574 ~]# service rabbitmq-server status
Status of node sa@localhost ...
[{pid,1862},
 {running_applications,
     [{rabbitmq_federation_management,"RabbitMQ Federation Management",
         "3.4.2"},
      {rabbitmq_management,"RabbitMQ Management Console","3.4.2"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.4.2"},
      {webmachine,"webmachine","1.10.3-rmq3.4.2-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.4.2-git680dba8"},
      {rabbitmq_federation,"RabbitMQ Federation","3.4.2"},
      {rabbitmq_stomp,"Embedded Rabbit Stomp Adapter","3.4.2"},
      {rabbitmq_management_agent,"RabbitMQ Management Agent","3.4.2"},
      {rabbit,"RabbitMQ","3.4.2"},
      {ssl,"Erlang/OTP SSL application","5.3.2"},
      {public_key,"Public key infrastructure","0.21"},
      {crypto,"CRYPTO version 2","3.2"},
      {asn1,"The Erlang ASN1 compiler version 2.0.4","2.0.4"},
      {os_mon,"CPO  CXC 138 46","2.2.14"},
      {inets,"INETS  CXC 138 49","5.9.7"},
      {mnesia,"MNESIA  CXC 138 12","4.11"},
      {amqp_client,"RabbitMQ AMQP Client","3.4.2"},
      {rabbitmq_auth_mechanism_ssl,
          "RabbitMQ SSL authentication (SASL EXTERNAL)","3.4.2"},
      {xmerl,"XML parser","1.3.5"},
      {sasl,"SASL  CXC 138 11","2.3.4"},
      {stdlib,"ERTS  CXC 138 10","1.19.4"},
      {kernel,"ERTS  CXC 138 10","2.16.4"}]},
 {os,{unix,linux}},
 {erlang_version,
     "Erlang R16B03 (erts-5.10.4) [source] [64-bit] [smp:2:2] [async-threads:30] [kernel-poll:true]\n"},
 {memory,
```

Vergewissern Sie sich, dass Logstash ordnungsgemäß funktioniert.

Dazu können Sie den folgenden Befehl verwenden:

```
ps -ef|grep logstash
service logstash status
```

```
[root@NWAPPLIANCE22574 ~]# ps -ef|grep logstash
logstash  1583     1  0 06:05 ?       00:01:09 /usr/bin/java -Djava.io.tmpdir=/var/lib/logstash -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Djava.awt.headless=true -XX:C
MSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -jar /opt/logstash/vendor/jar/jruby-complete-1.7.11.jar -I/opt/logstash/lib /opt/logstash/lib/logstash/runner
.rb agent --pluginpath /opt/logstash -f /etc/logstash/conf.d -l /var/log/logstash/logstash.log
root      8509  6921  0 09:31 pts/0    00:00:00 grep logstash
[root@NWAPPLIANCE22574 ~]# service logstash status
logstash is running
[root@NWAPPLIANCE22574 ~]#
```

Vergewissern Sie sich, dass der RabbitMQ-Server Port 5672 überwacht.

Geben Sie beispielsweise den folgenden Befehl ein:

```
netstat -tulnp|grep 5672
```

```
[root@NWAPPLIANCE22574 ~]# netstat -tulnp|grep 5672
tcp        0      0 127.0.0.1:5672              0.0.0.0:*                   LISTEN      1862/beam.smp
tcp        0      0 0.0.0.0:25672               0.0.0.0:*                   LISTEN      1862/beam.smp
[root@NWAPPLIANCE22574 ~]#
```

Suchen Sie nach Fehlern, die auf der Logstash-Ebene entstehen.

Sie können den folgenden Befehl für den Speicherort der Protokolldateien verwenden:

```
ls -l /var/log/logstash/logstash.*
```

```
[root@NWAPPLIANCE22574 ~]# ls -l /var/log/logstash/logstash.*
-rw-r--r--. 1 root     root        0 Apr 24 06:05 /var/log/logstash/logstash.err
-rw-r--r--. 1 logstash logstash 1043 Apr 24 06:04 /var/log/logstash/logstash.log
-rw-r--r--. 1 root     root       57 Apr 24 06:12 /var/log/logstash/logstash.stdout
[root@NWAPPLIANCE22574 ~]#
```

Eine vollständige Liste aller Probleme und möglichen Lösungen finden Sie in der Tabelle unter „Mögliche Lösungen“ oben.

Troubleshooting von NTP-Serverkonfigurationen

In diesem Thema werden möglicherweise auftretende Probleme von NTP-Serverkonfigurationen erläutert und Lösungen für diese Probleme bereitgestellt.

Probleme, die anhand von Meldungen im Bereich „NTP-Einstellungen“ oder anhand von Protokolldateien identifiziert werden

Dieser Abschnitt enthält Informationen über das Troubleshooting für Probleme, die anhand der in NetWitness Suite im Bereich „NTP-Einstellungen“ angezeigten Meldungen und anhand von Protokolldateien identifiziert werden.

Nachricht	Benutzeroberfläche **Es ist ein unerwarteter Fehler aufgetreten. Sehen Sie zuerst in den Protokollen nach und wenden Sie sich dann an den Customer Service, um den Fehler zu beheben.** **System Log:** **Timestamp Level Message** *yyyy-dd-mmThh:mm:ss:ms* ERROR com.rsa.smc.sa.adm.exception.MCOAgent Exception: No request sent, we did not discover any nodes
Mögliche Ursache	Die NetWitness Suite-Konfiguration auf niedriger Ebene ist fehlerhaft oder der unterstützende Service wird nicht ausgeführt.
Lösung	Wenden Sie sich an den Kundendienst.
Nachricht	Benutzeroberfläche **Ungültige Syntax des Hostnamens angegeben**.
Mögliche Ursache	Es wurde ein Hostname für einen NTP-Server eingegeben, der nicht der Syntax der IP-Adresse oder des vollständig qualifizierten Domainnamens entspricht.
Lösung	Geben Sie den Hostnamen mit der richtigen Syntax ein.
Nachricht	Benutzeroberfläche **Es wurde ein bereits vorhandener NTP-Server angegeben.**
Mögliche Ursache	Es wurde ein Hostname für einen NTP-Server eingegeben, der bereits in NetWitness Suite definiert ist.

Lösung	Geben Sie einen Hostnamen für einen NTP-Server ein, der nicht in NetWitness Suite konfiguriert ist.
Nachricht	Benutzeroberfläche **Der NTP-Server *Hostname* kann nicht erreicht werden**. Überprüfen Sie die Serveradresse und Ihre Firewalleinstellungen.
Mögliche Ursache	Die Serveradresse oder die Firewalleinstellungen sind möglicherweise falsch.
Lösung	Überprüfen Sie die Serveradresse und Ihre Firewalleinstellungen und korrigieren Sie sie gegebenenfalls.

Referenzen

Dieses Thema erhält Referenzmaterialien, in denen die Benutzeroberfläche zur Konfiguration von Systemeinstellungen in NetWitness Suite beschrieben wird und Parameter definiert werden. Administratoren konfigurieren Systemeinstellungen mithilfe der Optionen in der Ansicht Administration > System. Jeder Bereich wird in einem eigenen Thema beschrieben.

- Bereich „Globale Auditprotokollierungskonfigurationen“
- Bereich „Globale Benachrichtigungen“
  - Dialogfelder zum Definieren der Benachrichtigungsserver
  - Dialogfelder zum Definieren von Benachrichtigungsausgaben
  - Dialogfeld „Benachrichtigungsvorlage definieren“
  - Registerkarte „Ausgabe“
  - Registerkarte „Server“
  - Registerkarte Vorlagen
- Bereich „HTTP-Proxyeinstellungen“
- Bereich „E-Mail-Konfiguration“
- Bereich „Einstellungen für ESA“
- Investigation-Konfigurationsbereich
- Bereich „Konfiguration der Live-Services“
- Bereich „NTP-Einstellungen“
- Bereich Kontextmenüaktionen
- Bereich „Konfiguration alter Benachrichtigungen“

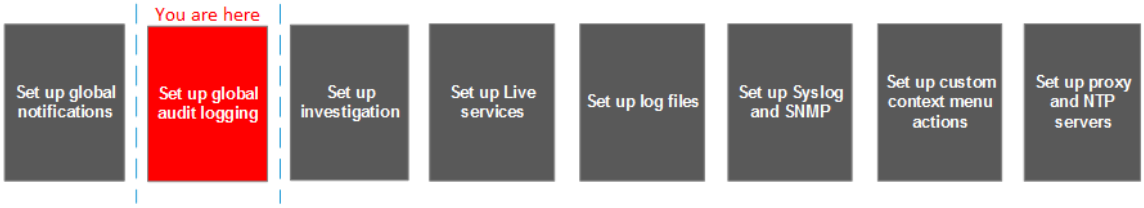
Bereich „Globale Auditprotokollierungskonfigurationen“

Im Bereich **Globale Auditprotokollierungskonfigurationen** (Admin > System > Globales Auditing) können Sie die globale Auditprotokollierung konfigurieren, indem Sie Konfigurationen hinzufügen, die definieren, wie globale Auditprotokolle an externe Syslog-Systeme weitergeleitet werden. Globale Auditprotokolle werden an den ausgewählten Benachrichtigungsserver in Ihrer globalen Auditprotokollierungskonfiguration mithilfe der ausgewählten Benachrichtigungsvorlage weitergeleitet.

Globale Auditprotokollierung bietet Security Analytics-Prüfern konsolidierte Einsichten in Benutzeraktivitäten innerhalb von NetWitness Suite in Echtzeit von einem zentralen Standort aus.

Workflow

Dieser Workflow zeigt die erforderlichen Verfahren zum Konfigurieren und Überprüfen des Bereichs „Globale Auditprotokollierungskonfigurationen“.



Bevor Sie eine globale Auditprotokollierungskonfiguration definieren können, müssen Sie einen Syslog-Benachrichtigungsserver unter Globale Benachrichtigungen > Registerkarte Server erstellen. Der Syslog-Benachrichtigungsserver ist das Ziel, an das die globalen Auditprotokolle gesendet werden. Als nächstes müssen Sie eine Auditprotokollierungsvorlage unter Globale Benachrichtigungen > Registerkarte Vorlagen auswählen oder definieren. Die Auditprotokollierungsvorlage definiert das Format und die Meldungsfelder der Auditprotokolle, die an den Log Decoder oder Syslog-Server eines Drittanbieters gesendet werden. Bei Verwendung eines Log Decoders implementieren Sie von Live aus den Common Event Format-Parser in Ihrem Log Decoder.

Hinweis: Die Registerkarte „Ausgabe“ unter Globale Benachrichtigungen muss nicht für die globale Auditprotokollierung konfiguriert werden.

Nachdem Sie eine globale Auditprotokollierungskonfiguration hinzugefügt haben, werden Auditprotokolle an den in der Konfiguration angegebenen Benachrichtigungsserver weitergeleitet. Testen Sie Ihre Auditprotokolle, um sicherzustellen, dass darin alle Auditereignisse aufgeführt werden, die in Ihrer Auditprotokollierungsvorlage definiert sind.

Was möchten Sie tun?

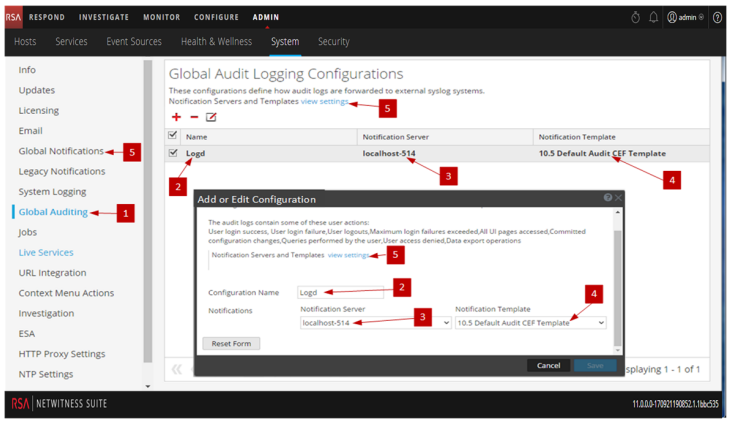
Rolle	Ich möchte...	Details anzeigen
Administrator	Erstellen Sie einen Syslog-Benachrichtigungsserver.	Konfigurieren eines Ziels zum Empfang globaler Auditprotokolle
Administrator	Eine Auditprotokollierungsvorlage auswählen.	Definieren einer Vorlage für die globale Auditprotokollierung
Administrator	Konfigurieren der globalen Auditprotokollierung	Definieren einer globalen Auditprotokollierungskonfiguration Das vollständige Verfahren finden Sie unter „Globalen Auditprotokollierung – Übergeordnetes Verfahren“ unter Konfigurieren der globalen Auditprotokollierung.
Administrator	Überprüfen von globalen Auditprotokollen	Überprüfen von globalen Auditprotokollen

Verwandte Themen

- Troubleshooting bei der globalen Auditprotokollierung
- Dialogfeld „Neue Konfiguration hinzufügen“
- Unterstützte CEF-Metaschlüssel
- Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung
- Referenz der globalen Auditprotokollierungsvorgänge
- Lokale Speicherorte für Auditprotokolle

Überblick

Das folgende Beispiel zeigt eine globale Auditprotokollierungskonfiguration. Diese Konfigurationen definiert, wie NetWitness Suite Auditprotokolle an externe Syslog-Systeme weiterleitet.



1	Der Bereich Globale Auditprotokollierungskonfigurationen wird angezeigt.
2	Name der globalen Auditprotokollierungskonfiguration.
3	Benachrichtigungsserver der globalen Auditprotokollierungskonfiguration.
4	Benachrichtigungsvorlage der globalen Auditprotokollierungskonfiguration.
5	Zeigt den Bereich „Globale Benachrichtigungen“, in dem Sie die erforderlichen Server und Vorlagen zum Konfigurieren einer globalen Auditprotokollierungskonfiguration festlegen.

Symbolleiste

In der folgenden Tabelle werden die Aktionen der Symbolleiste beschrieben

Symbol	Beschreibung
+	Fügt eine globale Auditprotokollierungskonfiguration hinzu.
−	Löscht eine globale Auditprotokollierungskonfiguration. Durch das Löschen einer globalen Auditprotokollierungskonfiguration werden die zugehörigen Benachrichtigungsserver- und Vorlagen nicht gelöscht. Nachdem Sie eine globale Auditprotokollierungskonfiguration gelöscht haben, wird die in dieser Konfiguration festgelegte Weiterleitung der globalen Auditprotokolle eingestellt.

Symbol	Beschreibung
	Bearbeitet eine globale Auditprotokollierungskonfiguration. Sie können das Ziel der globalen Auditprotokolle für Ihre Benutzeraudits ändern, indem Sie einen anderen Benachrichtigungsserver auswählen. Sie können auch das Format und die Meldungsfelder der globalen Auditprotokolleinträge ändern, indem Sie eine andere Benachrichtigungsvorlage auswählen. Sie können nicht ändern, welche NetWitness Suite Benutzeraktionen protokolliert und in den globalen Auditprotokollen versendet werden.

Konfigurationen

In der folgenden Tabelle werden die aufgeführten Konfigurationen beschrieben.

Titel	Beschreibung
	Wählen Sie das Kontrollkästchen neben einer Konfiguration aus, um eine einzelne Konfiguration auszuwählen. Wählen Sie das Kontrollkästchen in der Titelleiste der Tabelle aus, um alle Konfigurationen auszuwählen.
Name	Zeigt den Namen der globalen Auditkonfiguration an. Zum Beispiel können Sie die Konfigurationen auf der Grundlage des Ziels der globalen Auditprotokolle benennen, wie z. B. „HQ SA“ und „Mein Syslog-Server“.
Benachrichtigungsserver	Zeigt den Syslog-Benachrichtigungsserver an, der als Ziel für die globalen Auditprotokolle ausgewählt wurde. Wenn Sie globale Auditprotokolle an einen Log Decoder weiterleiten möchten, erstellen Sie einen Benachrichtigungsserver vom Syslog-Typ. Unter Konfigurieren eines Ziels zum Empfang globaler Auditprotokolle finden Sie Anweisungen zum Erstellen eines Syslog-Benachrichtigungsservers für die globale Auditprotokollierung.

Titel	Beschreibung
Benachrichtigungsvorlage	Zeigt die Auditprotokollierungs-Benachrichtigungsvorlage an, die für die Konfiguration ausgewählt wurde. Sie definiert das Format und die Meldungsfelder der Auditprotokolleinträge. Für Log Decoder verwenden Sie die **Audit-CEF-Standardvorlage**. Wenn bestimmte Anforderungen vorliegen, können Sie Felder zur CEF-Vorlage (Common Event Format) hinzufügen oder aus ihr entfernen. Definieren einer Vorlage für die globale Auditprotokollierung enthält Anweisungen und Unterstützte CEF-Metaschlüssel beschreibt die verfügbaren CEF-Metaschlüssel. Für Syslog-Server von Drittanbietern können Sie eine Standard-Auditprotokollierungsvorlage verwenden oder Ihr eigenes Format (CEF oder nicht CEF) definieren. Entsprechende Anweisungen finden Sie unter Definieren einer Vorlage für die globale Auditprotokollierung. Die verfügbaren Metaschlüsselvariablen werden im Abschnitt Unterstützte Metaschlüsselvariablen für die globale Auditprotokollierung beschrieben.

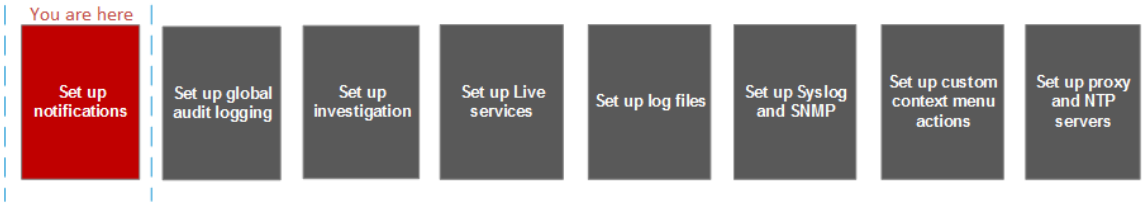
Bereich „Globale Benachrichtigungen“

Im Bereich „Globale Benachrichtigungen“ werden die Funktionen für die Konfiguration von Benachrichtigungseinstellungen erläutert. In Konfigurationen für globale Benachrichtigungen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Management, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert.

Im Bereich „Globale Benachrichtigungen“ können Sie folgende Einstellungen für globale Benachrichtigungen konfigurieren:

- Benachrichtigungsausgaben
- Benachrichtigungsserver
- Vorlagen

WorkFlow



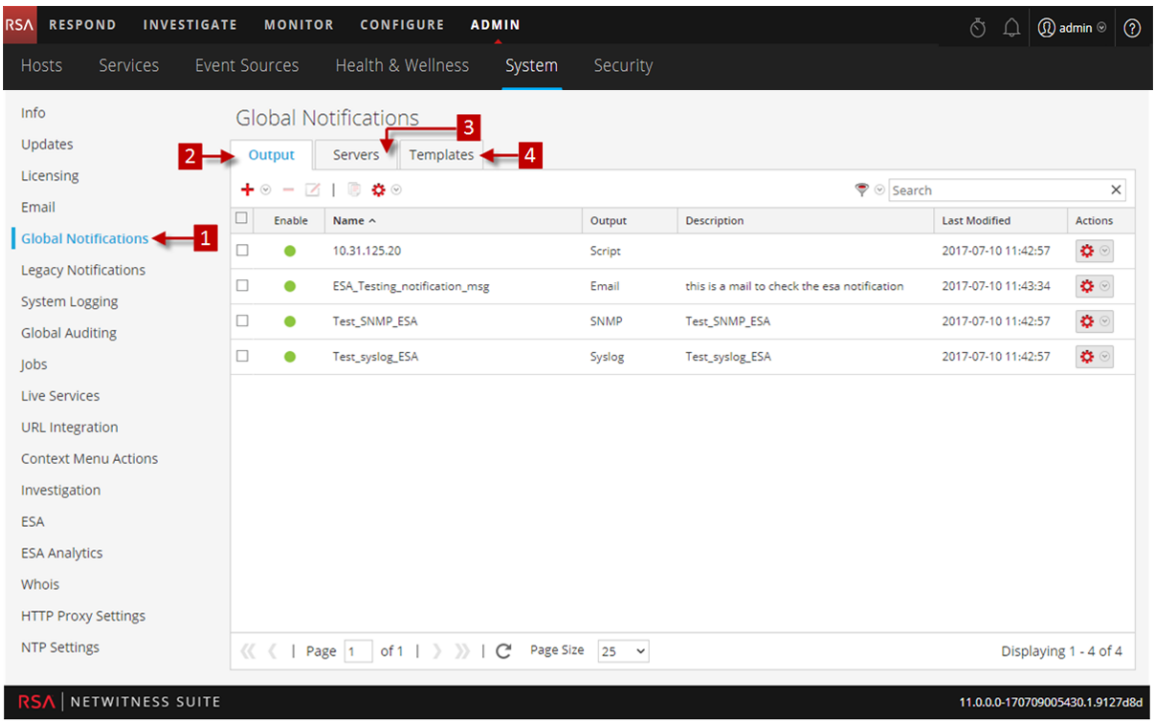
Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Konfigurieren von Benachrichtigungsservern	Registerkarte „Server“
Administrator	Konfigurieren von Benachrichtigungsausgaben	Registerkarte „Ausgabe“
Administrator	Konfigurieren von Vorlagen für Benachrichtigungen	Registerkarte Vorlagen

Verwandte Themen

- Konfigurieren Sie einen Syslog-Benachrichtigungsserver.
- Konfigurieren eines Skripts als Benachrichtigungsserver

Überblick



1 Zeigt den Bereich „Globale Benachrichtigungen“ an.

2 Zeigt die Registerkarte „Ausgabe“ an.

3 Zeigt die Registerkarte „Server“ an.

4 Zeigt die Registerkarte „Vorlagen“ an.

Symbolleiste und Funktionen

Der Bereich „Globale Benachrichtigungen“ verfügt über drei Registerkarten: Ausgabe, Server und Vorlagen.

Funktion	Beschreibung
Registerkarte „Ausgabe“	Auf dieser Registerkarte können Sie Benachrichtigungsausgaben konfigurieren. Weitere Informationen finden Sie unter „Registerkarte Ausgabe“.
Registerkarte „Server“	Auf dieser Registerkarte können Sie die Benachrichtigungsserver konfigurieren. Weitere Informationen finden Sie unter „Registerkarte Server“.

Funktion	Beschreibung
Registerkarte „Vorlagen“	Auf dieser Registerkarte können Sie Benachrichtigungsvorlagen konfigurieren. Weitere Informationen hierzu finden Sie unter „Registerkarte Vorlagen“.

In dieser Tabelle werden die Spalten im Raster für Benachrichtigungsausgaben und Benachrichtigungsserver beschrieben.

Spalte	Beschreibung
	Wählt eine Zeile für eine Aktion in der Symbolleiste aus. Wenn Sie auf das Kontrollkästchen im Spaltentitel klicken, werden alle Zeilen im Raster ausgewählt oder die Auswahl aller Zeilen wird aufgehoben.
Aktivieren	Gibt an, ob die Konfiguration aktiviert ist. Ein vollfarbiger grüner Kreis zeigt an, dass eine Konfiguration aktiviert ist. Ein leerer weißer Kreis zeigt an, dass eine Konfiguration nicht aktiviert ist.
Name	Ein Name, um die Konfiguration zu identifizieren oder zu kennzeichnen
Ausgabe	Die Konfigurationsausgabe. Die Ausgaben sind E-Mail, SNMP, Syslog und Skript.
Beschreibung	Eine kurze Beschreibung der Konfiguration
Zuletzt geändert	Zeigt das Datum und die Uhrzeit der letzten Konfigurationsänderung an.
Aktionen	In dieser Spalte kann ein Menü „Aktionen“  für die ausgewählte Konfiguration aufgerufen werden und die darin genannten Aktionen können auf die Konfiguration angewendet werden. Im Menü „Aktionen“ können Sie die Konfiguration löschen, bearbeiten, duplizieren und exportieren.

Diese Tabelle beschreibt die Spalten im Raster für Benachrichtigungsvorlagen.

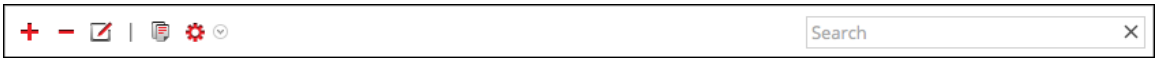
Spalte	Beschreibung
	Wählt eine Zeile für eine Aktion in der Symbolleiste aus. Wenn Sie auf das Kontrollkästchen im Spaltentitel klicken, werden alle Zeilen im Raster ausgewählt oder die Auswahl aller Zeilen wird aufgehoben.
