RSA NETWITNESS® SUITE

Leitfaden Systemwartung

für Version 11.0

Copyright © 1994–2017 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten.

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

NetWitness Suite-Systemwartung

Dieses Handbuch umfasst Aufgaben, die Administratoren nach der ersten Netzwerkeinrichtung durchführen, um NetWitness Suite zu ermöglichen, Hosts und Services im Netzwerk zu managen, das Netzwerk zu warten und zu überwachen, Jobs zu managen und die Performance abzustimmen.

Das folgende Diagramm zeigt die verschiedenen Systemwartungsaufgaben, die Sie ausführen können:

In den folgenden Themen werden diese Aufgaben beschrieben:

- Best Practices
- Überwachen von Integrität und Zustand in der NetWitness Suite
- Anzeigen von System- und Serviceprotokollen
- Verwalten von Abfragen mithilfe der URL-Integration
- Managen von NetWitness Suite-Aktualisierungen
- FIPS-Unterstützung
- Troubleshooting der NetWitness-Suite

Best Practices

Schützen von Ressourcen durch RSA-Richtlinien

Die im Lieferumfang von NetWitness Suite enthaltenen RSA Core-Richtlinien haben den Zweck, die Ressourcen Ihrer NetWitness Suite-Domain sofort zu schützen (bevor Sie Regeln konfigurieren, die für Ihre Umgebung und Ihre Sicherheitsrichtlinie spezifisch sind).

RSA empfiehlt, dass Sie sobald wie möglich E-Mail-Benachrichtigungen an die entsprechenden Eigentümer der Ressourcen für diese Richtlinien einrichten. So werden diese benachrichtigt, wenn Schwellenwerte für Performance und Kapazität überschritten werden, damit sie sofort handeln können.

RSA empfiehlt ebenfalls, dass Sie die Core-Richtlinien evaluieren und eine Richtlinie deaktivieren oder ihre Service/Gruppenzuordnung entsprechend Ihrer besonderen Monitoring-Anforderungen ändern.

Schützen von Ressourcen mit Richtlinien, die auf Ihrer Umgebung basieren

RSA Core-Richtlinien sind allgemein und bieten eventuell keinen ausreichenden Monitoring-Schutz für Ihre Umgebung. RSA empfiehlt, dass Sie über einen bestimmten Zeitraum Probleme sammeln, die von den RSA Core-Richtlinien nicht identifiziert werden, und Regeln konfigurieren, die helfen, diese Probleme zu verhindern.

Erstellen von Regeln und Benachrichtigungen mit Bedacht

RSA empfiehlt Ihnen, möglichst sicherzustellen, dass jede Regel und Richtlinie notwendig ist, bevor Sie sie implementieren. RSA empfiehlt auch, implementierte Richtlinien regelmäßig hinsichtlich ihrer Gültigkeit zu überprüfen. Ungültige Alarme und E-Mail-Benachrichtigungen können sich negativ auf den Fokus der Eigentümer von Ressourcen auswirken.

Troubleshooting von Problemen

RSA empfiehlt, das Thema Troubleshooting von Integrität und Zustand und Troubleshooting der NetWitness-Suite zu Rate zu ziehen, wenn Fehlermeldungen in der Benutzeroberfläche und in den Protokolldateien der Hosts und Services angezeigt werden.

Überwachen von Integrität und Zustand in der NetWitness Suite

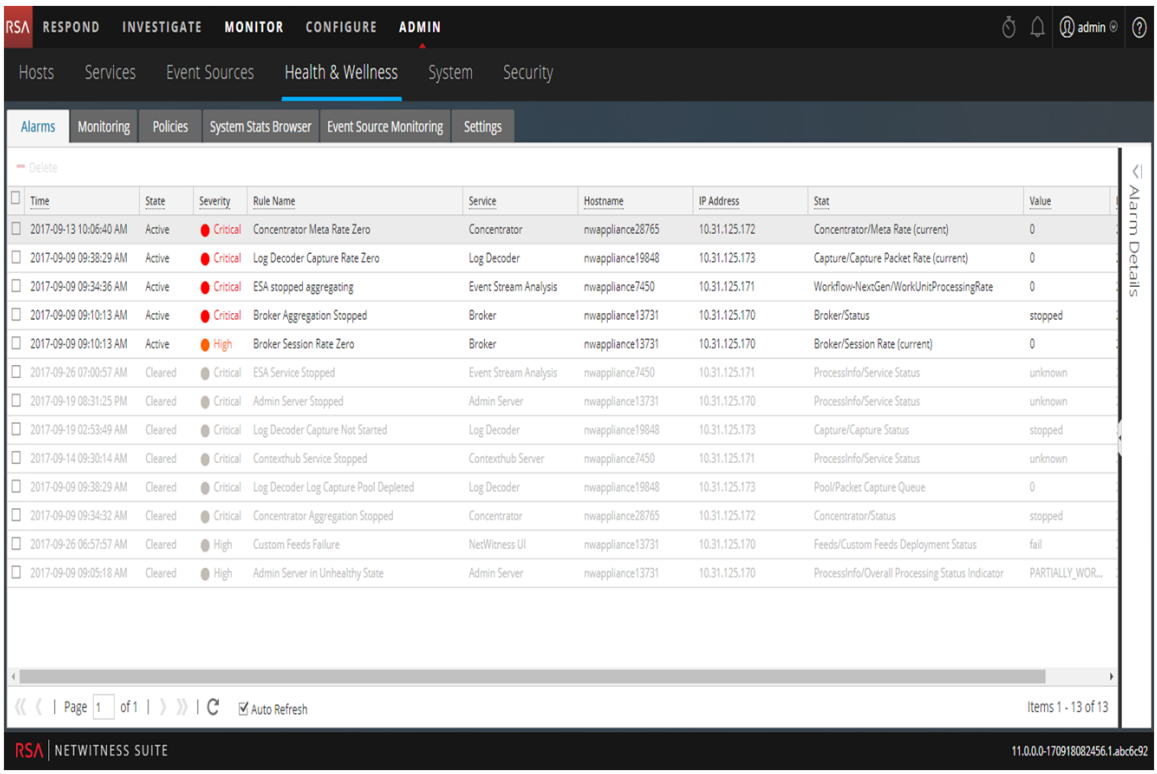
Das Modul „Integrität und Zustand“ von NetWitness Suite bietet folgende Möglichkeiten:

- Anzeigen der aktuellen Integrität von sämtlichen Hosts, den auf den Hosts ausgeführten Services und verschiedener Aspekte der Integrität der Hosts
- Überwachen der Hosts und Services in der Netzwerkumgebung
- Anzeigen der verschiedenen Ereignisquellen, die mit NetWitness Suite konfiguriert werden
- Anzeigen der Systemstatistiken für die ausgewählten Hosts, indem die Ansichten nach Bedarf gefiltert werden

Darüber hinaus können Sie die Überwachung von Archiver und Warehouse Connector konfigurieren, die Verfahren zum Überwachen der Hoststatistiken verwenden und mit den Systemprotokollen arbeiten, um NetWitness Suite zu überwachen.

Hinweis: Alle Benutzer verfügen standardmäßig über die Berechtigung, die gesamte Benutzeroberfläche „Integrität und Zustand“ anzuzeigen. Die Ansicht „Policys“ kann standardmäßig nur von den Administrator- und Operatorrollen gemanagt werden. Im Thema **Rollenberechtigungen** im *Handbuch zur Systemsicherheit und Benutzerverwaltung* finden Sie eine vollständige Liste der Standardberechtigungen für die NetWitness Suite-Benutzeroberfläche.

In der Abbildung werden das Modul „Integrität und Zustand“ der NetWitness Suite-Benutzeroberfläche und dessen verschiedene Bereiche dargestellt.



Richtlinien managen

Richtlinien werden entweder vom Benutzer definiert oder von RSA bereitgestellt. In einer Richtlinie werden definiert:

- Services und Hosts, für die die Richtlinie gilt
- Regeln, die statistische Schwellenwerte zu Alarmmeldungen festlegen
- Wann eine Richtlinie unterdrückt wird
- Wer bei Auslösung eines Alarms benachrichtigt wird und wann.

Die zugehörigen Referenzthemen finden Sie unter Vordefinierte Richtlinien für NetWitness Suite.

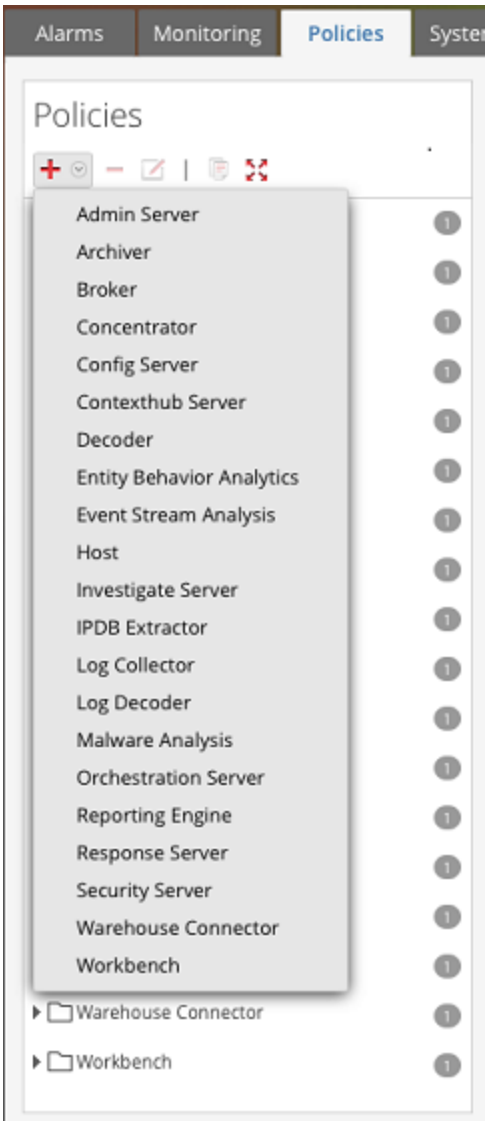
Hinweis: Sie können nun eine Richtlinie konfigurieren, um eine Benachrichtigung über den Ablaufstatus des PKI-Zertifikats (Public Key Infrastructure) zu senden.

Hinzufügen einer Richtlinie

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

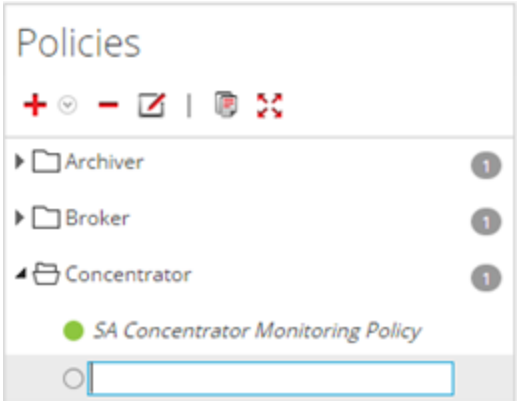
   Die Policy-Ansicht wird angezeigt.
3. Klicken Sie im Bereich **Policys** auf  .

   Es wird eine Liste der Hosts und Services angezeigt, für die Sie Integritätsrichtlinien erstellen können.

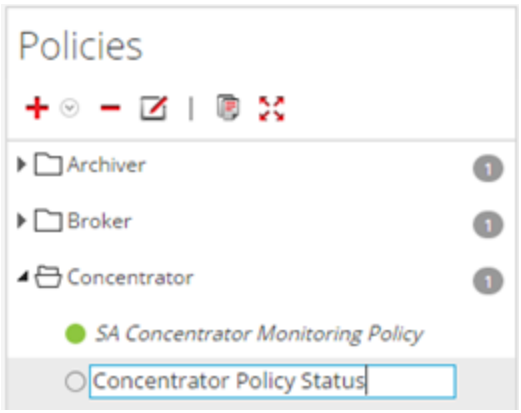


4. Wählen Sie einen Host oder Service aus (z. B. **Concentrator**).
   Für die PKI-Policy müssen Sie einen Host (z. B. Host) auswählen.
   Der Host oder Service wird im Bereich „Policys“ mit leerem Bereich „Policy-Details“

angezeigt.



5. Geben Sie im Bereich **Policys** einen Namen für die Richtlinie ein (z. B. **Concentrator-Richtlinienstatus**).



Der Name (z. B. **Concentrator-Policy-Status**) wird jetzt als Name der Policy im Bereich „Policy-Details“ angezeigt.

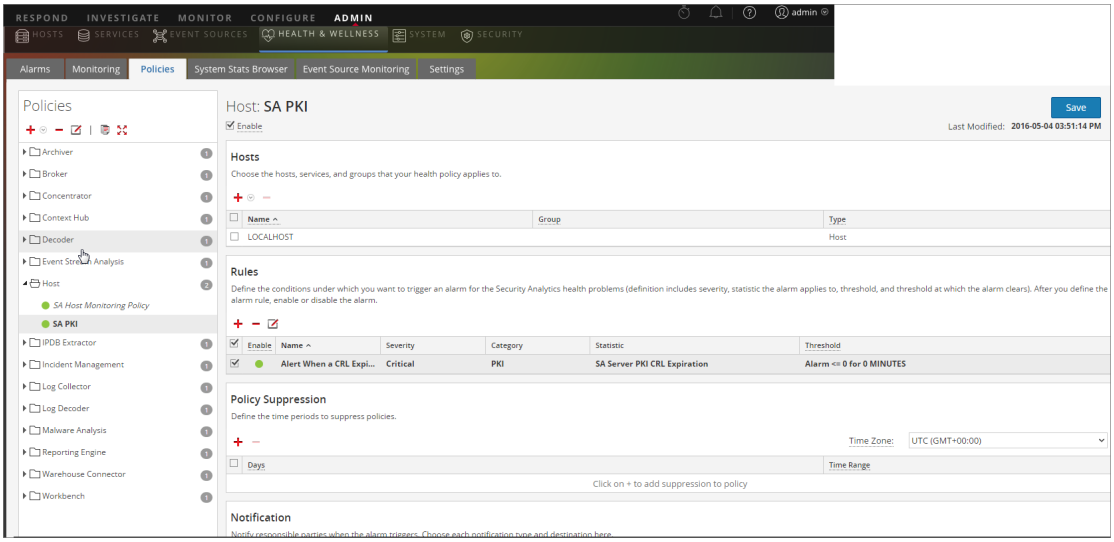
6. Erstellen Sie eine Policy im Bereich „Policy-Details“:
   a. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
   b. Fügen Sie die relevanten Services (in diesem Beispiel alle relevanten Concentrator-Services) hinzu, für die die Integritätsstatistik überwacht werden soll.
   Für die PKI-Policy müssen Sie den LOCALHOST zur Überwachung der Integritätsstatistiken auswählen.
   c. Fügen Sie relevante Regelbedingungen hinzu, die Sie für die Richtlinie konfigurieren möchten.
   d. Unterdrücken Sie die Durchsetzung der Richtlinie für die gewünschten Zeiträume.
   e. Fügen Sie alle gewünschten E-Mail-Benachrichtigungen für die Richtlinie an.
   f. Klicken Sie im Bereich „Richtliniendetails“ auf **Speichern**.

Die Richtlinie wird hinzugefügt.

Hinzufügen einer Policy – Beispiel

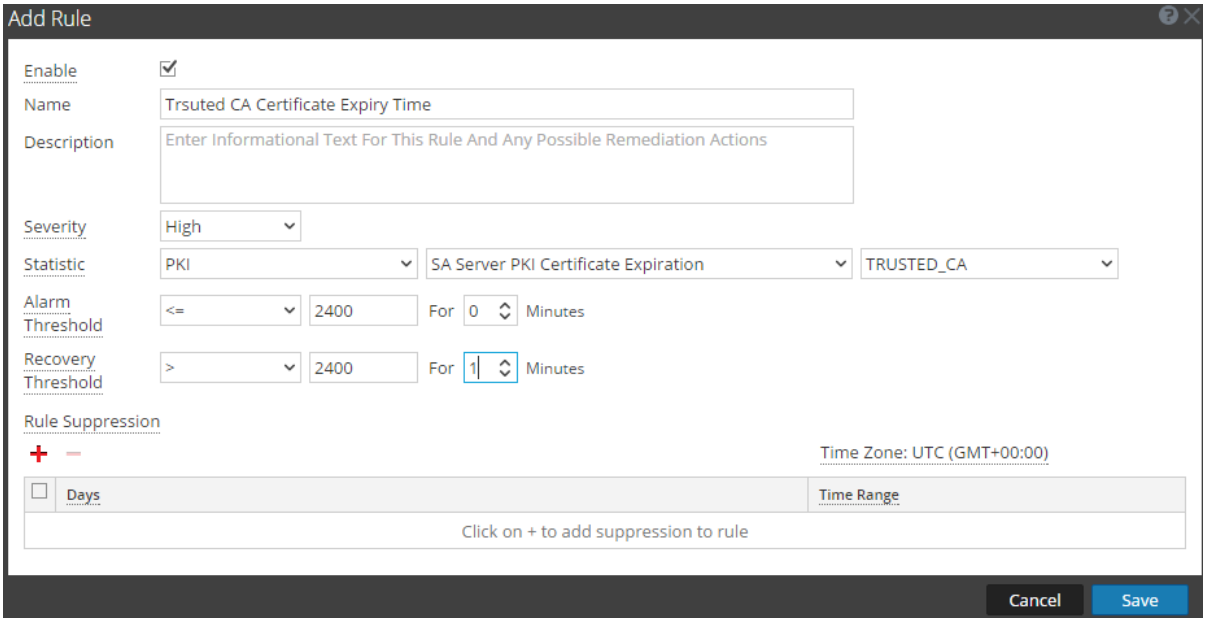
Nachstehend ist ein allgemeines Beispiel für die Konfiguration der PKI-Policy angegeben:

1. Fügen Sie eine neue PKI-Policy hinzu.

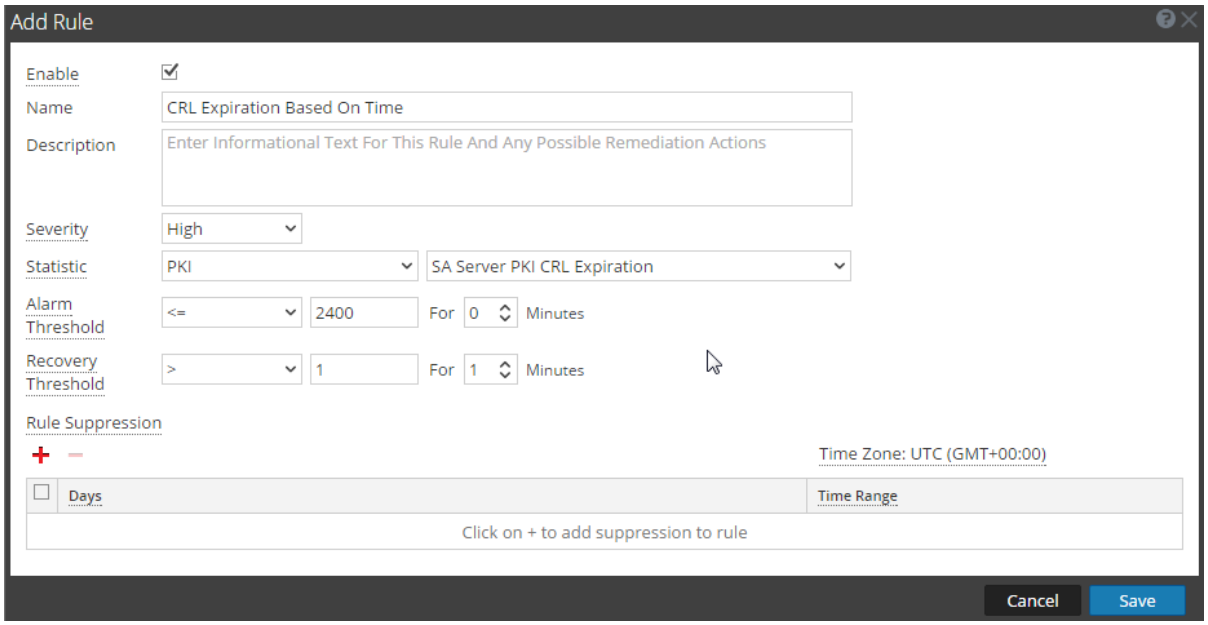


2. Fügen Sie eine Regel mit Statistiken hinzu:

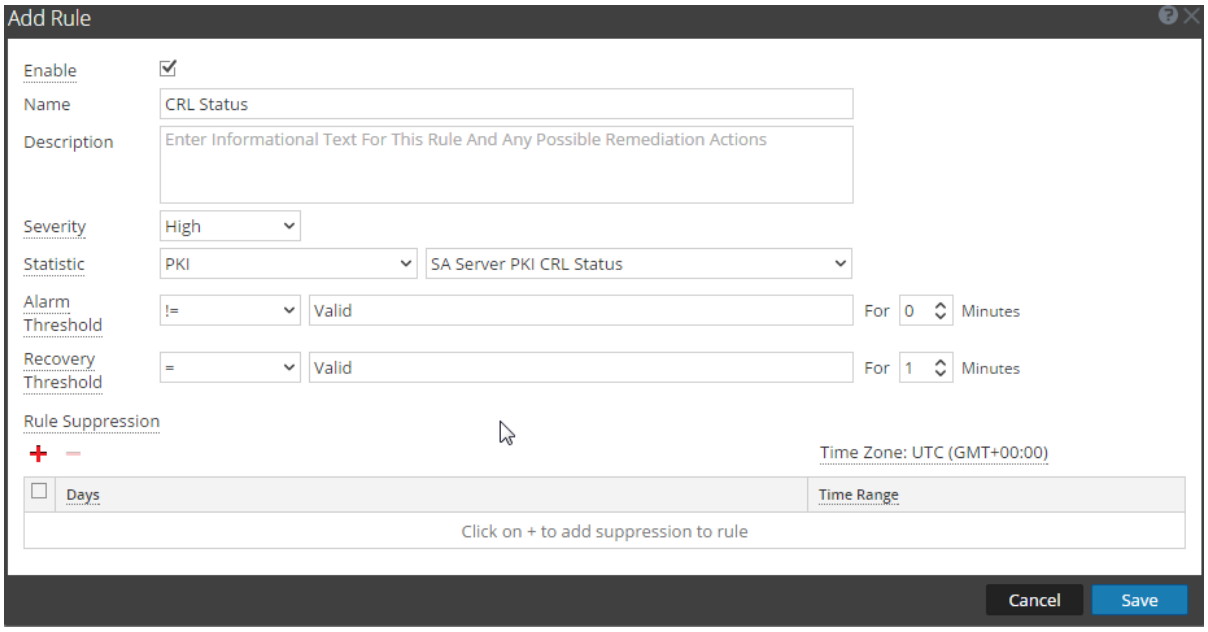
   - Für Ablaufdatum der Zertifizierungsstelle