Name	Ein Name, um die Vorlage zu identifizieren oder zu kennzeichnen.
Vorlagentyp	Der Typ der Vorlage. Die Typen sind Auditprotokollierung, Event Stream Analysis, Ereignisquellenüberwachung und Integritätsalarme.
Beschreibung	Eine kurze Beschreibung der Vorlage.
Aktionen	In dieser Spalte kann ein Menü „Aktionen“ für die ausgewählte Konfiguration aufgerufen werden und die darin genannten Aktionen können auf die Vorlage angewendet werden. Im Menü „Aktionen“ können Sie die Vorlage löschen, bearbeiten, duplizieren und exportieren.

Symbolleiste des Bereichs „Globale Benachrichtigungen“

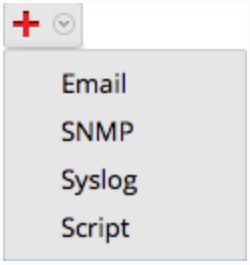
Die Symbolleiste des Bereichs Globale Benachrichtigungen befindet sich am oberen Rand der Registerkarten Ausgabe, Server und Vorlagen.

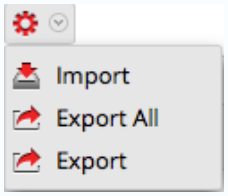
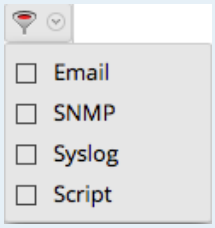
Die folgende Abbildung zeigt die Symbolleiste auf den Registerkarten Ausgabe und Server.

Die folgende Abbildung zeigt die Symbolleiste auf der Registerkarte Vorlagen.



Die folgende Tabelle beschreibt die Funktionen der Symbolleiste des Bereichs Globale Benachrichtigungen.

Funktion	Beschreibung
 	Fügt auf der Registerkarte Server einen Benachrichtigungsserver hinzu, fügt auf der Registerkarte Ausgabe eine Benachrichtigungsausgabe (Benachrichtigung) hinzu und fügt auf der Registerkarte Vorlagen eine Benachrichtigungsvorlage hinzu. Auf den Registerkarten „Server“ und „Ausgabe“ können Sie die Einstellungen für E-Mail-, SNMP-, Syslog- und Skriptbenachrichtigungen konfigurieren.
	Entfernt eine ausgewählte Benachrichtigungskonfiguration. Sie können Benachrichtigungsserver und Benachrichtigungstypen, die mit einer Konfiguration für globale Auditprotokollierung verknüpft sind, nicht löschen. Wenn Sie versuchen, eine Benachrichtigungsausgabe (Benachrichtigung) zu löschen, die von Warnmeldungen verwendet wird, wird eine Bestätigungsmeldung mit einer Warnung angezeigt, dass die diese Benachrichtigung verwendenden Warnmeldungen nicht mehr ordnungsgemäß funktionieren werden. In der Meldung wird die Anzahl der betroffenen Warnmeldungen angezeigt. Sie können eine Konfiguration auch löschen, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen > Löschen auswählen.
	Bearbeitet eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch bearbeiten, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“ > „Bearbeiten“ auswählen.
	Dupliziert eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch duplizieren, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen > Duplizieren auswählen.

Funktion	Beschreibung
	Zeigt die folgenden Optionen an: • **Importieren**: Importiert einen Benachrichtigungsserver bzw. -typ oder eine Benachrichtigungsvorlage. Beispiel: Auf der Registerkarte Server können Sie eine Benachrichtigungsserverkonfiguration importieren. • **Alle exportieren**: Exportiert alle Konfigurationen. Beispiel: Auf der Registerkarte Server können Sie alle Benachrichtigungsserverkonfigurationen exportieren. • **Export**: Exportiert eine ausgewählte Konfiguration. Sie können eine Konfiguration auch exportieren, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“ > „Exportieren“ auswählen.
	Filtert nach E-Mail, SNMP, Syslog oder Skript.
	Sucht im Raster nach Konfigurationen.

Dialogfelder zum Definieren der Benachrichtigungsserver

In diesem Thema werden die Dialogfelder zum Definieren der Benachrichtigungsserver beschrieben, über die die Einstellungen für die verschiedenen Typen von Benachrichtigungsservern konfiguriert werden. Benachrichtigungsserver werden auf der Registerkarte Administration > System > Benachrichtigungen > Server konfiguriert.

Benachrichtigungen werden in NetWitness Suite von einer Reihe von Komponenten verwendet, darunter Event Stream Analysis (ESA), Reagieren und Global Audit Logging. Die Benachrichtigungseinstellungen werden als Benachrichtigungsserver bezeichnet. Sie können auf der Registerkarte „Server“ in der Ansicht „Administration“ > „System“ im Bereich „Benachrichtigungen“ mehrere Benachrichtigungsserverkonfigurationen erstellen.

In NetWitness Suite können die folgenden Typen von Benachrichtigungsservereinstellungen konfiguriert werden:

- E-Mail
- SNMP
- Syslog
- Skript

Für die globale Auditprotokollierung können Sie nur Syslog-Benachrichtigungsserver verwenden.

Die Verfahren im Zusammenhang mit Benachrichtigungsservern werden unter Konfigurieren von Benachrichtigungsservern beschrieben.

So rufen Sie die Dialogfelder zum Definieren der Benachrichtigungsserver auf:

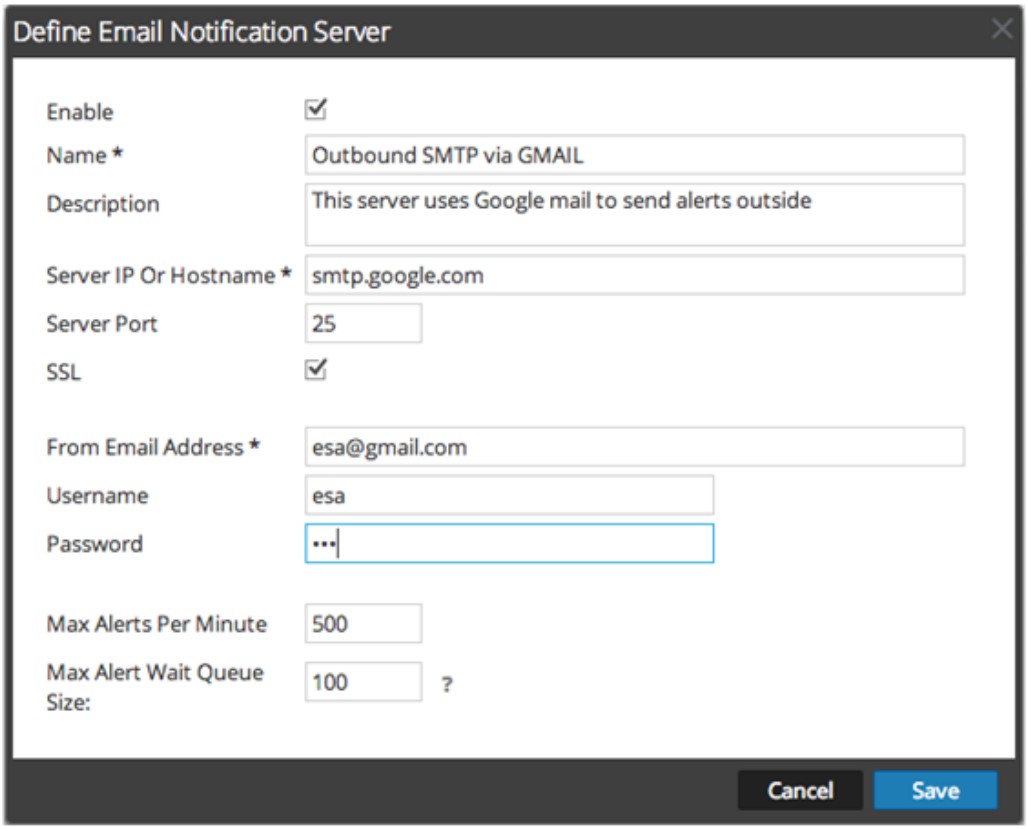
1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im linken Navigationsbereich **Globale Benachrichtigungen** aus.
3. Klicken Sie im Bereich **Benachrichtigungsserver** auf + und wählen Sie einen Benachrichtigungstyp aus (E-Mail, SNMP, Syslog oder Skript).
   Das Dialogfeld „Benachrichtigungsserver definieren“ wird zur Auswahl angezeigt.

Es gibt vier Dialogfelder zur Konfiguration der Benachrichtigungsserver.

E-Mail

Mit E-Mail-Benachrichtigungsservern können Sie E-Mail-Servereinstellungen zum Senden von Warnmeldungsbenachrichtigungen konfigurieren.

In der folgenden Abbildung ist das Dialogfeld „E-Mail-Benachrichtigungsserver definieren“ dargestellt.



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die E-Mail-Benachrichtigungsserver definieren müssen.

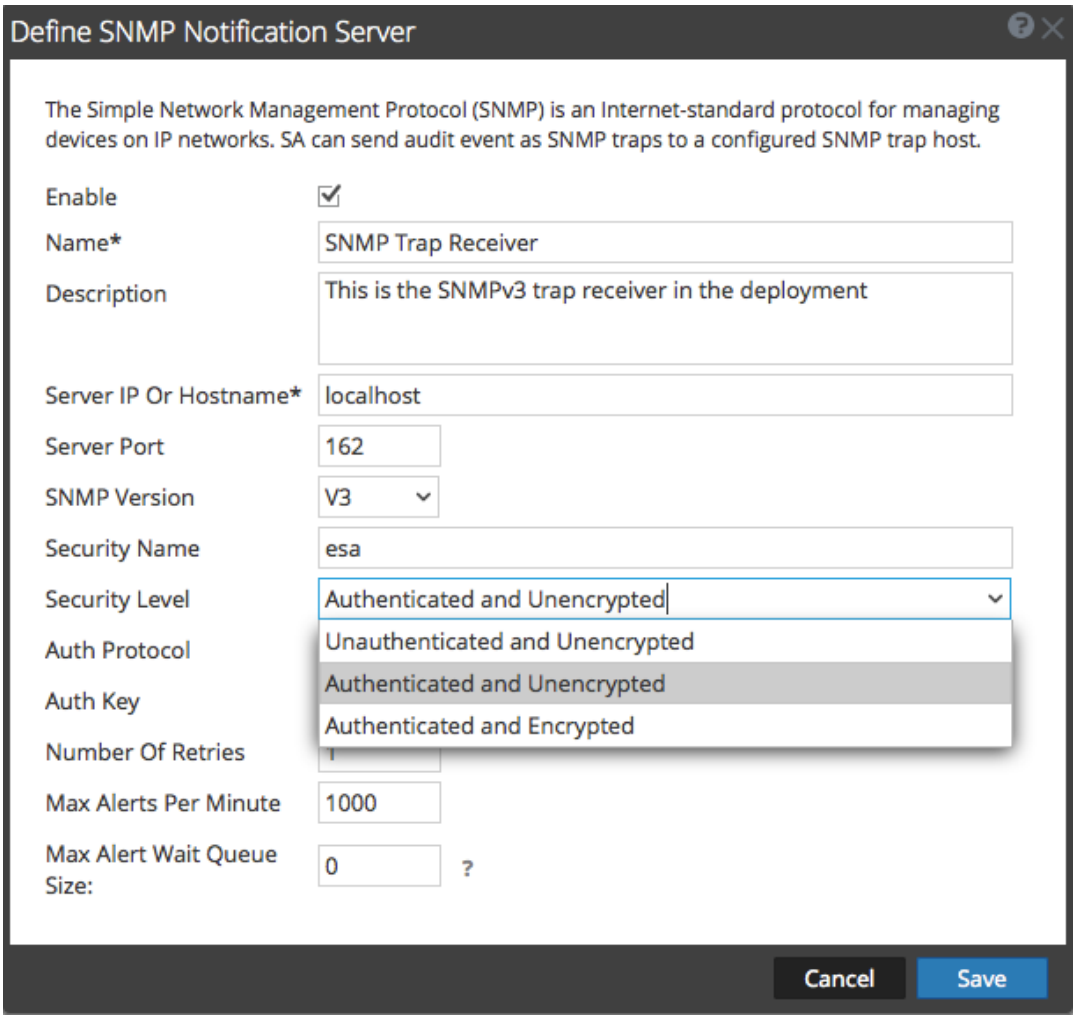
Parameter	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Benachrichtigungsservers.
Beschreibung	Eine kurze Beschreibung des Benachrichtigungsservers.
IP-Adresse oder Hostname des Servers	Hostname des E-Mail-Servers. Für ESM-/SMS- und ESA-Benachrichtigungen müssen Sie nur den Hostnamen/vollständig qualifizierten Domainnamen angeben.
Serverport	Port des Servers

Parameter	Beschreibung
SSL	Aktivieren Sie dieses Kontrollkästchen, wenn die Kommunikation über SSL erfolgen soll.
Absender-E-Mail-Adresse	Das E-Mail-Konto, von dem Sie E-Mail-Benachrichtigungen senden möchten.
Benutzername	Der Benutzername für die Anmeldung beim E-Mail-Konto, wenn der SMTP-Server zur erfolgreichen Übermittlung von E-Mail-Nachrichten eine Benutzerauthentifizierung erfordert.
Password	Das Benutzerpasswort für die Anmeldung beim E-Mail-Konto, wenn der SMTP-Server zur erfolgreichen Übermittlung von E-Mail-Nachrichten eine Benutzerauthentifizierung erfordert.
Max. Warnmeldungen pro Minute	Gibt die maximale Anzahl von Warnmeldungen pro Minute an.
Max. Größe von Warnmeldungen in der Warteschlange	Gibt die maximale Anzahl von Warnmeldungen an, die in die Warteschlange gestellt werden können, bevor sie gelöscht werden.

SNMP

Mit SNMP-Benachrichtigungsservern können Sie SNMP-Trap-Hosteinstellungen als Benachrichtigungsserver zum Senden von Warnmeldungsbenachrichtigungen konfigurieren.

Die folgende Abbildung zeigt das Dialogfeld „SNMP-Benachrichtigungsserver definieren“.



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die SNMP-Benachrichtigungsserver definieren müssen.

Parameter	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Benachrichtigungsservers.
Beschreibung	Eine kurze Beschreibung des Benachrichtigungsservers.
IP-Adresse oder Hostname des Servers	Die IP-Adresse des SNMP-Trap-Hosts oder der Hostname.

Parameter	Beschreibung
Serverport	Die Nummer des Überwachungsports auf dem SNMP-Trap-Host.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>SNMP-Version</td><td>Die SNMP-Version. Folgende Optionen stehen zur Verfügung:
V1
V2C
V3
Wenn Sie die SNMP-Version 3 (v3) auswählen, werden die folgenden Parameter angezeigt:

<table><tr><th>Parameter</th><th>Beschreibung</th></tr><tr><td>Benachrichtigungstyp</td><td>Basierend auf dem Benachrichtigungstyp wird jedes Mal, wenn SNMP-Meldungen erzeugt werden, eine Warnmeldung gesendet.
Die folgenden Benachrichtigungstypen werden unterstützt:
Informieren – Trap Informieren wird bestätigt. Der Absender erhält vom Empfänger eine Bestätigung.
Trap – Trap ist eine nicht bestätigte Benachrichtigung</td></tr><tr><td>Autorisierende Engine-ID (diese Option ist nur für den Benachrichtigungstyp TRAP verfügbar)</td><td>Bezeichnung zum Identifizieren der Agenten. Autorisierende Engine-ID zusammen mit dem Benutzernamen wird verwendet, um den Agent eindeutig zu identifizieren.</td></tr><tr><td>Sicherheitsebene</td><td>Definiert die Sicherheitsebene. Folgende Optionen stehen zur Verfügung:
Nicht authentifiziert und</td></tr></table></td></tr>
</table>

Parameter	Beschreibung	
		unverschlüsselt • Authentifiziert und unverschlüsselt • Authentifiziert und verschlüsselt
	Auth-Protokoll (Diese Option steht nur für Sicherheitsstufe Authentifiziert und Unverschlüsselt und Authentifiziert und Verschlüsselt zur Verfügung)	Authentifizierungsprotokoll, das verwendet wird, um einen Benutzer zu überprüfen, bevor er Zugriff auf den Server erhält. Es sind folgende Optionen verfügbar: • SHA • MD5
	Authentifizierungsschlüssel (Diese Option steht nur für Sicherheitsstufe Authentifiziert und Unverschlüsselt und Authentifiziert und Verschlüsselt zur Verfügung)	Ein Passwort, die Sie für die Authentifizierung verwenden können.
	Datenschutzprotokoll (Diese Option steht nur für Sicherheitsstufe Authentifiziert und Verschlüsselt zur Verfügung)	Das Datenschutzprotokoll ist eine Verschlüsselungsmethode für den Datenaustausch.
	Privater Schlüssel (Diese Option steht nur für	Ein Passwort, das Sie für die Verschlüsselung verwenden

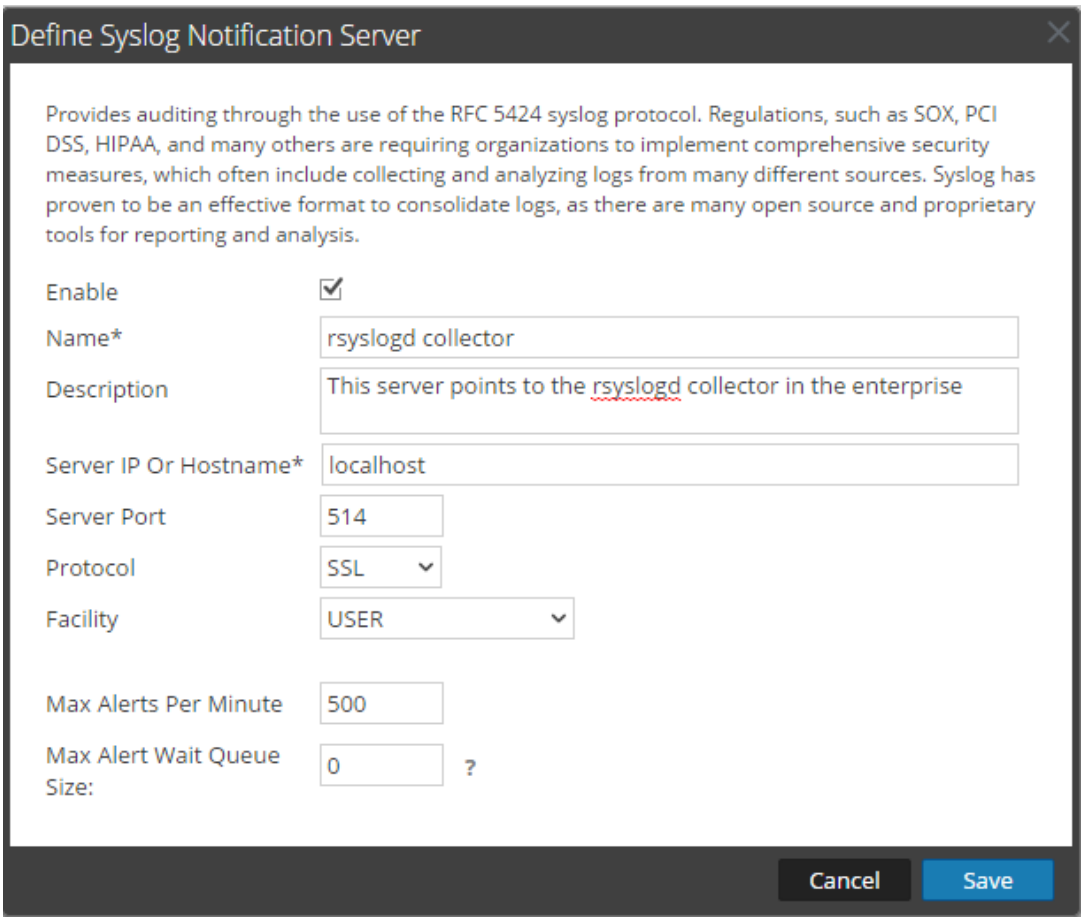
Parameter	Beschreibung
	Sicherheitsstufe Authentifiziert und Verschlüsselt zur Verfügung) können.
Community	Die Communityzeichenfolge, die zur Authentifizierung auf dem SNMP-Trap-Host verwendet wird. Der Standardwert ist **öffentlich**.
Anzahl erneuter Versuche	Die Anzahl der Wiederholungen für den Trap.
Max. Warnmeldungen pro Minute	Maximale Anzahl von Warnmeldungen pro Minute.
Max. Größe von Warnmeldungen in der Warteschlange	Maximale Anzahl von Warnmeldungen, die in die Warteschlange gestellt werden können, bevor sie gelöscht werden.

Syslog

Mit Syslog-Benachrichtigungsservern können Sie Syslog-Einstellungen als Benachrichtigungsserver zum Senden von Benachrichtigungen konfigurieren. Wenn diese Funktion aktiviert ist, wird das Auditing von Syslog über das Syslog-Protokoll RFC 5424 bereitgestellt. Da es für Syslog zahlreiche systemeigene und Open-Source-Tools für das Reporting und Analysen gibt, hat sich Syslog als effektives Format zur Konsolidierung von Protokollen erwiesen.

Benachrichtigungsserver, die mit globalen Konfigurationen zur Auditprotokollierung verknüpft sind, können nicht deaktiviert werden.

Die folgende Abbildung zeigt das Dialogfeld „Syslog-Benachrichtigungsserver definieren“.



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die Syslog-Benachrichtigungsserver definieren müssen.

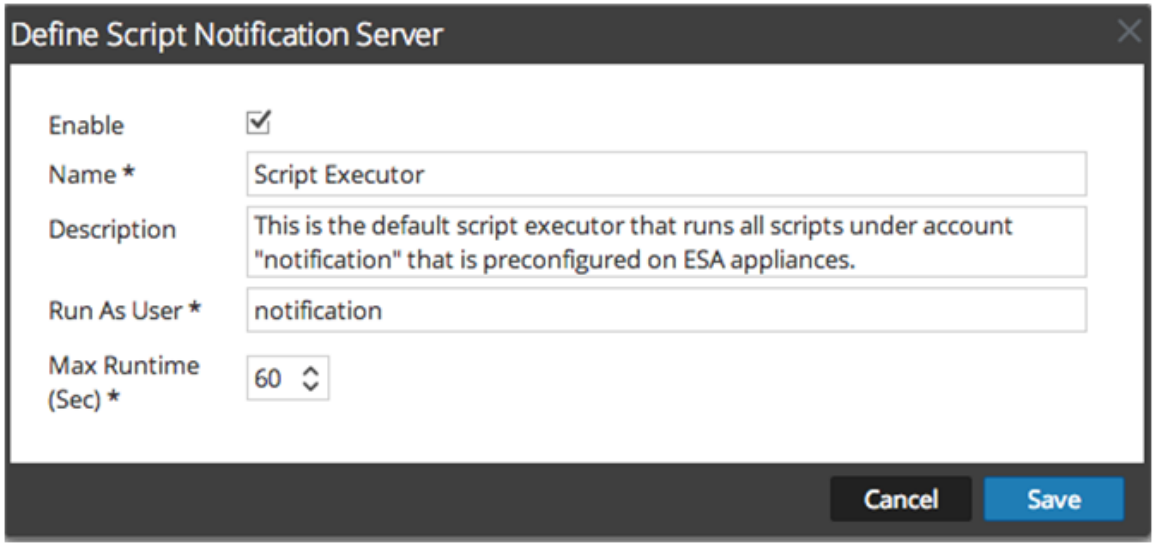
Parameter	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Benachrichtigungsservers.
Beschreibung	Eine kurze Beschreibung des Benachrichtigungsservers.
IP-Adresse oder Hostname des Servers	Der Name des Hosts, auf dem der Ziel-Syslog-Prozess ausgeführt wird.
Serverport	Die Nummer des Ports, den der Ziel-Syslog-Prozess überwacht.

Parameter	Beschreibung
Protokoll	Das für die Übertragung der Syslog-Dateien zu verwendende Protokoll.
Gerät	Die für alle ausgehenden Nachrichten zu verwendende designierte Syslog-Installation. Hiermit wird angegeben, mit welchem Programmtyp die Nachricht protokolliert wird. Einige mögliche Werte sind KERN, USER, MAIL und DAEMON. Mit dieser Option kann die Konfigurationsdatei festlegen, dass Nachrichten von anderen Installationen unterschiedlich behandelt werden.
Max. Warnmeldungen pro Minute	Maximale Anzahl von Warnmeldungen pro Minute. Dieses Feld wird für die Globale Auditprotokollierung nicht verwendet.
Max. Größe von Warnmeldungen in der Warteschlange	Maximale Anzahl von Warnmeldungen, die in die Warteschlange gestellt werden können, bevor sie gelöscht werden. Dieses Feld wird für die Globale Auditprotokollierung nicht verwendet.

Skript

Mit Skriptbenachrichtigungsservern können Sie das Skript als Benachrichtigungsserver konfigurieren.

Die folgende Abbildung zeigt das Dialogfeld Skriptbenachrichtigungsserver definieren.



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die Skriptbenachrichtigungsserver definieren müssen.

Parameter	Beschreibung
Aktivieren	Wählen Sie dies aus, um den Benachrichtigungsserver zu aktivieren.
Name	Ein Name zum Identifizieren oder Bezeichnen des Benachrichtigungsservers.
Beschreibung	Eine kurze Beschreibung des Benachrichtigungsservers.
Als Benutzer ausführen	Der Name der Benutzeridentität, unter der das Skript ausgeführt wird. Die Standardbenutzeridentität lautet **Benachrichtigung**. Für ESA kann keine andere Einstellung ausgewählt werden, es sei denn, Sie haben das Konto auf dem ESA-Host erstellt.
Max. Laufzeit (Sek.)	Die maximale Dauer (in Sekunden), die das Skript ausgeführt werden kann.

Dialogfelder zum Definieren von Benachrichtigungsausgaben

In diesem Thema werden die verschiedenen Dialogfelder für die Benachrichtigungsausgabe beschrieben. Sie konfigurieren Benachrichtigungsausgaben auf der Registerkarte ADMIN > System > Benachrichtigungen > Ausgabe. Benachrichtigungen sind im Wesentlichen die Ziele, die für das Versenden von Benachrichtigungen verwendet werden. Für ESA können Sie mithilfe von Benachrichtigungen definieren, wie Sie ESA-Warnmeldungen empfangen möchten. Im Folgenden sind die verschiedenen Benachrichtigungen aufgeführt, die von NetWitness Suite unterstützt werden:

- E-Mail
- SNMP
- Syslog
- Skript

Beschreibungen von Verfahren in Bezug auf Benachrichtigungen finden Sie in Konfigurieren von Benachrichtigungsausgaben.

So greifen Sie auf die Dialoge zur Definition von Benachrichtigungen zu:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich **Optionen** die Option **Globale Benachrichtigungen** aus.
3. Klicken Sie auf der Registerkarte **Ausgabe** auf + und wählen Sie dann eine Benachrichtigungsausgabe (E-Mail, SNMP, Syslog oder Skript).
   Das Dialogfeld „Benachrichtigung definieren“ wird Ihnen zur Auswahl angezeigt.

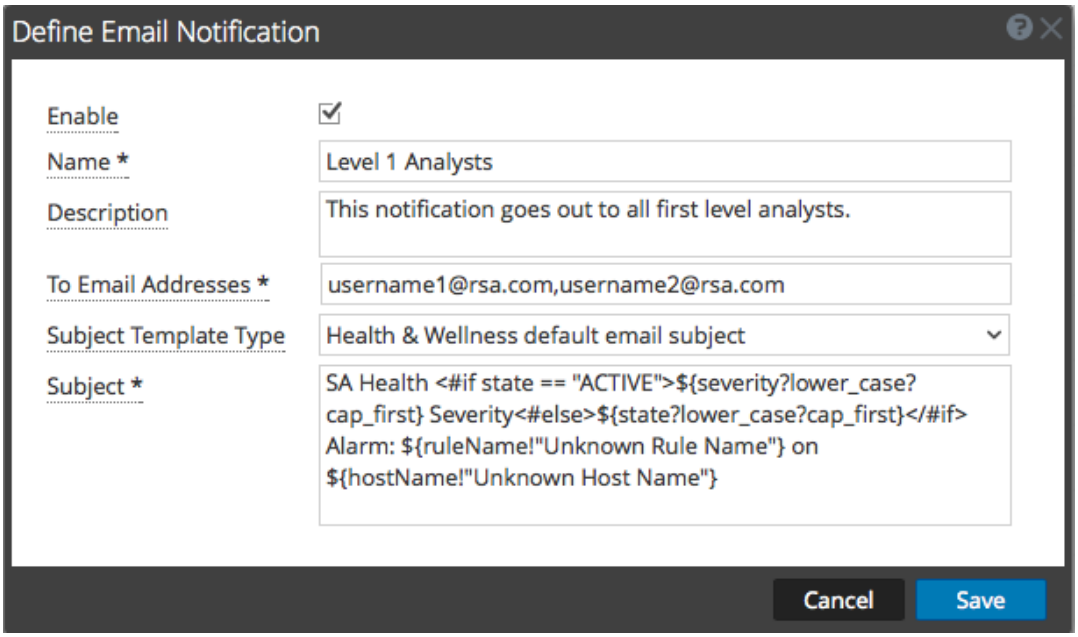
Funktionen

Es gibt vier Benachrichtigungsdialoge, die Ihnen erlauben, Benachrichtigungsausgaben zu konfigurieren.

E-Mail

Mithilfe der E-Mail-Benachrichtigungen können Sie Ziel-E-Mail-Adressen definieren, an die Sie die Warnmeldungen senden können. Darüber hinaus können Sie im Betreff der E-Mail eine angepasste Beschreibung hinzufügen und mehrere Ziel-E-Mail-Adressen definieren.

Die folgende Abbildung zeigt das Dialogfeld „E-Mail-Benachrichtigung definieren“:



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die E-Mail-Benachrichtigungen definieren müssen.

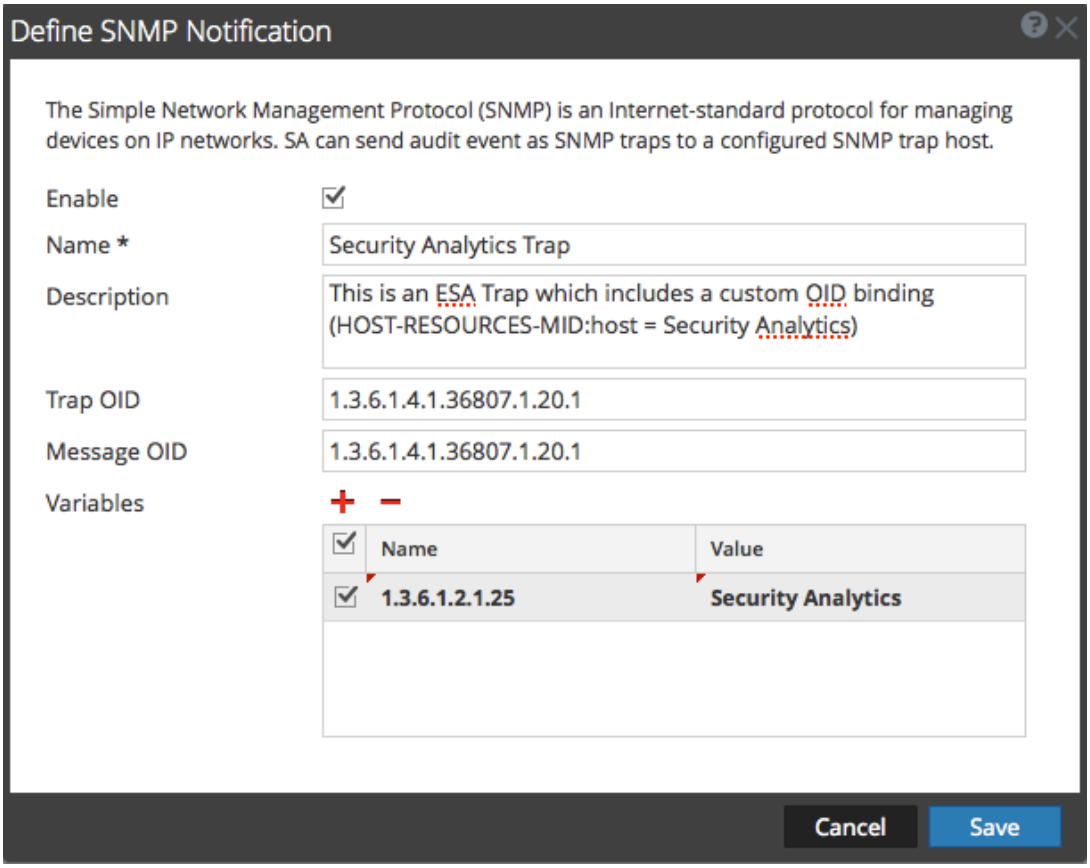
Parameter	Beschreibung
Aktivieren	Wählen oder aktivieren Sie die Benachrichtigung.
Name	Ein Name, um die Benachrichtigung zu identifizieren oder zu kennzeichnen.
Beschreibung	Eine kurze Beschreibung der Benachrichtigung.
E-Mail-Adressen der Empfänger	Beschreibt die Ziel-E-Mail-Adressen, an die die Warnmeldung gesendet werden muss. **Hinweis:** Sie können mehrere E-Mail-Adressen definieren.
Betreffvorlagentyp	Listet die verfügbaren Vorlagen zur Erstellung eines Betreffs auf. Wenn Sie eine Vorlage wählen, wird das Feld Betreff automatisch mit dem Code für Ihre gewählte Vorlage ausgefüllt.

Parameter	Beschreibung
Betreff	Angepasste Beschreibung der ausgelösten Warnmeldung. Diese Informationen werden automatisch eingetragen, wenn Sie eine der vordefinierten Vorlagen aus dem Drop-down-Menü für den Vorlagentyp „Betreff“ auswählen. **Hinweis:** Wie Sie einen benutzerdefinierten Betreff angeben, erfahren Sie unter Einbeziehen der Standardbetreffzeile für E-Mails im *Leitfaden Systemwartung*.

SNMP

Mithilfe von SNMP-Benachrichtigungen können Sie die SNMP-Einstellungen für das Versenden von Warnmeldungsbenachrichtigungen definieren.

Die folgende Abbildung zeigt das Dialogfeld „SNMP-Benachrichtigung definieren“.



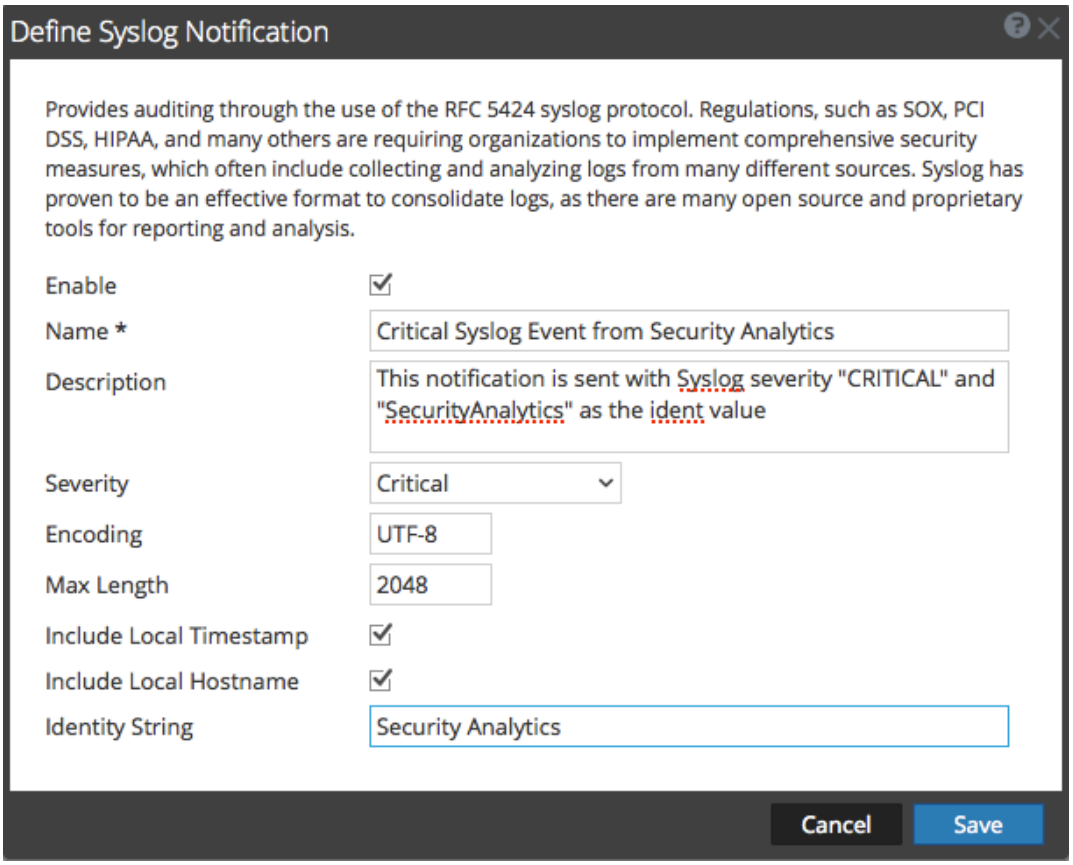
In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die SNMP-Benachrichtigungen definieren müssen.

Parameter	Beschreibung
Aktivieren	Wählen oder aktivieren Sie die Benachrichtigung.
Name	Ein Name, um die Benachrichtigung zu identifizieren oder zu kennzeichnen.
Beschreibung	Eine kurze Beschreibung der Benachrichtigung.
Trap-OID	Die Objekt-ID der SNMP-Trap auf dem Trap-Host, der das Ereignis empfängt. Der Standardwert ist **1.3.6.1.4.1.36807.1.20.1**. Dieser Wert ist ein hierarchischer Name, der das System repräsentiert, das die Trap erzeugt. 1.3.6.1.4.1 ist das gemeinsame Präfix für alle Unternehmen und 36807.1.20.1 kennzeichnet NetWitness Suite.
Meldungs-OID	Der Meldungsobjektbezeichner der SNMP-Trap.
Variablen	Zusätzliche Informationen, die in der Trap enthalten sein sollten. Bei dieser Variablen handelt es sich um ein name:value-Paar.

Syslog

Bei Syslog-Benachrichtigungen können Sie die Syslog-Einstellungen für das Senden von Warnmeldungsbenachrichtigungen definieren.

Die folgende Abbildung zeigt das Dialogfeld „Syslog-Benachrichtigungen definieren“.



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die Syslog-Benachrichtigungen definieren müssen.

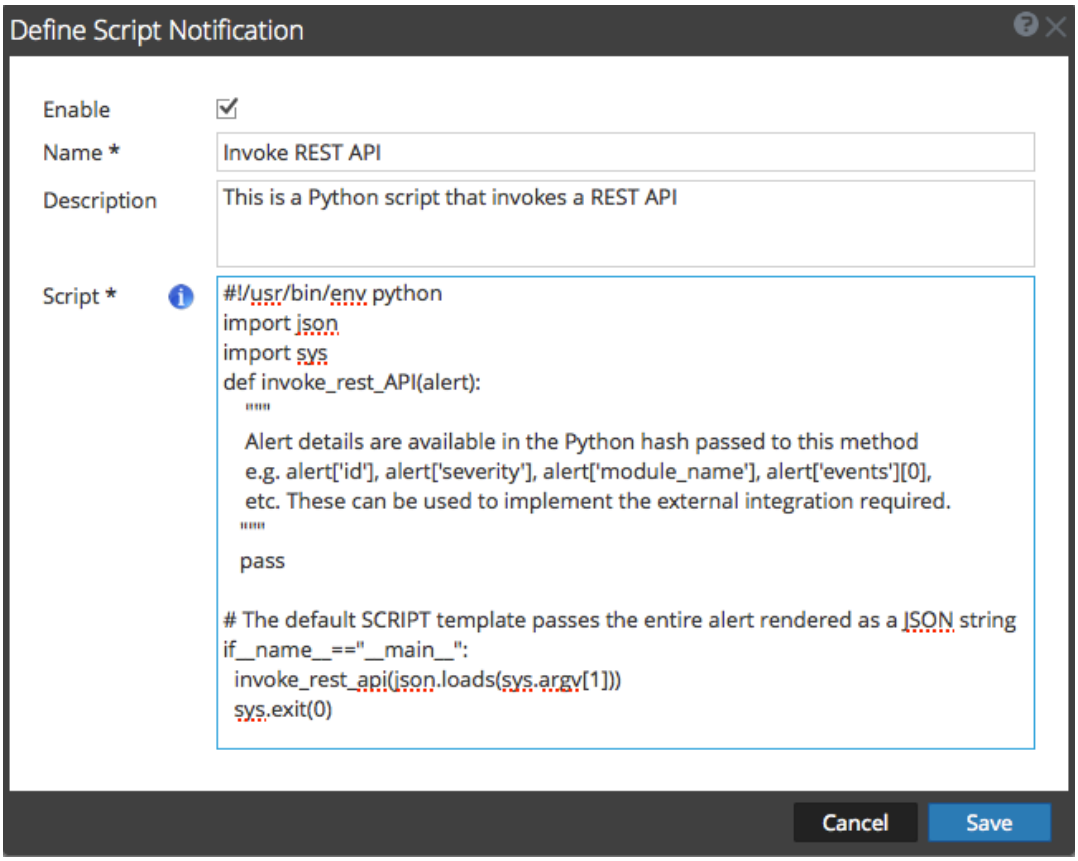
Parameter	Beschreibung
Aktivieren	Wählen oder aktivieren Sie die Benachrichtigung.
Name	Ein Name, um die Benachrichtigung zu identifizieren oder zu kennzeichnen.
Beschreibung	Eine kurze Beschreibung der Benachrichtigung.
Schweregrad	Definiert den Schweregrad der Warnmeldung.
Codierung	Definiert das Codierungsformat. In einigen Umgebungen, in denen keine regulären Zeichensätze verwendet werden (z. B. japanische Zeichen), hilft dieses Feld bei der Auswahl der richtigen Zeichencodierung.

Parameter	Beschreibung
Max. Länge	Die maximale Länge einer Syslog-Meldung in Byte. Der Standardwert ist **2.048**. Nachrichten, die die maximal zulässige Länge überschreiten, werden gekürzt, wenn das Kontrollkästchen **Zu lange Syslog-Meldungen kürzen** unter „Administration“ > „System“ > „Alte Benachrichtigungen“ aktiviert ist. Weitere Informationen finden Sie im Bereich „Konfiguration alter Benachrichtigungen“.
Lokalen Zeitstempel hinzufügen	Wählen Sie diesen Parameter, um den lokalen Zeitstempel in Meldungen hinzuzufügen.
Lokalen Hostnamen hinzufügen	Wählen Sie diesen Parameter, um den lokalen Hostnamen in Syslog-Meldungen hinzuzufügen.
Identitätszeichenfolge	Dies ist eine Identitätszeichenfolge, die jeder Syslog-Warnmeldung vorangestellt werden muss. Wenn die Zeichenfolge leer ist, wird den ausgehenden Syslog-Warnmeldungen keine Identitätszeichenfolge vorangestellt. Hiermit können Sie Warnmeldungen von ESA kennzeichnen.

Skript

Mithilfe von Skriptbenachrichtigungen können Sie das Skript definieren, das in Reaktion auf die Warnmeldung ausgeführt wird. Sie können ein beliebiges Skript für ESA-Benachrichtigungen angeben.

Die folgende Abbildung zeigt das Dialogfeld „Skriptbenachrichtigung definieren“:



In der folgenden Tabelle sind die verschiedenen Parameter aufgeführt, die Sie für die Skriptbenachrichtigungen definieren müssen.

Parameter	Beschreibung
Aktivieren	Wählen oder aktivieren Sie die Benachrichtigung.
Name	Ein Name, um die Benachrichtigung zu identifizieren oder zu kennzeichnen.
Beschreibung	Eine kurze Beschreibung der Benachrichtigung.
Skript	Definiert das Skript.

Dialogfeld „Benachrichtigungsvorlage definieren“

Im Bereich Globale Benachrichtigungen können Sie globale Benachrichtigungen für Benachrichtigungsserver, Benachrichtigungsausgaben und Benachrichtigungsvorlagen konfigurieren. In der Registerkarte Vorlagen werden die Vorlagen für die einzelnen Benachrichtigungen konfiguriert. In der Vorlage „Benachrichtigung“ werden die Felder „Format“ und „Meldung der Benachrichtigungen“ festgelegt. Nutzen Sie zum Konfigurieren und Bearbeiten von Vorlagen das Dialogfeld „Vorlage definieren“ oder wählen Sie eine Standardvorlage aus.

Sie können folgende Vorlagentypen definieren:

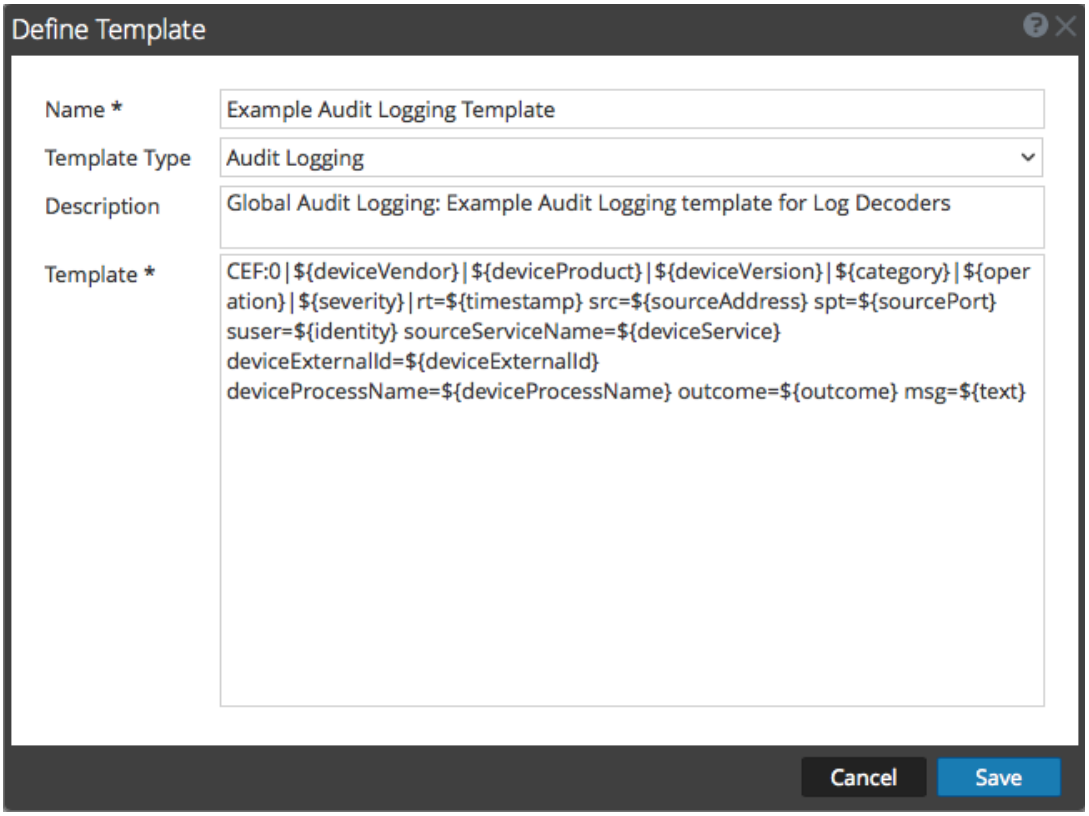
- Auditprotokollierung
- Event Stream Analysis
- Ereignisquellenüberwachung
- Warnmeldungen zur Integrität

Für Benachrichtigungsvorlagen verwendete Verfahren werden unter Konfigurieren von Vorlagen für Benachrichtigungen beschrieben.

So greifen Sie auf das Dialogfeld „Vorlage definieren“ zu:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im linken Navigationsbereich **Globale Benachrichtigungen > Registerkarte Vorlage** aus.
3. Klicken Sie im Bereich **Benachrichtigungskonfigurationen** auf  oder wählen Sie eine Konfiguration und klicken Sie auf  .

Es wird das Dialogfeld **Vorlage definieren** angezeigt.



Funktionen

In der folgenden Tabelle werden die Funktionen im Dialogfeld Vorlage definieren beschrieben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Benachrichtigungsvorlage ein.
Vorlagentyp	Wählen Sie den Typ der zu erstellenden Vorlage aus: • **Auditprotokollierung**: Verwenden Sie diese Vorlage für Globale Auditprotokollierung. • **Event Stream Analysis**: Verwenden Sie diesen Vorlagentyp für ESA-Warnmeldungsbenachrichtigungen. • **Ereignisquellenüberwachung**: Verwenden Sie diesen Vorlagentyp für ESM-Benachrichtigungen. • **Integritätsalarme**: Verwenden Sie diesen Vorlagentyp für Benachrichtigungen zu Integrität und Zustand.

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die Vorlage ein. Wenn Sie beispielsweise eine Benachrichtigungsvorlage für Log Decoders erstellen, die für die globale Auditprotokollierung verwendet werden soll, können Sie dies in der Beschreibung angeben.