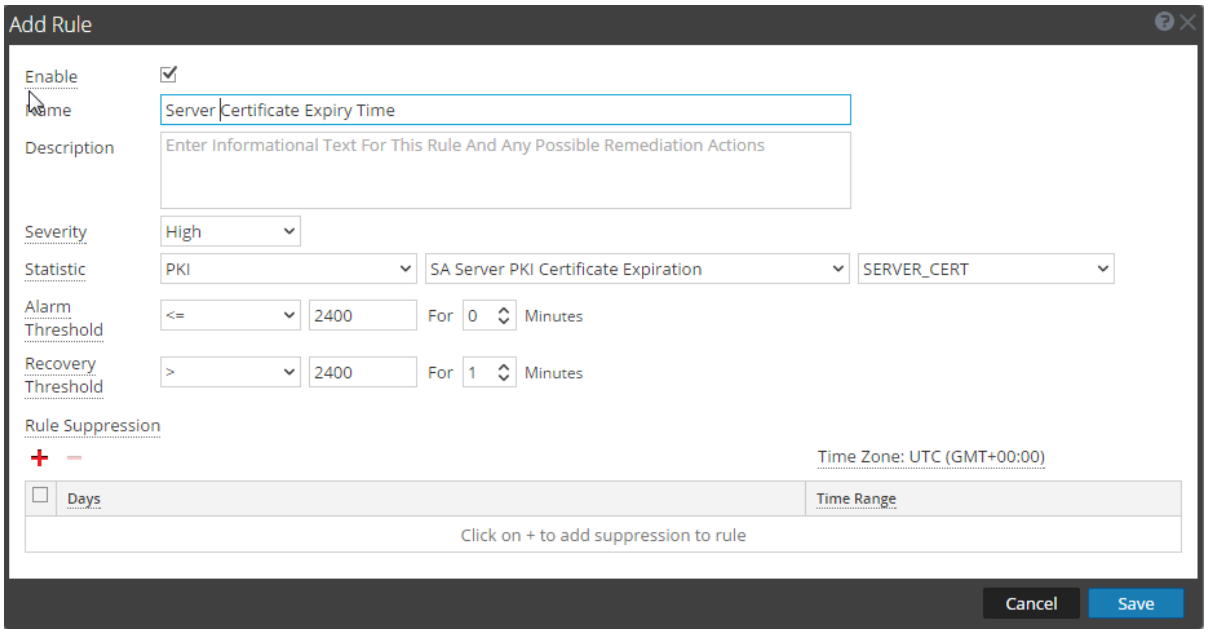
   - Für Ablaufdatum der Zertifikatrückrufliste



- Für Status der Zertifikatrückrufliste



- Für das Ablaufdatum des Serverzertifikats



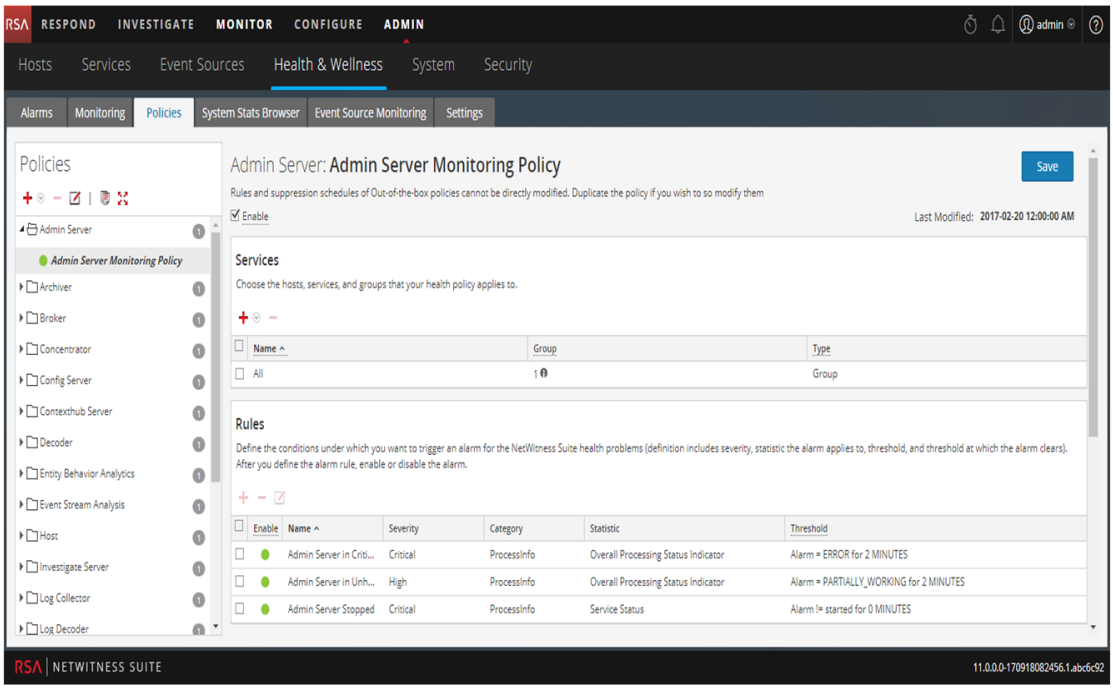
Bearbeiten einer Richtlinie

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Policy-Ansicht wird angezeigt.
3. Wählen Sie eine Richtlinie (z. B. **Concentrator-Richtlinienstatus**) unter einem Host oder Service aus.

   Der Bereich „Policy-Details“ wird angezeigt.
4. Klicken Sie auf .

   Der Policy-Name (z. B. **Überwachungs-Policy des Administrationsservers**) und der Bereich „Policy-Details“ können nun bearbeitet werden.



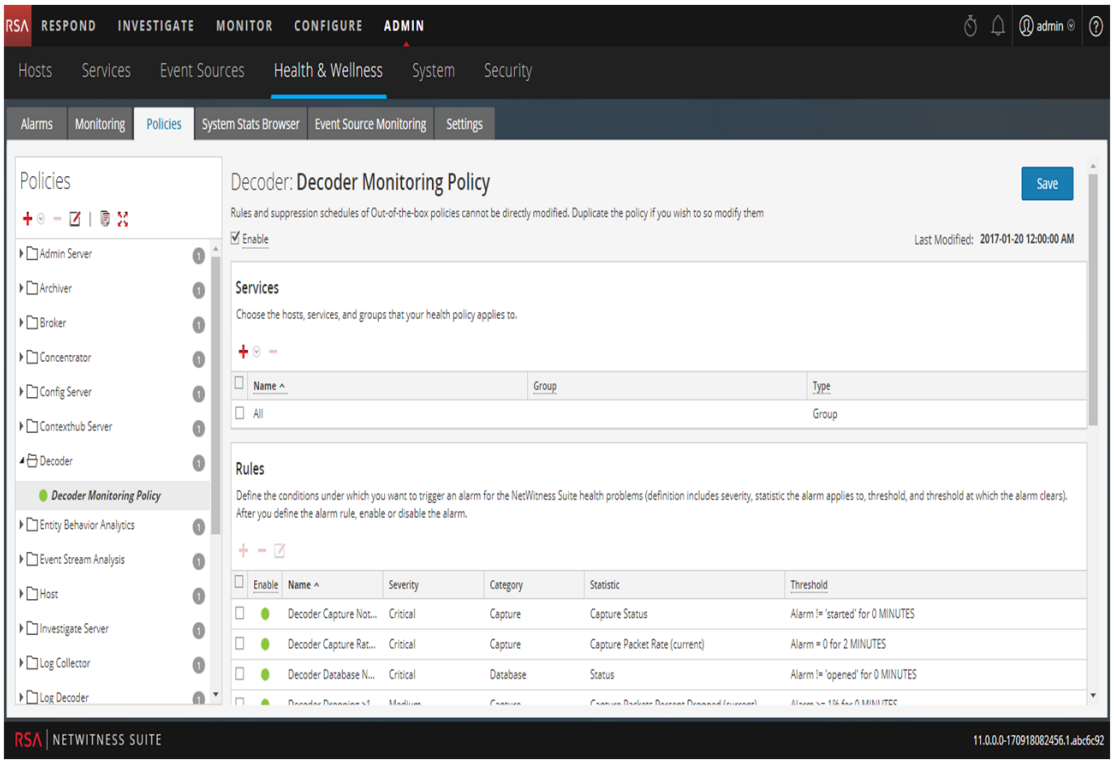
5. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie im Bereich „Richtliniendetails“ auf **Speichern**. Sie können:
   - den Namen der Richtlinie bearbeiten.
   - die Richtlinie aktivieren oder deaktivieren
   - Hosts und Services in der Richtlinie hinzufügen oder löschen
   - Regeln in der Richtlinie hinzufügen, löschen oder ändern
   - Unterdrückungen in der Richtlinie hinzufügen/bearbeiten/löschen
   - Benachrichtigungen in der Richtlinie hinzufügen/bearbeiten/löschen

Hinweis: Speichern wendet die Richtlinienregeln basierend auf der Auswahl von aktivieren/deaktivieren an. Dadurch werden auch die Regelbedingungs-Timer für geänderte Regeln sowie die gesamte Richtlinie zurückgesetzt.

Duplizieren einer Richtlinie

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.
3. Wählen Sie eine Richtlinie (z. B. **Concentrator-Richtlinienstatus**) unter einem Host oder Service aus.
4. Klicken Sie auf . NetWitness Suite kopiert die Policy und listet Sie mit einer an den

Originalnamen der Policy angefügten **(1)** auf.



5. Klicken Sie auf und benennen Sie die Policy um (benennen Sie z. B. **Decoder-Überwachungs-Policy (1)** in **Neuen Concentrator-Policy-Status** um).

> **Hinweis:** Eine duplizierte Richtlinie ist standardmäßig deaktiviert und die Host- und Servicezuweisungen werden nicht dupliziert. Weisen Sie der duplizierten Policy alle relevanten Hosts und Services zu, bevor Sie sie zur Überwachung von Integrität und Zustand der NetWitness Suite-Infrastruktur einsetzen.

Zuweisen von Services oder Gruppen

So weisen Sie Hosts oder Services einer Richtlinie zu:

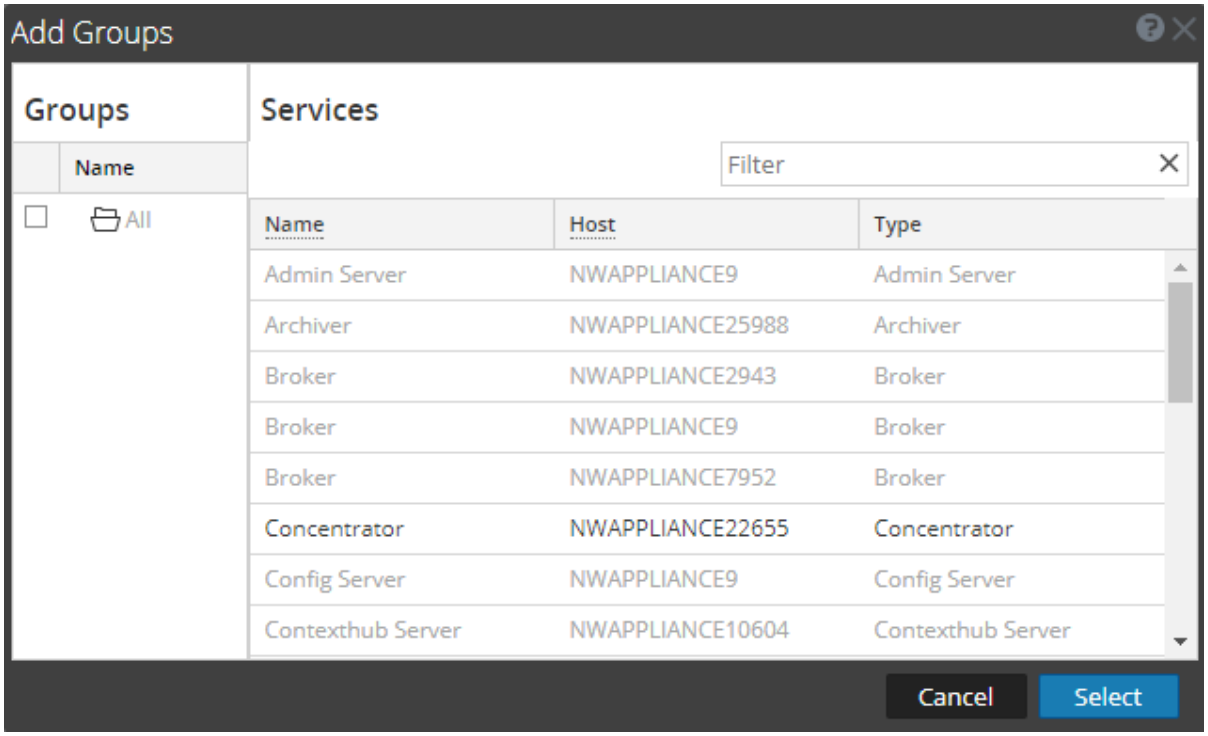
1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Policy-Ansicht wird angezeigt.
3. Wählen Sie eine Richtlinie (z. B. **Erste Richtlinie**) unter einem Host oder Service aus.

   Der Bereich „Policy-Details“ wird angezeigt.
4. Klicken Sie in der Symbolleiste der Liste „Services und Gruppen“ auf .
5. Wählen Sie eine der folgenden Aktionen aus:

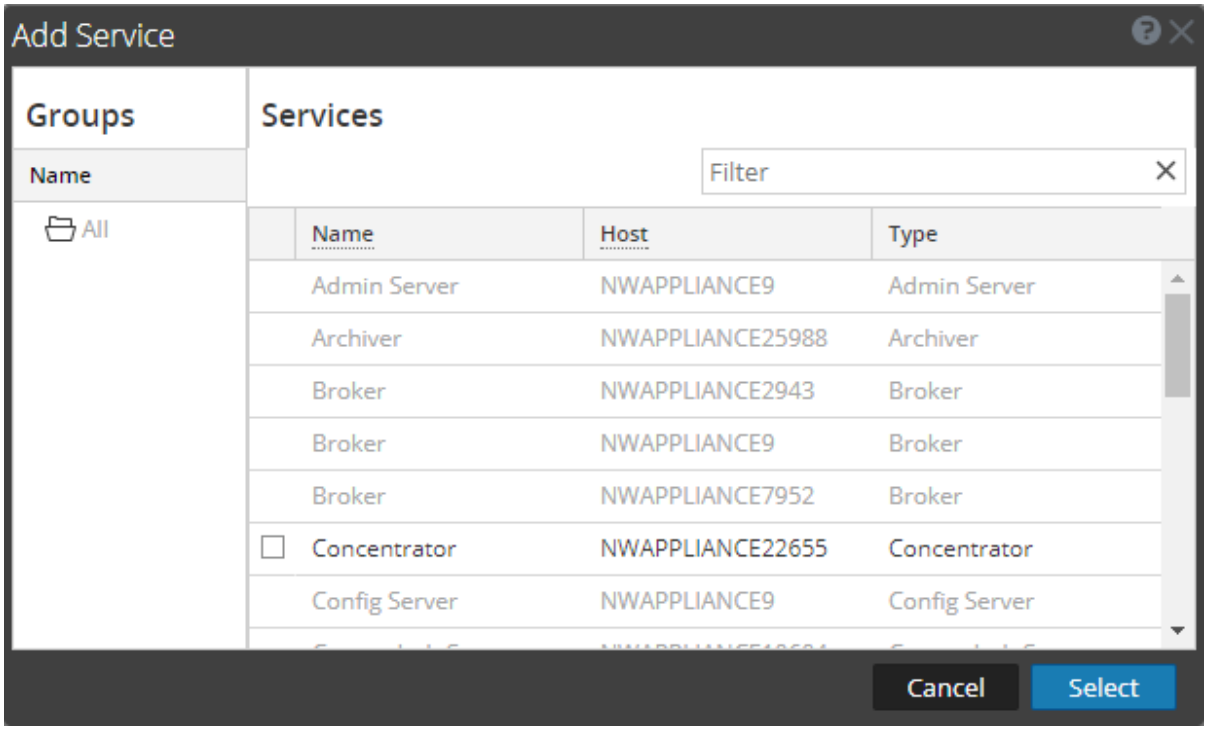
- Für Hosts wählen Sie im Auswahlmenü **Gruppen** oder **Hosts** aus.
- Für Services wählen Sie im Auswahlmenü **Gruppen** oder **Services** aus.

6. Je nachdem, ob Sie Services oder Gruppen zuweisen möchten, führen Sie eine der folgenden Aktionen aus:
   - **Gruppen**: Es wird das Dialogfeld **Gruppen** angezeigt. Hier können Sie vordefinierte Gruppen von Hosts oder Services auswählen.



   - **Services**: Es wird das Dialogfeld **Services** angezeigt. Hier können Sie einzelne Services

auswählen.



7. Aktivieren Sie das Kontrollkästchen neben den Gruppen oder Services, die Sie der Richtlinie zuweisen möchten, klicken Sie im Dialogfeld auf **Auswählen** und dann im Bereich „Richtliniendetails“ auf **Speichern**.

Hinweis: Die Services werden basierend auf dem Policy-Typ für die Auswahl gefiltert. Beispiel: Für eine Richtlinie vom Typ „Concentrator“ können Sie nur Concentrator-Services auswählen.

Entfernen von Services oder Gruppen

So entfernen Sie einen Host oder Service aus einer Richtlinie:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Ansicht Policys wird angezeigt.
3. Wählen Sie eine Richtlinie unter einem Service aus.

   Der Bereich „Policy-Details“ wird angezeigt.
4. Wählen Sie einen Host oder Service aus.

5. Klicken Sie auf − .

   Der Host oder Service wird aus der Policy entfernt.

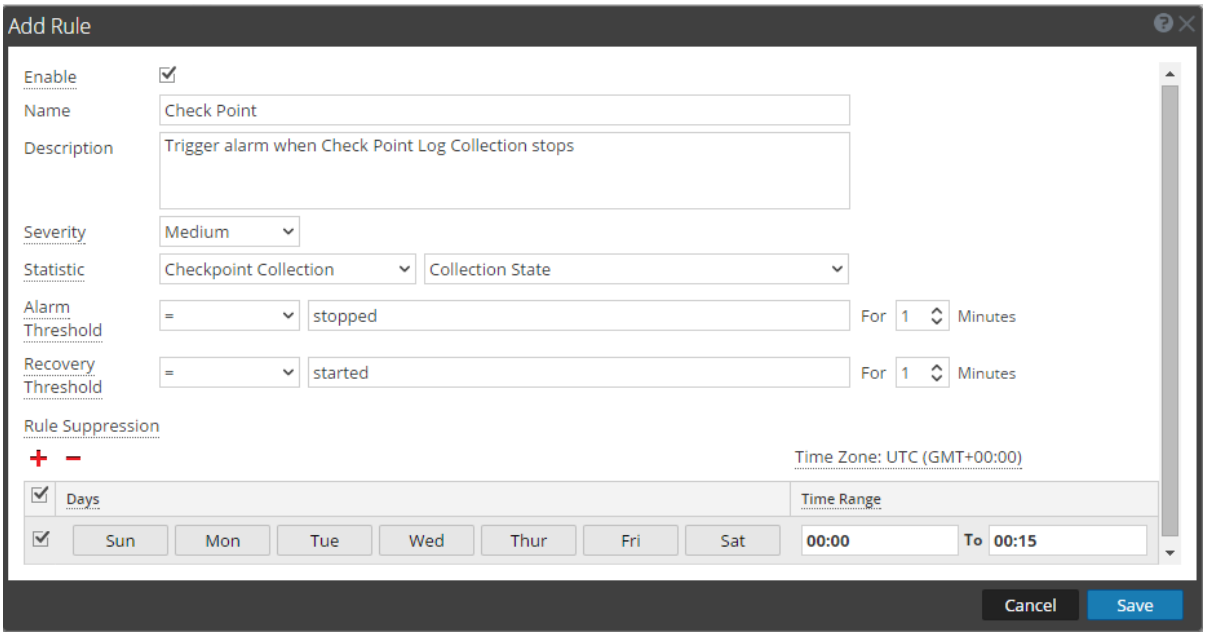
Hinzufügen oder Bearbeiten einer Regel

So fügen Sie einer Richtlinie eine Regel hinzu:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Policy-Ansicht wird angezeigt.
3. Wählen Sie eine Richtlinie (z. B. **Kontrollpunkt**) unter einem Host oder Service aus.

   Der Bereich „Policy-Details“ wird angezeigt.
4. Je nachdem, ob Sie eine vorhandene Regel hinzufügen oder eine Regel bearbeiten möchten, führen Sie einen der folgenden Schritte aus:
   - Zum Hinzufügen klicken Sie in der Symbolleiste der Liste „Regeln“ auf +.
   - Zum Bearbeiten wählen Sie in der Liste „Regeln“ eine Regel aus und klicken Sie auf .
5. Bearbeiten Sie das Dialogfeld, um die Regel zu definieren oder zu aktualisieren.
6. Fügen Sie das Feld **Beschreibung** hinzu, wie im folgenden Beispiel gezeigt.



7. Klicken Sie auf **OK**.

   Die Regel wird zur Policy hinzugefügt (oder aktualisiert).

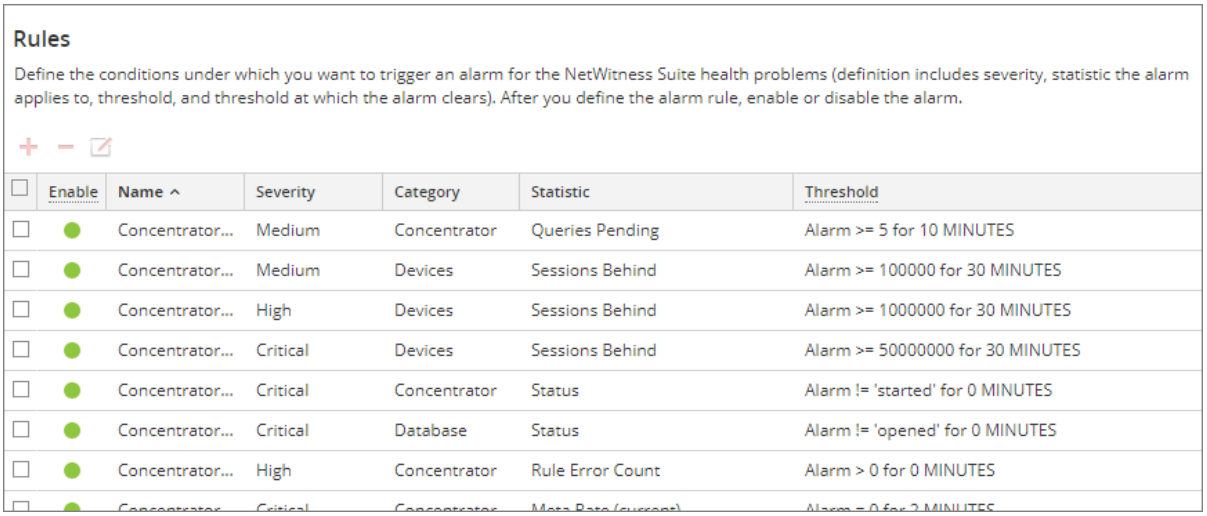
Ein- oder Ausblenden der Regelbedingungsspalten

So blenden Sie Regelbedingungsspalten im Bereich „Regeln“ ein oder aus:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Ansicht Policys wird angezeigt.
3. Wählen Sie eine Richtlinie unter einem Service aus.

   Der Bereich Richtliniendetails wird angezeigt.
4. Navigieren Sie zum Bereich **Regeln**.



5. Klicken Sie auf **v** rechts neben **Kategorie**, wählen Sie **Spalten** aus und deaktivieren Sie die Regelbedingungen **Statisch** und **Schwellenwert**.

   Sie können jede Regelspalte aktivieren oder deaktivieren, um sie ein- bzw. auszublenden. Der Bereich **Regeln** wird ohne die Regelbedingungen angezeigt.

Löschen einer Regel

So entfernen Sie einen Host oder Service aus einer Richtlinie:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Policys**.

   Die Policy-Ansicht wird angezeigt.
3. Wählen Sie eine Policy unter einem Service aus.

   Der Bereich „Policy-Details“ wird angezeigt.
4. Wählen Sie eine Regel in der Liste **Regeln** aus (z. B. **Kontrollpunkt**).