Vorlage	Geben Sie das Format für die Vorlage an. Im Thema Definieren einer Vorlage für die globale Auditprotokollierung erfahren Sie, wie Sie eine Auditprotokollierungsvorlage zur Verwendung für die globale Auditprotokollierung definieren. Weitere Informationen zum Definieren einer Vorlage für Event Stream Analysis (ESA) finden Sie unter Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen.

Registerkarte „Ausgabe“

Im Bereich **Globale Benachrichtigungen**, Registerkarte **Ausgabe** (Admin > System > Benachrichtigungen > Ausgabe) können Sie Benachrichtigungsausgaben konfigurieren. In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Management, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert.

In den Konfigurationen für die **Benachrichtigungsausgabe** werden E-Mail-Adressen und Betreffzeilen, SNMP-Trap-OID-Einstellungen, Syslog-Ausgabeeinstellungen und Skriptcode definiert.

Benachrichtigungen sind die Ziele, die für vom ESA-Service gesendete Warnmeldungsbenachrichtigungen konfiguriert wurden. Sie können mithilfe der Registerkarte Ausgabe Folgendes als Ziel konfigurieren:

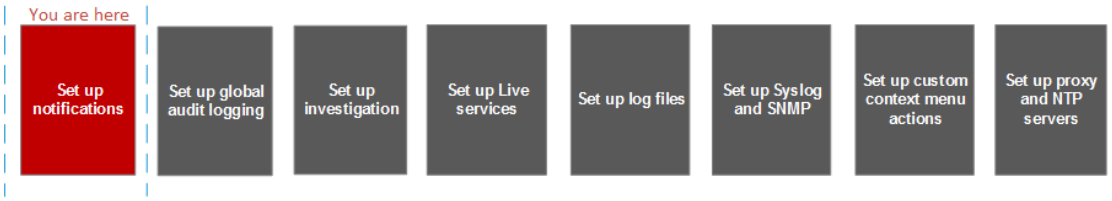
- E-Mail
- SNMP
- Syslog
- Skript

Hinweis: Die Registerkarte „Ausgabe“ für die globale Auditprotokollierung muss nicht konfiguriert werden. Detaillierte Schritte finden Sie unter Konfigurieren der globalen Auditprotokollierung.

Workflow

Der Workflow zeigt die erforderlichen Verfahren zum Konfigurieren und überprüfen der Ausgabe für globale Benachrichtigungen. Hier können Sie folgende Aufgaben ausführen:

- Konfigurieren der E-Mail-Einstellungen als Benachrichtigung
- Konfigurieren von SNMP-Einstellungen als Benachrichtigung
- Konfigurieren von Syslog-Einstellungen als Benachrichtigung
- Konfigurieren eines Skripts als Benachrichtigung



Was möchten Sie tun?

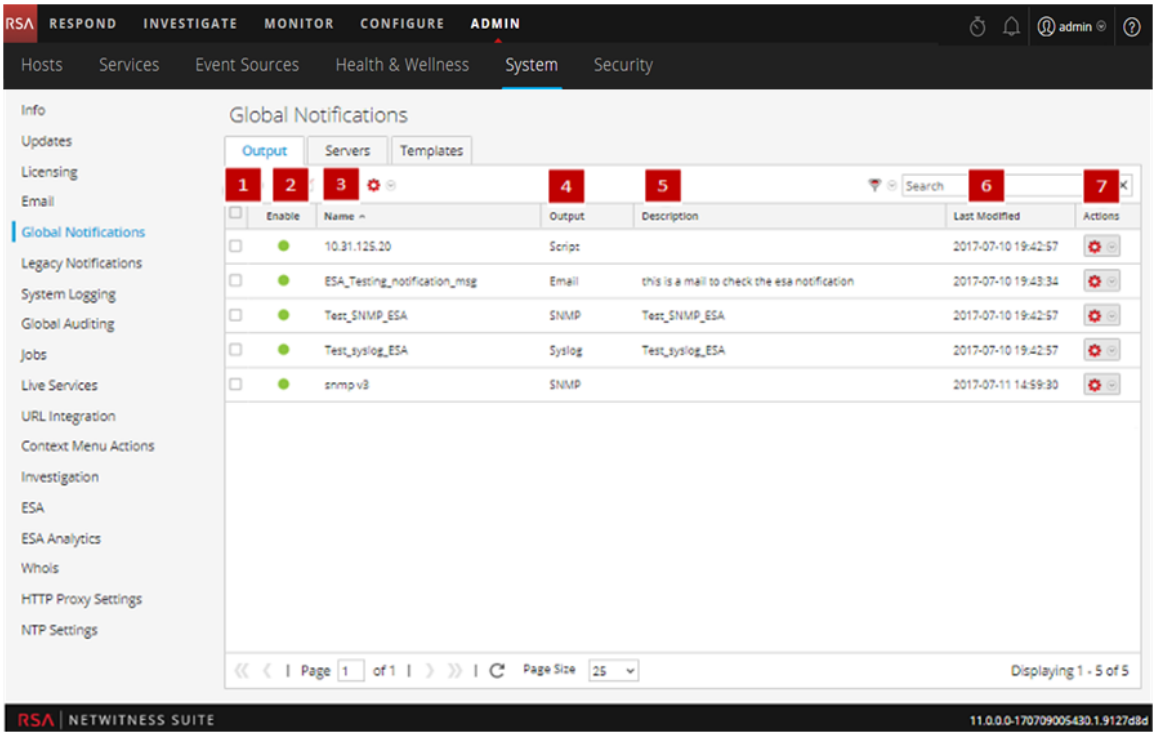
Rolle	Ich möchte...	Details anzeigen
Administrator	Definieren von Benachrichtigungsausgaben.	Konfigurieren von Benachrichtigungsausgaben

Verwandte Themen

- Benachrichtigungsausgaben – Übersicht
- Konfigurieren von E-Mail als Benachrichtigung
- Konfigurieren von Skript als Benachrichtigung
- Konfigurieren von SNMP als Benachrichtigung
- Konfigurieren von Syslog als Benachrichtigung

Überblick

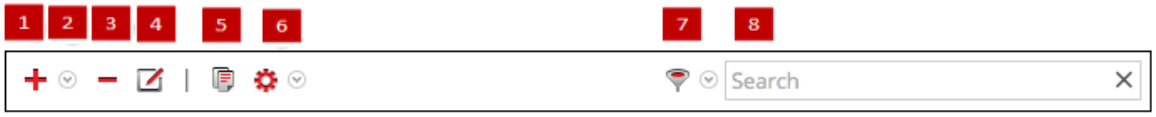
Das folgende Beispiel zeigt die globale Benachrichtigungsausgaben-Konfiguration.



1 Wählt eine Zeile für eine Aktion in der Symbolleiste aus. Durch Aktivieren des Kontrollkästchens im Spaltentitel werden alle Zeilen im Raster ausgewählt oder deren Auswahl aufgehoben.

2	Gibt an, ob die Konfiguration aktiviert ist. Ein vollfarbiger grüner Kreis zeigt an, dass eine Konfiguration aktiviert ist. Ein leerer weißer Kreis zeigt an, dass eine Konfiguration nicht aktiviert ist.
3	Identifiziert oder kennzeichnet eine Konfiguration
4	Identifiziert die Konfigurationsausgabe. Die Ausgaben sind E-Mail, SNMP, Syslog und Skript.
5	Beschreibt die Speicherkonfiguration.
6	Zeigt das Datum und die Uhrzeit der letzten Konfigurationsänderung an.
7	In dieser Spalte kann ein Menü „Aktionen“ für die ausgewählte Konfiguration aufgerufen werden und die darin genannten Aktionen können auf die Konfiguration angewendet werden. Im Menü „Aktionen“ können Sie die Konfiguration löschen, bearbeiten, duplizieren und exportieren.

Die Symbolleiste des Bereichs globale Benachrichtigungen befindet sich oben im Ausgabe-Tag und bietet die folgenden Optionen:



1	Fügt eine Benachrichtigungsausgabe hinzu
2	Konfiguriert die Einstellungen für E-Mail, SNMP, Syslog und Skript-Benachrichtigungen.
3	Entfernt eine ausgewählte Benachrichtigungskonfiguration. Sie können Benachrichtigungsserver und Benachrichtigungstypen, die mit einer Konfiguration für globale Auditprotokollierung verknüpft sind, nicht löschen. Wenn Sie versuchen, eine Benachrichtigungsausgabe (Benachrichtigung) zu löschen, die von Warnmeldungen verwendet wird, wird eine Bestätigungsmeldung mit einer Warnung angezeigt, dass die diese Benachrichtigung verwendenden Warnmeldungen nicht mehr ordnungsgemäß funktionieren werden. In der Meldung wird die Anzahl der betroffenen Warnmeldungen angezeigt. Sie können eine Konfiguration auch löschen, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen > Löschen auswählen.
4	Bearbeitet eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch bearbeiten, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“ die Optionen > „Bearbeiten“ auswählen.

5 Dupliziert eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch duplizieren, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen  > Duplizieren auswählen.

6 Zeigt die folgenden Optionen an:

- **Importieren**: Importiert einen Benachrichtigungsserver bzw. -typ oder eine Benachrichtigungsvorlage. Beispiel: Auf der Registerkarte Server können Sie eine Benachrichtigungsserverkonfiguration importieren.
- **Alle exportieren**: Exportiert alle Konfigurationen. Beispiel: Auf der Registerkarte Server können Sie alle Benachrichtigungsserverkonfigurationen exportieren.
- **Export**: Exportiert eine ausgewählte Konfiguration. Sie können eine Konfiguration auch exportieren, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“  > „Exportieren“ auswählen.

7 Filtert nach E-Mail, SNMP, Syslog oder Skript.

8 Sucht im Raster nach Konfigurationen.

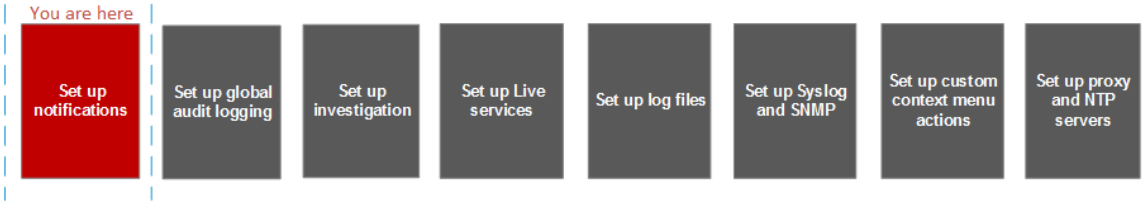
Registerkarte „Server“

In diesem Thema werden die Komponenten der Registerkarte Globale Benachrichtigungen > Server beschrieben. Auf dieser Registerkarte können Sie die Benachrichtigungsserver konfigurieren. In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Management, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert.

Benachrichtigungsserver werden auf der Registerkarte „Server“ konfiguriert. Auf der Registerkarte **Server** fügen Sie die Server hinzu, von denen Sie Benachrichtigungen vom System erhalten möchten. Für Globale Auditprotokollierung definieren Sie Log Decoder als Syslog-Benachrichtigungsserver.

Event Stream Analysis kann Benachrichtigungen per E-Mail, SNMP oder Syslogan Benutzer senden, wenn eine Warnmeldung für den ESA-Service ausgelöst wurde. Diese Absender von Warnmeldungsbenachrichtigungen werden als Benachrichtigungsserver bezeichnet. Sie können mehrere Benachrichtigungseinstellungen konfigurieren und beim Definieren einer ESA-Regel verwenden. Beispielsweise können Sie mehrere E-Mail-Server oder Syslog-Server konfigurieren und die Einstellungen beim Definieren einer ESA-Regel verwenden.

Workflow



Der Workflow zeigt die erforderlichen Verfahren zum Konfigurieren und überprüfen der Server für globale Benachrichtigungen. Hier können Sie folgende Aufgaben ausführen:

- Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver
- Konfigurieren der SNMP-Einstellungen als Benachrichtigungsserver
- Konfigurieren der Syslog-Einstellungen als Benachrichtigungsserver
- Konfigurieren eines Skripts als Benachrichtigungsserver

Was möchten Sie tun?

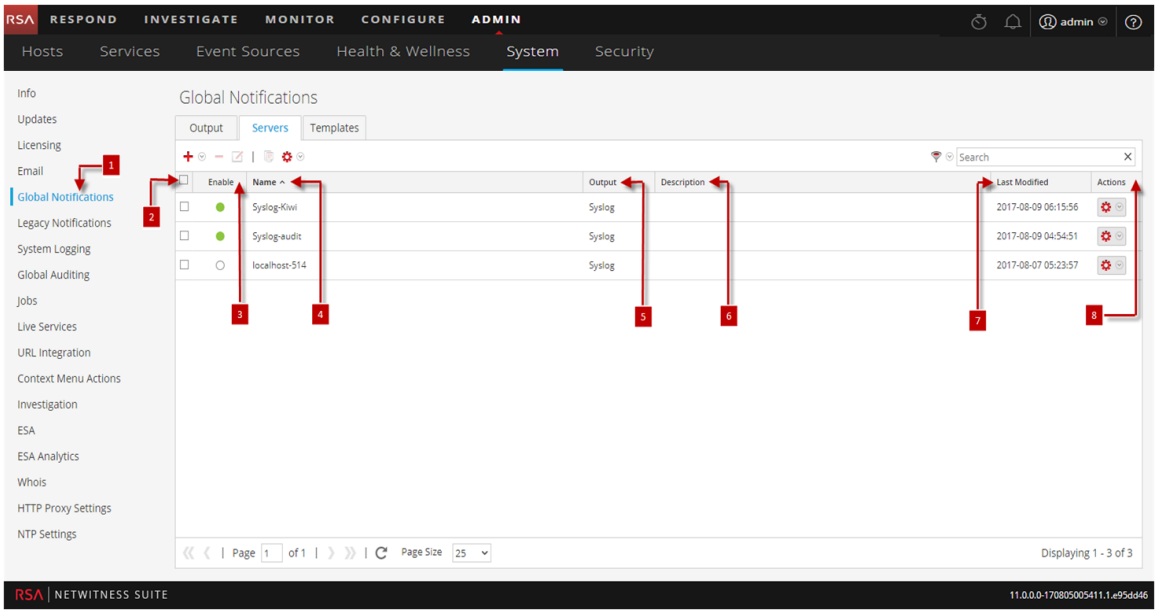
Rolle	Ich möchte...	Details anzeigen
Administrator	Benachrichtigungsserver definieren	Konfigurieren von Benachrichtigungsservern

Verwandte Themen

- Übersicht über Benachrichtigungsserver
- Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver
- Konfigurieren eines Skripts als Benachrichtigungsserver
- Konfigurieren der SNMP-Einstellungen als Benachrichtigungsserver
- Konfigurieren Sie einen Syslog-Benachrichtigungsserver.

Überblick

Das folgende Beispiel zeigt die globale Benachrichtigungsserver-Konfiguration.



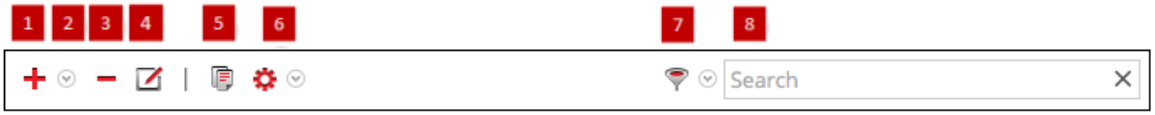
1	Zeigt den Bereich Registerkarte Server.
2	Wählt eine Zeile für eine Aktion in der Symbolleiste aus. Durch Aktivieren des Kontrollkästchens im Spaltentitel werden alle Zeilen im Raster ausgewählt oder deren Auswahl aufgehoben.
3	Gibt an, ob die Konfiguration aktiviert ist. Ein vollfarbiger grüner Kreis zeigt an, dass eine Konfiguration aktiviert ist. Ein leerer weißer Kreis zeigt an, dass eine Konfiguration nicht aktiviert ist.
4	Identifiziert oder kennzeichnet eine Konfiguration
5	Identifiziert die Konfigurationsausgabe. Die Ausgaben sind E-Mail, SNMP, Syslog und Skript.

6 Beschreibt die Speicherkonfiguration.

7 Zeigt das Datum und die Uhrzeit der letzten Konfigurationsänderung an.

8 In dieser Spalte kann ein Menü „Aktionen“ für die ausgewählte Konfiguration aufgerufen werden und die darin genannten Aktionen können auf die Konfiguration angewendet werden. Im Menü „Aktionen“ können Sie die Konfiguration löschen, bearbeiten, duplizieren und exportieren.

Die Symbolleiste des Bereichs globale Benachrichtigungen befindet sich oben im Ausgabe-Tag und bietet die folgenden Optionen:



1 Fügt eine Benachrichtigungsausgabe hinzu

2 Konfiguriert die Einstellungen für E-Mail, SNMP, Syslog und Skript-Benachrichtigungen.

3 Entfernt eine ausgewählte Benachrichtigungskonfiguration. Sie können Benachrichtigungsserver und Benachrichtigungstypen, die mit einer Konfiguration für globale Auditprotokollierung verknüpft sind, nicht löschen. Wenn Sie versuchen, eine Benachrichtigungsausgabe (Benachrichtigung) zu löschen, die von Warnmeldungen verwendet wird, wird eine Bestätigungsmeldung mit einer Warnung angezeigt, dass die diese Benachrichtigung verwendenden Warnmeldungen nicht mehr ordnungsgemäß funktionieren werden. In der Meldung wird die Anzahl der betroffenen Warnmeldungen angezeigt. Sie können eine Konfiguration auch löschen, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen > Löschen auswählen.

4 Bearbeitet eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch bearbeiten, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“ die Optionen „Bearbeiten“ auswählen.

5 Dupliziert eine Benachrichtigungskonfiguration. Sie können eine Konfiguration auch duplizieren, indem Sie sie auswählen und anschließend in der Spalte Aktionen die Optionen > Duplizieren auswählen.

6 Zeigt die folgenden Optionen an:

- **Importieren**: Importiert einen Benachrichtigungsserver bzw. -typ oder eine Benachrichtigungsvorlage. Beispiel: Auf der Registerkarte Server können Sie eine Benachrichtigungsserverkonfiguration importieren.
- **Alle exportieren**: Exportiert alle Konfigurationen. Beispiel: Auf der Registerkarte Server können Sie alle Benachrichtigungsserverkonfigurationen exportieren.
- **Export**: Exportiert eine ausgewählte Konfiguration. Sie können eine Konfiguration auch exportieren, indem Sie sie auswählen und anschließend in der Spalte „Aktionen“  > „Exportieren“ auswählen.

7 Filtert nach E-Mail, SNMP, Syslog oder Skript.

8 Sucht im Raster nach Konfigurationen.

Registerkarte Vorlagen

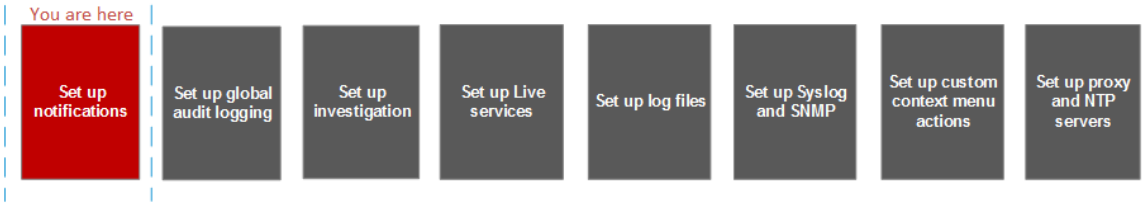
Auf der Registerkarte „Vorlagen“ können Sie Benachrichtigungsvorlagen konfigurieren. In globalen Benachrichtigungenkonfigurationen werden die Benachrichtigungseinstellungen für Ereignisquellenmanagement (Event Source Management, ESM), Integrität und Zustand, globale Auditprotokollierung, Event Stream Analysis (ESA) und Reagieren definiert. Benachrichtigungsvorlagen definieren das Format und die Meldungsfelder von Benachrichtigungen.

Sie können eine Standardvorlage auswählen oder je nach Vorlagentyp Vorlagen für E-Mail, SNMP, Syslog und Skript konfigurieren. Bei ESA-Vorlagen (Event Stream Analysis) können Sie E-Mail, SNMP, Syslog und Skript konfigurieren. Bei Auditprotokollierungsvorlagen können Sie Syslog konfigurieren.

Event Stream Analysis-Vorlagen gelten nicht für eine bestimmte Art Warnmeldungsbenachrichtigung. Dieselbe Vorlage kann für alle Benachrichtigungstypen verwendet werden.

Beim Upgrade von NetWitness Suite 10.4 werden alle vorhandenen Vorlagen auf den Event Stream Analysis-Vorlagentyp migriert.

Workflow



Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Dialogfeld „Benachrichtigungsvorlage definieren“	Konfigurieren von Vorlagen für Benachrichtigungen

Verwandte Themen

Konfigurieren von Vorlagen für globale Benachrichtigungen

Konfigurieren von Vorlagen

Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen

Löschen einer Vorlage

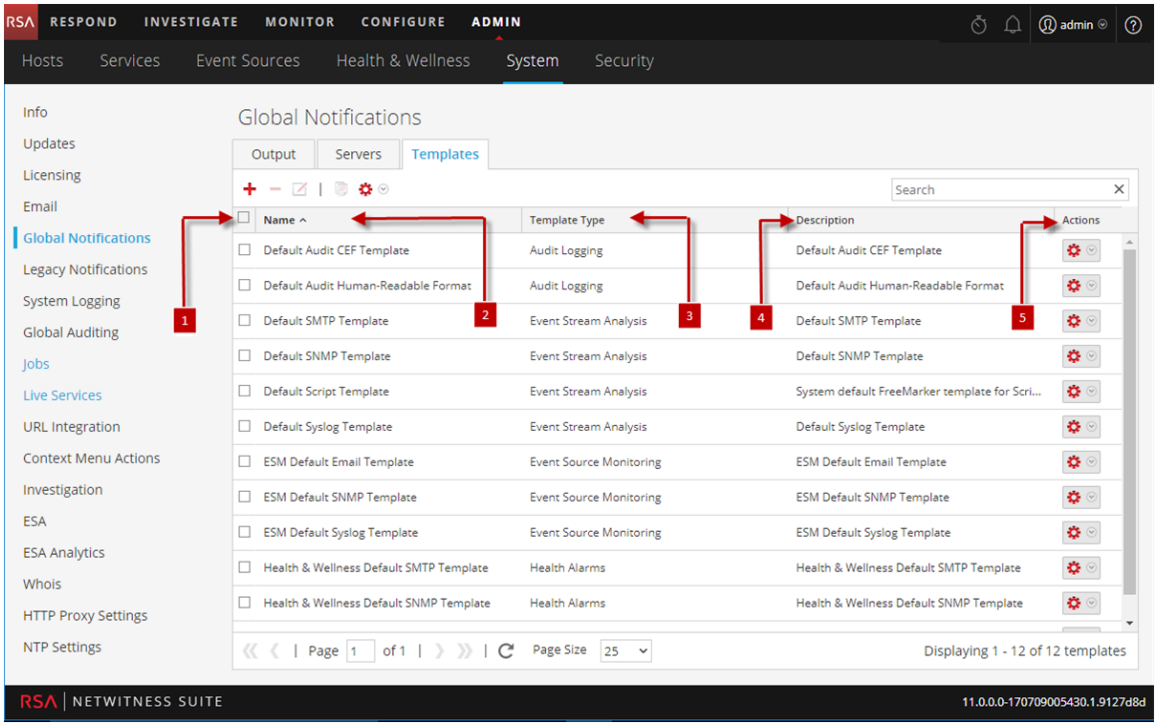
Duplizieren einer Vorlage

Bearbeiten einer Vorlage

Importieren und Exportieren einer Vorlage für globale Benachrichtigungen

Überblick

Das folgende Beispiel zeigt die Registerkarte „Globale Benachrichtigungsvorlagen“.



1	Wählt eine Zeile für eine Aktion in der Symbolleiste aus. Durch Aktivieren des Kontrollkästchens im Spaltentitel werden alle Zeilen im Raster ausgewählt oder deren Auswahl aufgehoben.
2	Identifiziert oder kennzeichnet die Vorlagen
3	Wählen Sie eine Vorlagenart
4	Beschreibt die Vorlagen
5	In dieser Spalte kann ein Menü „Aktionen“ für die ausgewählten Vorlagen aufgerufen werden und die darin genannten Aktionen können auf die Vorlage angewendet werden. Im Menü „Aktionen“ können Sie die Konfiguration löschen, bearbeiten, duplizieren und exportieren.

Bereich „HTTP-Proxyeinstellungen“

De Bereich „HTTP-Proxyeinstellungen“ enthält eine Einführung in die Proxysupportfunktionen des Bereichs Ansicht Administration > System > HTTP-Proxyeinstellungen.

Hinweis: Proxyunterstützung ist nur für HTTP- und HTTPS-Proxy, aber nicht für SOCKS5 verfügbar.

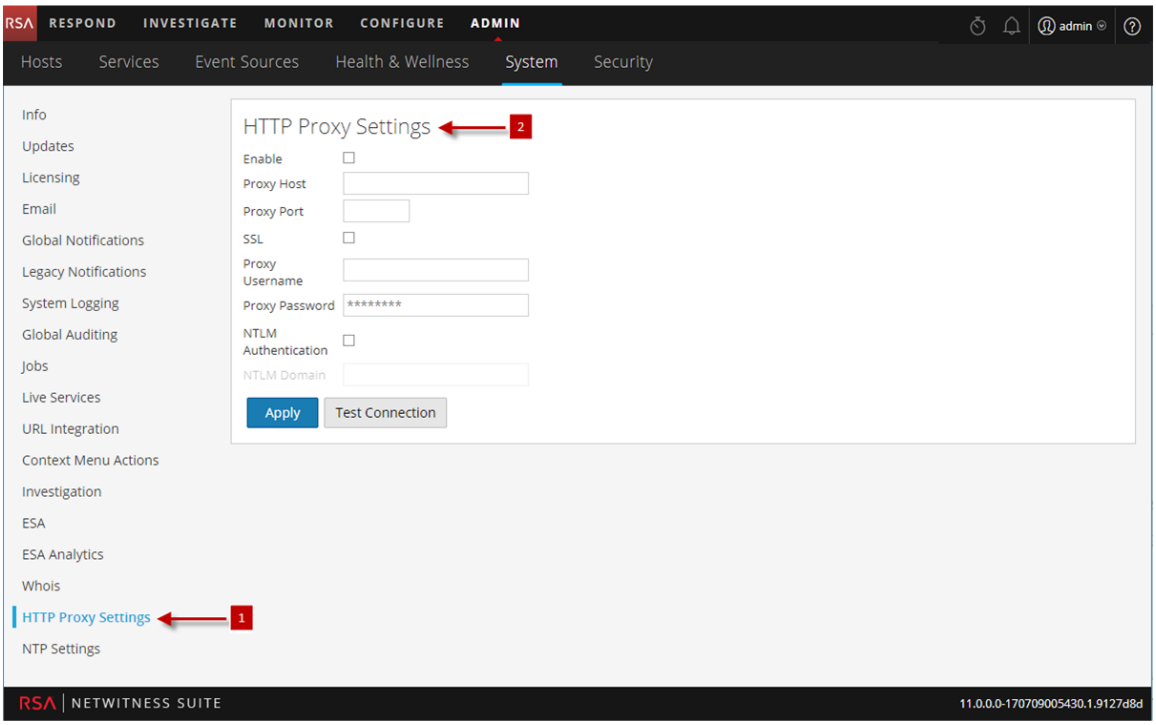
Der Bereich „HTTP-Proxyeinstellungen“ stellt eine Benutzeroberfläche für die Konfiguration eines Proxy zur Verwendung in allen NetWitness Suite-Modulen und -Services bereit. Über die Proxyeinstellungen wird ein Proxy eingerichtet, der verwendet wird, wenn in NetWitness Suite ein Proxy benötigt wird. Die Einstellungen in diesem Bereich setzen alle Proxyeinstellungen außer Kraft, die für einen einzelnen Service wie etwa Malware Analysis oder Live konfiguriert wurden.

Verwandte Themen

Konfigurieren des Proxy für NetWitness-Suite

Überblick

Das folgende Beispiel zeigt den Bereich „HTTP-Proxyeinstellungen“.



1. Der Bereich „HTTP-Proxyeinstellungen“ wird angezeigt.
2. Ermöglicht das Konfigurieren des HTTP-Proxyeinstellungen.

Symbolleiste und Funktionen

In dieser Tabelle werden die Funktionen im Abschnitt Proxyeinstellungen beschrieben.

Funktion	Beschreibung
Aktivieren	Aktiviert die Systemproxykonfiguration zur Verwendung in NetWitness Suite.
Proxy-Host	Der Hostname für den Proxy-Host.
Proxyport	Der zur Kommunikation auf dem Proxy-Host verwendete Port.
Proxybenutzername	(Optional) Der Benutzername, der zur Anmeldung am Proxyhost verwendet wird, wenn der Proxy Authentifizierung erfordert.
Proxypasswort	(Optional) Das Benutzerpasswort, das zur Anmeldung am Proxyhost verwendet wird, wenn der Proxy Authentifizierung erfordert.
Verwenden von NTLM-Authentifizierung	Verwenden Sie NT LAN-Manager-Authentifizierung und Sitzungssicherheitsprotokolle.
NTLM-Domain	Der Name der NTLM-Domain.
Use SSL	(Optional) Aktivieren Sie Kommunikation mithilfe von SSL.
Anwenden	Wendet alle Änderungen an, und sie werden sofort wirksam.

Bereich „E-Mail-Konfiguration“

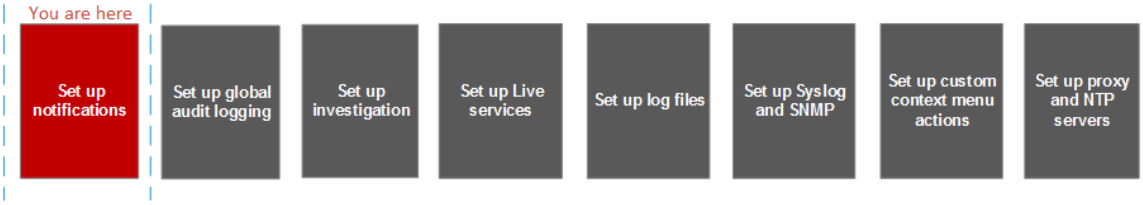
Der Bereich „E-Mail-Konfiguration“ bietet Informationen über E-Mail-Konfigurationseinstellungen in der Ansicht System > Bereich E-Mail-Konfiguration. RSA NetWitness® Suitesendet per E-Mail Benachrichtigungen an die Benutzer über verschiedene Systemereignisse. Damit Sie diese E-Mail-Benachrichtigung konfigurieren können, müssen Sie zunächst den SMTP-E-Mail-Server konfigurieren (siehe Konfigurieren von E-Mail-Servern und Benachrichtigungskonten).

Der Bereich „E-Mail-Konfiguration“ bietet eine Möglichkeit zur:

- Konfiguration des E-Mailservers.
- Richten Sie ein E-Mail-Konto für den Erhalt von Benachrichtigungen ein.
- Anzeige von Statistiken zu E-Mail-Vorgängen.

Workflow

Dieser Workflow zeigt die erforderlichen Verfahren zum Konfigurieren und Überprüfen des Bereichs „E-Mail“.



Was möchten Sie tun?

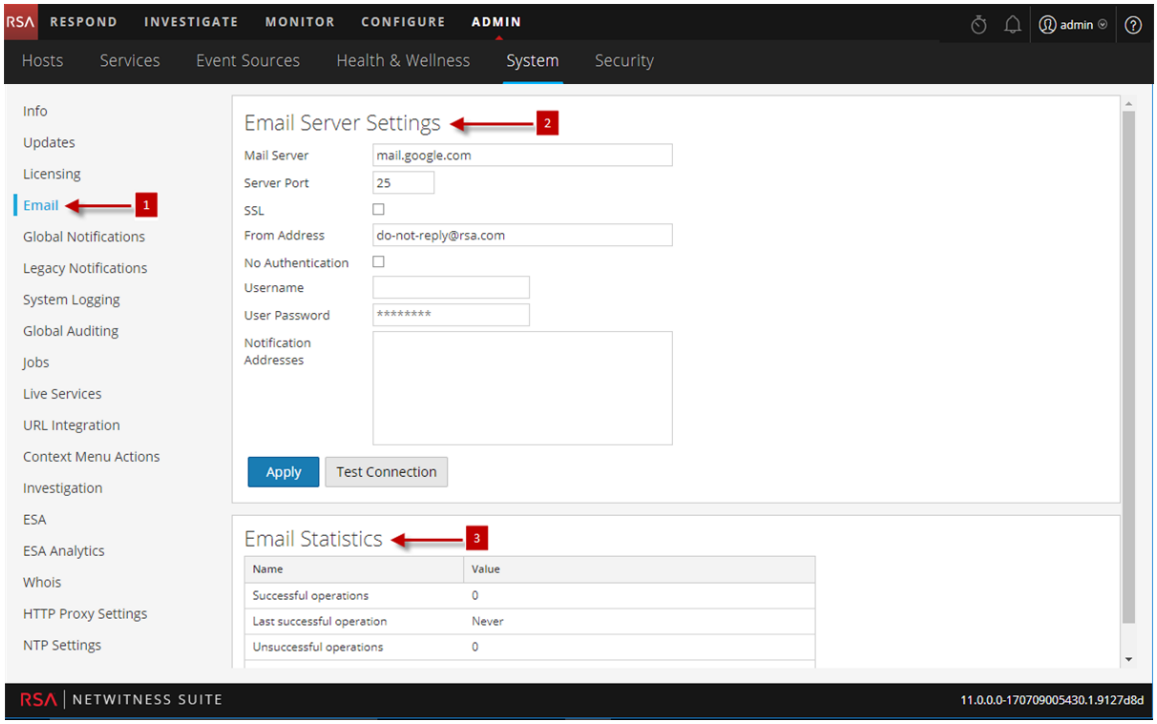
Rolle	Ich möchte...	Details anzeigen
Administrator	Konfigurieren des SMTP-E-Mail-Servers	Konfigurieren von E-Mail-Servern und Benachrichtigungskonten
Administrator	Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver	Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver
Administrator	Einrichten, überprüfen und aktivieren des E-Mail-Kontos	E-Mail-Benachrichtigung erhalten

Verwandte Themen

- Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver
- Konfigurieren von E-Mail als Benachrichtigung
- Konfigurieren von E-Mail-Servern und Benachrichtigungskonten

Überblick

Das folgende Beispiel zeigt eine E-Mail-Konfiguration. Die Konfiguration definiert, wie Ereignisse per E-Mail übermittelt werden.



1	Zeigt den E-Mail-Konfigurationsbereich.
2	Ermöglicht das Konfigurieren von E-Mail-Servereinstellungen.
3	Enthält Feedback über E-Mail-Vorgänge.

Symbolleiste und Funktionen

Der Bereich **E-Mail-Konfiguration** umfasst zwei Abschnitte: **E-Mail-Server-Einstellungen** und **E-Mail-Statistiken**.

E-Mail-Server-Einstellungen

Konfigurieren Sie im Abschnitt **E-Mail-Server-Einstellungen** die folgenden Parameter.

Funktion	Beschreibung
Mailserver	Der E-Mail-Servername. Der Standardwert ist **mail.google.com**.
Serverport	Der für den Versand und Empfang von E-Mails genutzte Serverport. Der Standardwert ist **25**.
SSL verwenden	Die Einstellung für die Nutzung von SSL bei der Kommunikation zwischen E-Mail-Server und NetWitness Suite. Standardmäßig wird SSL nicht verwendet (nicht aktiviert).
Absenderadresse	Die Adresse, die in allen E-Mails von NetWitness Suite angezeigt wird. Die Standard-E-Mail-Adresse lautet **do-not-reply@rsa.com**.
Benutzername	Der Benutzername für den Zugriff auf den E-Mail-Server. Der Standardwert ist **leer**.
Benutzerpasswort	Das Benutzerpasswort für den Zugriff auf den E-Mail-Server. Der Standardwert ist **leer**.
Verbindung testen	Testet die Verbindung mit dem E-Mail-Server.
Anwenden	Wendet die E-Mail-Konfiguration auf diese NetWitness Suite-Instanz an.

E-Mail-Statistiken

Der Abschnitt E-Mail-Statistiken enthält Feedback über die Anzahl der erfolgreichen und fehlgeschlagenen E-Mail-Operationen sowie den Zeitpunkt der letzten erfolgreichen und fehlgeschlagenen E-Mail-Operation. Für jede Statistik werden der Name der Statistik und der Wert angezeigt.

Bereich „Einstellungen für ESA“

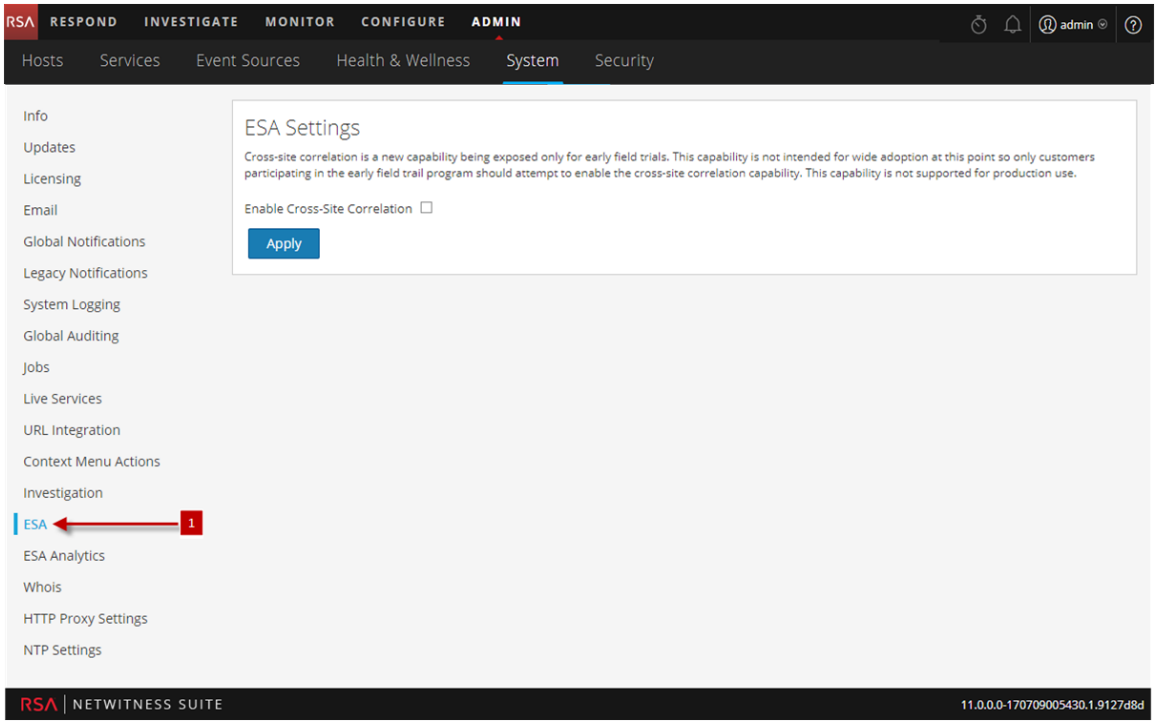
Im Bereich „Einstellungen für ESA“ können Sie die siteübergreifende Korrelation aktivieren und deaktivieren. Die siteübergreifende Korrelation ist eine neue Funktion, die nur für frühe Feldversuche bereitgestellt wird. Diese Funktion ist nicht für eine breite Übernahme vorgesehen.

Achtung: Es sollten nur die Kunden, die am Programm früher Feldversuche teilnehmen, die Funktion der siteübergreifenden Korrelation aktivieren. Diese Funktion wird für den Produktionseinsatz nicht unterstützt.

Verwandte Themen

- Definieren einer Vorlage für ESA-Warnmeldungsbenachrichtigungen
- Leitfaden Investigation und Malware Analysis
- Context Hub-Konfigurationsleitfaden

Überblick



1	Zeigt den Bereich „„Einstellungen für ESA“ an.

Symbolleiste und Funktionen

Die Funktionen des Bereichs Einstellungen für ESA sind Folgende:

- Kontrollkästchen Siteübergreifende Korrelation aktivieren: Wenn aktiviert, ist siteübergreifende Korrelation in ESA aktiviert. Wenn Sie eine Bereitstellung in ADMIN > Warnmeldungen > Konfigurieren hinzufügen, können Sie zur zentralen Regelverarbeitung den gleichen Regelsatz auf mehreren ESA-Services ausführen.
- Schaltfläche Anwenden: Aktiviert Ihre Auswahl.

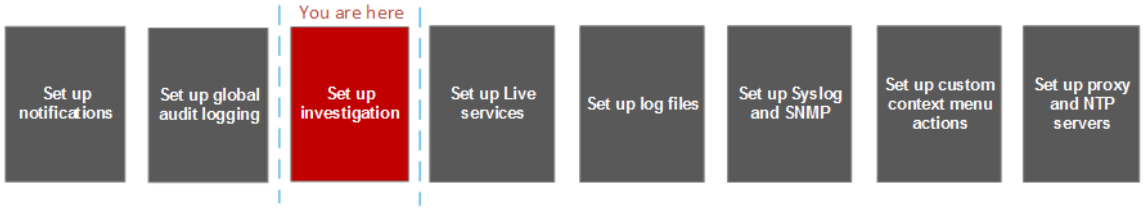
Investigation-Konfigurationsbereich

In diesem Thema werden die Funktionen im Bereich „Investigation“ „Konfiguration“ der Ansicht „System“ vorgestellt. Über diese Benutzeroberfläche können Administratoren die systemweiten Einstellungen konfigurieren, die NetWitness Suite Investigation zur Analyse von Daten und Rekonstruktion von Ereignissen verwendet.

Über die Investigation-Konfigurationseinstellungen kann ein Administrator die Anwendungsperformance für Ermittlungen managen. Wenn Analysten bei der Ermittlung Sitzungen analysieren und wiederherstellen, kann die Performance durch Operationen wie das Laden, Suchen, Visualisieren und Wiederherstellen großer Datenmengen beeinträchtigt werden.

Hinweis: Analysten können auch individuelle Einstellungen für Investigation in der Profilansicht und in der Navigationsansicht festlegen.

Workflow



Was möchten Sie tun?

Rolle	Ich möchte...	Details anzeigen
Administrator	Konfigurieren der Einstellungen für Navigation, Ereignisse und Kontextabfrage	Konfigurieren von Ermittlungseinstellungen
Administrator	Löschen des Rekonstruktionscaches für Services	Konfigurieren von Ermittlungseinstellungen

Verwandte Themen

- Standardverfahren

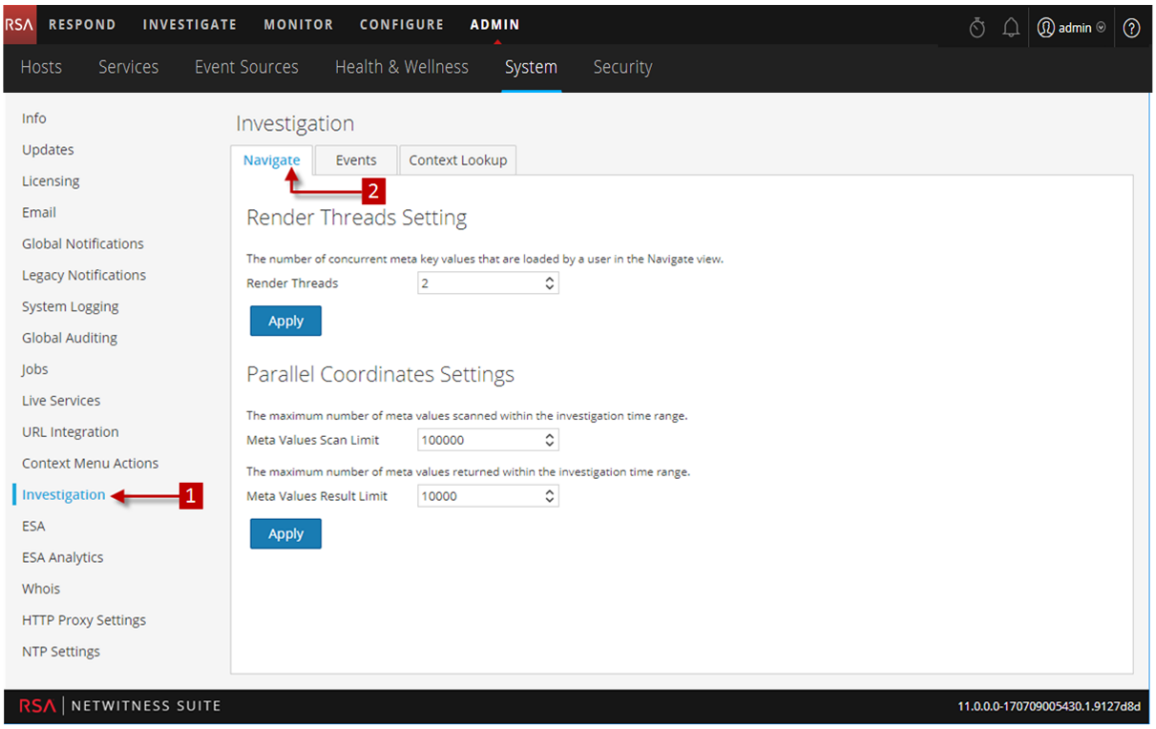
Überblick

Der Bereich „Investigation-Konfiguration“ umfasst drei Registerkarten: „Navigieren“, „Ereignisse“ und „Kontextabfrage“.

Obwohl die meisten Felder auf den Registerkarten eine Auswahlliste mit spezifischen Inkrementen über eine Reihe möglicher Werte haben, können Sie einen Wert innerhalb des erlaubten Bereichs auch manuell eingeben. Ein ungültiger Eintrag wird angezeigt, indem das Feld rot markiert wird. Wenn gültige Werte ausgewählt werden, werden die Änderungen durch ein Klicken auf Anwenden in einem gegebenen Bereich sofort wirksam.

Registerkarte Navigieren

Die folgende Abbildung zeigt die Registerkarte Navigieren.



1 Der Bereich Investigation-Konfiguration wird angezeigt.

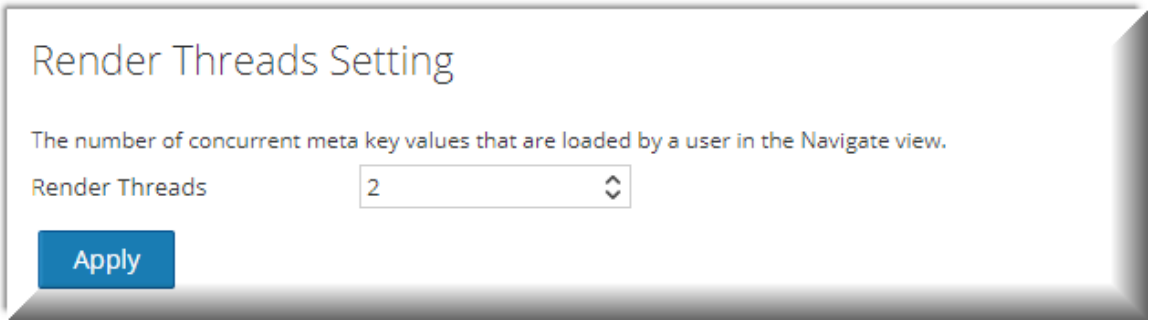
2 Zeigt die Registerkarte Navigieren.

Symbolleiste und Funktionen

Die Registerkarte Navigieren hat zwei Abschnitte: Render-Threadeinstellung und Einstellungen zu Parallelkoordinaten.

Render-Threadeinstellung

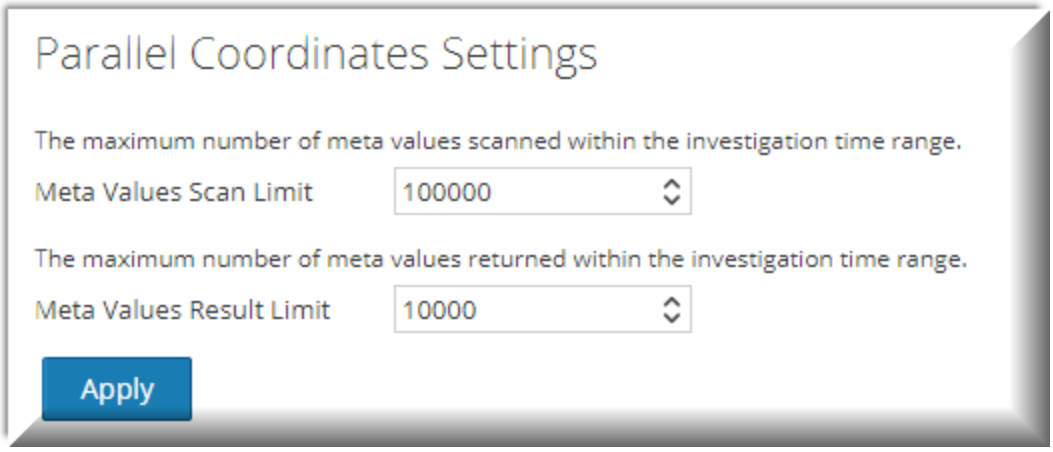
Die Render-Threadeinstellung ist ein auswählbarer Wert zwischen 1 und 20, der die Anzahl gleichzeitiger Ladevorgänge (von Werten) in der Navigationsansicht definiert. Der Standardwert ist 1.