5. Klicken Sie auf .
   Die Regel wird aus der Policy entfernt.

Unterdrücken einer Regel

1. Klicken Sie auf die Registerkarte **Policys**.
   Die Policy-Ansicht wird angezeigt.
2. Wählen Sie eine Policy unter einem Service aus.
   Der Bereich „Policy-Details“ wird angezeigt. Sie können Zeiträume für die Regelunterdrückung beim erstmaligen Hinzufügen der Regel festlegen oder die Regel bearbeiten und Zeiträume für die Unterdrückung festlegen.
3. Hinzufügen oder Bearbeiten einer Regel
4. Legen Sie im Bereich **Regelunterdrückung** im Dialogfeld **Regel hinzufügen** oder **Regel bearbeiten** die Tage und Zeiträume fest, für die die Regel unterdrückt werden soll.

Unterdrücken einer Richtlinie

1. Fügen Sie eine Policy hinzu oder bearbeiten Sie diese.
   Die Policy-Ansicht wird angezeigt.
2. Im Bereich **Richtlinienunterdrückung**:
   a. Wählen Sie in der Drop-down-Liste **Zeitzone** eine Zeitzone aus.
      Diese Zeitzone gilt für die gesamte Richtlinie (sowohl Richtlinienunterdrückung als auch Regelunterdrückung).
   b. Klicken Sie in der Symbolleiste auf  .
   c. Legen Sie die Tage und Zeiträume fest, für die die Richtlinie unterdrückt werden soll.

Hinzufügen einer E-Mail-Benachrichtigung

So fügen Sie eine E-Mail-Benachrichtigung zu einer Richtlinie hinzu:

1. Fügen Sie eine Policy hinzu oder bearbeiten Sie diese.
   Die Policy-Ansicht wird angezeigt.
2. Im Bereich **Benachrichtigung**:
   a. Klicken Sie in der Symbolleiste auf  .
      Eine leere E-Mail-Benachrichtigungszeile wird angezeigt.

b. Wählen Sie die E-Mail aus:

- Benachrichtigungstypen in der Spalte „Empfänger“ (weitere Informationen über die Quelle der Werte in dieser Drop-down-Liste finden Sie unter **Konfigurieren von Benachrichtigungstypen** im *NetWitness SuiteSystemkonfigurationsleitfaden*).
- Benachrichtigungsserver in der Spalte „Benachrichtigungsserver“ (weitere Informationen über die Quelle der Werte in dieser Drop-down-Liste finden Sie unter **Konfigurieren von Benachrichtigungsservern** im *NetWitness SuiteSystemkonfigurationsleitfaden*).
- Vorlagenserver in der Spalte „Vorlage“ (weitere Informationen über die Quelle der Werte in dieser Drop-down-Liste finden Sie unter **Konfigurieren von Benachrichtigungsvorlagen** im *NetWitness SuiteSystemkonfigurationsleitfaden*).

> **Hinweis:** Wenn Sie in Ihren E-Mail-Benachrichtigungen zu Integrität und Zustand für die angegebenen Empfänger die Standardbetreffzeile aus der Vorlage „Integrität und Zustand“ verwenden möchten, lesen Sie die Informationen unter **Einbeziehen der Standardbetreffzeile für E-Mails**.

Löschen einer E-Mail-Benachrichtigung

So fügen Sie eine E-Mail-Benachrichtigung zu einer Richtlinie hinzu:

1. Fügen Sie eine Policy hinzu oder bearbeiten Sie diese.
   Die Policy-Ansicht wird angezeigt.
2. Im Bereich **Benachrichtigung**:
   a. Wählen Sie eine E-Mail-Benachrichtigung aus.
   b. Klicken Sie auf .
   Die Benachrichtigung wurde entfernt.

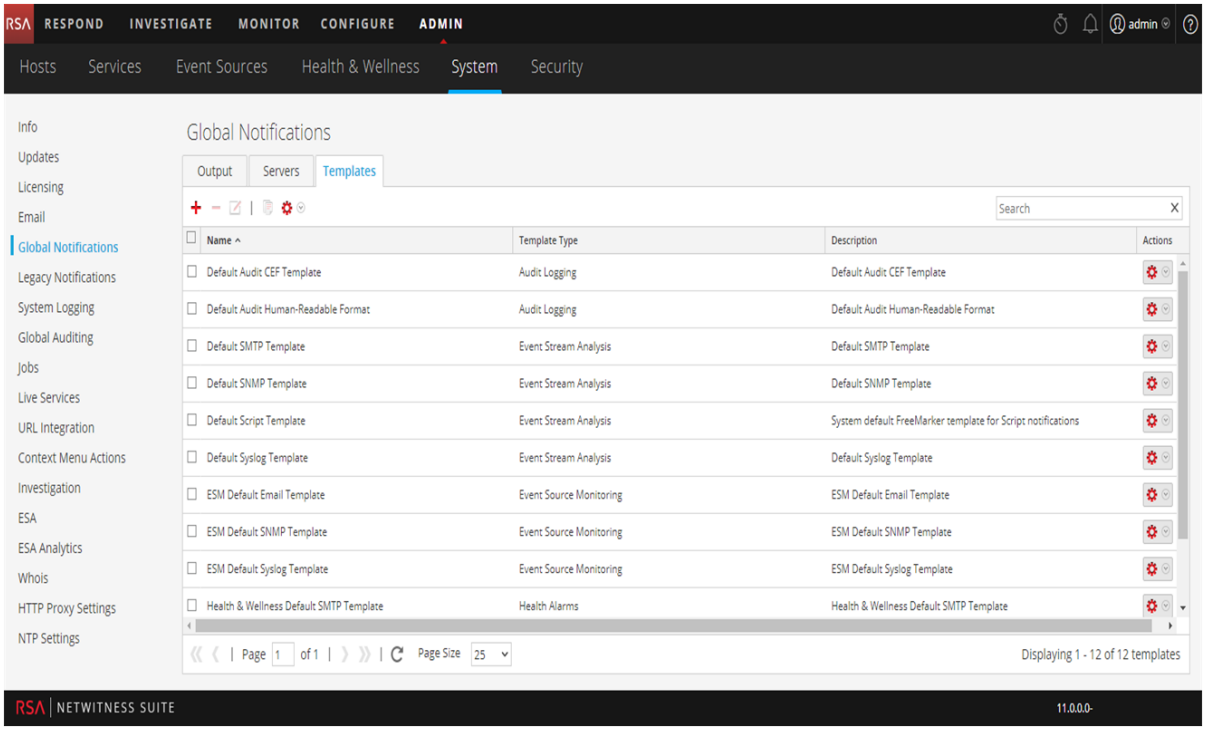
Einbeziehen der Standardbetreffzeile für E-Mails

Die durch von Ihnen für Richtlinien eingerichtete Benachrichtigungen erzeugten E-Mails enthalten nicht die Betreffzeile aus den E-Mail-Benachrichtigungsvorlagen in Integrität und Zustand. Sie müssen die Betreffzeile in den auskommentierten Betreffzeilen konfigurieren. Dieses Verfahren zeigt, wie Sie eine Betreffzeile in die Vorlagen einfügen.

Die zugehörigen Referenzthemen finden Sie unter Ansicht „Richtlinien“ und Vordefinierte Richtlinien für NetWitness Suite.

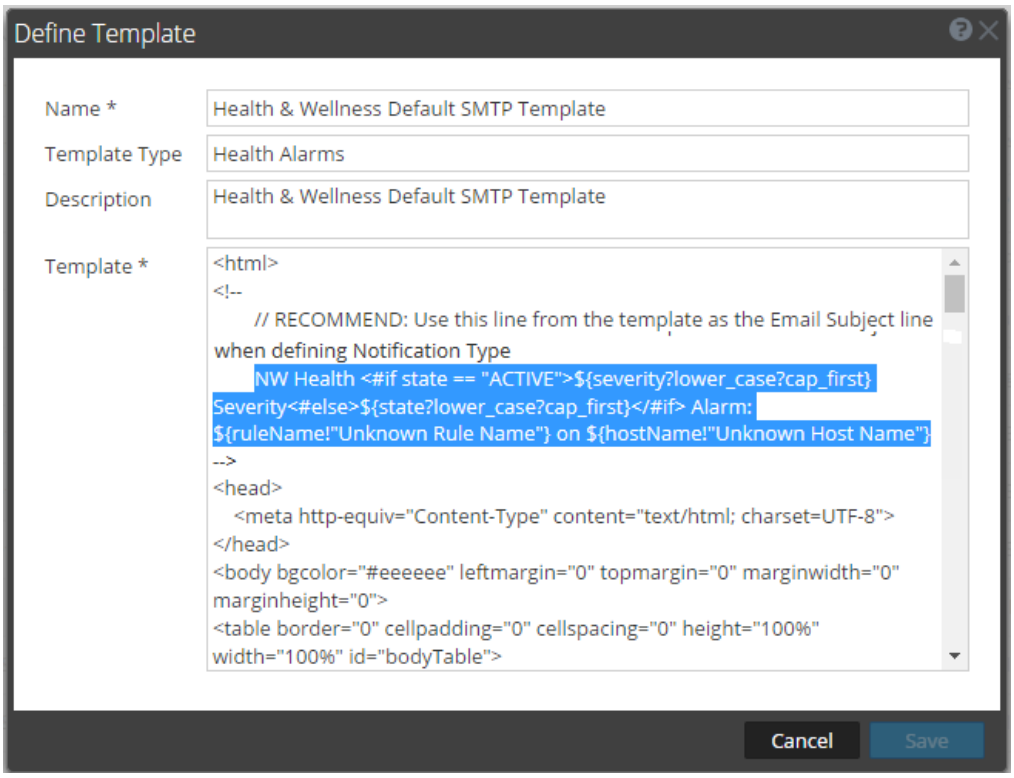
So beziehen Sie die Betreffzeile einer E-Mail-Vorlage aus Integrität und Zustand in Ihre E-Mail-Benachrichtigung ein:

1. Navigieren Sie zu **ADMINISTRATION > System**.
2. Wählen Sie im Optionsbereich **Globale Benachrichtigungen** aus.
3. Wählen Sie eine E-Mail-Vorlage aus Integrität und Zustand (z. B. **SMTP-Standardvorlage für Integrität und Zustand**) aus.



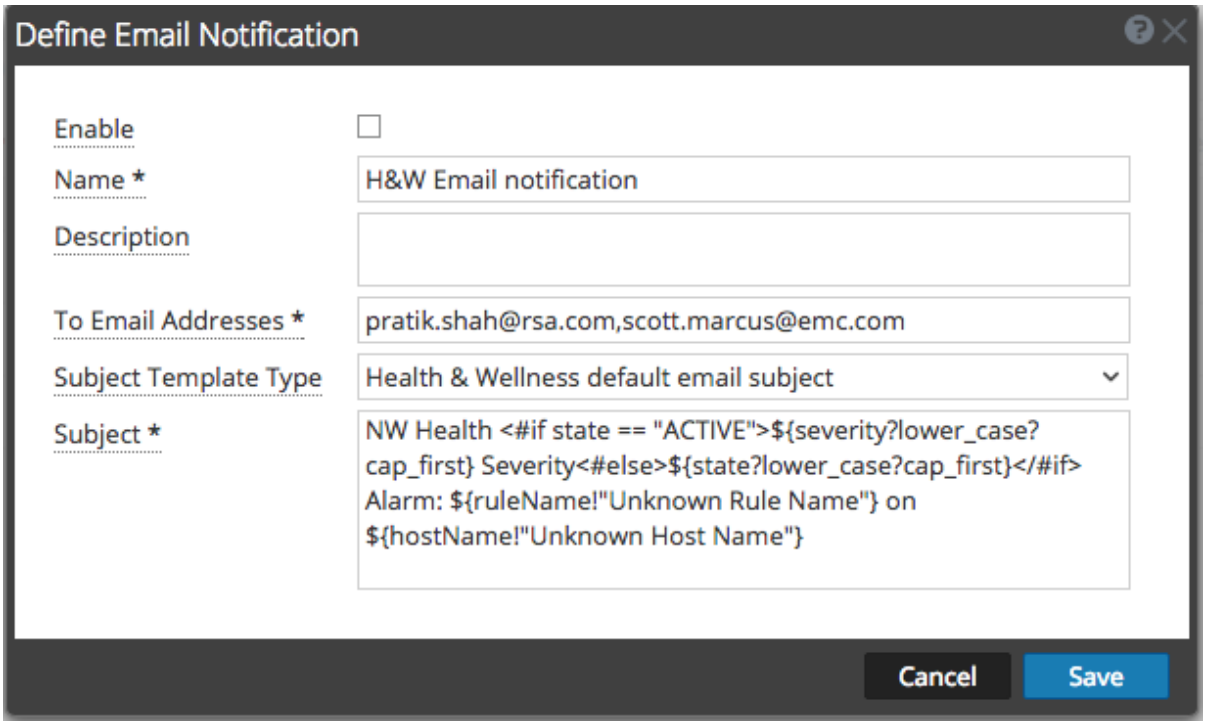
Das Dialogfeld „Vorlage definieren“ wird angezeigt.

4. Klicken Sie auf  und kopieren Sie dann im Feld **Vorlage** die Betreffzeile in die Zwischenablage (markieren Sie die Betreffzeile und drücken Sie Strg+C).



5. Klicken Sie auf **Abbrechen**, um die Vorlage zu schließen.
6. Klicken Sie auf die Registerkarte **Ausgabe** und wählen Sie eine Benachrichtigung aus (z. B. **Integrität und Zustand**).
7. Klicken Sie auf .

   Das Dialogfeld **E-Mail-Benachrichtigung definieren** wird angezeigt.
8. Ersetzen Sie den Wert im Textfeld **Betreff** durch die Betreffzeile in der Zwischenablage (markieren Sie den vorhandenen Text und drücken Sie Strg+V).



9. Klicken Sie auf **Speichern**.

Systemstatistik überwachen

Der Systemstatistikbrowser filtert Statistiken nach dem ausgewählten Host, der auf dem Host ausgeführten Komponente, der statistischen Kategorie, der individuellen Statistik oder einer beliebigen Kombination aus Host, Komponente, Kategorie und Statistik. Sie können auch die Reihenfolge auswählen, in der diese Informationen angezeigt werden.

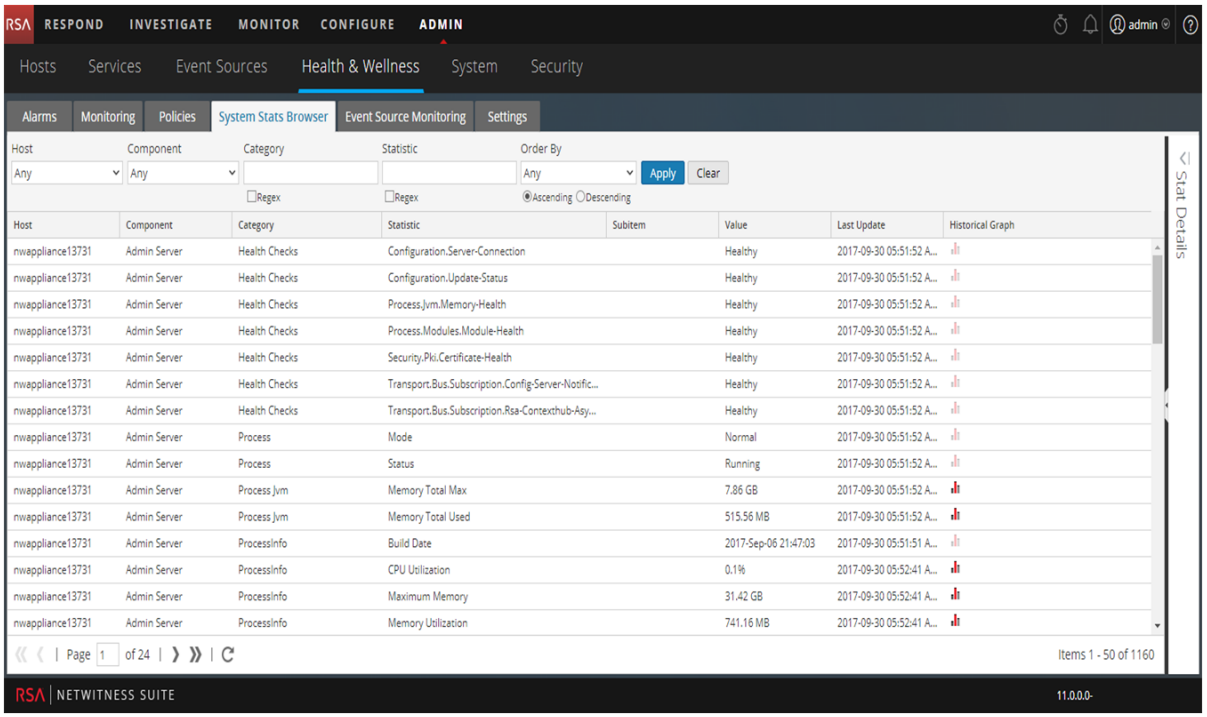
So greifen Sie auf die Ansicht „Systemstatistikbrowser“ zu:

1. Navigieren Sie zu **ADMINISTRATION** > **Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.

2. Klicken Sie auf die Registerkarte **Systemstatistikbrowser**.

Die Registerkarte Systemstatistikbrowser wird angezeigt.



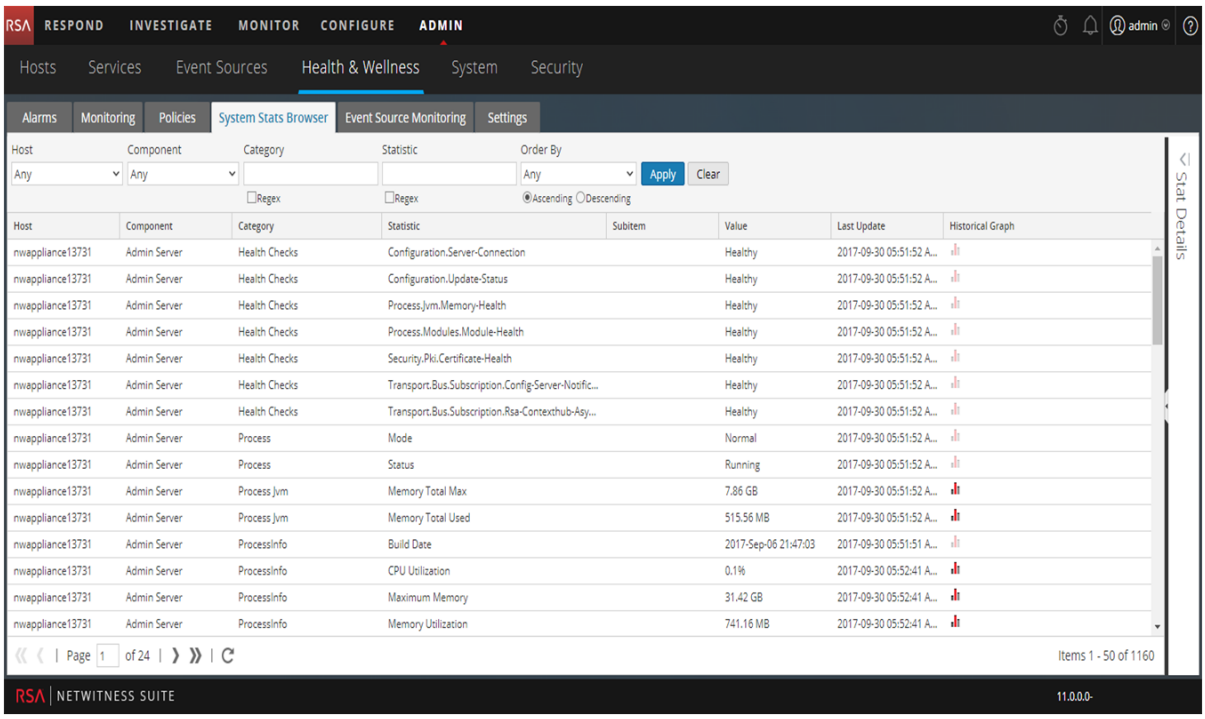
Filtersystemstatistiken

Sie können die Systemstatistiken zur Überwachung auf eine der folgenden Arten filtern:

- Statistiken, die für einen bestimmten Host gesammelt wurden
- Statistiken, die für eine bestimmte Komponente gesammelt wurden
- Statistiken, die zu einem bestimmten Typ gesammelt wurden oder die zu einer bestimmten Kategorie gehören
- Statistiken, die geordnet anhand der gewählten Auswahl aufgelistet wurden

So filtern Sie die Liste der Systemstatistiken:

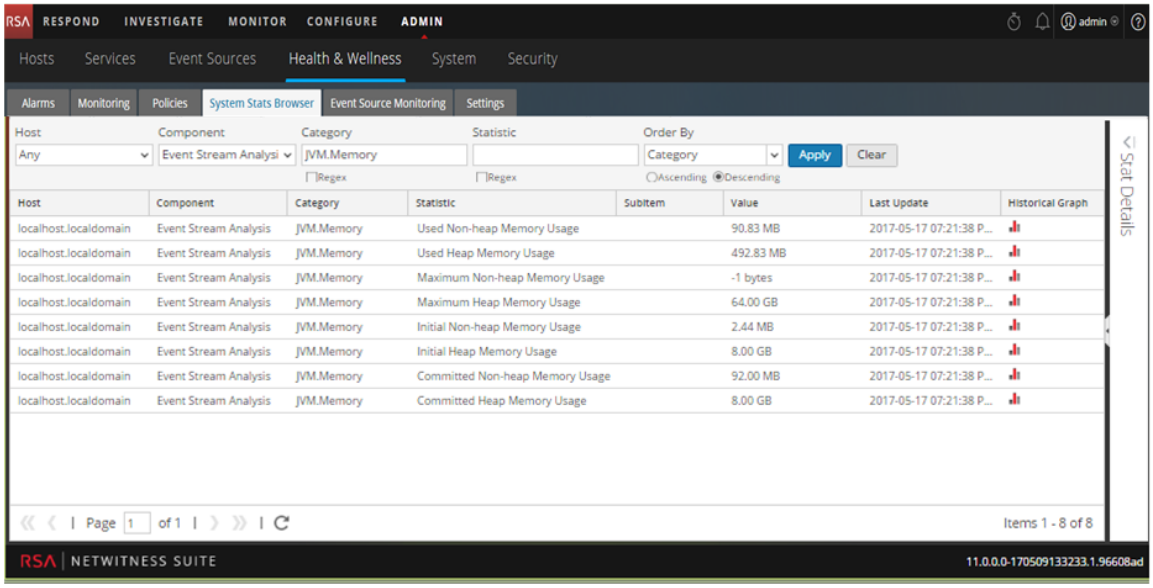
1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Klicken Sie auf **Systemstatistikbrowser**.
   Die Registerkarte „Systemstatistikbrowser“ wird angezeigt.



Filtern Sie die Liste der Systemstatistiken auf eine der folgenden Arten:

- Zur Anzeige der Systemstatistiken eines bestimmten Hosts wählen Sie den Host in der Drop-down-Liste **Host** aus.
  Die Systemstatistiken für den ausgewählten Host werden angezeigt.
- Zur Anzeige der Systemstatistiken einer bestimmten Komponente wählen Sie die Komponente in der Drop-down-Liste **Komponente** aus.
  Die Systemstatistiken für die ausgewählte Komponente werden angezeigt.
- Zur Anzeige der Systemstatistiken einer bestimmten Kategorie geben Sie den Kategorienamen im Feld **Kategorie** ein.
  Wählen Sie **Regex** aus, um den Regex-Filter zu aktivieren. Der Text wird nach einem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Wenn Regex nicht ausgewählt wurde, ist der Musterabgleich mit einfachen Platzhaltern möglich.
  Die Systemstatistiken für die ausgewählte Kategorie werden angezeigt.
- Zur Anordnung der Liste der Statistiken in einer bestimmten Reihenfolge können Sie die Reihenfolge in der Spalte **Sortieren nach** festlegen.
- Zur Anzeige einer bestimmten Statistik für mehrere Hosts geben Sie den Statistiknamen im Feld **Statistik** ein.
  Wählen Sie **Regex** aus, um den Regex-Filter zu aktivieren. Der Text wird nach einem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Wenn Regex nicht ausgewählt wurde, ist der Musterabgleich mit einfachen Platzhaltern möglich.
  Die Systemstatistiken für die ausgewählte Statistik werden angezeigt.