Einstellungen zu Parallelkoordinaten

Die Einstellungen zu Parallelkoordinaten gelten für die Parallelkoordinatenvisualisierung in der Navigationsansicht. Es gibt eine feste Höchstgrenze für die Datenmenge, die als Parallelkoordinatendiagramm gerendert werden kann. In NetWitness Suite kann der Administrator hier die Grenzwerte für Parallelkoordinaten konfigurieren.

Hinweis: Die empfohlenen Einstellungen für bessere Performance sind **Scangrenzwert für Metawerte: 100.000** und **Ergebnisgrenzwert für Metawerte: 1.000-10.000**.



In der folgenden Tabelle werden die Einstellungen zu Parallelkoordinaten beschrieben.

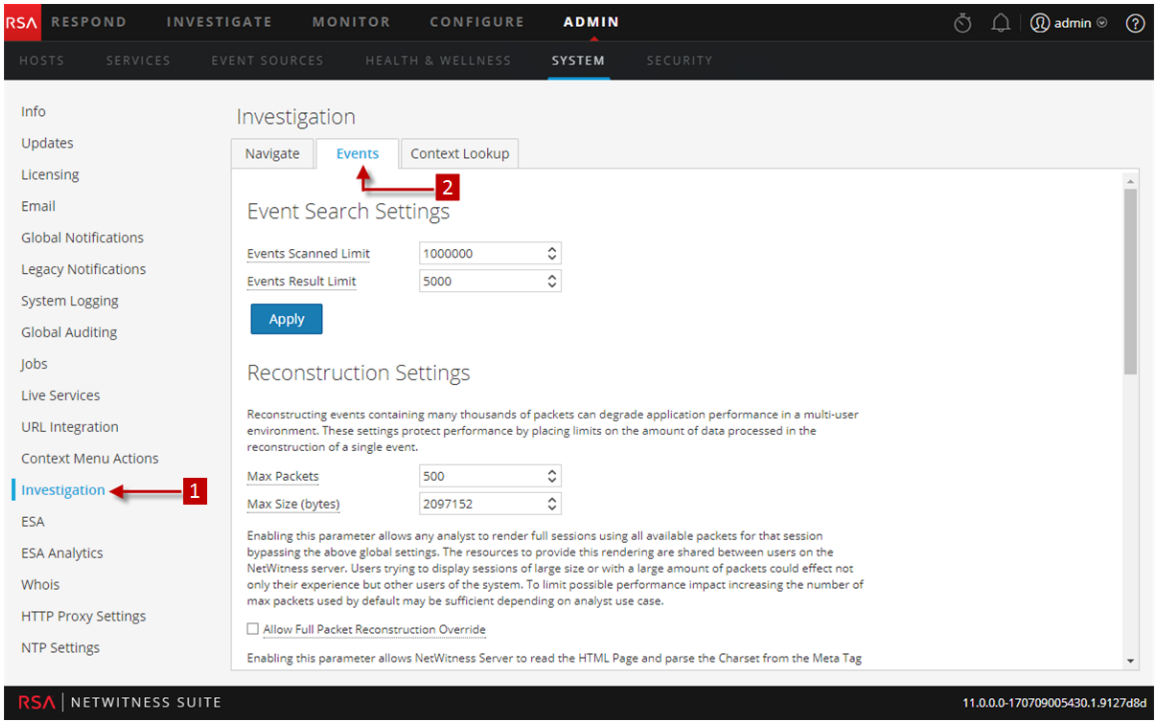
Parameter	Beschreibung
Scangrenzwert für Metawerte	Die maximale Anzahl von Metawerten, die innerhalb des Ermittlungszeitraums gescannt werden, den der Analyst in der Navigationsansicht ausgewählt hat. Mögliche Werte liegen im Bereich zwischen 1.000 und 10.000.000. Der Standardwert lautet 100.000.

Parameter	Beschreibung
Ergebnisgrenzwert für Metawerte	Die maximale Anzahl von Metawerten, die innerhalb des Ermittlungszeitraums zurückgegeben werden, den der Analyst in der Navigationsansicht ausgewählt hat. Mögliche Werte liegen im Bereich zwischen 100 und 1.000.000.000. Der Standardwert ist 10.000.

Überblick

Registerkarte „Ereignisse“

Die folgende Abbildung zeigt die Registerkarte Ereignisse.



Diesem Bereich zugeordnete Verfahren werden zur Verfügung gestellt in Standardverfahren.

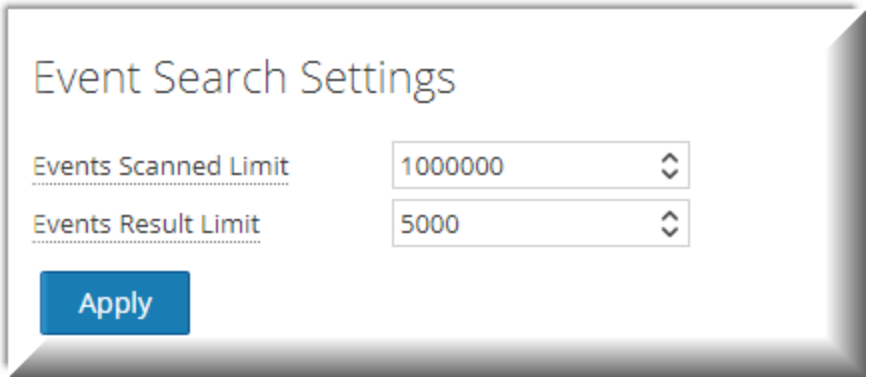
1. Der Bereich Investigation-Konfiguration wird angezeigt.
2. Zeigt die Registerkarte „Ereignisse“ an.

Symbolleiste und Funktionen

Auf der Registerkarte Ereignisse können Einstellungen bezüglich der Ermittlung von Ereignissen konfiguriert werden. Diese Registerkarte ist in vier Abschnitte aufgeteilt: Sucheinstellungen für Ereignisse, Rekonstruktionseinstellungen, Einstellungen für Rekonstruktion der Webansicht und Rekonstruktionscacheeinstellungen.

Sucheinstellungen für Ereignisse

Mithilfe der Sucheinstellungen für Ereignisse kann die Anzahl der gescannten Ereignisse bei der Suche in der Ereignisansicht begrenzt werden.



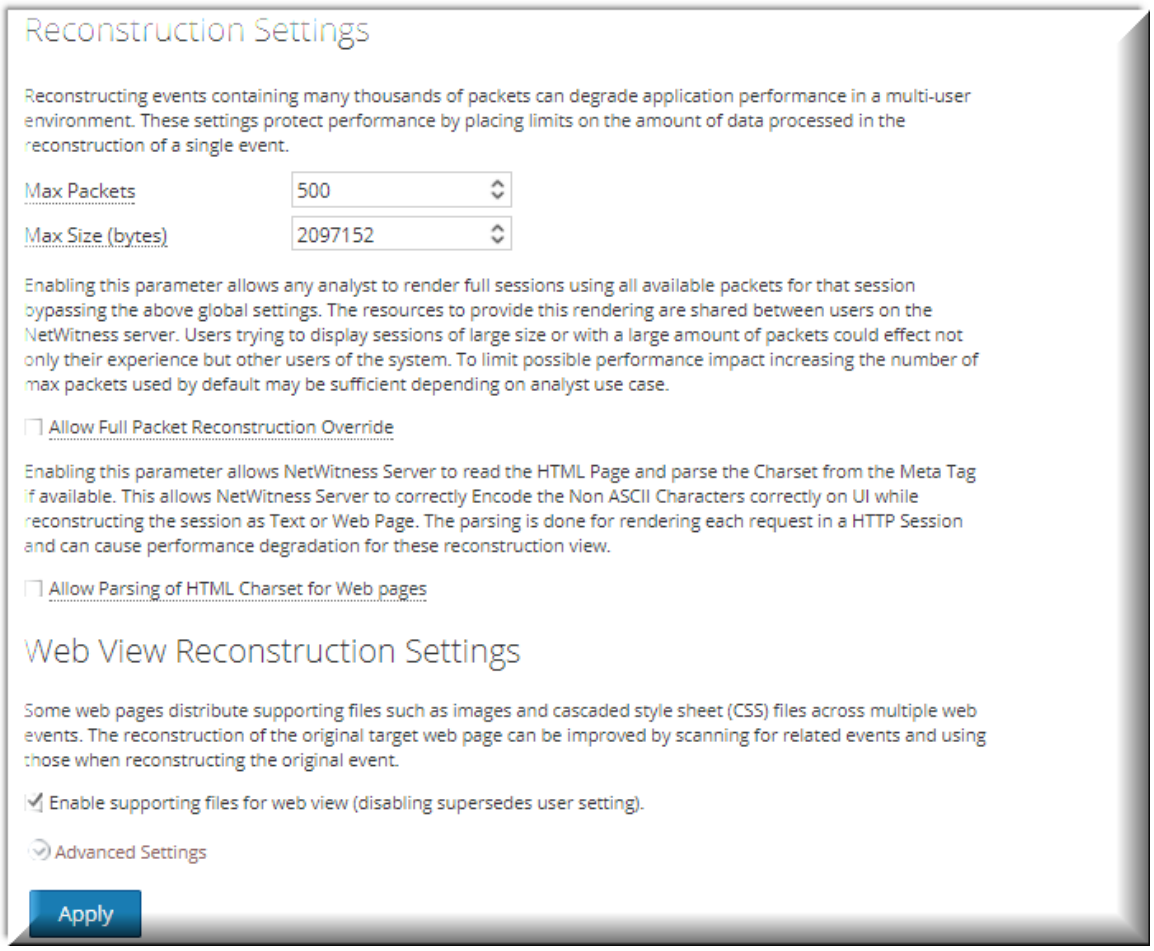
In der folgenden Tabelle werden die Sucheinstellungen für Ereignisse beschrieben.

Parameter	Beschreibung
Limit für gescannte Ereignisse	Die maximale Anzahl der gescannten Ereignisse bei der Suche in der Ereignisansicht.
Ereignisergebnis-Grenzwert	Die maximale Anzahl der wiederzugebenden Ereignisse bei der Suche in der Ereignisansicht.

Rekonstruktionseinstellungen

Wenn Analysten Sitzungen rekonstruieren, die sie untersuchen, können einige Ereignisse sehr groß sein und viele Tausend Quellpakete enthalten. Das Rekonstruieren dieser Sitzungen, insbesondere in einer Mehr-Benutzer-Umgebung, kann die Anwendungsperformance beeinträchtigen. Die Rekonstruktionseinstellungen erlauben es einem Administrator, die Anzahl der Pakete und die Größe eines einzelnen Ereignisses während der Rekonstruktion zu begrenzen.

Hinweis: Der Abschnitt Rekonstruktionseinstellungen kann für Webansichten außer Kraft gesetzt werden (unter Einstellungen für Rekonstruktion der Webansicht).



In der folgenden Tabelle werden die Funktionen der Rekonstruktionseinstellungen beschrieben.

Parameter	Beschreibung
Maximale Anzahl von Paketen pro Ereignis	Diese Einstellung schützt die Performance, indem die Anzahl der Pakete begrenzt wird, die für eine einzige Ereignisrekonstruktion verarbeitet werden. Mögliche Werte liegen im Bereich zwischen 100 und 10.000 Paketen. Sie können manuell eingegeben oder in Schritten von 100 aus der Auswahlliste ausgewählt werden. Der Standardwert ist 100 Pakete.

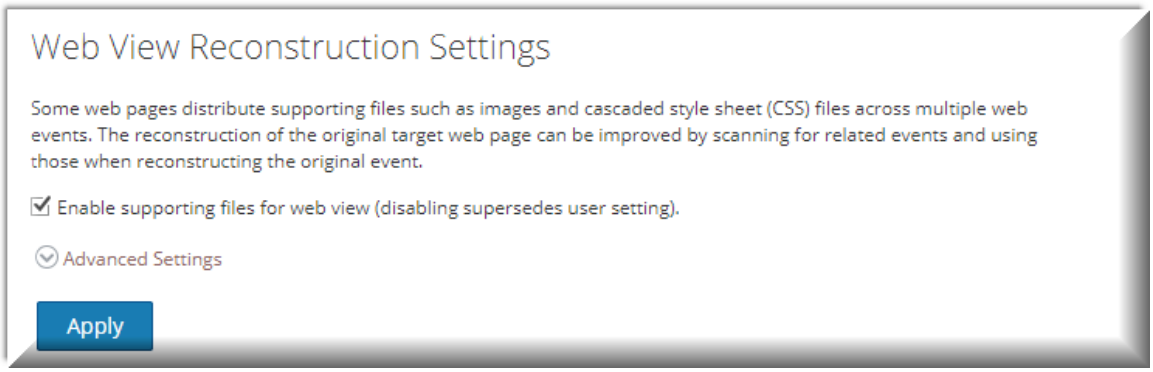
Parameter	Beschreibung
Maximale Größe pro Ereignis (in Byte)	Diese Einstellung schützt die Performance, indem die maximale Größe (in Byte) einer einzigen Ereignisrekonstruktion begrenzt wird. Mögliche Werte liegen im Bereich zwischen 102.400 und 104.857.600 Byte. Sie können manuell eingegeben oder in Schritten von 10.240 aus der Auswahlliste ausgewählt werden. Der Standardwert ist 2.097.152 Byte.
Außerkraftsetzung von vollständiger Paketrekonstruktion zulassen	Wenn dieses Kontrollkästchen aktiviert ist, steht dem Analysten im Bereich Ereignisrekonstruktion die der Schaltfläche „Mehr Pakete verwenden“ zur Verfügung. Dadurch kann der NW-Server Ereignisse mithilfe der im Ereignis verfügbaren Pakete neu erstellen.
Analysieren des HTML-Zeichensatzes für Webseiten zulassen	Mit dieser Option kann NetWitness-Server die Webseite-Codierung im HTML-Metatag anstelle der HTTP-Kopfzeile identifizieren. Die Einstellung ist standardmäßig deaktiviert.

Einstellungen für Rekonstruktion der Webansicht

Mithilfe der Einstellungen für Rekonstruktion der Webansicht kann ein Administrator Einstellungen konfigurieren, die die Rekonstruktion einer Webansicht verbessern, indem verbundene Ereignisse gescannt und rekonstruiert werden, die dieselben Begleitdateien enthalten. Wenn NetWitness Suite eine Webansicht rekonstruiert, die mehrere Ereignisse umfasst, kann die Rekonstruktion des Zielereignisses verbessert werden, indem verbundene Ereignisse gescannt und rekonstruiert werden, die dieselben Begleitdateien enthalten, wie etwa Bilder und CSS-Dateien (Cascading Style Sheet).

- Die einzigen gescannten verbundenen Ereignisse sind Ereignisse vom Servicetyp HTTP, mit derselben Quelladresse wie das Zielereignis und einem Zeitstempel innerhalb eines spezifizierten Zeitbereichs vor und nach dem Zielereignis.
- Die maximale Anzahl zu scannender verbundener Ereignisse ist konfigurierbar.

Durch Klicken auf die Option Erweiterte Einstellungen werden alle konfigurierbaren Einstellungen in diesem Abschnitt angezeigt.



In der folgenden Tabelle werden die Einstellungen für Rekonstruktion der Webansicht beschrieben.

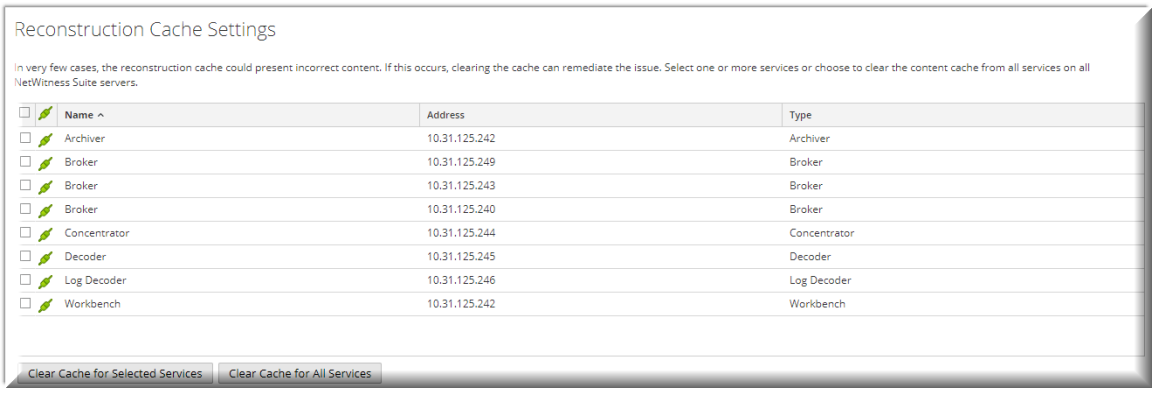
Parameter	Beschreibung
Begleitdateien für Webansicht zulassen	Diese Option legt fest, wie Webansichten, die verbundene Daten in anderen Sitzungen haben, rekonstruiert werden. Die Standardeinstellung ist „Aktiviert“. Wenn sie aktiviert ist, können Begleitdateien von verbundenen Ereignissen bei der Rekonstruktion von Webansichten verwendet werden. Zusätzliche Einstellungen zur Kalibrierung der Performance werden in diesem Abschnitt aktiviert und Analysten haben die Option, die Verwendung von CSS in Rekonstruktionen zu aktivieren. Wenn sie deaktiviert ist, werden Begleitdateien von verbundenen Ereignissen nicht verwendet und die Einstellung, dass Analysten die Verwendung von CSS in Rekonstruktionen aktivieren können, ist deaktiviert.

Parameter	Beschreibung
Zeitbereich für das Scannen von verbundenen Ereignissen	Verfügbar, wenn **Begleitdateien für Webansicht zulassen** aktiviert ist. Konfiguriert den Zeitbereich, innerhalb dessen NetWitness Suite verbundene Ereignisse scannt, die den Servicetyp „HTTP“ und dieselbe Quelladresse wie das Zielereignis aufweisen. Dies ist ein Dezimalwert zwischen 0 und 60. • Sekunden vor Zielereignis • Sekunden nach Zielereignis
Begrenzen der Anzahl verarbeiteter verbundener Ereignisse	Ermöglicht die Konfiguration der maximalen Anzahl verbundener Ereignisse, die NetWitness Suite innerhalb des angegebenen Zeitbereichs scannt, um Begleitdateien für das Zielereignis zu erkennen. Standardmäßig ist dies deaktiviert. Wenn es aktiviert ist, wird das Feld Maximale Anzahl verbundener Ereignisse aktiv.
Maximale Anzahl verbundener Ereignisse	Wenn **Begrenzen der Anzahl verarbeiteter Ereignisse** aktiviert ist, gibt dieses Feld die maximale Anzahl verbundener Ereignisse an, die NetWitness Suite innerhalb des angegebenen Zeitbereichs scannt, um Begleitdateien für das Zielereignis zu erkennen. Dies ist ein auswählbarer Wert zwischen 10 und 1.000, der in Schritten von 100 erhöht werden kann. Der Standardwert ist 100.
Begrenzen der Anzahl der Pakete und der Größe der einzelnen verbundenen Ereignisse	Setzt die allgemeinen Einstellungen für die maximale Anzahl der Pakete und die maximale Größe (in Byte) für einzelne verbundene Ereignisse außer Kraft.

Parameter	Beschreibung
Maximale Anzahl von Paketen pro Ereignis	Mögliche Werte liegen im Bereich zwischen 100 und 10.000 Paketen. Sie können in Schritten von 100 aus der Auswahlliste ausgewählt werden. Der Standardwert ist 100 Pakete.
Maximale Größe pro Ereignis (in Byte)	Mögliche Werte liegen im Bereich zwischen 102.400 und 104.857.600 Paketen. Sie können in Schritten von 10.240 aus der Auswahlliste ausgewählt werden. Der Standardwert ist 524.288 Byte.

Rekonstruktionscacheeinstellungen

In einigen Fällen kann der Rekonstruktionscache falsche Inhalte darstellen. Aus diesem Grund löscht NetWitness Suite Rekonstruktionen, deren Daten älter als einen Tag sind, aus dem Cache. Der Cache wird täglich um Mitternacht geleert. Zwischen den täglichen Cachebereinigungen können bestimmte Aktionen dazu führen, dass ein nicht mehr gültiger Cache für die Rekonstruktion verwendet wird. Bei Bedarf können Administratoren für einen oder mehrere Services, die mit dem aktuellen NetWitness-Server verbunden sind, den Cache manuell leeren.



In der folgenden Tabelle werden die Funktionen der Rekonstruktionscacheeinstellungen beschrieben.

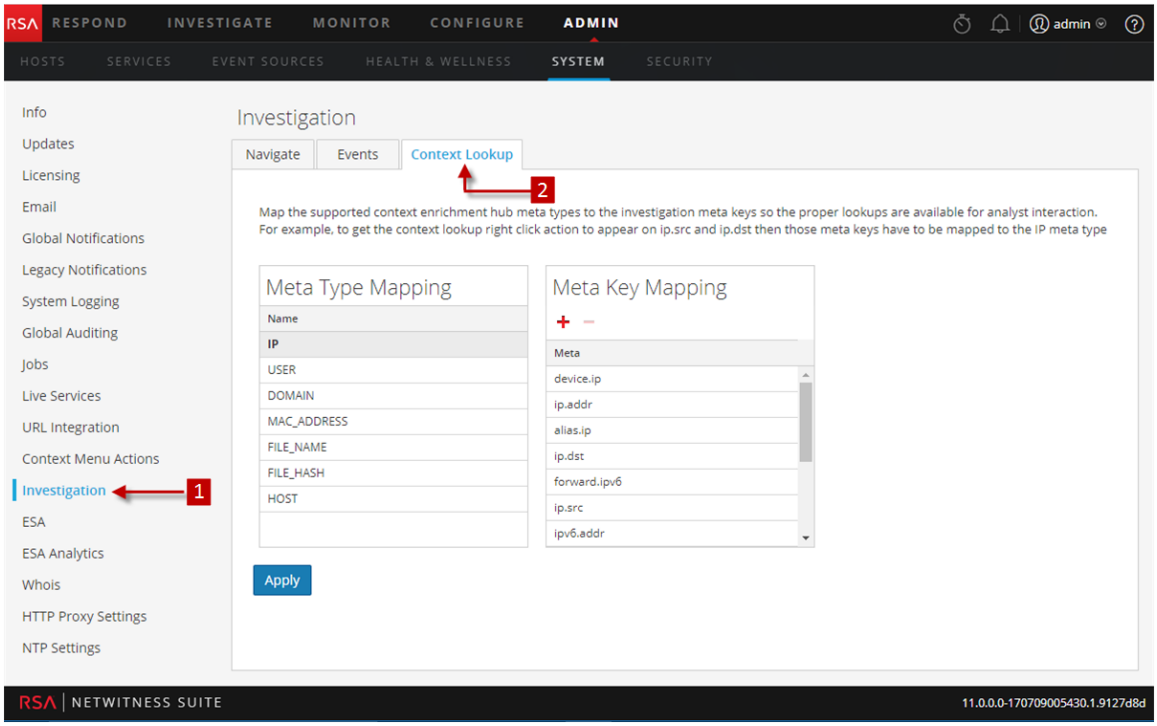
Funktion	Beschreibung
Auswahlfeld	Auswahlfeld in einzelnen Zeilen und in der Titelleiste erlauben die Auswahl von einem oder mehreren oder allen Services, für die der Cache manuell geleert werden muss.

Funktion	Beschreibung
Cache für ausgewählte Services leeren	Leert den Rekonstruktionscache für jeden ausgewählten Service.
Cache für alle Services leeren	Leert den Rekonstruktionscache für alle Services.

Überblick

Registerkarte „Kontextabfrage“

In der folgenden Abbildung ist die Registerkarte „Kontextabfrage“ dargestellt.



Die Verfahren zu diesem Bereich finden Sie unter Managen der Metatyp- und Metaschlüsselzuordnung im *Context Hub-Konfigurationsleitfaden*.

1. Der Bereich Investigation-Konfiguration wird angezeigt.
2. Zeigt die Registerkarte Kontextabfrage.

Symbolleiste und Funktionen

In der Registerkarte „Kontextabfrage“ kann der Administrator die Zuordnung der Investigation-Metaschlüssel und des Investigation-Metadatentyps konfigurieren. Der Administrator kann Investigation-Metaschlüssel zur Liste der von Context Hub unterstützten Metadatentypen hinzufügen oder entfernen.

In der folgenden Tabelle sind die Funktionen der Registerkarte „Kontextabfrage“ beschrieben.

Funktion	Beschreibung
+	Fügt einen Metaschlüssel zum ausgewählten Metadatentyp hinzu, der vom Context Hub-Service unterstützt wird.
−	Löscht den Metaschlüssel aus dem ausgewählten Metadatentyp.
Anwenden	Speichert die an der Registerkarte „Kontextabfrage“ vorgenommenen Änderungen.

Bereich „Konfiguration der Live-Services“

Der Bereich „Konfiguration der Live-Services“ bietet eine Einführung der Funktionen zur Einrichtung Ihres Live-Kontos und der CMS-Serververbindung.

Das Live-Konto besteht aus zwei Abschnitten: „RSA Live-Status“ und „Live Feedback-Aktivitätsprotokoll herunterladen“. **Melden** Sie sich durch Eingabe Ihrer Anmeldedaten für das Live-Konto an, um auf die Live-Services zuzugreifen. Bitte wenden Sie sich an den RSA Kundendienst, um Ihr Live-Konto für NetWitness Suite zu aktivieren. Wenn Sie die Bestätigung erhalten haben, dass Ihr Live-Konto eingerichtet wurde, können Sie die CMS-Serververbindung konfigurieren, wie unter Konfigurieren der Einstellungen von Live-Services beschrieben.

Der Bereich „Live-Services“ enthält die Benutzeroberfläche für:

- Das Live-Konto
- Die Planung für die Aktualisierung von Live-Inhalten und Einstellungen für die Benachrichtigung von Aktualisierungen
- Teilnahme an Live Feedback
- Freigabe von Nutzungsdetails zu Live-Inhalten
- RSA Live Connect (Betaversion)

Dialogfeld „Neue Funktionen eingeführt“

Wenn Sie sich zum ersten Mal bei NetWitness Suite anmelden, wird das Dialogfeld **Neue Funktionen eingeführt** angezeigt.

Funktion	Beschreibung
Accept	Indem Sie auf „Annehmen“ klicken, stimmen Sie Folgendem zu: • Teilnahme an Live Feedback • Zulassen, dass NetWitness Suite RSA die Nutzungsmetriken und Versionen der NW-Hosts über Ihre Umgebung sendet, vorausgesetzt ein Live-Konto ist konfiguriert • Erhalten von Threat Intelligence-Daten von Live Connect
Einstellungen anzeigen	Durch Klicken auf **Einstellungen anzeigen** gelangen Sie zur Benutzeroberfläche der Live-Services, in der Sie die Einstellungen anzeigen können. Wenn Sie das Live-Konto nicht konfiguriert haben, wird ein maskierter Bildschirm angezeigt.

Weitere Informationen über Live Feedback finden Sie unter Übersicht über Live Feedback

Weitere Informationen über Analystenverhalten und Datenfreigabe finden Sie im Thema **NetWitness-Feedback und Datenfreigabe** im *Handbuch Live Services Management*.

Informationen über Bedrohungseinblicke in Live Connect finden Sie unter Konfigurieren der Einstellungen von Live-Services.

Workflow

Was möchten Sie tun?

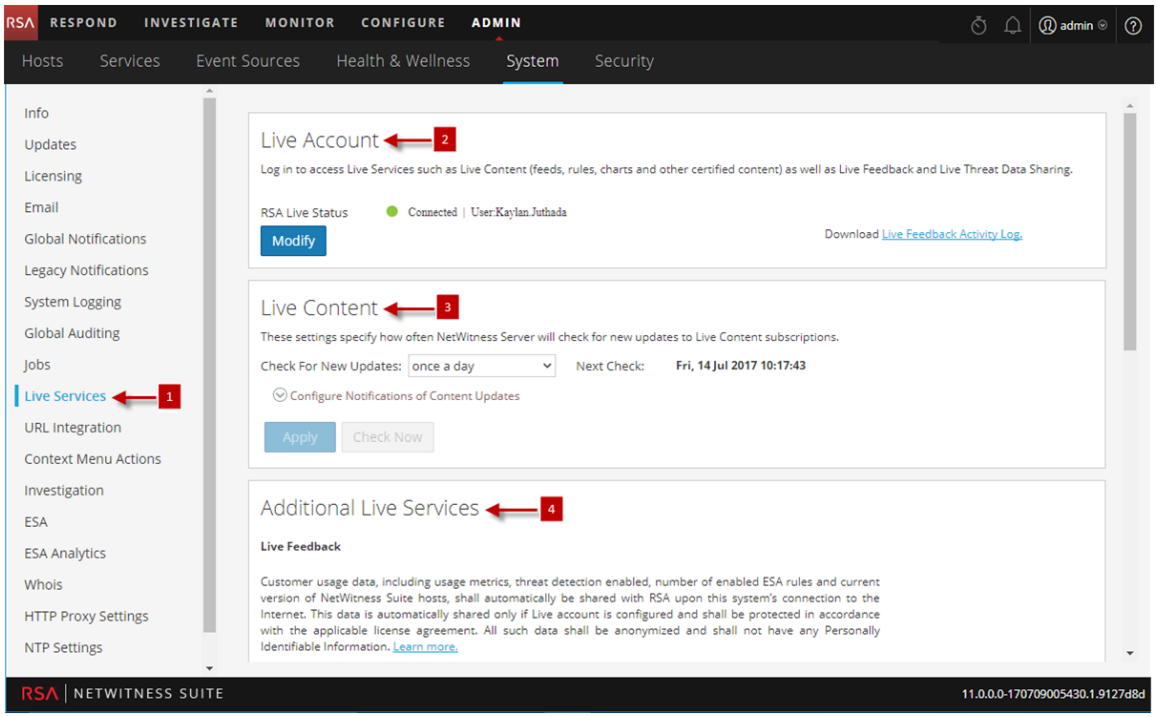
Rolle	Ziel	Details anzeigen
Administrator	Konfigurieren eines Live-Kontos, CMS-Serververbindung	Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver
Administrator	Hochladen von Daten in RSA für Live Feedback	Hochladen von Daten in RSA für Live Feedback
Administrator	Einrichten und Überprüfen des Bereichs „Konfiguration der Live-Services“	Bereich „Konfiguration der Live-Services“
Administrator	Übersicht über Live Feedback	Übersicht über Live Feedback

Verwandte Themen

- Übersicht über Live Feedback
- Konfigurieren der Einstellungen von Live-Services
- Hochladen von Daten in RSA für Live Feedback
- Handbuch Live-Services-Management

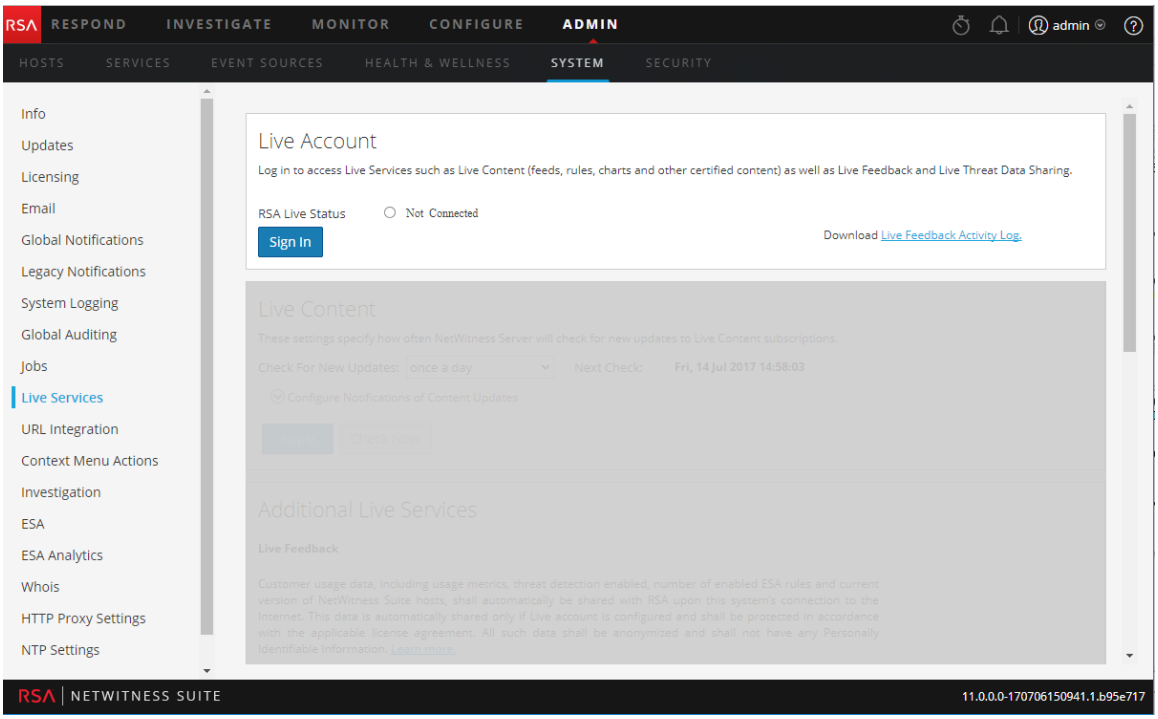
Überblick über Live-Services

Sie greifen im Menü über**ADMIN > SYSTEM > Live-Services** auf diese Ansicht zu.



Hinweis: Wenn Sie sich nicht mit Ihren Anmeldedaten für das Live-Konto angemeldet haben, wird ein maskierter Bildschirm angezeigt.

1. Anzeige des Bereichs „Konfiguration der Live-Services-“
2. Eingabe der Live-Konto-Anmeldedaten mithilfe der Kundenbetreuung.
3. Bereitstellung von Update auf Live-Inhalte
4. Weitere Live-Services bieten Live Feedback.



Symbolleiste und Funktionen

Der Bereich „Live-Konfiguration“ umfasst drei Abschnitte: „Live-Konto“, „Live-Inhalte“ und „Weitere Live-Services“

Abschnitt Live-Konto

Die Live-Anmeldedaten müssen im Abschnitt **Live-Konto** eingegeben werden. Zur Einrichtung des Live-Kontos für einen Benutzer benötigen Sie den Benutzernamen, das Passwort und die Live-URL für das RSA Content Management System. Diese Information wird von Customer Care bereitgestellt.

In der folgenden Tabelle werden die Funktionen des Abschnitts Live-Konto beschrieben.

Funktion	Beschreibung
Host	Die Live-URL für das Content Management System. Der Standardwert verweist auf das RSA CMS unter **cms.netwitness.com**.
Port	Der Kommunikationsport, über den Live Anforderungen an das Content Management System sendet. Der Standardwert für dieses Feld ist **443**, das ist der Kommunikationsport auf dem Contentmanagement-System.
SSL	Ermöglicht dem Benutzer die Kommunikation über SSL.
Benutzername	Der Benutzername für das Live-Konto, der von RSA Customer Care bereitgestellt wurde.

Funktion	Beschreibung
Password	Das Benutzerpasswort für das Live-Konto, das von RSA Customer Care bereitgestellt wurde.
Überprüfen der Verbindung	Prüft, ob die Verbindung erfolgreich hergestellt wurde.
Anwenden	Speichert die Konfiguration und wendet sie an.

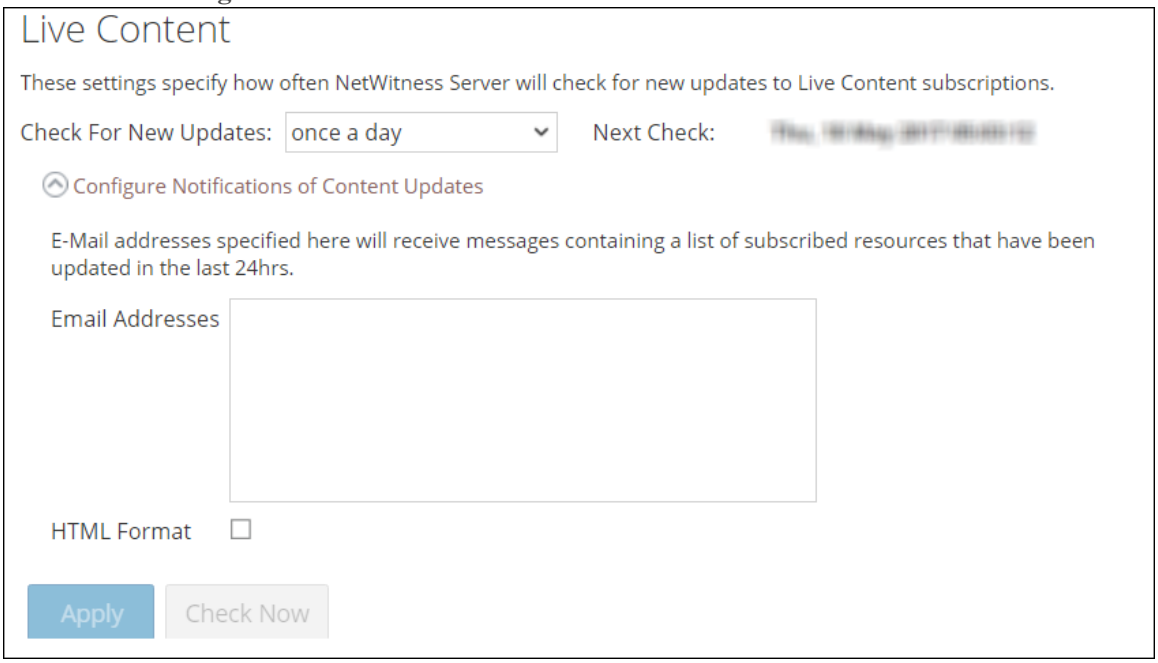
Im Abschnitt „Live-Konto“ können Sie Live Feedback-Verlaufsdaten herunterladen und teilen, indem Sie auf „Live Feedback-Aktivitätsprotokoll“ klicken.

Weitere Informationen zum Herunterladen der Verlaufsdaten finden Sie unter Hochladen von Daten in RSA für Live Feedback.

Bereich „Live-Inhalte“

Sie können das Synchronisationsintervall für Live-Inhalte, in dem NetWitness Suite nach neuen Aktualisierungen für Live-Inhalte sucht, sowie die entsprechende Benachrichtigung konfigurieren:

Verwenden Sie das Feld **Auf neue Aktualisierungen prüfen**, um das Intervall zu ändern. Wählen Sie ein Intervall aus der Drop-down-Liste aus. Der Standardwert für diese Einstellung ist **Einmal am Tag**.



In der folgenden Tabelle werden die Funktionen des Abschnitts „Live-Inhalte“ beschrieben.

Funktion	Beschreibung
Auf neue Aktualisierungen prüfen	Diese Einstellung gibt an, wie oft NetWitness Suite nach neuen Aktualisierungen der Live-Abonnements sucht und die abonnierten Ressourcen und Tags synchronisiert: • Einmal am Tag • Zweimal am Tag • Viermal am Tag • Jede Stunde • Jede zweite Stunde • Jede halbe Stunde Der Standardwert für diese Einstellung ist einmal am Tag.
Nächste Prüfung	Gibt die Uhrzeit und das Datum der nächsten geplanten Live-Synchronisation basierend auf dem konfigurierten Prüfintervall an.
E-Mail-Adressen	Die hier angegebenen E-Mail-Adressen erhalten Nachrichten mit einer Liste der abonnierten und in den letzten 24 Stunden aktualisierten Ressourcen.
HTML-Format	Gibt das Format von E-Mail-Nachrichten an. • Aktiviert = HTML • Deaktiviert = Text
Jetzt prüfen	Anstatt auf den nächsten geplanten Ressourcenzyklus zu warten, zwingt diese Option Live dazu, sofort mit der Synchronisation der abonnierten Ressourcen in dieser Instanz von NetWitness Suite zu beginnen. **Achtung:** Seien Sie vorsichtig, wenn Sie diese Funktion wählen, da die Synchronisation ein Neuladen des Parsers auslösen kann, wenn im Aktualisierungszyklus ein Lua-Parser oder Flex-Parser eingesetzt wird. Dies ist ein- oder zweimal täglich akzeptabel, aber ständige erneute Ladevorgänge des Parsers können zu Paketverlusten beim Decoder führen. Wenn dies das anfängliche Setup ist und Sie keine Live-Ressourcenabonnements konfiguriert haben, führen Sie nicht Jetzt Synchronisieren aus. Warten Sie, bis Sie Abonnements konfiguriert haben.

Funktion	Beschreibung
Anwenden	Wendet die geänderte Konfiguration auf das Verhalten der Abonnementsynchronisation an. Die Änderungen werden sofort wirksam. Das Feld **Die nächste Live-Synchronisation ist geplant für** wird aktualisiert, wenn sich die Zeit geändert hat.

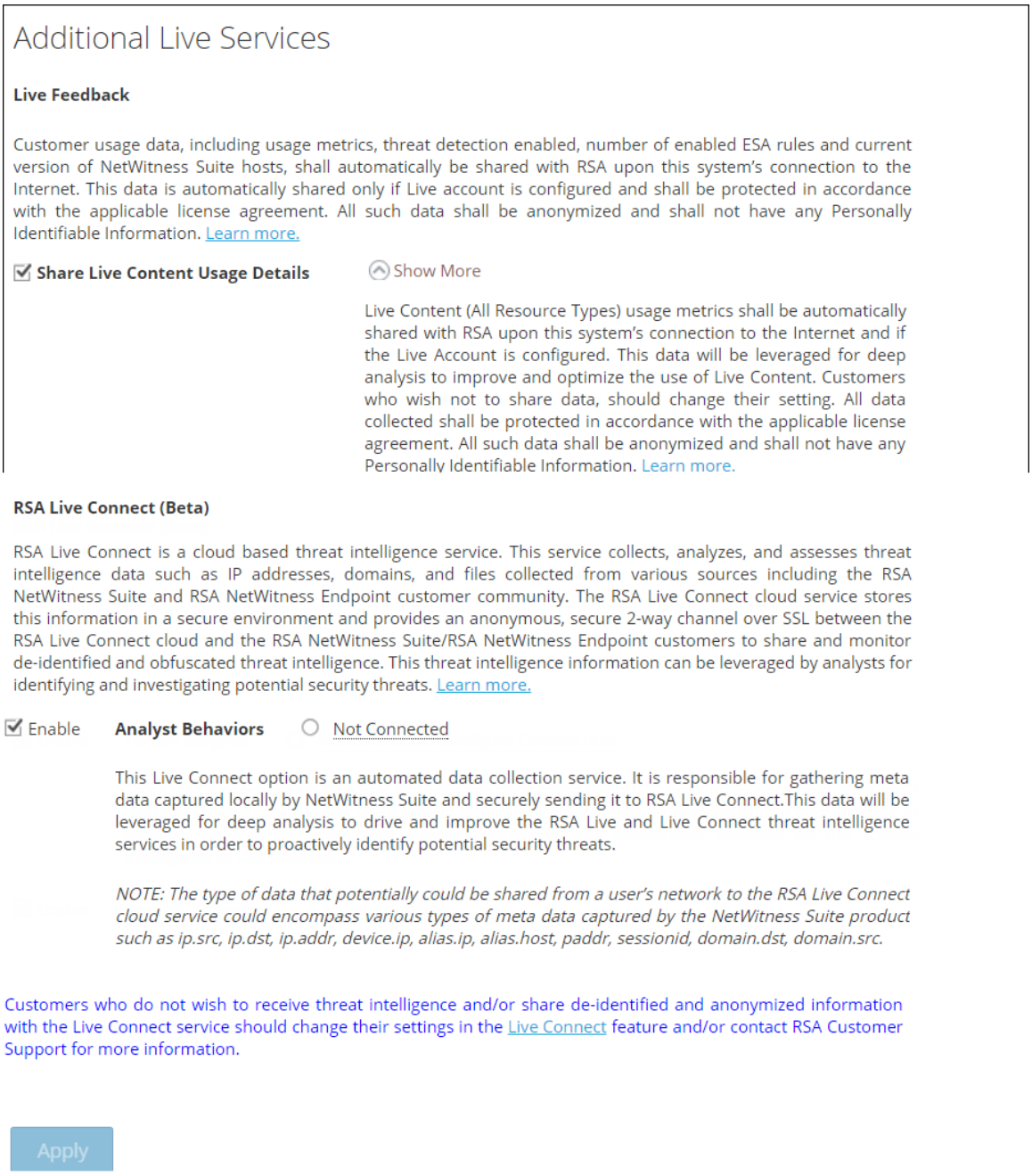
Erzwingen einer sofortigen Synchronisation

Klicken Sie auf **Jetzt prüfen**, um die Synchronisation sofort zu erzwingen. NetWitness Suite sucht in den abonnierten Ressourcen nach Aktualisierungen.

Anstatt auf den nächsten geplanten Ressourcenzyklus zu warten, zwingt diese Option Live dazu, sofort mit der Synchronisation der abonnierten Ressourcen in dieser Instanz von NetWitness Suite zu beginnen. Damit können unter anderem die unmittelbaren Auswirkungen einer Konfigurationsänderung angezeigt werden, wenn z. B. ein neuer Service hinzugefügt wurde oder neue Ressourcen auf die automatische Bereitstellung umgestellt wurden. Die geplante Synchronisation kann auch Stunden später stattfinden, wenn Live-Services für eine mehrmals täglich stattfindende Synchronisation eingerichtet wurde.

Achtung: Wenn ein Flex-Parser im Aktualisierungszyklus bereitgestellt ist, kann die Synchronisation einen erneuten Ladevorgang des Parsers auslösen. Dies ist ein- oder zweimal täglich akzeptabel, aber ständige erneute Ladevorgänge des Parsers können zu Paketverlusten beim Decoder führen. Wenn dies das anfängliche Setup ist und Sie keine Live-Ressourcenabonnements konfiguriert haben, führen Sie nicht Jetzt Synchronisieren aus. Warten Sie, bis Sie Abonnements konfiguriert haben.

Weitere Live-Services



Hinweis: Klicken Sie auf „Weitere Informationen über die von RSA gesammelten Daten". Weitere Informationen finden Sie unter Übersicht über Live Feedback.

In den folgenden Tabellen werden die Funktionen im Bereich „Weitere Live-Services" beschrieben.

Funktion	Beschreibung

Live Feedback	Gibt die Datentypen an, die von RSA erfasst werden:
	• Produktname
	• Produkt/Version
	• Produktinstanz
	• Aktivierungsschlüssel
	• Details der einzelnen Komponenten wie:
	  • ID
	  • Name
	  • Version
	  • Instanzen-ID
	• Metriken für jede Komponente

Weitergabe von Nutzungsdetails zu Live - Inhalten	Ermöglicht NetWitness Suite das anonyme Senden von technischen Daten zu Nutzungsmetriken zu Inhalten an RSA. Diese Option ist standardmäßig aktiviert.
RSA Live Connect	Bietet weitere Informationen über Live Connect-Service und die Konfiguration von Live-Services.
Aktivieren (Bedrohungseinblicke)	Ermöglicht die Funktion Bedrohungseinblicke bei denen Live Connect als Datenquelle für den Context-Hub-Service hinzugefügt wird und der Analyst kann während der Ermittlung Daten zu Bedrohungsinformationen abrufen. Stellen Sie sicher, dass dieser Context-Hub bereits vor dem Aktivieren dieser Funktion konfiguriert ist. Diese Option ist standardmäßig aktiviert (ausgewählt).
Aktivieren (Analystenverhalten)	Ermöglicht NetWitness Suitedas anonyme Senden technischer Daten zu Ihrer Umgebung an RSA. Diese Option ist standardmäßig aktiviert (ausgewählt).

Funktion	Beschreibung
Anwenden	Wendet die konfigurierten Änderungen an. Die Änderungen werden sofort wirksam. **Hinweis:** Diese Option gilt nur für Bedrohungseinblicke und Analystenverhalten.

Informationen über die Teilnahme an Live Feedback

Wenn Sie an Live Feedback teilnehmen, werden relevante Informationen zur weiteren Verbesserung erfasst. Weitere Informationen über Live Feedback finden Sie unter Übersicht über Live Feedback.

Bei der Installation von NetWitness Suite werden Sie aufgefordert, an Live Feedback teilzunehmen. Informationen finden Sie unter Konfigurieren der Einstellungen von Live-Services.

Bei Bedarf können Sie manuell Nutzungsverlaufsdaten herunterladen und diese in RSA freigeben. Informationen zum Herunterladen der Nutzungsverlaufsdaten und zum Freigeben der Daten in RSA finden Sie unter Hochladen von Daten in RSA für Live Feedback.

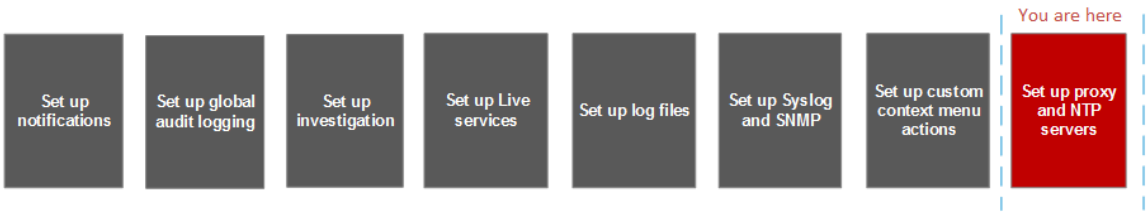
Bereich „NTP-Einstellungen“

Der Bereich „NTP-Einstellungen“ ist ein Protokoll zum Synchronisieren der Uhrzeiten von Hostcomputern über ein Netzwerk. Weitere Informationen über NTP finden Sie auf der Startseite (http://www.ntp.org/).