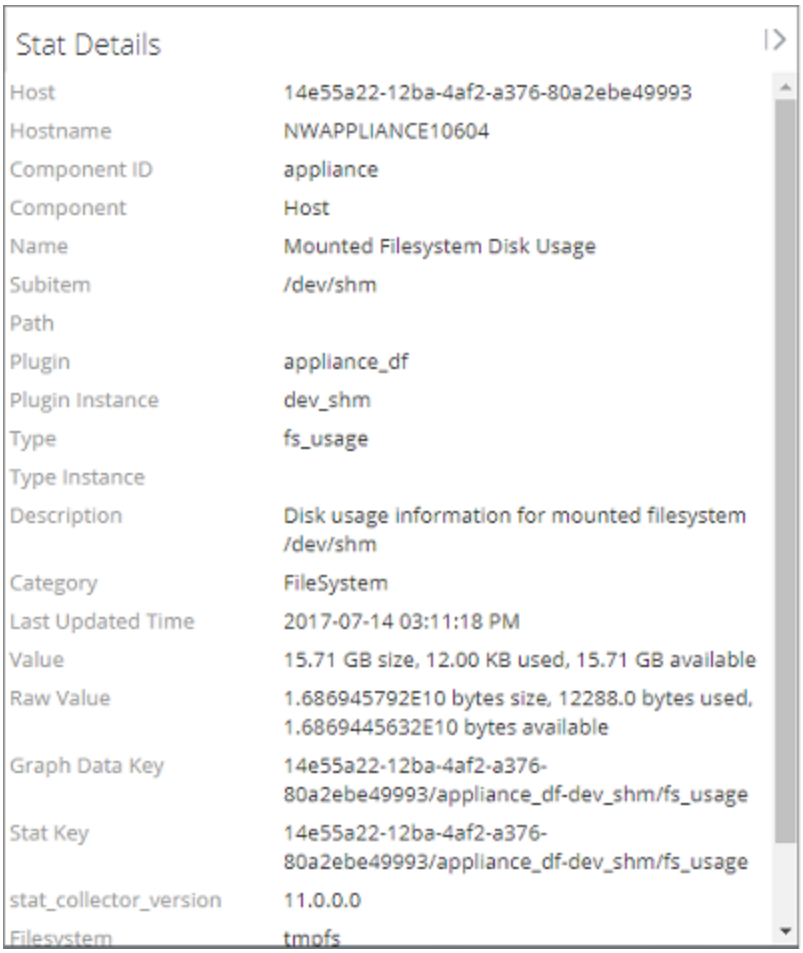
Die folgende Abbildung zeigt den Systemstatistikbrowser gefiltert nach dem NWAPPLIANCE10604-Host. Die Einträge sind in absteigender Reihenfolge nach der statistischen Kategorie sortiert.



3. So zeigen Sie Details zu einer individuellen Statistik an:

   a. Wählen Sie zum Auswählen einer Statistik eine Zeile aus.

   b. Klicken Sie auf <|.
   Der Bereich „Statistikdetails“ wird angezeigt.



Weitere Informationen über die verschiedenen Parameter in der Ansicht **ADMINISTRATION** > **Integrität und Zustand** > **Systemstatistikbrowser** finden Sie unter Ansicht „Systemstatistikbrowser“.

Anzeigen eines Verlaufsdiagramms für Systemstatistiken

Das Verlaufsdiagramm der erfassten Systemstatistiken liefert Informationen über die Statistikentwicklung in einem ausgewählten Zeitbereich.

So zeigen Sie ein Verlaufsdiagramm an:

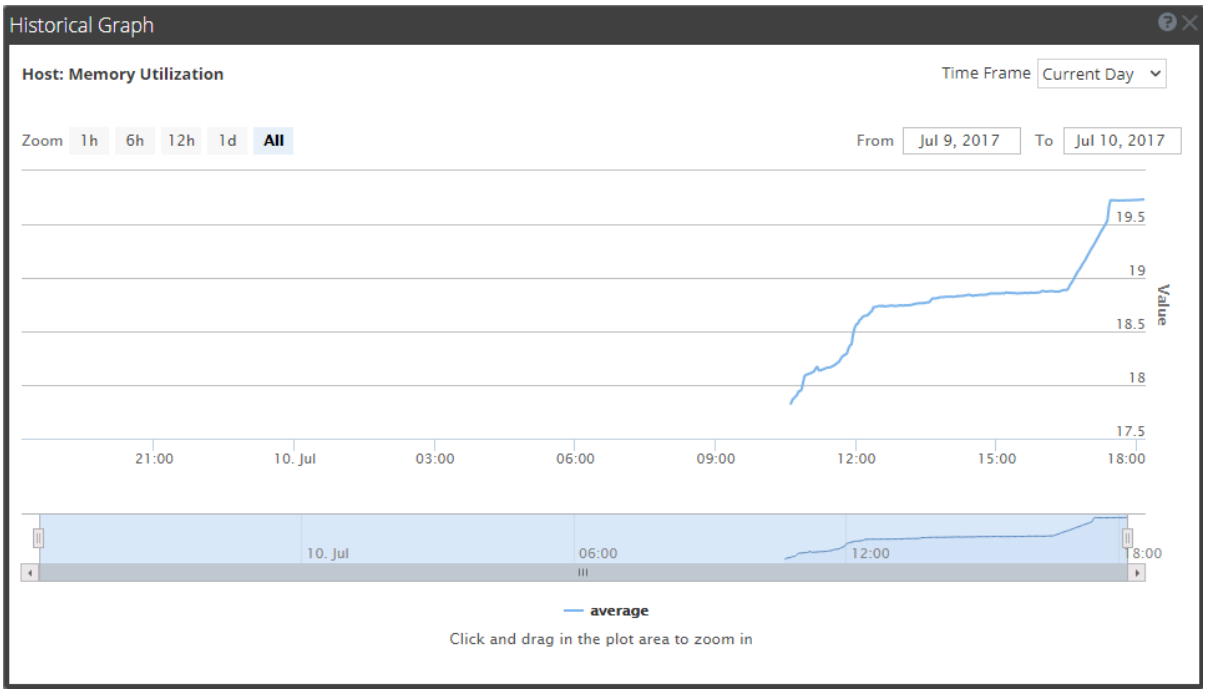
1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.

2. Klicken Sie auf die Registerkarte **Systemstatistikbrowser**.
3. Geben Sie auf der Registerkarte „Systemstatistikbrowser“ die Filterkriterien an, um die gewünschten Statistiken anzuzeigen.
4. Wählen Sie in der Spalte **Verlaufsdiagramm** aus.

Das Verlaufsdiagramm für die ausgewählte Statistik wird angezeigt.

In der Abbildung unten ist ein Beispiel für ein Verlaufsdiagramm zur Arbeitsspeicherauslastung eines Hosts zu sehen.



Die angepasste grafische Ansicht gibt die für den heutigen Tag erfassten Statistiken wieder, wobei die Werte für eine Stunde angezeigt werden (10:15 bis 11:15 Uhr). Bewegen Sie den Mauszeiger über das Diagramm, um die Details zu einem bestimmten Zeitpunkt anzuzeigen. In der Abbildung wird z. B. die Arbeitsspeicherauslastung um 11:00 Uhr angezeigt.

Hinweis: Sie können die Grafikansicht anpassen, indem Sie den Zeitrahmen und den Datumsbereich auswählen. Sie können vergrößern mithilfe des Vergrößerungswerts, des Zeitfensters oder indem Sie einfach in den Zeichenbereich klicken und ziehen. Weitere Informationen über die Parameter für die Anpassungs- und Zoomfunktionen finden Sie unter Verlaufsdiagramm für Systemstatistiken. Eine Unterbrechung oder Lücke in einer Diagrammlinie weist darauf hin, dass der Service oder Host zu diesem Zeitpunkt nicht verfügbar war.

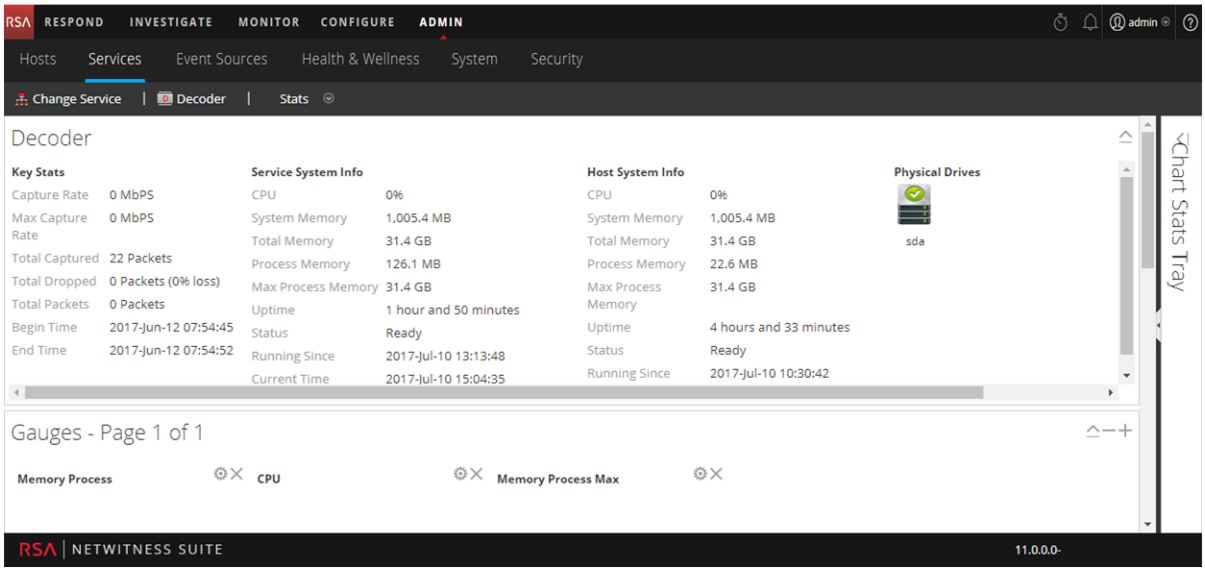
Überwachen von Servicestatistiken

NetWitness Suite bietet die Möglichkeit, den Servicestatus und Serviceaktivitäten zu überwachen. In der Ansicht Services-Statistik werden wichtige Statistiken, Servicesysteminformationen und Hostsysteminformationen zu einem Gerät angezeigt. Außerdem stehen mehr als 80 Statistiken zur Verfügung, die in Messdiagrammen und Zeitplandiagrammen angezeigt werden können. Nur Statistiken für Sitzungsgröße, Sitzungen und Pakete sind in Verlaufs-Zeitachsendiagrammen sichtbar.

Je nach Servicetyp stehen zwar verschiedene Statistiken zur Verfügung, bestimmte Elemente gelten jedoch für alle Core-Geräte.

So überwachen Sie Servicestatistiken in NetWitness Suite:

1. Navigieren Sie zu **ADMINISTRATION > Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie einen Service aus und klicken Sie dann in der Spalte „Aktionen“ auf **Ansicht > Statistiken**.



3. So passen Sie die Ansicht an: Sie können Diagramme einblenden oder ausblenden; rufen Sie die Diagrammstatistikbereich auf, um alle verfügbaren Diagramme zu sehen. Sie können einen Abschnitt nach oben oder unten ziehen, um die Reihenfolge zu ändern. Ziehen Sie z. B. den Abschnitt Messdiagramme nach oben, sodass er sich über dem Abschnitt Zusammenfassungsstatistik befindet.

Hinzufügen von Statistiken zu einem Messdiagramm oder einem Diagramm

In der Ansicht Gerätestatistiken können Sie die überwachten Statistiken für einzelne Geräte anpassen. Die Diagrammstatistikbereich listet alle verfügbaren Statistiken für den Service auf. Die Anzahl an Statistiken variiert je nach überwachtem Servicetyp. Jede Statistik im Diagrammstatistikbereich kann in einem Messdiagramm oder in einem Zeitplandiagramm angezeigt werden. Nur Statistiken für Sitzungsgröße, Sitzungen und Pakete sind in Verlaufs-Zeitachsendiagrammen sichtbar.

Erstellen eines Messdiagramms für eine Statistik

So erstellen Sie ein Messdiagramm für eine Statistik in der Ansicht Servicestatistiken:

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

   Die Ansicht der Admin-Services wird angezeigt.

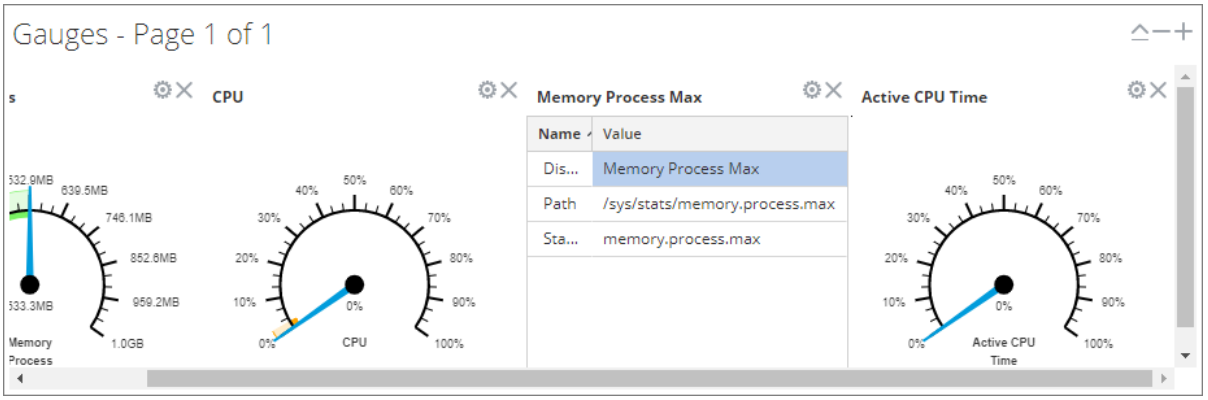
2. Wählen Sie einen Service und anschließend **Ansicht > Statistiken** in der Spalte „Aktionen“ aus.

   Rechts wird der Diagrammstatistikbereich angezeigt.

3. Wenn der Bereich ausgeblendet wird, klicken Sie auf , um die Liste der verfügbaren Statistiken anzuzeigen.

4. Klicken Sie im **Diagrammstatistikbereich** auf eine beliebige Statistik und ziehen Sie sie in den Abschnitt **Messdiagramme**.

   Ein Messdiagramm für die Statistik wird erstellt. Wenn nicht genug Platz für das Messdiagramm vorhanden ist, wird eine neue Seite im Abschnitt Messdiagramme erstellt und das Messdiagramm auf die neue Seite gesetzt. Im Beispiel wurde das Diagramm „Aktive CPU-Zeit“ aus dem Diagrammstatistikbereich gezogen und im Abschnitt „Messdiagramme“ hinzugefügt.

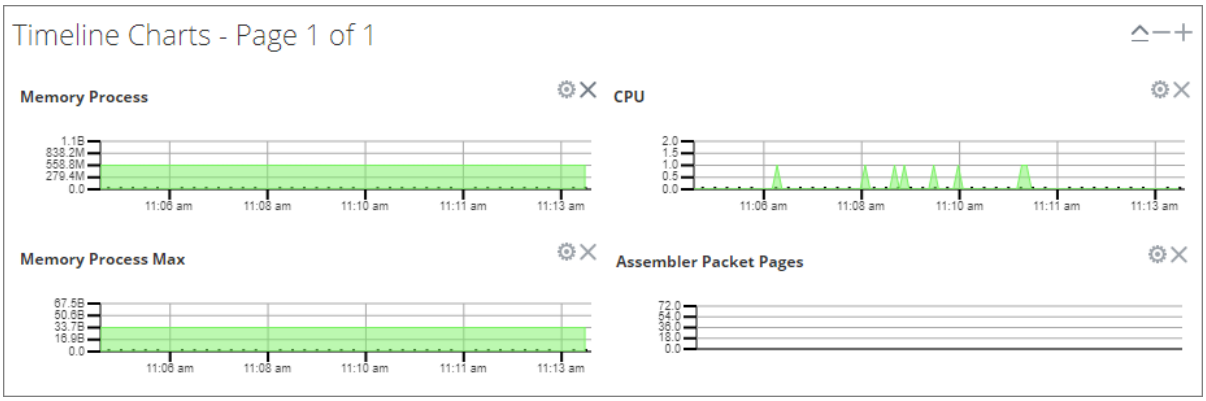


Erstellen eines Zeitplandiagramms für eine Statistik

So erstellen Sie einen Zeitplan für eine Statistik:

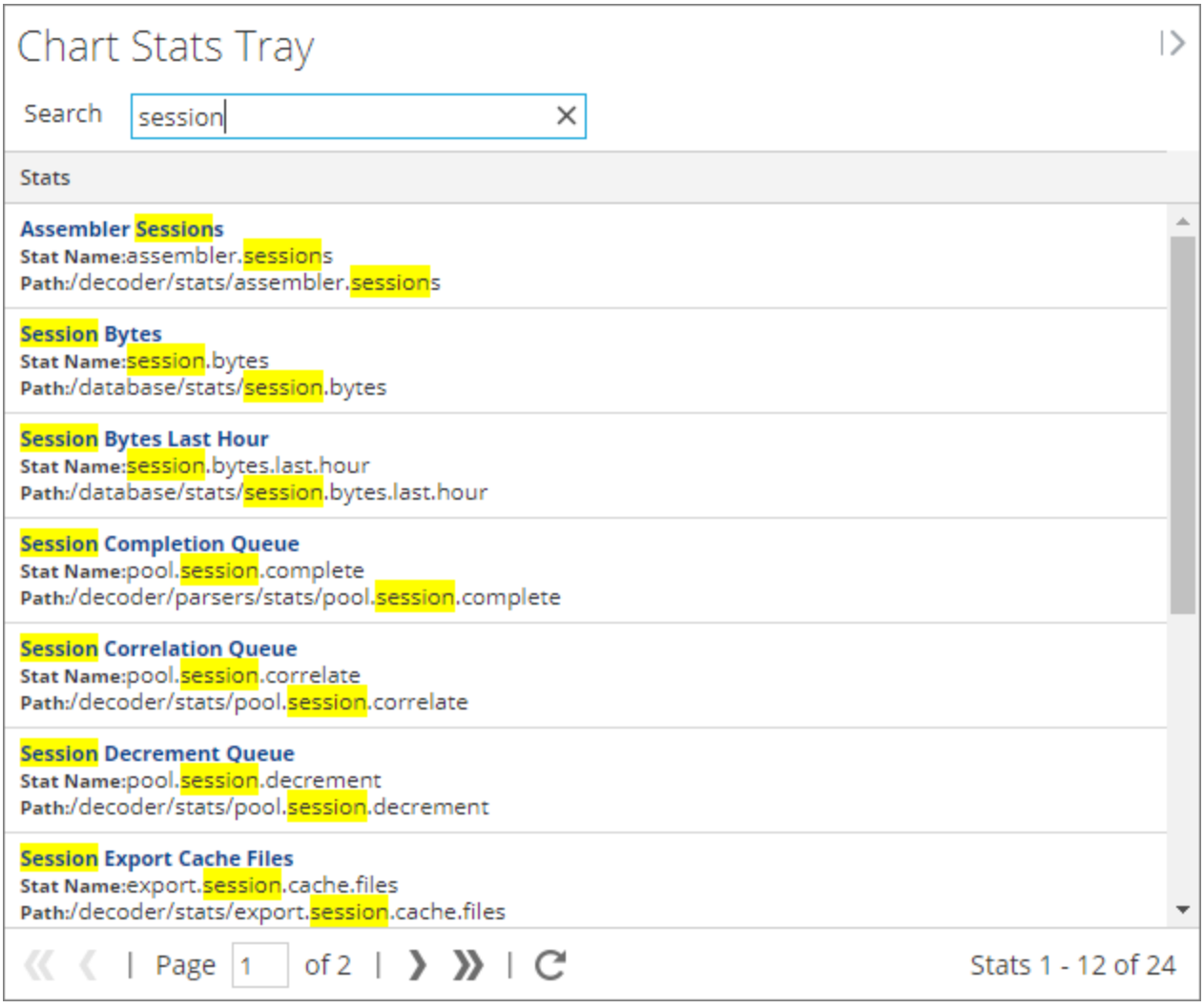
Klicken Sie im **Diagrammstatistikbereich** auf eine Statistik und ziehen Sie sie in den Abschnitt **Zeitachsendiagramm** oder **Verlaufs-Zeitachsendiagramm**.

Ein Zeitachsendiagramm wird für die Statistik erstellt. Wenn nicht genug Platz für das Diagramm vorhanden ist, wird eine neue Seite im Abschnitt „Zeitachsendiagramm“ erstellt und das Diagramm auf die neue Seite gesetzt. Im Beispiel wurde das Diagramm „Assembler-Paketseiten“ aus dem Bereich Zeitachsendiagramm gezogen und dem Diagrammstatistikbereich hinzugefügt.



Suchen nach einer Statistik im Diagrammstatistikbereich

Zur Suche nach einer Statistik geben Sie einen Suchbegriff, z. B. **Sitzung**, im Feld „Suchen“ ein und drücken Sie die **EINGABETASTE**. Passende Statistiken werden mit markiertem passenden Wort angezeigt.

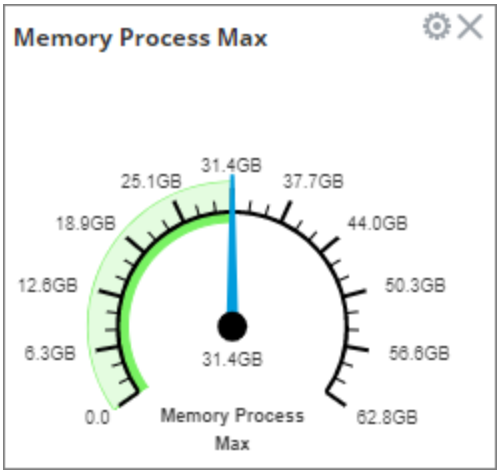


Bearbeiten der Eigenschaften von Statistik-Messdiagrammen

Der Abschnitt „Messdiagramme“ der Ansicht „Servicestatistik“ präsentiert Statistiken in Form eines analogen Rundinstruments. Die Eigenschaften jedes einzelnen Messdiagramms sind bearbeitbar; alle Messdiagramme haben einen bearbeitbaren Titel und einige verfügen über zusätzliche bearbeitbare Eigenschaften.

Bearbeiten der Eigenschaften von Messdiagrammen

1. Navigieren Sie zu **ADMINISTRATION > Services**.
   Die Ansicht der Administrationsservices wird angezeigt.
2. Wählen Sie einen Service aus und klicken Sie in der Spalte „Aktionen“ auf **Ansicht > Statistiken**.
   Die Servicestatistikansicht beinhaltet den Abschnitt „Messdiagramme“.
3. Gehen Sie zu dem Messdiagramm, dessen Eigenschaften Sie bearbeiten möchten (zum Beispiel **Speicherprozess**).



4. Klicken Sie auf das Eigenschaftssymbol ( ), um die Parameternamen und -werte anzuzeigen.
5. Doppelklicken Sie zur Hervorhebung des Werts im Feld **Angezeigter Name** auf den Wert, zum Beispiel **Speicherprozess**.