Hinweis: NetWitness Suite-Core-Hosts müssen mit dem NW-Host über UDP-Port123 kommunizieren können, um die NTP-Zeitsynchronisation durchzuführen.

Sie können in der Ansicht **ADMIN** > **System** > **NTP-Einstellungen** einen oder mehrere NTP-Server konfigurieren. Nach der Konfiguration eines NTP-Servers verwendet NetWitness Suite NTP zum Synchronisieren der Uhrzeiten der Hostcomputer. Sie konfigurieren mehrere NTP-Server zwecks Failover.

Workflow



Was wird von Ihnen erwartet?

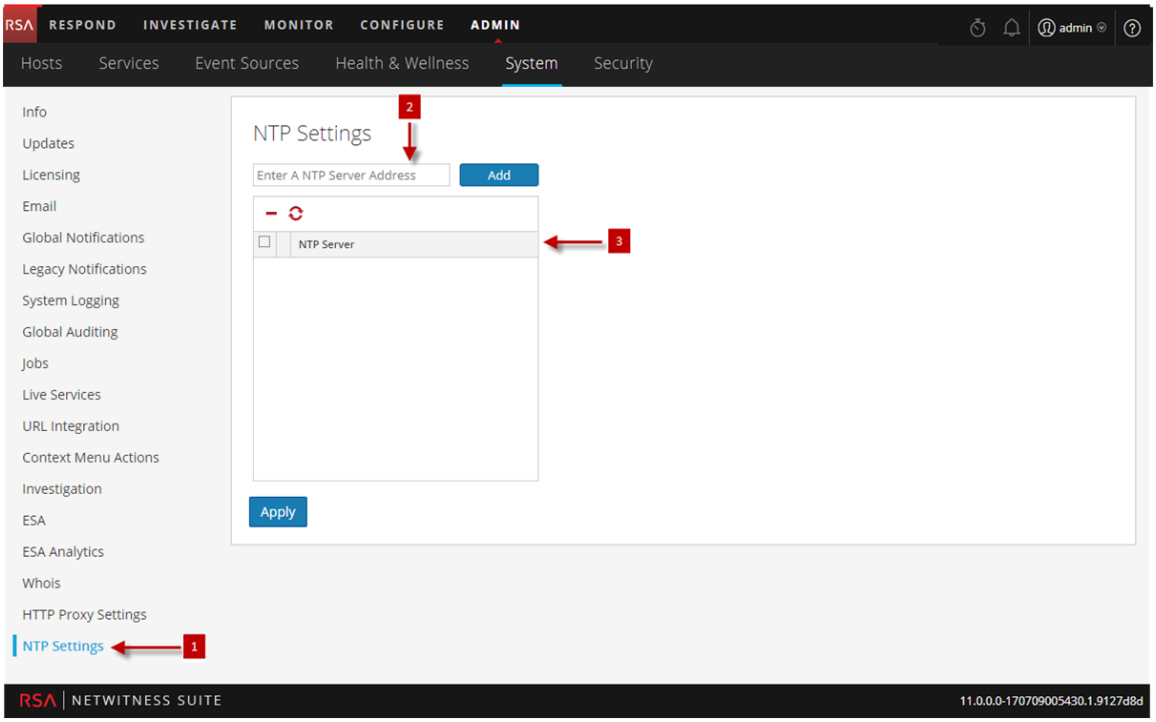
Rolle	Ziel	Details anzeigen
Administrator	Hinzufügen oder Ändern eines NTP-Servers	Konfigurieren von NTP-Servern

Verwandte Themen

- Konfigurieren von NTP-Servern
- Troubleshooting von NTP-Serverkonfigurationen

Überblick

Das folgende Beispiel zeigt den Bereich „NTP-Einstellungen“. Der Bereich bestimmt, wie ein NTP-Server zum Bereich „NTP-Einstellungen“ hinzugefügt werden kann.



1 Zeigt den Bereich „NTP-Einstellungen“ an.

2 Geben Sie eine IP-Adresse oder einen Hostnamen für den NTP-Server an.

3 Klicken Sie auf einen vorhandenen Hostnamen.

Symbolleiste und Funktionen

In der folgenden Tabelle werden die Einstellungen im Bereich „NTP-Einstellungen“ beschrieben.

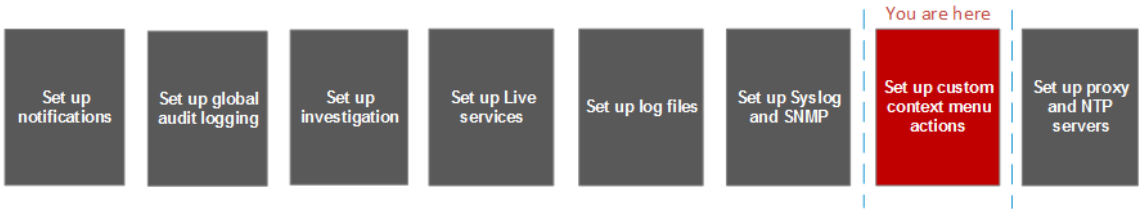
Einstellung	Beschreibung
	Geben Sie eine IP-Adresse oder einen Hostnamen für den NTP-Server an.
Hinzufügen	Fügt den NTP-Server zu NetWitness Suite hinzu.
	Löscht den ausgewählten NTP-Server.
	Synchronisiert den ausgewählten NTP-Server.
	Wählt den NTP-Server aus, den Sie löschen oder synchronisieren möchten.

Einstellung	Beschreibung
NTP-Server	Die IP-Adresse oder der Hostname des NTP-Servers. Wenn Sie auf einen vorhandenen Hostnamen klicken, wird der Hostname durch NetWitness Suite bearbeitbar und es werden die folgenden Befehlsschaltflächen angezeigt: • **Aktualisieren**: Ihre Änderungen werden angewendet. • **Abbrechen**: Ihre Änderungen werden abgebrochen.
Anwenden	Wendet die Einstellungen des NTP-Servers an und synchronisiert die Uhrzeiten des Hostcomputers für NTP.

Bereich Kontextmenüaktionen

Im Bereich „Kontextmenüaktionen“ können die Administratoren integrierte Kontextmenüaktionen anzeigen und benutzerdefinierte Kontextmenüaktionen, die als Optionen in einem Kontextmenü angezeigt werden, hinzufügen, bearbeiten oder löschen.

Workflow



Was möchten Sie tun?

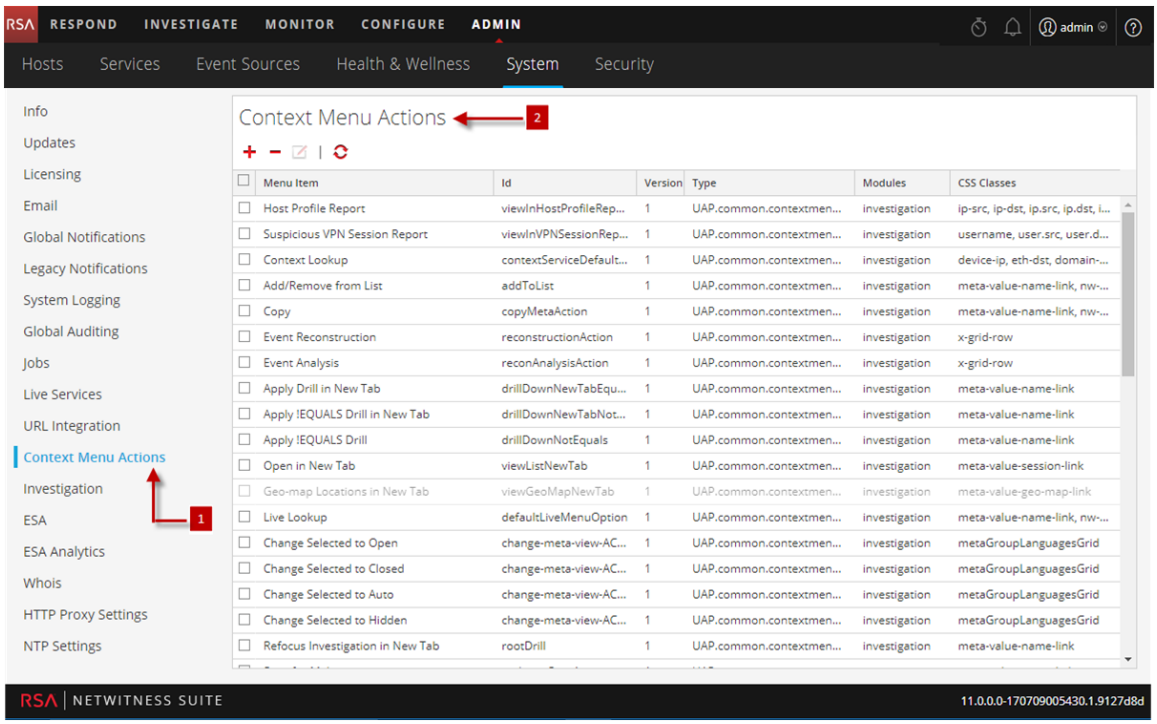
Rolle	Ziel	Details anzeigen
Administrator	Bereich „Benutzerdefinierte Kontextmenüaktionen“	Hinzufügen benutzerdefinierter Kontextmenüaktionen

Verwandte Themen

- Hinzufügen benutzerdefinierter Kontextmenüaktionen

Überblick

In der folgenden Abbildung ist ein Beispiel für den Bereich „Kontextmenüaktionen“ dargestellt.



1	Zeigt den Bereich „Kontextmenüaktionen“ an.
2	Mit der Symbolleiste kann der Benutzer Kontextmenüaktionen hinzufügen, bearbeiten und löschen.

Symbolleiste und Funktionen

Der Bereich „Kontextmenüaktionen“ enthält ein Raster und eine Symbolleiste. In der folgenden Tabelle werden die Optionen der Symbolleiste und die Funktionen des Rasters erläutert.

Funktionen	Beschreibung
+	Zeigt das Dialogfeld „Kontextmenü-Konfiguration“ an, in dem Sie eine neue Kontextaktion erstellen können.
↻	Aktualisiert die Liste.
−	Löscht die ausgewählten Kontextaktionen. NetWitness Suite fordert keine Bestätigung an, wenn Sie die Aktion löschen möchten. Die ausgewählten Aktionen werden sofort gelöscht und dieser Schritt kann nicht abgebrochen werden.

Funktionen	Beschreibung
	Zeigt das Dialogfeld „Kontextaktion bearbeiten“ an, in dem Sie eine vorhandene Kontextaktion bearbeiten können.
Menüelement	Das Menüelement, wie es im Kontextmenü angezeigt wird. Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `displayName`. Im Folgenden ist eine Zeile mit Beispielcode angegeben: `"displayName": "User Agent String Lookup”`
ID	Die eindeutige ID für die Kontextaktion. Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `id`. Im Folgenden ist eine Zeile mit Beispielcode angegeben: `"id": "UserAgentStringAction"`
Version	Die Versionsnummer der Kontextaktion. Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `version`. Im Folgenden ist eine Zeile mit Beispielcode angegeben: `"version": "1"`
Typ	Die Art der Kontextaktion. Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `type`.. Alle NetWitness Suite-Kontextaktionstypen beginnen mit der folgenden Zeichenfolge: `UAP.common.contextmenu.actions`. Der letzte Teil der Zeichenfolge identifiziert das Menü in NetWitness Suite, z. B. `URLContextAction` oder `LivePostContextAction`. Im Folgenden ist eine Zeile mit Beispielcode angegeben: `"type": "UAP.common.contextmenu.actions.URLContextAction"`

Funktionen	Beschreibung

Module	Die Namen der Module, in denen die Kontextaktion verfügbar ist. Derzeit sind alle integrierten Kontextmenüaktionen für das Modul „Investigation“ vorgesehen.
	Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `modules`.
	Im Folgenden ist eine Zeile mit Beispielcode angegeben:
	`"modules": [`
	`"investigation"`
	`],`

Modulklassen	Die CSS-Klassen, die die Namen der Modulansichten identifizieren, in denen die Kontextaktion verfügbar ist. Derzeit sind alle integrierten Kontextmenüaktionen für das Modul „Investigation“ vorgesehen. Die Nicht-Metaschlüssel-Modulklassen werden unten stehend ausführlich beschrieben.
	Im Folgenden sind einige Zeilen mit Beispielcode angegeben:
	`"moduleClasses": [`
	`"UAP.investigation.navigate.view.NavigationPanel", <-- Enabled in Navigate pane-->`
	`"UAP.investigation.events.view.EventGrid"`
	`],`

CSS-Klassen	Die CSS-Klassen, für die die Kontextmenüaktion gilt. Die CSS-Klassen definieren, an welcher Stelle im Modul „Investigation“ das Kontextmenü eingeblendet wird, wenn Sie mit der rechten Maustaste klicken. Bei der Erstellung einer Kontextmenüaktion lautet der Parameter `cssClasses`.
	Im Folgenden ist eine Zeile mit Beispielcode angegeben:
	`"cssClasses": [`
	`"client"`
	`]`
	Bei den meisten CSS-Klassen, die Sie hinzufügen können, handelt es sich um Metaschlüssel. Sie können auch bestimmte Nicht-Metaschlüssel-CSS-Klassen hinzufügen. Im Folgenden finden Sie weitere Einzelheiten und Beispiele.

CSS-Klassen und Beispiele

Bei CSS-Klassen kann es sich um Metaschlüssel und Nicht-Metaschlüssel handeln.

Metaschlüssel-CSS-Klassen

Einen CSS-Klassentyp, den Sie hinzufügen können, sind Metaschlüssel. Beim Definieren einer CSS-Klasse ändern Sie einen eventuell vorhandenen Punkt bei Metaschlüsseln in einen Bindestrich. Beispiel: Der Metaschlüssel `alias.host` wird zur CSS-Klasse `alias-host`. Der Metaschlüssel `ip.src` wird zur CSS-Klasse `ip-src`.

Nicht-Metaschlüssel-CSS-Klassen

Integrierte Nicht-Metaschlüssel-CSS-Klassen sind ebenfalls verfügbar. Die Klassen in der folgenden Tabelle definieren Aktionen und den Teil der Benutzeroberfläche, an dem die Aktion verfügbar ist.

CSS-Klasse	Typ	Beschreibung
`meta-value-session-link`	Aktion	Bei Metasitzungsanzahl offen
`meta-value-name-link`	Aktion	Bei Metawertenamen offen
`nw-event-value`	Aktion	Verwendung für die Rekonstruktion von Kontextaktionen bei Metawert
`UAP.investigation.navigate.view.NavigationPanel`	Benutzeroberfläche	Gilt für die Navigationsansicht
`UAP.investigation.events.view.EventGrid`	Benutzeroberfläche	Gilt für die Ereignisansicht
`UAP.investigation.reconstruction.view.content.ReconstructedEventDataGrid`	Benutzeroberfläche	Gilt für die Ereignisrekonstruktionsansicht

Beispiel

Dies ist ein kommentiertes Beispiel einer Kontextmenüaktion zur Validierung des Benutzer-Agent aus dem Clientanwendungs-Metaschlüssel (Client). Die Kommentare werden automatisch entfernt, sobald sie in der Systemansicht des Moduls „Administration“ angewendet wurden. Das neue Menüelement wird nach dem Neustart des Browsers angezeigt.

```
{
     "displayName": "User Agent String Lookup”, <!-- What name shows up
in NW UI -->
     "cssClasses": [
         “client”  <!-- What meta key to launch from -->
     ],
     "description": "",
     "type": "UAP.common.contextmenu.actions.URLContextAction",
     "version": "1",
     "modules": [
         "investigation"
     ],
     "local": "false",
     "groupName": "externalLookupGroup”, <!-- What group to show link
in. Remove line to show in main list -->
     "urlFormat": "http://www.useragentstring.com/?uas={0}&getText=all”, <!-- The
{0} gets replaced with whatever was right clicked on -->
     "disabled": "",
     "id": "UserAgentStringAction",
    "moduleClasses": [
         "UAP.investigation.navigate.view.NavigationPanel”, <-- Enabled
in Navigate pane-->
        “UAP.investigation.events.view.EventGrid” <-- Enabled in Event
View pane -->
     ],
     "openInNewTab": "true",
     "order": "15"
 }
```

Bereich „Konfiguration alter Benachrichtigungen“

Der Bereich „Konfiguration alter Benachrichtigungen“ dient zur Konfiguration von Syslog- und SNMP-Benachrichtigungseinstellungen. Diese Konfigurationen werden für Berechtigungen, Legacy-Ereignisquellenmanagement (Event Source Management, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung verwendet.

Die Verfahren im Zusammenhang mit diesen Einstellungen werden unter Konfigurieren von Syslog- und SNMP-Einstellungen beschrieben.

Workflow

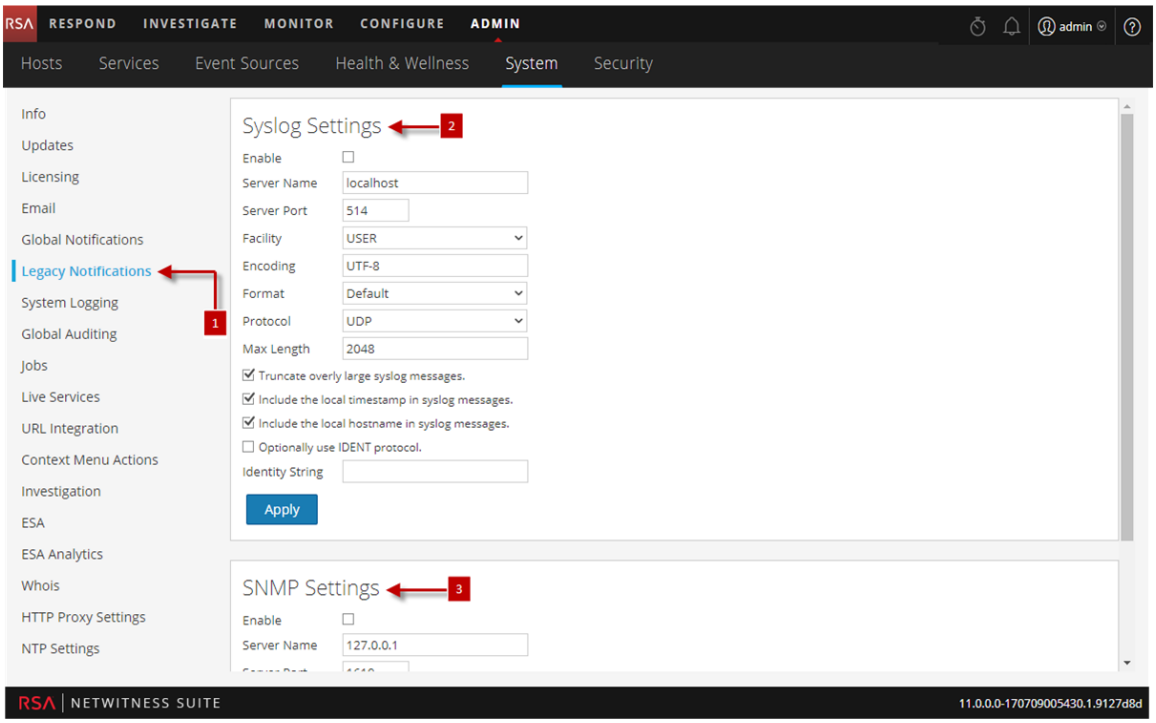
Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Konfigurieren von Syslog-Einstellungen	Konfigurieren von Syslog- und SNMP-Einstellungen
Administrator	Konfigurieren von SNMP-Einstellungen	Konfigurieren von Syslog- und SNMP-Einstellungen

Verwandte Themen

- Konfigurieren von Syslog- und SNMP-Einstellungen

Überblick



1	Zeigt den Bereich „Konfiguration alter Benachrichtigungen“ an.
2	Ermöglicht dem Benutzer die Konfiguration von Syslog-Benachrichtigungen für Berechtigungen, Legacy-Ereignisquellenmanagement (Event Source Management, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung verwendet.
3	Ermöglicht dem Benutzer die Konfiguration von SNMP-Benachrichtigungen für Berechtigungen, Legacy-Ereignisquellenmanagement (Event Source Management, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung verwendet.

Symbolleiste und Funktionen

Der Bereich „Konfiguration alter Benachrichtigungen“ besteht aus zwei Abschnitten: „Syslog-Einstellungen“ und „SNMP-Einstellungen“.

Syslog-Einstellungen

In der folgenden Tabelle werden die verfügbaren Optionen für die Konfiguration von Syslog-Benachrichtigungen für die Funktionen Berechtigung, Legacy-Ereignisquellenmanagement (Event Source Management, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung beschrieben.

Funktion	Beschreibung
Aktivieren	Aktiviert die hier konfigurierten Syslog-Einstellungen.
Servername	Gibt den Host an, auf dem der Ziel-Syslog-Prozess ausgeführt wird.
Serverport	Gibt den Port an, den der Ziel-Syslog-Prozess überwacht.
Facility	Gibt die designierte Syslog-Facility an, die für alle ausgehenden Nachrichten verwendet wird. Mögliche Werte sind KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL1 bis LOCAL7.
Codierung	Gibt die Codierung an, die für Text in Syslog-Nachrichten zu verwenden ist; zum Beispiel UTF-8.
Format	Gibt das Nachrichtenformat an. Die möglichen Werte sind: Standard, PCI-DSS oder SEC
Protokoll	Gibt das Kommunikationsprotokoll an, das zum Senden von Syslog verwendet wird: UDP oder TCP. Standardmäßig ist das UDP-Protokoll ausgewählt.
Max. Länge	Gibt die die maximal zulässige Länge einer Syslog-Meldung in Byte an. Der Standardwert ist **2.048**. Meldungen, die die maximal zulässige Länge überschreiten, werden gekürzt, wenn das Kontrollkästchen **Zu lange Syslog-Meldungen kürzen** aktiviert ist.
Zu lange Syslog-Meldungen kürzen	Wenn aktiviert, werden alle Meldungen, die die maximale Länge überschreiten, gekürzt.
Lokalen Zeitstempel in Syslog-Meldungen einfügen	Wenn aktiviert, fügt NetWitness Suite den lokalen Zeitstempel in Meldungen ein.

Funktion	Beschreibung
Lokalen Hostnamen in Syslog-Meldungen einfügen	Wenn aktiviert, fügt NetWitness Suite den lokalen Hostnamen in Syslog-Meldungen ein.
IDENT-Protokoll verwenden (optional)	Wenn aktiviert, stellt NetWitness Suite den ausgehenden Syslog-Warnmeldungen die Identitätszeichenfolge voran.
Identitätszeichenfolge	Dies ist eine Identitätszeichenfolge, die jeder Syslog-Warnmeldung vorangestellt werden muss. Wenn die Zeichenfolge leer ist, wird den ausgehenden Syslog-Warnmeldungen keine Identitätszeichenfolge vorangestellt. Sie können damit die Quelle der Warnmeldung identifizieren. Viele Benutzer verwenden dafür den Namen des Programms, das die Syslog-Meldung sendet.
Anwenden	Setzt die Syslog-Konfigurationseinstellungen in Kraft.

SNMP-Einstellungen

In der folgenden Tabelle werden die verfügbaren Optionen für die Konfiguration von SNMP-Benachrichtigungen für die Funktionen Berechtigung, Legacy-Ereignisquellenmanagement (Event Source Management, ESM), Warehouse Connector-Überwachung und Archiver-Überwachung beschrieben.

Funktion	Beschreibung
Aktivieren	Aktiviert die hier konfigurierten SNMP-Einstellungen.
Servername	Gibt den SNMP-Trap-Host an.
Serverport	Gibt den abhörenden Port auf dem SNMP-Trap-Host an.
SNMP-Version	Gibt die SNMP-Version an, **v1** oder **v2c**.
Trap-OID	Gibt die Objekt-ID für die SNMP-Trap auf dem Trap-Host an, der das Auditereignis empfängt. Der Standardwert ist **0.0.0.0.0.1**.

Funktion	Beschreibung
Community	Gibt die Community-Zeichenfolge an, die zur Authentifizierung auf dem SNMP-Trap-Host verwendet wird. Der Standardwert ist **öffentlich**.
Aktivieren	Aktiviert die hier konfigurierten SNMP-Benachrichtigungen.
Anwenden	Setzt die SNMP-Konfigurationseinstellungen in Kraft.