   Hinweis: Auf die anderen beiden Werte zu klicken, bewirkt nichts, weil die Eigenschaften im Messdiagramm nicht bearbeitbar sind.

6. Geben Sie einen neuen Wert für den angezeigten Namen ein und klicken Sie auf das **Eigenschaftssymbol** ( ).
   Der neue Titel ersetzt **Speicherprozess**.

Hinzufügen von Statistiken zum Abschnitt Messdiagramme

Sie können mehr Messdiagramme hinzufügen, indem Sie eine Statistik aus dem **Diagrammstatistikbereich** in den Abschnitt **Messdiagramme** ziehen.

1. Klicken Sie zum Erweitern des Diagrammstatistikbereichs auf <|.
2. Scrollen Sie nach unten und wählen Sie eine Statistik aus, zum Beispiel **Sitzungsrate (maximal)**.
3. Ziehen Sie die Statistik in den Abschnitt **Messdiagramme**.
   Das neue Messdiagramm wird im Abschnitt „Messdiagramme“ angezeigt.

Bearbeiten von Eigenschaften von Zeitachsendiagrammen

Zeitachsendiagramme zeigen Statistiken in einem laufenden Zeitplan an. Die Ansicht Servicestatistik umfasst zwei Zeitachsentypen: aktuelle Zeitachse und historische Zeitachse. Sie können jede beliebige verfügbare Statistik in den Diagrammstatistikbereich im Bereich „Zeitachsendiagramm“ ziehen und ablegen. Nur Statistiken für Sitzungsgröße, Sitzungen und Pakete sind in Verlaufs-Zeitachsendiagrammen sichtbar. Die Eigenschaften eines Zeitachsendiagramms lassen sich bearbeiten, ebenso wie die Titel aller Zeitachsendiagramme. Außerdem lassen sich bei einigen Zeitachsendiagrammen weitere Eigenschaften bearbeiten.

So greifen Sie auf die Diagramme zu:

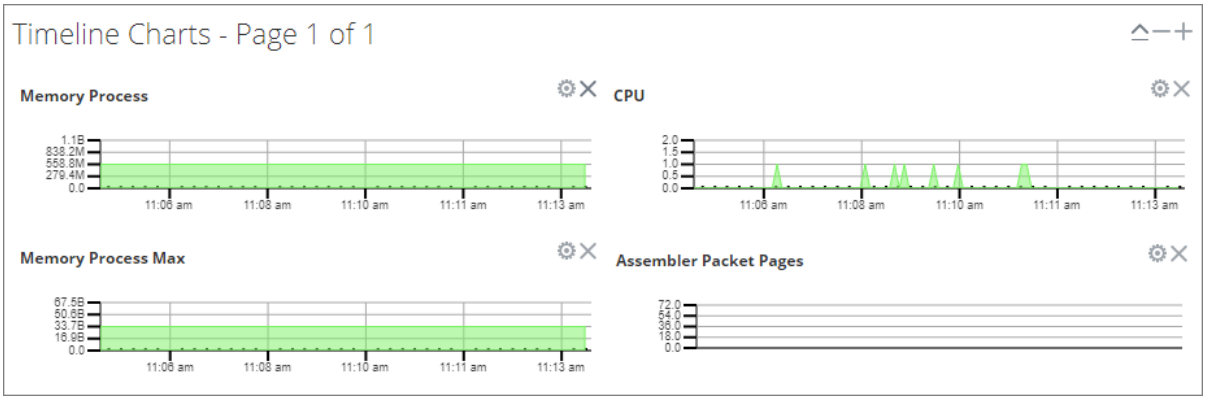
1. Navigieren Sie zu **ADMINISTRATION > Services**.
2. Wählen Sie einen Service aus und klicken Sie auf **Statistiken**.

   Die Ansicht Servicestatistik wird angezeigt. Die Diagramme befinden sich in dieser Ansicht.

Bearbeiten der Eigenschaften einer Zeitachse

So bearbeiten Sie die Eigenschaften eines Zeitachsendiagramms:

1. Gehen Sie zum Zeitachsendiagramm, für das Sie Eigenschaften bearbeiten möchten (zum Beispiel **Speicherprozess**).



2. Klicken Sie auf das **Eigenschaftssymbol** ( ), um die Parameternamen und -werte anzuzeigen.
3. Doppelklicken Sie auf einen Wert (zum Beispiel das Feld **Angezeigter Name**), damit dieser bearbeitet werden kann.

   Hinweis: Das Anklicken der anderen beiden Werte hat keine Funktion, da die Eigenschaften sich im Diagramm nicht bearbeiten lassen.

4. Geben Sie einen neuen Wert ein und klicken Sie auf das Symbol **Eigenschaften** ( ).

   Das Zeitachsendiagramm wird mit neuen Werten angezeigt.

Bearbeiten der Eigenschaften einer historischen Zeitachse

So bearbeiten Sie die Eigenschaften eines Verlaufs-Zeitachsendiagramms:

1. Wechseln Sie zu „Verlaufs-Zeitachsendiagramme“.
2. Klicken Sie auf das **Eigenschaftssymbol** ( ), um die Parameternamen und -werte anzuzeigen.
3. Klicken Sie auf einen Wert (zum Beispiel **27.01.2015** im Feld **Anfangsdatum**), damit dieser bearbeitet werden kann.
4. Geben Sie einen neuen Wert ein.
5. Bearbeiten Sie das **Enddatum** und den **Angezeigten Namen**, falls erforderlich.
6. Klicken Sie auf das **Eigenschaftssymbol** ( ).

   Die historische Zeitachse wird mit den neuen Werten angezeigt.

Hinweis: Wenn Sie die Eigenschaften des Verlaufs-Zeitachsendiagramms auf die Standardeinstellungen zurücksetzen möchten, damit die Werte dynamisch aktualisiert werden, entfernen Sie das Anfangs- und das Enddatum, platzieren Sie den Cursor in das Feld „Anfangsdatum“ und aktualisieren Sie Ihren Browser.

Hinzufügen von Statistiken zu Zeitachsendiagrammen

Sie können Zeitachsendiagramme hinzufügen, indem Sie eine Statistik aus dem Diagrammstatistikbereich in den Zeitachsenabschnitt ziehen.

1. Klicken Sie zum Erweitern des Diagrammstatistikbereichs auf .
2. Scrollen Sie nach unten und wählen Sie eine Statistik aus, zum Beispiel **Sitzungsrate (maximal)**.
3. Ziehen Sie die Statistik in den **Zeitachsenabschnitt**.

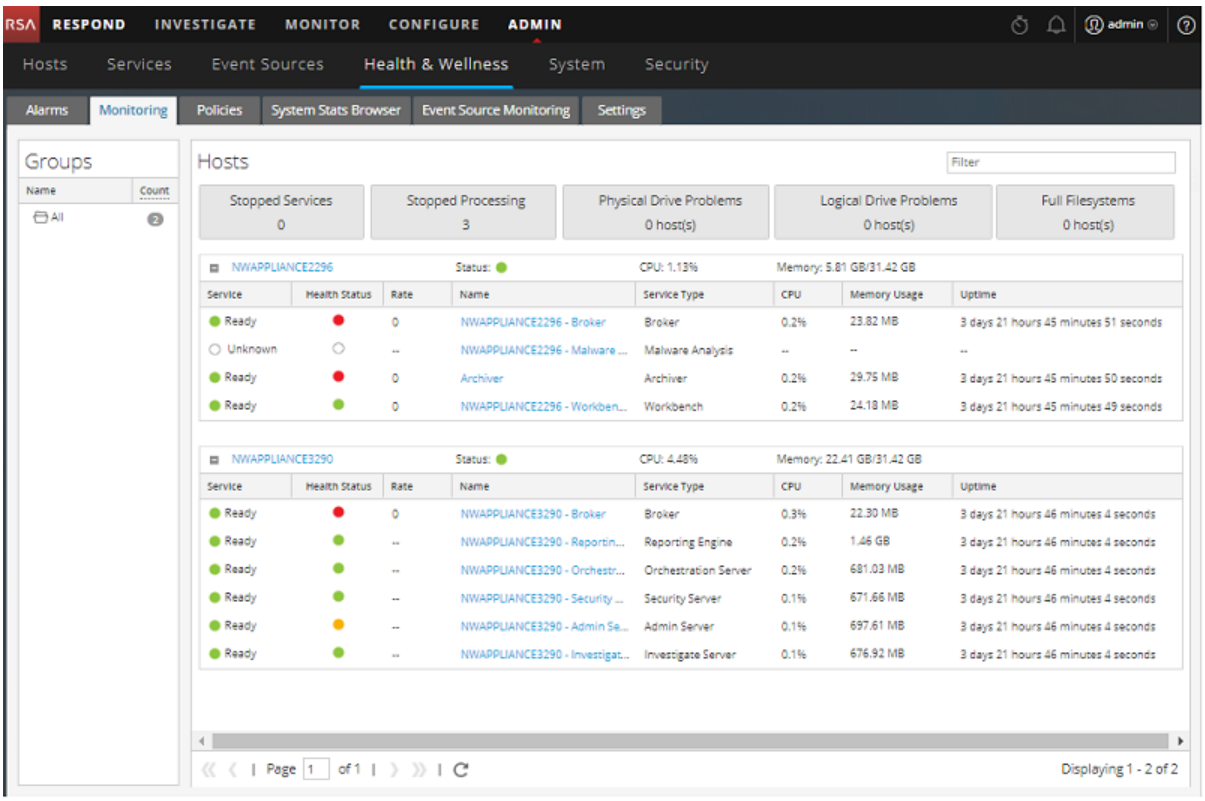
   Die neue Zeitachse wird im Zeitachsenabschnitt dargestellt.

Überwachen von Hosts und Services

NetWitness Suite bietet die Möglichkeit, den Status der installierten Hosts und Services zu überwachen. Sie können den aktuellen Zustand aller Hosts und der darauf ausgeführten Services, deren CPU-Auslastung und Speichernutzung sowie die Host- und Servicedetails anzeigen.

So überwachen Sie Hosts und Services in NetWitness Suite:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Wählen Sie die Registerkarte **Überwachen** aus.
   Standardmäßig wird eine Liste aller Hosts und der ihnen zugeordneten Services angezeigt, die zur Gruppe **Alle** gehören.
   Außerdem wird der Betriebszustand sowie die CPU- und Arbeitsspeichernutzung für jeden Host angegeben.



Klicken Sie links neben einem Host auf ⊞ (⊞ wird angezeigt, wenn Services auf einem Host installiert sind).

3. Es wird eine Liste der auf dem ausgewählten Host installierten Services angezeigt. Für jeden Service wird der Name, der Betriebszustand, die CPU- und Arbeitsspeichernutzung sowie die Ausführungsdauer angezeigt.

Filtern von Hosts und Services in der Überwachungsansicht

Sie können Hosts und Services in der Überwachungsansicht auf eine der folgenden Weisen filtern:

- Hosts, die zu einer bestimmten Gruppe gehören
- Ein bestimmter Host und die zugehörigen Services
- Hosts, dessen Services beendet sind
- Hosts, dessen Services die Verarbeitung beendet haben oder bei denen die Verarbeitung abgeschaltet wurde
- Hosts, bei denen Probleme mit dem physischen Laufwerk vorliegen
- Hosts, bei denen Probleme mit dem logischen Laufwerk vorliegen
- Hosts, die vollständige Dateisysteme haben

Weitere Informationen finden Sie unter Ansicht „Überwachung“.

So filtern Sie Hosts und Services:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird standardmäßig mit geöffneter Registerkarte „Alarme“ angezeigt.

2. Wählen Sie die Registerkarte **Überwachen** aus.
3. Filtern Sie die Hosts und Services auf eine der folgenden Arten:
   - Wenn Sie eine Liste der Hosts und der ihnen zugeordneten Services anzeigen möchten, die zu einer bestimmten Gruppe gehören, wählen Sie die Gruppe im Bereich Gruppen aus.

     Alle Hosts und die ihnen zugeordneten Services, die zur angegebenen Gruppe gehören, werden im Bereich „Hosts“ angezeigt.

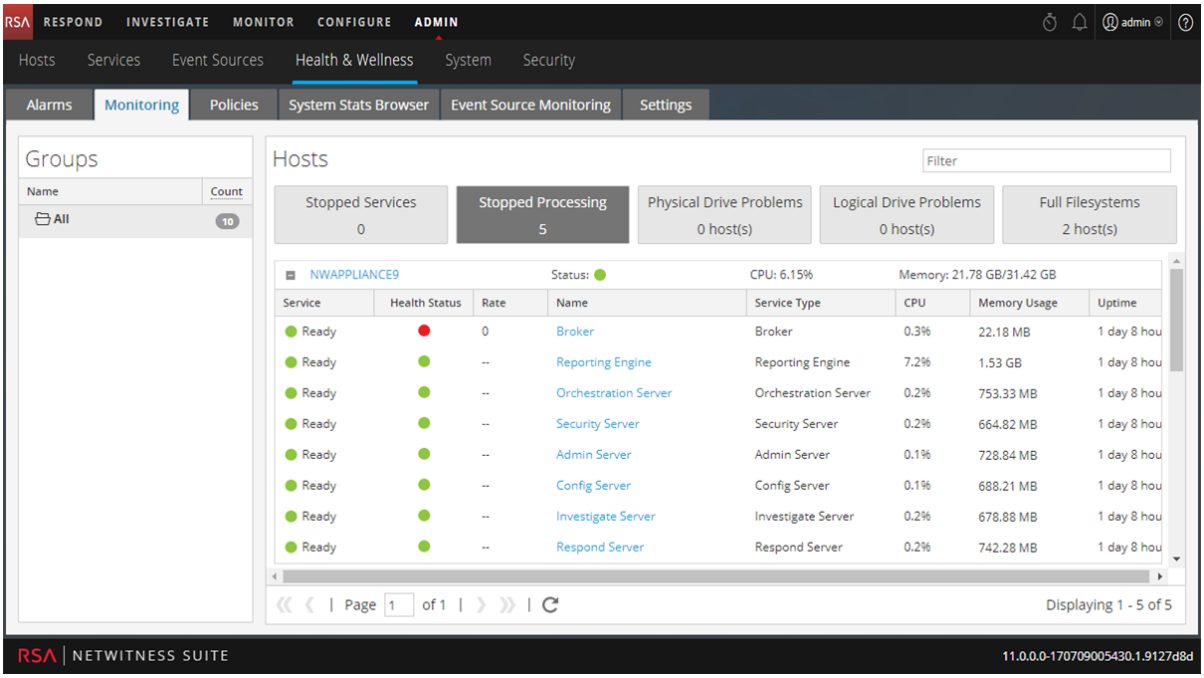
     Hinweis: Die Gruppierung der Hosts wird aus der Gruppe abgeleitet, die auf der Seite „Administration“ erstellt wurde. Alle Gruppen, die auf der Seite „Administration“ erstellt wurden, werden hier angezeigt.

     Beispiel: Wenn Sie die Gruppe **LC_Gruppe** im Bereich „Gruppen“ auswählen, wird eine Liste aller Hosts angezeigt, die zu dieser Gruppe gehören.

- Wenn Sie eine Liste aller Services anzeigen möchten, deren Verarbeitung beendet wurde, klicken Sie auf **Beendete Verarbeitung** im Bereich „Hosts“.

  Es wird eine Liste aller Hosts angezeigt, die mindestens einen Service mit dem Status „Beendete Verarbeitung“ haben.

  Hinweis: Die Schaltflächen oben zeigen die Systemstatistiken für alle in NetWitness Suite konfigurierten Hosts an und ändern sich nicht beim Anwenden von Filtern auf Gruppen.



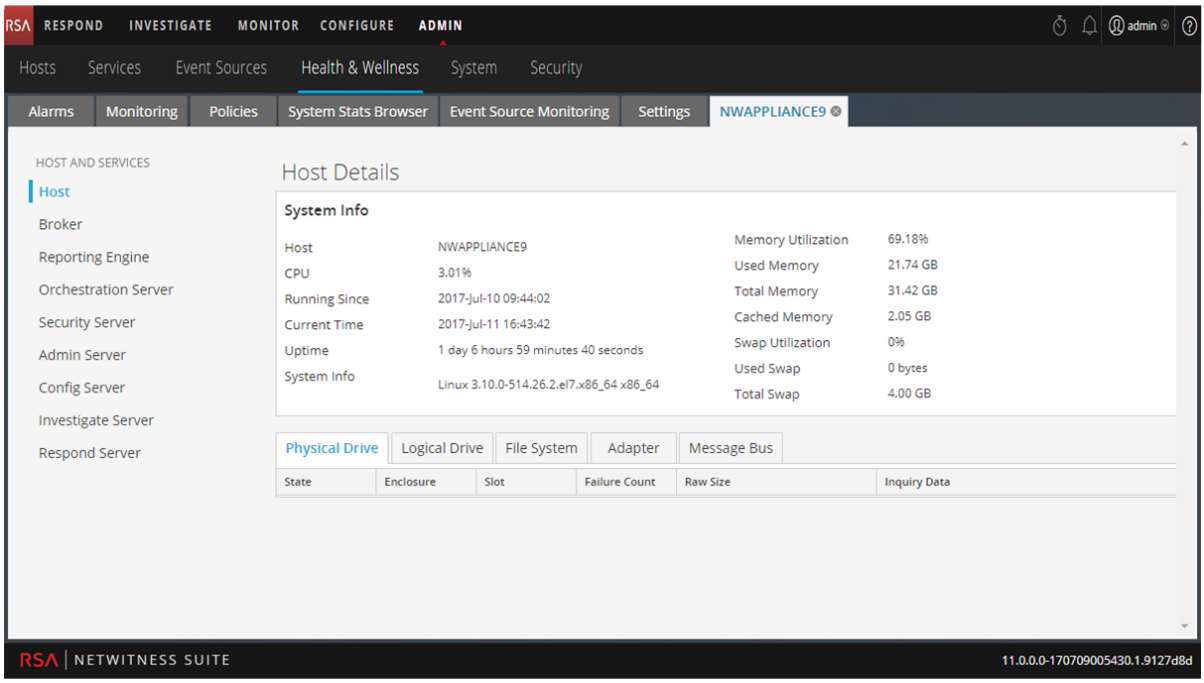
Hinweis: Auf ähnliche Weise können Sie die Liste der Hosts und der ihnen zugeordneten Services filtern, indem Sie den richtigen Filter auswählen:
- Klicken Sie auf „Beendete Services“, um eine Liste aller beendeten Services anzuzeigen.
- Klicken Sie auf „Probleme mit physischem Laufwerk“, um eine Liste der Hosts anzuzeigen, bei denen Probleme mit dem physischen Laufwerk vorliegen.
- Geben Sie den Namen eines Hosts im Feld „Filter“ ein, um nur den gewünschten Host und die Services anzuzeigen, die auf dem Host ausgeführt werden.

Überwachen von Hostdetails

Sie können die Details zum Host anzeigen, wie Arbeitsspeicher und CPU-Nutzung, Systeminformationen, physisches Laufwerk, logisches Laufwerk und Dateisystemdetails, um genauere Ermittlungen auszuführen, wenn Probleme mit dem Host auftreten.

So zeigen Sie die Details zum Host an:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Wählen Sie die Registerkarte **Überwachen** aus.
3. Klicken Sie im Bereich **Hosts** auf einen Host.
   Die Ansicht „Details zum Host“ wird als neue Seite angezeigt.



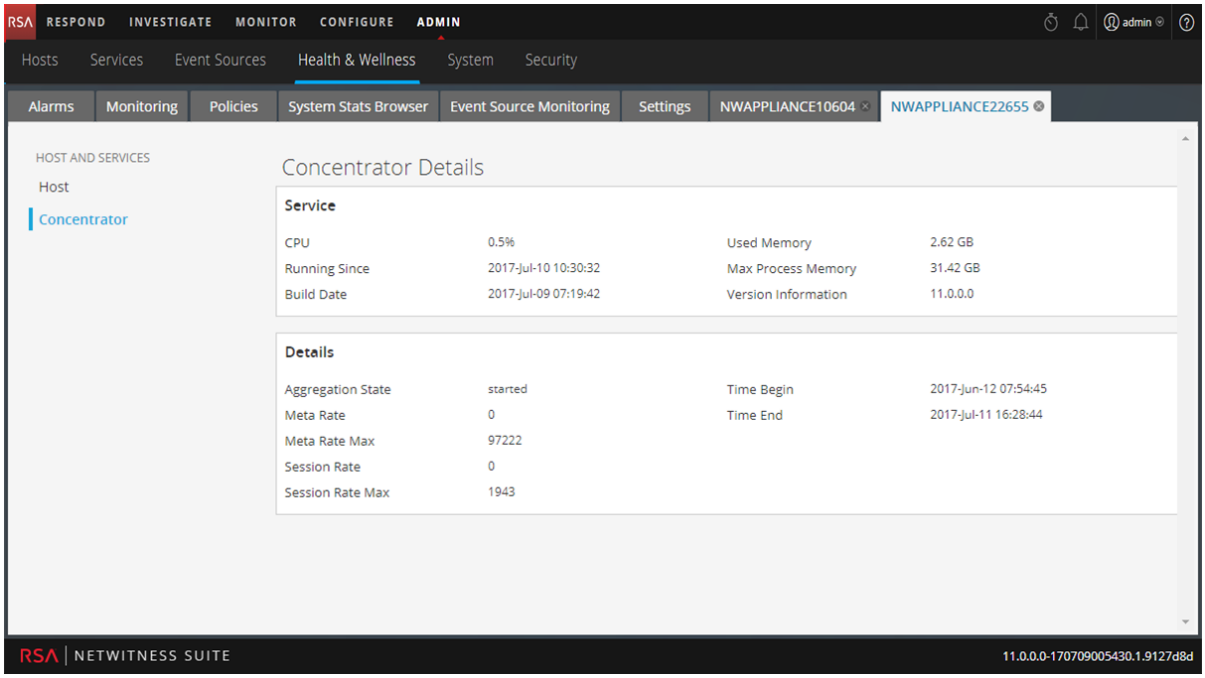
Überwachen von Servicedetails

Sie können die Details zu einem Service anzeigen, zum Beispiel die Speicher- und CPU-Auslastung, Systeminformationen und je nach ausgewähltem Service verschiedene weitere Daten.

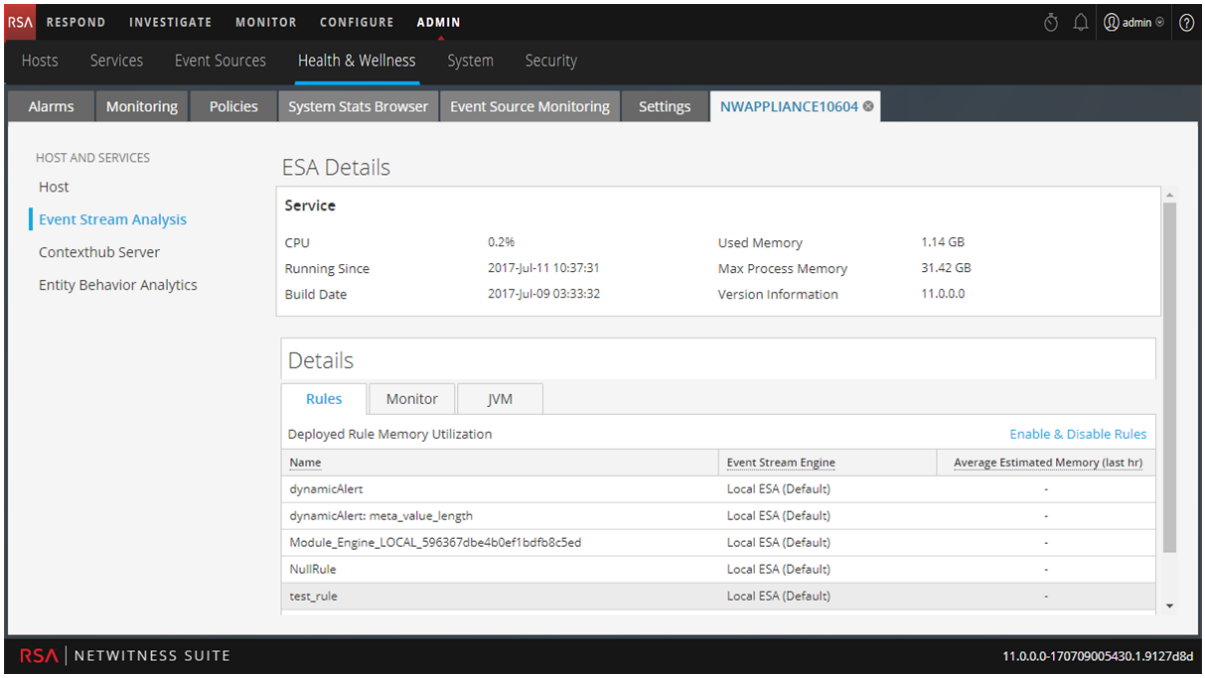
So zeigen Sie Servicedetails an:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Wählen Sie die Registerkarte **Überwachen** aus.
3. Klicken Sie im Bereich „Hosts“ auf ⊞ für einen Host.
   Es wird eine Liste mit den Services angezeigt, die auf dem Host ausgeführt werden.
4. Klicken Sie auf einen Service.

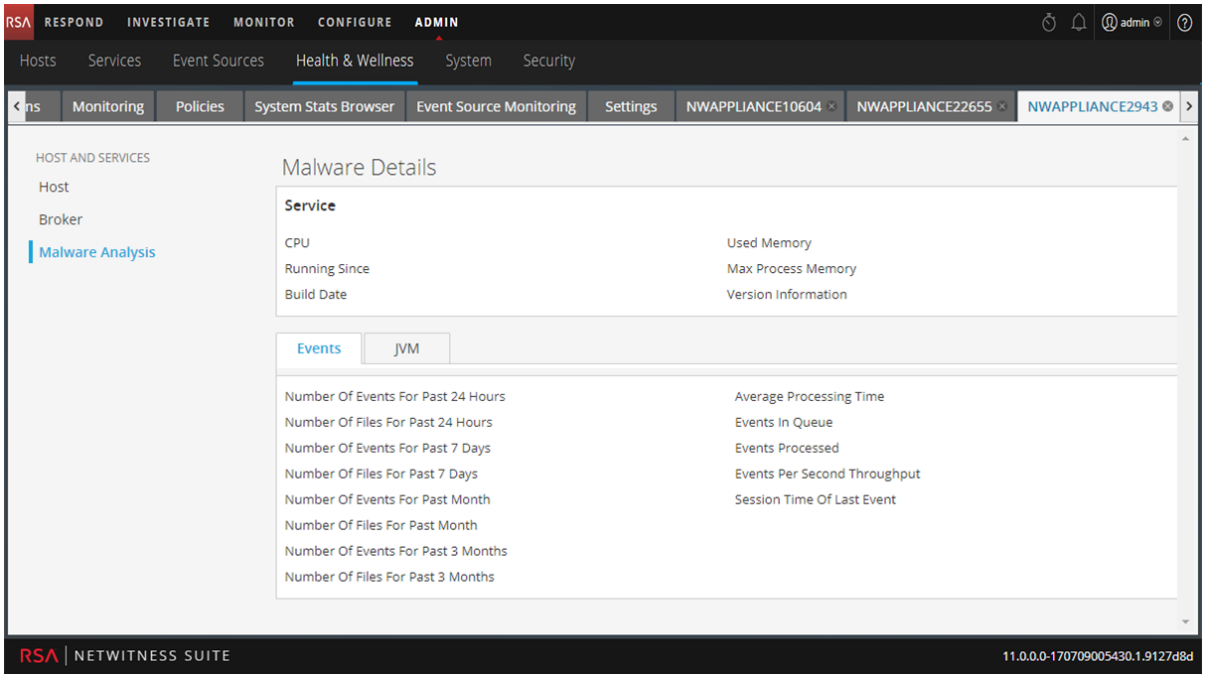
Die Ansicht „Servicedetails“ wird als neue Seite angezeigt. Die Ansicht „Servicedetails“ der Services Archiver, Broker, Concentrator und Decoder haben die Bereiche **Service** und **Details**.



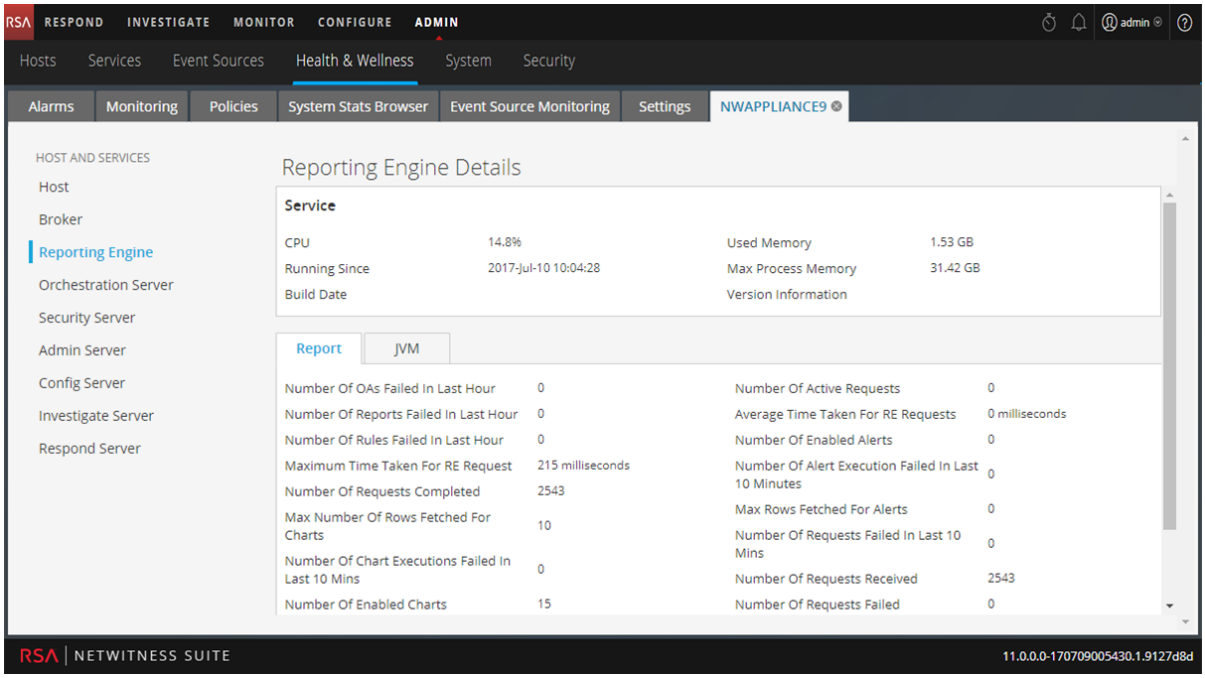
Die Ansicht „Servicedetails“ des ESA-Services (Event Stream Analysis) enthält die Bereiche **Service** und **Details** sowie die Registerkarten **Überwachung** und **JVM**, auf denen zusätzliche Statistiken aufgeführt werden.



Die Ansicht „Servicedetails“ des Malware Analysis-Services enthält den Bereich **Service** und die Registerkarten **Regeln, Ereignisse** und **JVM**, auf denen zusätzliche Statistiken aufgeführt werden.



Die Ansicht „Servicedetails“ des Reporting Engine-Services enthält den Bereich **Service** und die Registerkarten **Bericht** und **JVM**, auf denen zusätzliche Statistiken aufgeführt werden.



Hinweis: Sie können auch auf die Seite „Servicedetails“ zugreifen, indem Sie auf die Services klicken, die im Bereich „Optionen“ der Ansicht „Details zum Host“ aufgeführt sind.

Eine detaillierte Beschreibung der Detailansicht für den jeweiligen Service finden Sie unter Ansicht „Überwachung“.

Überwachen von Ereignisquellen

Die Ereignisquellenüberwachung in NetWitness Suite bietet folgende Funktionen:

- Unterstützung für Failovers
- Konsolidierte Liste von Ereignisquellen und zugehörigen Collector- und Log Decoder-Geräten
- Regex-Unterstützung für Regeln
- Außerbetriebnahme
- Filterfunktionen
- Verlaufsdiagramm

Außerdem können Sie Ereignisquellen überwachen, die Anzahl der für einen Quelltyp generierten Ereignisse prüfen und ein Verlaufsdiagramm der erfassten Ereignisse anzeigen. Um Ereignisquellen zu überwachen, müssen Sie die Ereignisquellen so konfigurieren, dass sie Benachrichtigungen erzeugen und senden, falls erforderlich.

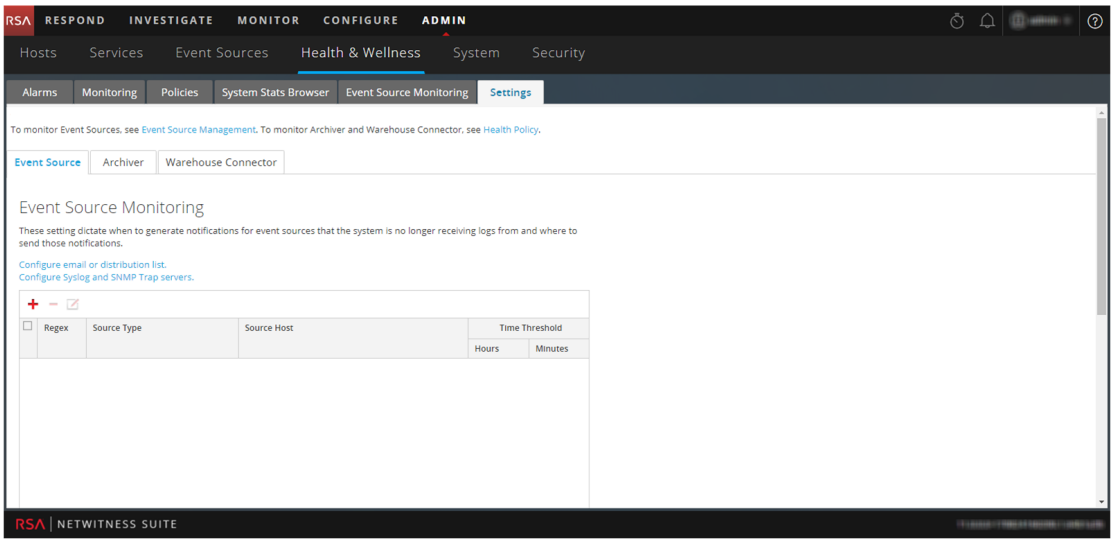
Konfigurieren der Ereignisquellenüberwachung

Um Ereignisquellen zu überwachen, müssen Sie die Ereignisquellen so konfigurieren, dass sie Benachrichtigungen erzeugen und senden, falls erforderlich. Weitere Informationen finden Sie unter Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Ereignisquellen.

So konfigurieren und aktivieren Sie die Ereignisüberwachung in NetWitness Suite:

1. Navigieren Sie zu **ADMINISTRATION** > **Integrität und Zustand**.
2. Wählen Sie **Einstellungen** > **Ereignisquelle** aus.

   Die Registerkarte „Ereignisquelle“ wird angezeigt.

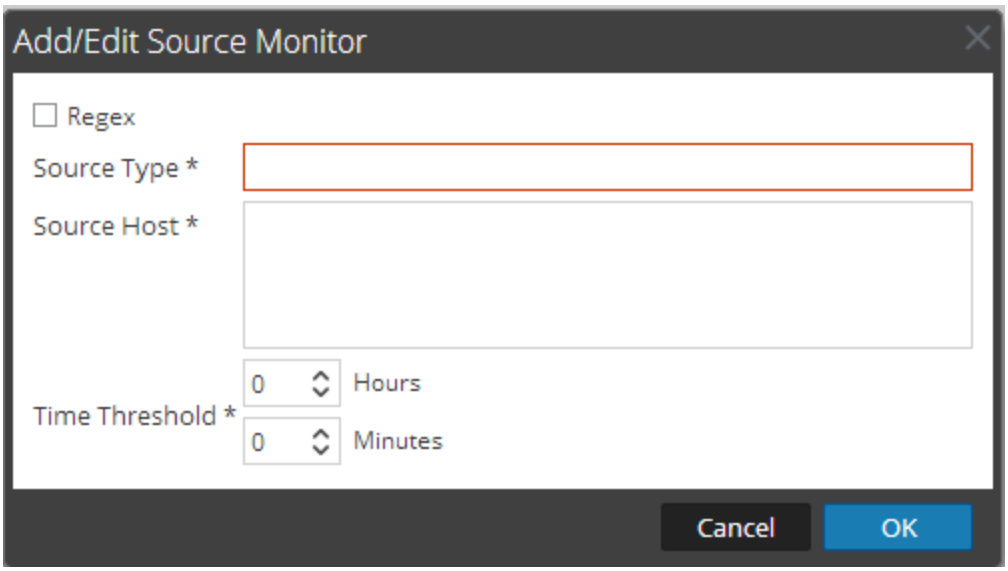


3. Klicken Sie unter **Ereignisquellenüberwachung** auf +.

   Das Dialogfeld „Quellüberwachung hinzufügen oder bearbeiten“ wird angezeigt.

4. Definieren Sie den **Quelltyp**, den **Quellhost** und den **Zeitschwellenwert** für die Quelle der zu überwachenden Ereignisquelle, um zu erkennen, wenn NetWitness Suite keine Protokolle mehr von ihr empfängt. Wenn Sie keinen **Zeitschwellenwert** angeben, überwacht NetWitness Suite die Ereignisquelle solange, bis Sie einen Schwellenwert angeben.

   Hinweis: Für den **Quelltyp** und **Quellhost** müssen Sie die Werte angeben, die Sie für die Ereignisquelle auf der Registerkarte **Ereignisquellen** in der Ansicht **Administration** > **Services** > Log Collector-Service > **Ansicht** > **Konfiguration** konfiguriert haben. Fügen Sie die Ereignisquellen hinzu, die Sie überwachen möchten, oder ändern Sie sie. Die beiden Parameter, die eine Ereignisquelle identifizieren, sind **Quelltyp** und **Quellhost**. Sie können **Globbing** (Musterzuordnung und Platzhalterzeichen) verwenden, wenn Sie den **Quelltyp** und den **Quellhost** der Ereignisquellen angeben.



5. Klicken Sie auf **OK**.

   Die Ereignisquelle wird im Bereich angezeigt.

6. Führen Sie eine der folgenden Aktionen durch, um die Benachrichtigungsmethode zu konfigurieren:

   - Wählen Sie **E-Mails oder Verteilerlisten konfigurieren**.

     Der Bereich „ADMINISTRATION > System > E-Mail-Konfiguration“ wird angezeigt, in dem Sie angeben können, an wen Benachrichtigungen gesendet werden sollen.

   - Wählen Sie **Syslog- und SNMP-Trap-Server konfigurieren**.

     Der Bereich Administration > Systemauditkonfiguration wird angezeigt, in dem Sie die Syslog- und SNMP-Traps konfigurieren können, an die Benachrichtigungen gesendet werden.

7. Klicken Sie auf **Anwenden**.

   NetWitness Suite beginnt mit der Versendung von Benachrichtigungen, wenn es keine Ereignisse mehr aus dieser Ereignisquelle empfängt und der Zeitschwellenwert abgelaufen ist.

Weitere Informationen zu den Parametern in der Ansicht „Einstellungen“ der Ereignisquellenüberwachung finden Sie unter Ansicht „Ereignisquellenüberwachung“.

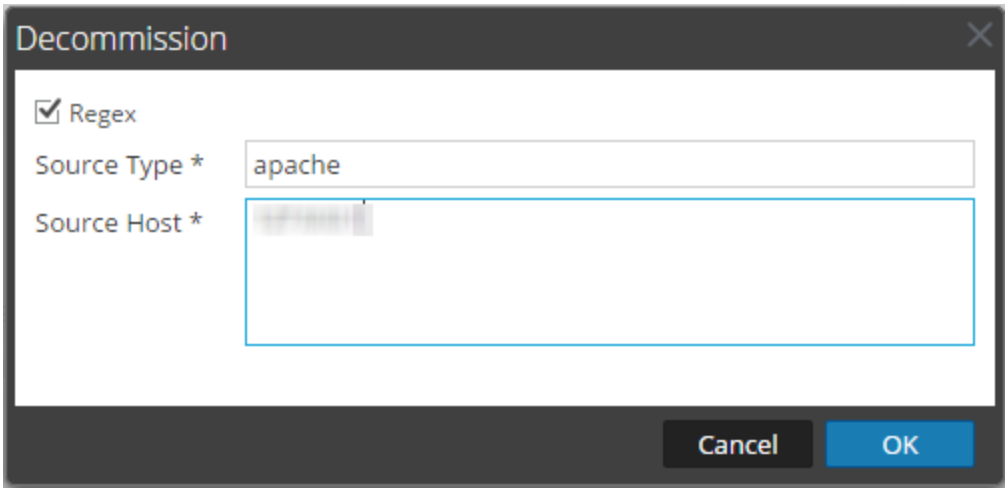
Außerbetriebnahme der Ereignisquellenüberwachung

Wenn ein Log Collector-Service (Local Collector oder Remote Collector), für den Sie die Ereignisquellenüberwachung eingerichtet haben, nicht mehr betriebsbereit ist, werden Sie von NetWitness Suite benachrichtigt, dass keine Ereignisse eingehen, bis Sie die Sammlung außer Betrieb nehmen.

Achtung: Wenn Sie einen Failover Local Collector für einen Remote Collector konfiguriert haben und für den Local Collector ein Failover zu einem Stand-by Log Decoder durchgeführt wurde, müssen Sie den Local Collector außer Betrieb nehmen, um die Benachrichtigungen zu stoppen.

So nehmen Sie die Ereignisquellenüberwachung für eine Ereignisquelle außer Betrieb:

1. Navigieren Sie zu **ADMINISTRATION** > **Integrität und Zustand**.
2. Wählen Sie **Einstellungen** > **Ereignisquelle** aus.
   Die Registerkarte **Ereignisquelle** wird angezeigt.
3. Klicken Sie unter **Außerbetriebnahme** auf +.
   Das Dialogfeld **Außerbetriebnahme** wird angezeigt.
4. Definieren Sie den **Quelltyp** und den **Quellhost** für die Quelle, für die Sie die Benachrichtigungen der Ereignisüberwachung stoppen möchten.



Filtern von Ereignisquellen

Sie können einen Filter setzen, um die folgenden Informationen anzeigen zu lassen:

- Ereignisse, die einer bestimmten Ereignisquelle angehören.
- Ereignisse, die einem bestimmten Ereignisquellentyp angehören.
- Ereignisse, die von einer bestimmten Protokollsammlung gesammelt wurden.
- Die Ereignisliste wird basierend auf folgenden Angaben sortiert: Ereignisquellentyp, Log Collector, Log Decoder oder Zeitpunkt des letzten Ereignisses.

So filtern Sie die Liste der Ereignisquellen:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
2. Klicken Sie auf **Ereignisquellenüberwachung**.
3. Filtern Sie die Liste nach einer der folgenden Methoden:

- Zur Anzeige der von einer bestimmten Ereignisquelle generierten Ereignisse geben Sie diese Ereignisquelle im Feld **Ereignisquelle** ein. Wählen Sie **Regex**, um den Regex-Filter zu aktivieren, und klicken Sie auf **Anwenden**. Der Text wird nach dem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Dieses Feld unterstützt zudem die globale Musterzuordnung.
  Alle die von der angegebenen Ereignisquelle generierten Ereignisse werden angezeigt.
- Zur Anzeige der Ereignisse, die von einem bestimmten Log Collector gesammelt werden, wählen Sie einen Log Collector aus der Drop-down-Liste aus und klicken Sie auf **Anwenden**.
  Eine Liste aller Ereignisse, die von diesem bestimmten Log Collector aus verschiedenen Ereignisquellen gesammelt wurden, wird angezeigt.

Hinweis: Außerdem können Sie einen der folgenden Filter festlegen:
– Zur Anzeige von Ereignissen, die einem bestimmten Ereignisquellentyp angehören, wählen Sie den Ereignisquellentyp aus und klicken Sie auf **Anwenden**.
– Zur Anzeige von Ereignissen, die in einem bestimmten Zeitrahmen empfangen wurden, legen Sie einen Zeitrahmen fest und klicken Sie auf **Anwenden**. Sie können die Abfrageergebnisse zudem so filtern, dass nur Ereignisquellen enthalten sind, die in einer festgelegten Zeit Protokolle erstellt haben oder die in dieser Zeit keine Protokolle erstellt haben.

Weitere Informationen und Beschreibungen zu den verschiedenen Parametern erhalten Sie in der Ansicht „Ereignisquellenüberwachung“.

Anzeigen eines Verlaufsdiagramms für die für eine Ereignisquelle erfassten Ereignisse

Das Verlaufsdiagramm der aus einer Ereignisquelle erfassten Ereignisse zeigt Informationen dazu an, wie die Sammlung in einem ausgewählten Zeitrahmen variierte.

So zeigen Sie ein Verlaufsdiagramm an:

1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.
   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Klicken Sie auf **Ereignisquellenüberwachung**.
   Die Ansicht Ereignisquellenüberwachung wird angezeigt.
3. Wählen Sie in der Spalte **Verlaufsdiagramm** das Symbol  aus.
   Das Verlaufsdiagramm für die ausgewählte Ereignisquelle wird angezeigt.

In der Abbildung unten sehen Sie ein Beispiel des Verlaufsdiagramms für den Ereignisquellentyp **winevent_snare**.

Die angepasste Grafikansicht gibt die für den aktuellen Tag erfassten Ereignisse wieder, wobei die Werte über einen einstündigen Zeitraum aufgezeichnet werden (09:05 bis 10:05 Uhr). Bewegen Sie den Mauszeiger über das Diagramm, um die Details zu einem bestimmten Zeitpunkt anzuzeigen. In der Abbildung wird z. B. die Durchschnittsrate der Sammlung um 09.30 Uhr angezeigt.

Hinweis: Sie können die Grafikansicht anpassen, indem Sie den Zeitrahmen und den Datumsbereich auswählen. Sie können vergrößern mithilfe des Vergrößerungswerts, des Zeitfensters oder indem Sie einfach in den Zeichenbereich klicken und ziehen. Weitere Informationen zu den Parametern für Anpassung und Zoomfunktionen finden Sie unter Verlaufsdiagramme für „Integrität und Zustand“ für die von einer Ereignisquelle erfassten Ereignisse.

Wenn keine Daten im Diagramm angezeigt werden, kann das eine der folgenden Ursachen haben:

- Die Ereignisquelle funktioniert derzeit nicht.
- Die Ereignisquelle verarbeitet derzeit keine Daten.

Überwachen von Alarmen

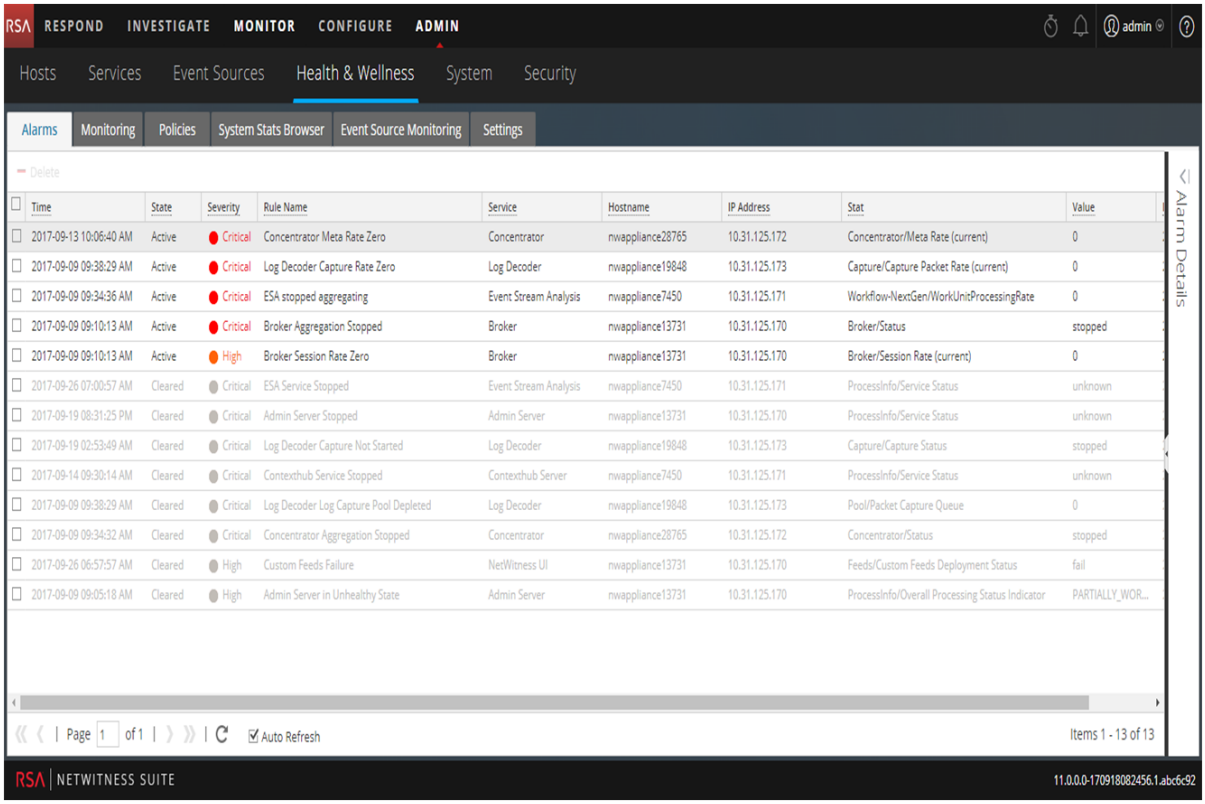
Sie können Alarme in der Benutzeroberfläche „Integrität und Zustand“ für die Hosts und Services in Ihrer NetWitness Suite-Domain einrichten und überwachen. Alarme werden in der Ansicht als **Aktiv** angezeigt, wenn die durch die Richtlinienregeln definierten statistischen Schwellenwerte für Hosts und Services überschritten wurden. Alarme werden ausgegraut und wechseln in den Status **Gelöscht**, wenn der Löschschwellenwert überschritten wurde.

Die Parameter für Alarme werden im Abschnitt Richtlinien managen festgelegt.Richtlinien managen Weitere Informationen finden Sie unter Ansicht „Integrität und Zustand“ – Ansicht „Alarme“.

So überwachen Sie die in NetWitness Suite eingerichteten Alarme:

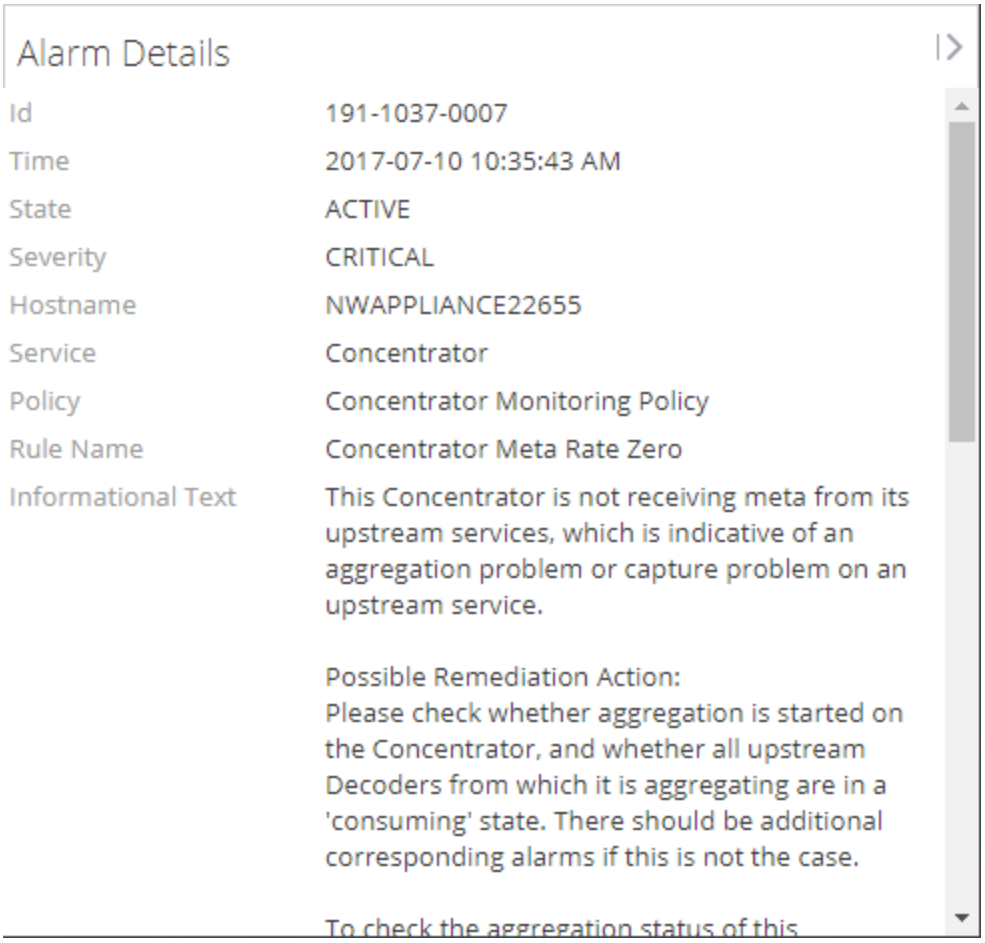
1. Navigieren Sie zu **ADMINISTRATION > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird standardmäßig mit geöffneter Registerkarte „Alarme“ angezeigt.



2. Klicken Sie auf den Alarm, für den Sie die Details im Bereich „Details“ anzeigen möchten.

3. Klicken Sie auf (Erweitern), um die Details für den ausgewählten Alarm anzuzeigen.



Überwachen von Integrität und Zustand mit SNMP-Warnmeldungen

Sie können eine NetWitness-Server-Komponente überwachen, um Warnmeldungen proaktiv mithilfe von SNMP (Simple Network Management Protocol) basierend auf Schwellenwerten oder Systemfehlern zu senden.

Die Auslastung kann für folgende Komponenten von NetWitness Suite überwacht werden:

- CPU-Auslastung, die einen definierten Schwellenwert erreicht
- Arbeitsspeicherauslastung, die einen definierten Schwellenwert erreicht
- Festplattenauslastung, die einen definierten Schwellenwert erreicht

SNMP-Konfiguration

Die NetWitness-Server können so konfiguriert werden, dass sie SNMPv3-Schwellenwert-Traps und Überwachungs-Traps senden. Schwellenwert-Traps werden in Verbindung mit konfigurierten Node-Schwellenwerten von den NetWitness Suite Core-Anwendungen selbst gesendet. Überwachungs-Traps werden vom SNMP-Daemon selbst für die in seiner Konfigurationsdatei angegebenen Elemente gesendet. Der Kunde muss den SNMP-Daemon auf einem anderen Service einrichten, um SNMP-Traps von NetWitness Suite empfangen zu können. Sie können SNMP auf NetWitness Suite in der Konfigurationseinstellung für den NetWitness-Server einrichten. Weitere Informationen finden Sie unter **Servicekonfigurationseinstellungen** im *Leitfaden für die ersten Schritte mit NetWitness Suite-Hosts und -Services* für den spezifischen Host.

Schwellenwerte

Schwellenwerte können für alle Servicestatistiken eingerichtet werden, die die setLimit-Meldung akzeptieren können. Sie können die aktuellen Schwellenwerte mithilfe der getLimit-Meldung abrufen. Zum Festlegen einer Begrenzung können Sie einen unteren und oberen Schwellenwert angeben.

Wenn der Wert dieser Statistik den unteren oder oberen Schwellenwert erreicht, wird ein SNMP-Trap ausgelöst, der angibt, dass der Schwellenwert erreicht ist. Der Trap wird nicht ausgelöst, wenn der Wert unter dem unteren Schwellenwert oder über dem oberen Schwellenwert liegt. Es wird jedoch ein anderer Trap ausgelöst, wenn der Wert wieder in den normalen Bereich zurückkehrt (d. h. über dem unteren und unter dem oberen Schwellenwert liegt).

Sie müssen den Schwellenwert für den Service mithilfe der Service-Explorer-Ansicht oder der REST-API festlegen.

Im Folgenden ist ein Beispiel für einen Schwellenwert zur Überwachung der CPU-Auslastung angegeben (unter 10 % oder über 90 %):

```
/sys/stats/cpu setLimit low=10 high=90
```

Im Folgenden ist ein Beispiel angegeben, wie der Schwellenwert mithilfe der REST-API festgelegt wird:

```
http://<log decoder>:50102/sys/stats/cpu?msg=setLimit&low=10&high=90
```

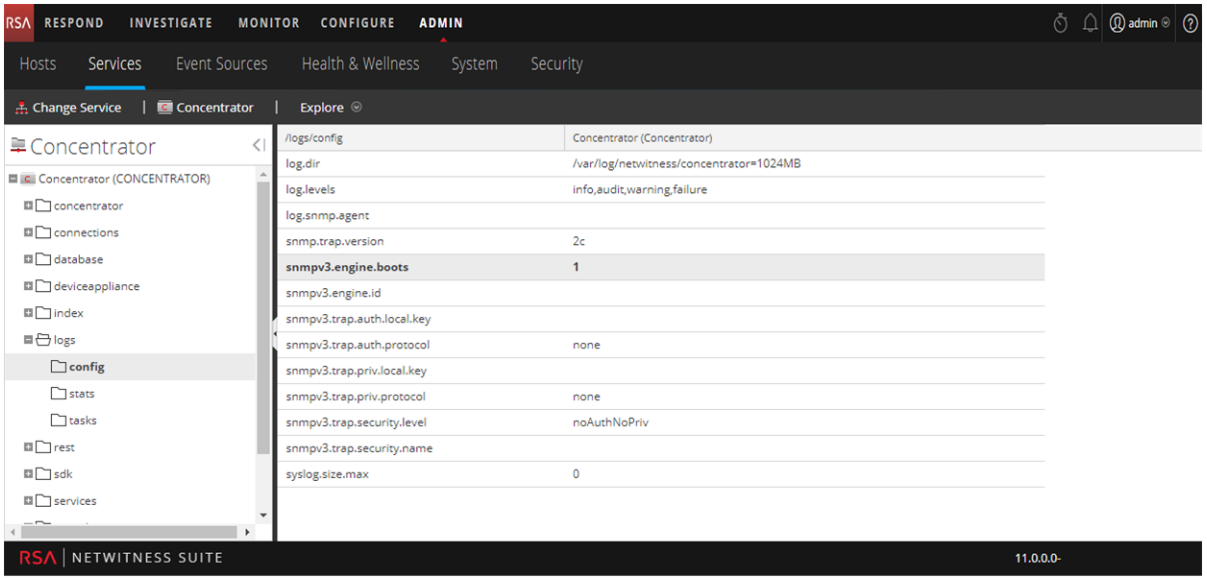
Wenn die CPU-Auslastung einen Spitzenwert von 90 % oder höher erreicht, wird ein SNMP-Trap erzeugt:

```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu
old=77% new=91
```

Konfigurieren von SNMPv3 für einen Host

1. Navigieren Sie zu **ADMINISTRATION > Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Service aus.

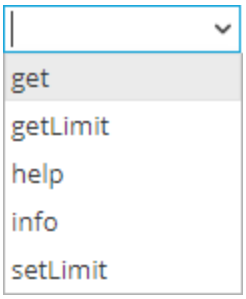
3. Wählen Sie in der Spalte Aktionen die Optionen **Ansicht > Durchsuchen** aus.
4. Blenden Sie die Liste in der Node-Liste ein und wählen Sie einen Konfigurationsordner aus, zum Beispiel „logs > config“.
5. Stellen Sie die SNMPv3-Konfiguration ein.



Festlegen des Schwellenwerts für einen Service

1. Navigieren Sie zu **ADMINISTRATION > Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie den Service aus.
3. Wählen Sie in der Spalte Aktionen die Optionen **Ansicht > Durchsuchen** aus.
4. Blenden Sie die Liste in der Node-Liste ein und wählen Sie einen Statistikordner aus.
5. Wählen Sie eine Statistik aus, z. B. cpu, und klicken Sie mit der rechten Maustaste darauf.
6. Wählen Sie im Drop-down-Menü die Option **Eigenschaften** aus.

   Der Bereich „Eigenschaften“ wird angezeigt. Der Bereich „Eigenschaften“ enthält eine Drop-down-Liste mit verfügbaren Meldungen für den Parameter.



7. Wählen Sie „setLimit“ aus.
8. Legen Sie untere und obere Werte fest.

Troubleshooting von Integrität und Zustand

Häufige Probleme bei allen Hosts und Services

In der Schnittstelle Integrität und Zustand können falsche Statistiken angezeigt werden, wenn:

- einige oder alle Hosts und Services nicht korrekt bereitgestellt und aktiviert sind.
- Sie eine Bereitstellung mit gemischten Versionen verwenden (d. h. Hosts, die auf verschiedene NetWitness Suite-Versionen aktualisiert wurden).
- unterstützende Services nicht ausgeführt werden.

Probleme, die durch Meldungen in der Oberfläche oder den Protokolldateien angezeigt werden

Dieser Abschnitt enthält Troubleshooting-Informationen zu Problemen, die durch Meldungen angezeigt werden, die von NetWitness Suite in der Oberfläche „Integrität und Zustand“ angezeigt oder in deren Protokolldateien dokumentiert werden.

Meldung	Benutzeroberfläche **Es kann keine Verbindung zum System Management Service hergestellt werden.**
	SMS-Protokolle (System Management Service):
	
	`Caught an exception during connection recovery!`
	`java.io.IOException`
	`at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:106)`
	`at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:102)`
	`at com.rabbitmq.client.impl.AMQConnection.start (AMQConnection.java:346)`
	`at com.rabbitmq.client.impl.recovery.RecoveryAwareAMQConnectionFa`

```
ctory.
newConnection(RecoveryAwareAMQConnectionFactory.java:36)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
recoverConnection(AutorecoveringConnection.java:388)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
beginAutomaticRecovery(AutorecoveringConnection.java:360)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.acc
ess$000(AutorecoveringConnection.java:48)
 at
com.rabbitmq.client.impl.recovery.AutorecoveringConnection$1.
shutdownCompleted(AutorecoveringConnection.java:345)
 at
com.rabbitmq.client.impl.ShutdownNotifierComponent.notifyListe
ners(ShutdownNotifierComponent.java:75)
 at com.rabbitmq.client.impl.AMQConnection$MainLoop.run
(AMQConnection.java:572)
 at java.lang.Thread.run(Thread.java:745)
 Caused by: com.rabbitmq.client.ShutdownSignalException:
connection error
 at com.rabbitmq.utility.ValueOrException.getValue
(ValueOrException.java:67)
 at
com.rabbitmq.utility.BlockingValueOrException.uninterruptibleG
etValue(BlockingValueOrException.java:33)
 at
com.rabbitmq.client.impl.AMQChannel$BlockingRpcContinuation.ge
tReply
(AMQChannel.java:343)
 at com.rabbitmq.client.impl.AMQConnection.start
(AMQConnection.java:292)
 ... 8 more
```

	Caused by: java.net.SocketException: Connection reset at java.net.SocketInputStream.read (SocketInputStream.java:189) at java.net.SocketInputStream.read (SocketInputStream.java:121) at java.io.BufferedInputStream.fill (BufferedInputStream.java:246) at java.io.BufferedInputStream.read (BufferedInputStream.java:265) at java.io.DataInputStream.readUnsignedByte (DataInputStream.java:288) at com.rabbitmq.client.impl.Frame.readFrom(Frame.java:95) at com.rabbitmq.client.impl.SocketFrameHandler.readFrame (SocketFrameHandler.java:139) at com.rabbitmq.client.impl.AMQConnection$MainLoop.run (AMQConnection.java:532)
Mögliche Ursache	RabbitMQ-Service wird nicht auf dem NetWitness-Server ausgeführt.

Lösung	Starten Sie den RabbitMQ-, SMS- und NetWitness Suite-Service mithilfe der folgenden Befehle neu.
	`systemctl restart rabbitmq-server`
	`systemctl restart rsa-sms`
	`systemctl restart jetty`

Meldung/ Problem	Benutzeroberfläche **Es kann keine Verbindung zum System Management Service hergestellt werden.**
Ursache	Der System Management Service, der RabbitMQ- oder der Mongo-Service wird nicht ausgeführt.

Lösung	Führen Sie auf dem NetWitness-Server die folgenden Befehle aus, um zu überprüfen, ob alle diese Services ausgeführt werden.
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is not running.`
	`[root@nwserver ~]# systemctl start rsa-sms`
	`Starting RSA NetWitness SMS :: Server...`
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is running (5687).`
	`[root@nwserver ~]# systemctl status mongod`
	`mongod (pid 2779) is running...`
	`systemctl status rabbitmq-server`
	`Status of node nw@localhost ...`
	`[{pid,2501},`
	`{running_applications,`
	`[{rabbitmq_federation_management,"RabbitMQ Federation Management",`
	`"3.3.4"},`

Meldung/ Problem	Benutzeroberfläche: **Es kann keine Verbindung zum System Management Service hergestellt werden.**
Mögliche Ursache	Partition `/var/lib/rabbitmq` ist zu 70 % oder mehr belegt.
Lösung	Wenden Sie sich an den Kundendienst.

Meldung/ Problem	Benutzeroberfläche **Hostmigration fehlgeschlagen.**
Mögliche Ursache	Ein oder mehrere NetWitness Suite-Services haben möglicherweise den Status **Beendet**.
Lösung	Überprüfen Sie, ob die folgenden Services ausgeführt werden, und starten

	Sie dann den NetWitness-Server neu: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Meldung/ Problem	Benutzeroberfläche **Server nicht verfügbar.**
Mögliche Ursache	Ein oder mehrere NetWitness Suite-Services haben möglicherweise den Status **Beendet**.
Lösung	Überprüfen Sie, ob die folgenden Services ausgeführt werden, und starten Sie dann den NetWitness-Server neu: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Response Server, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, Workbench.

Meldung/ Problem	Benutzeroberfläche: **Server nicht verfügbar.**
Mögliche Ursache	Der System Management Service (SMS), der RabbitMQ- oder der Mongo-Service wird nicht ausgeführt.

Lösung 1	Führen Sie auf dem NetWitness-Server die folgenden Befehle aus, um zu überprüfen, ob alle diese Services ausgeführt werden.
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is not running.`
	`[root@nwserver ~]# systemctl start rsa-sms`
	`Starting RSA NetWitness SMS :: Server...`
	`[root@nwserver ~]# systemctl status rsa-sms`
	`RSA NetWitness SMS :: Server is running (5687).`
	`[root@nwserver ~]# systemctl status mongod`

	mongod (pid 2779) is running... systemctl status rabbitmq-server Status of node nw@localhost ... [{pid,2501}, {running_applications, [{rabbitmq_federation_management,"RabbitMQ Federation Management", "3.3.4"},
Lösung 2	Stellen Sie sicher, dass die Partition `/var/lib/rabbitmq` zu weniger als 75 % belegt ist.
Lösung 3	Prüfen Sie die NetWitness-Server-Protokolldateien (`var/lib/netwitness/uax/logs/nw.log`) auf Fehler.

Meldung/ Problem	ContextHub wird beendet und ermöglicht es Ihnen nicht, Datenquellen und Listen hinzuzufügen oder zu bearbeiten.
Mögliche Ursache	Der Speicher ist zu mindestens 95 % voll.
Lösung 1	Vergrößern Sie den Speicher durch Aktualisieren der YML-Datei, die sich im Verzeichnis „/etc/netwitness/contexthub-server/ contexthub-server.yml“ befindet. Geben Sie beispielsweise zum Vergrößern des Speichers von 120 GB auf 150 GB einen Wert (in Byte) ein, indem Sie den relevanten Parameter bearbeiten: `rsa.contexthub.data.disk-size: 161061273600`
Lösung 2	Löschen Sie eine unerwünschte oder nicht verwendete große Liste.
Lösung 3	Konfigurieren Sie den TTL-Index für die Liste, um automatisch STIX- und TAXI-Daten zu löschen und Speicherplatz zu bereinigen.

Meldung/ Problem	Context Hub wird auf einem festen Arbeitsspeicher ausgeführt und 50 % ist für den Cache reserviert. Wenn der Cache zu 100 % voll ist, reagiert der Cache nicht mehr. Bei allen neuen Suchvorgängen ist die Reaktion langsam.

Mögliche Ursache	Der Cache ist zu mindestens 50 % voll.
Lösung 1	Standardmäßig bereinigt Context Hub den Cache alle 30 Minuten. Reduzieren Sie die Cacheablaufzeit von Datenquellen.
Lösung 2	Deaktivieren Sie den Cache für Datenquellen.
Lösung 3	Vergrößern Sie den RAM des CH Java-Prozesses durch Bearbeiten der Option `-Xmx`, die in der Datei „/etc/netwitness/contexthub-server/contexthub-server.conf“ verfügbar ist. Suche Sie in `JAVA_OPTS` nach der Option `-Xmx`. Bearbeiten Sie den Eintrag beispielsweise wie folgt: `-Xmx8G` , wobei `8G` für 8 GB Speicherplatz steht. Starten Sie dann den ContextHub-Service neu. **Hinweis:** Der Arbeitsspeicher ist kleiner als der verfügbare Systemspeicher. Beachten Sie, dass viele andere Services auf dem Host ausgeführt werden.

Meldung/ Problem	Die Listendatenquelle zeigt eine fehlerhafte Statistik oder einen fehlerhaften Status an.
Mögliche Ursache 1	Folgendes ist nicht möglich: • Zugriff auf die Datenquelle • Analysieren oder Lesen einer CSV-Datei • Schematische Darstellung von nicht übereinstimmenden CSV-Dateien
Mögliche Ursache 2	Authentifizierung beim Zugriff auf die Datenquelle nicht möglich.
Lösung 1	Achten Sie darauf, die CSV-Datei am richtigen Speicherort zu speichern, d. h im Verzeichnis „/var/lib/netwitness/contexthub-server/data/“, und überprüfen Sie die erforderlichen Leseberechtigungen.
Lösung 2	Vergewissern Sie sich, dass das während der Konfiguration der Datenquelle angegebene Schema der CSV-Datei übereinstimmt. Wenn

	dies nicht der Fall ist, erstellen Sie entweder eine neue Datenquelle mit dem neuen Schema oder bearbeiten Sie die CSV-Datei, um das Schema anzupassen. Beispiel: Bei der Konfigurierung einer Listendatenquelle mit einem Schema mit Spalte 1, Spalte 2 und Spalte 3. Und bei der nächsten Aktualisierung der CSV-Datei, bei der die Anzahl der Spalten erhöht bzw. verringert oder Reihenfolge der Spalten geändert wird. In diesem Fall stimmt das Schema nicht überein und die konfigurierte Listendatenquelle zeigt den Status „Fehlerhaft“ in der Statistik für Integrität und Zustand an.
Lösung 3	Vergewissern Sie sich, dass das Passwort korrekt ist. Um die Bearbeitung der Datenquelle zu bestätigen, geben Sie das Passwort ein und klicken Sie auf „Verbindung testen“. Weitere Informationen zu den oben genannten Lösungen finden Sie im Thema „Konfigurieren von Listen als Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.

Nicht in der Benutzeroberfläche oder den Protokollen dokumentierte Fehler

Dieser Abschnitt enthält Troubleshooting-Informationen zu Problemen, die nicht durch Meldungen angezeigt werden, die von NetWitness Suite in der Oberfläche „Integrität und Zustand“ angezeigt oder in deren Protokolldateien dokumentiert werden. Beispiel: Es können falsche statistische Informationen in der Oberfläche angezeigt werden.

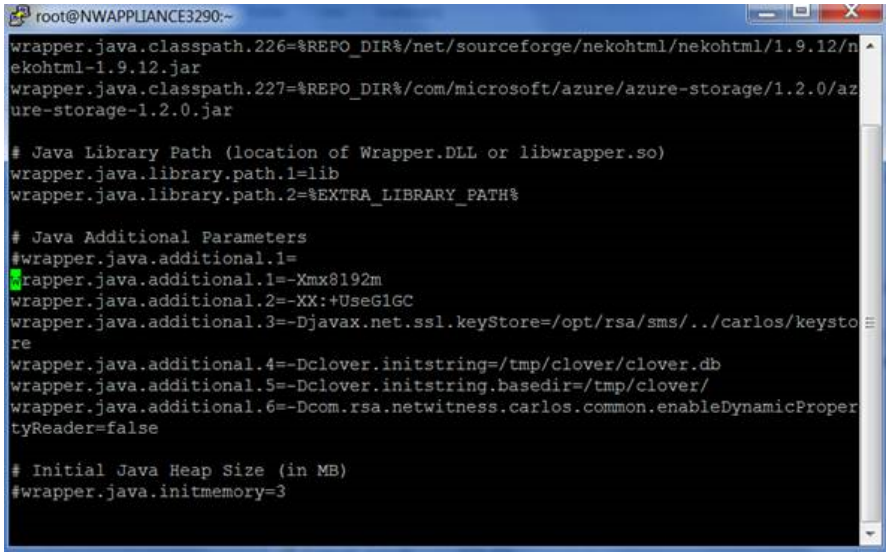
Problem	Falsche Statistiken in der Oberfläche Integrität und Zustand.
Mögliche Ursache	Der SMS-Service wird nicht ausgeführt. Der SMS-Service muss auf dem NetWitness-Server ausgeführt werden.
Lösung	Starten Sie den SMS-Service neu.

Problem	NetWitness Suite zeigt nicht an, auf welche Version ein Upgrade durchgeführt wurde, bis Sie jettysrv (den jeTTy-Server) neu starten.
Mögliche Ursache	Beim Überprüfen einer Verbindung durch NetWitness Suite wird alle 30 Sekunden ein Service abgefragt, um zu überprüfen, ob er aktiv ist. Wird der Service während dieser 30 Sekunden erneut angezeigt, erhält er keine

Lösung	neue Version.
	1. Beenden Sie den Service manuell. 2. Warten Sie, bis angezeigt wird, dass der Service offline ist. 3. Starten Sie den Service neu. NetWitness Suite zeigt die richtige Version an.

Problem	Der NetWitness-Server zeigt die Seite **Service nicht verfügbar** nicht an.
Mögliche Ursache	Nach einem Upgrade auf NetWitness Suite Version 10.5 ist JDK 1.8 nicht die Standardversion. Dies führt dazu, dass jettysrv (der jeTTy-Server) nicht gestartet wird. Ohne den jeTTy-Server kann der NetWitness Suite-Server die Seite **Service nicht verfügbar** nicht anzeigen.
Lösung	Starten Sie den jettysrv neu.

Problem	Der SMS-Service wurde angehalten und die folgende Fehlermeldung wird in der Protokolldatei angezeigt: `java.lang.OutOfMemoryError: Java heap space`
Lösung	Sie können mit der folgenden Lösung den Speicher je nach Ihren Anforderungen erhöhen. 1. Öffnen Sie die Datei „/opt/rsa/esa/conf/wrapper.conf“.



2. Ersetzen Sie `wrapper.java.additional.1=-Xmx8192m` durch: `wrapper.java.additional.1=-Xmx16g`
3. Starten Sie den SMS-Service neu:
   `systemctl start rsa-sms`

Managen von NetWitness Suite-Aktualisierungen

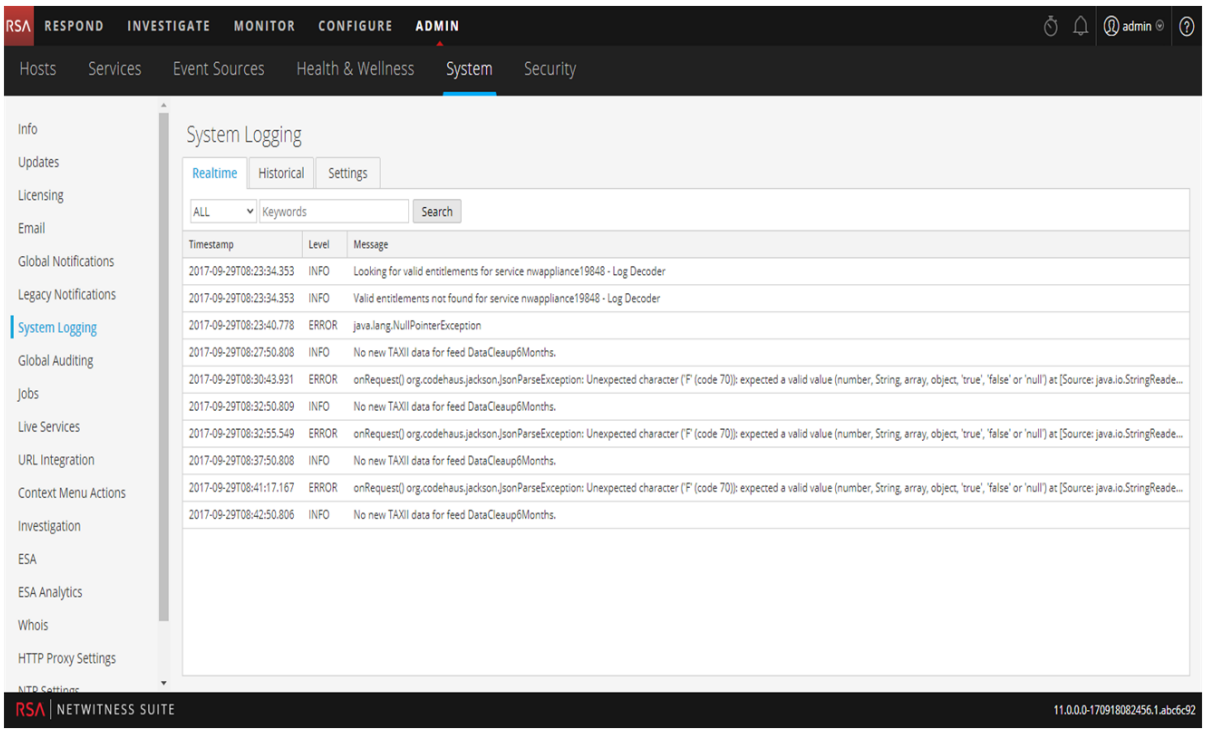
RSA veröffentlicht regelmäßig Softwareversionsaktualisierungen von NetWitness Suite im Bestreben, das Produkt fortlaufend zu verbessern. Eine Softwareversionsaktualisierung besteht aus einer Freigabe, einem Service Pack oder einem Patch (einschließlich Sicherheitspatch) und zusätzlicher Software, auf der die Freigabe, das Service Pack oder das Patch beruht. Benutzerhandbücher werden für jede Aktualisierung der Softwareversion bereitgestellt, die detaillierte Schritte zur Installation der Aktualisierung enthalten. Laden Sie unbedingt den Aktualisierungsleitfaden der jeweiligen Version von RSA Link herunter (https://community.rsa.com/community/products/netwitness) und führen Sie die die dort beschriebenen Schritte aus. Zusätzliche Informationen finden Sie im Thema „Aktualisieren des vorhandenen Hosts auf die neue Version“ im *Leitfaden für die ersten Schritte mit Hosts und Services* und im Thema Bereich „Systemaktualisierungen“ – Registerkarte „Einstellungen“.

Anzeigen von System- und Serviceprotokollen

NetWitness Suite ermöglicht die Anzeige von System- und Serviceprotokollen. Beim Einsehen der Serviceprotokolle können Sie auch Meldungen für den Service oder Host auswählen.

Systemprotokolle anzeigen

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

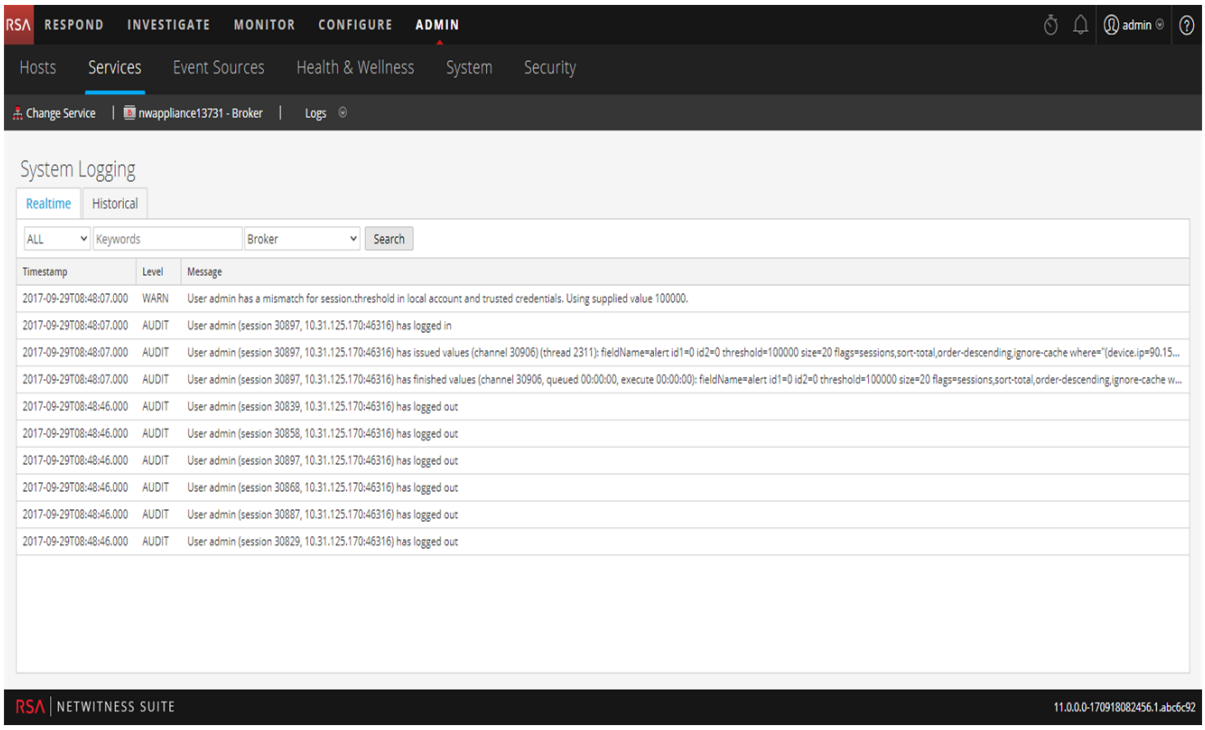


Anzeigen von Serviceprotokollen

So zeigen Sie NetWitness Suite-Serviceprotokolle an:

1. Navigieren Sie zu **ADMINISTRATION > Services**.
2. Wählen Sie im Raster **Services** einen Service aus.

3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Protokolle** aus.



Filtern von Protokolleinträgen

So filtern Sie die auf der Registerkarte Echtzeit angezeigten Ergebnisse:

1. (Optional) Wählen Sie für System- und Serviceprotokolle eine **Protokollebene** und/oder ein **Schlüsselwort** aus. Systemprotokolle haben sieben Protokollebenen. Serviceprotokolle haben nur sechs Protokollebenen, da sie nicht über die Ebene **TRACE** verfügen. Der Standardwert ist **ALLE** Protokolleinträge.
2. (Optional) Wählen Sie für Serviceprotokolle den Service aus: Host oder Service.
3. Klicken Sie auf **Filter**.

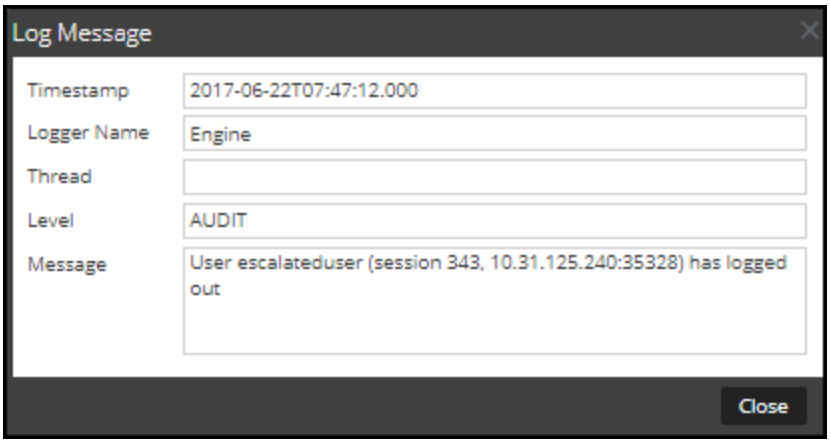
   Die Ansicht wird mit den letzten 10 Einträgen aktualisiert, die mit dem Filter übereinstimmen. Wenn neue übereinstimmende Protokolleinträge verfügbar werden, wird die Ansicht mit diesen Einträgen aktualisiert.

Anzeigen von Details zu einem Protokolleintrag

Jede Zeile des Rasters Protokoll auf der Registerkarte Echtzeit enthält zusammenfassende Informationen zu einem Protokolleintrag. So zeigen Sie alle Details an:

1. Doppelklicken Sie auf einen Protokolleintrag.

   Das Dialogfeld **Protokollmeldung**, das den Zeitstempel, den Protokollierungsnamen, den Thread, die Ebene und die Meldung enthält, wird angezeigt.



2. Klicken Sie nach dem Betrachten auf **Schließen**.

Zugreifen auf die Protokolldatei der Reporting Engine

Alle Protokolldateien

Die Reporting Engine speichert folgende Protokolle im Verzeichnis **rsasoc/rsa/soc/reporting-engine/log**:

- Aktuelle Protokolle in der Datei **reporting-engine.log**.
- Backupkopien früherer Protokolle in der Datei **reporting-engine.log.***.
- Alle UNIX-Skriptprotokolle in den Dateien, die die folgende Syntax haben: **reporting-engine.sh_*timestamp*.log** (zum Beispiel **reporting-engine.sh_20120921.log**).

Die Reporting Engine schreibt selten Befehlszeilen-Fehlermeldungen in die Datei **rsasoc/nohup.out**.

Upstart-Protokolle

Die Reporting Engine fügt die Protokollmeldungen, die vom Upstart-Daemon geschriebene Ausgabe und die Befehle, die zum Starten der Reporting Engine verwendet werden, an das Verzeichnis **/var/log/secure** an.

Bei einer Upstart-Protokolldatei handelt es sich um eine Systemprotokolldatei, die nur von einem Root-Benutzer gelesen werden kann. Die Reporting Engine erzeugt Protokolldateien, behält Backupkopien der vorherigen Protokolldateien bei, speichert UNIX-Skriptprotokolldateien und fügt Upstart-Protokolldateien an ein anderes Verzeichnis an.

Suchen und Exportieren von Verlaufsprotokollen

NetWitness Suite bietet eine durchsuchbare Ansicht des NetWitness Suite-Protokolls oder des Serviceprotokolls in einer Seitenansicht. Wenn es erstmals geladen wird, zeigt das Raster die letzte Seite der Protokolleinträge für das System oder den Service an. Sie können aus der aktuellen Ansicht Protokolle exportieren.

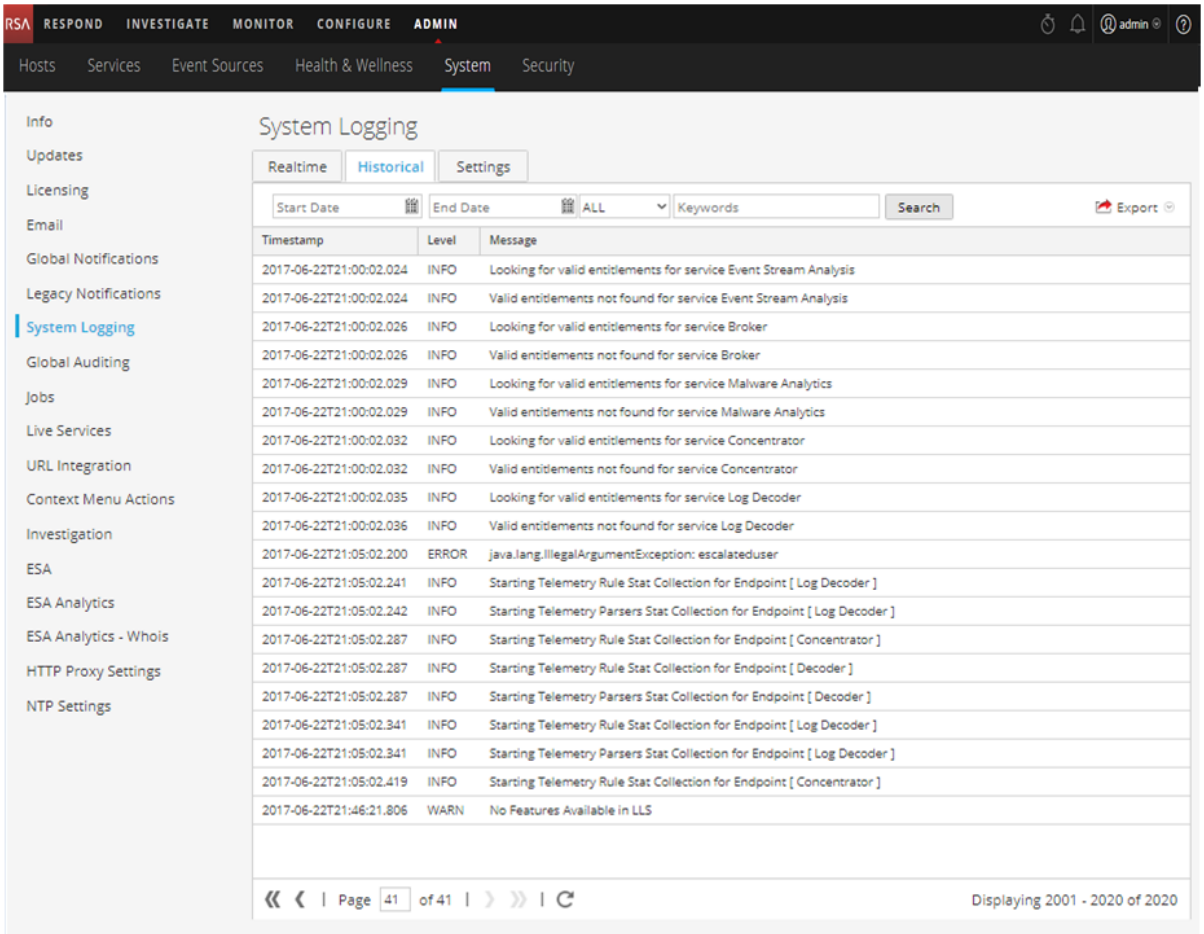
Anzeigen des Systemverlaufsprotokolls

So zeigen Sie das Verlaufsprotokoll für das System an:

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

   Der Bereich „Systemprotokollierung“ wird standardmäßig mit angezeigter Registerkarte „Echtzeit“ geöffnet.
3. Klicken Sie auf die Registerkarte **Historisch**.

   Eine Liste von Verlaufsprotokollen für das System wird angezeigt.



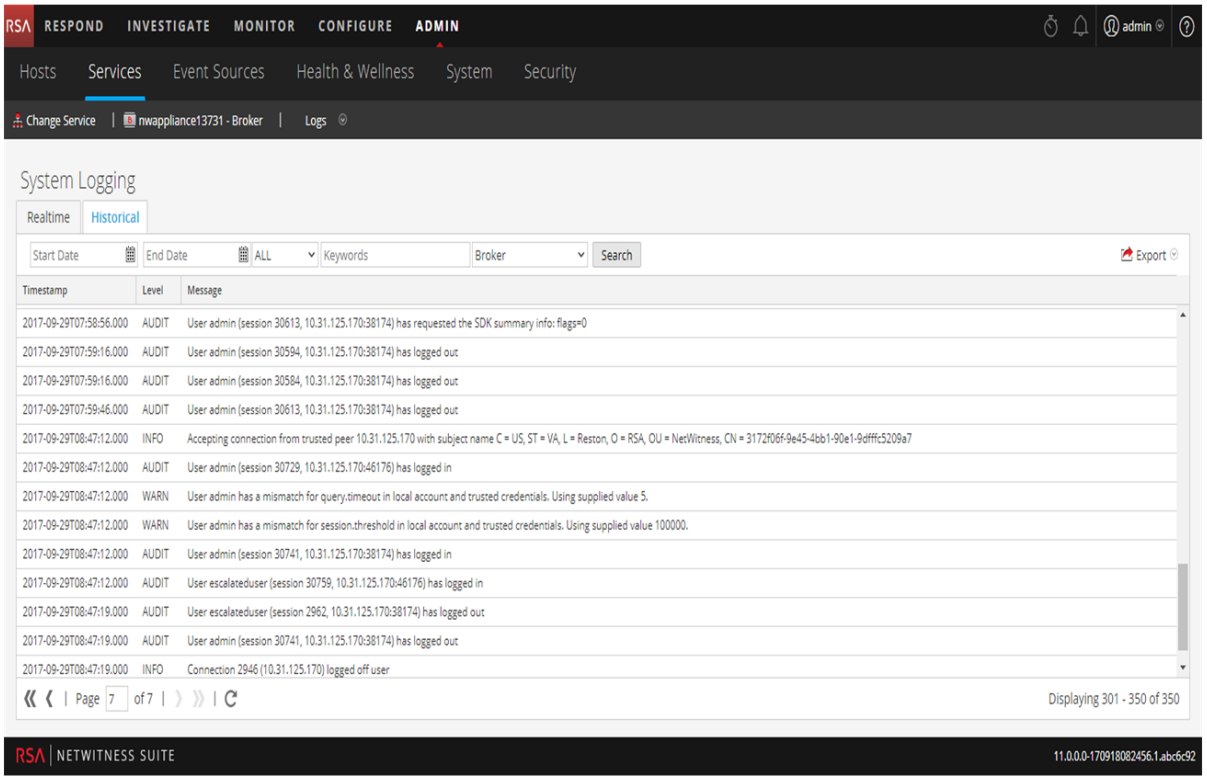
Anzeigen eines Serviceverlaufsprotokolls

So zeigen Sie das Verlaufsprotokoll für Services an:

1. Wählen Sie die Optionen **ADMINISTRATION > Services** aus.
2. Wählen Sie einen Service aus.
3. Wählen Sie in der Spalte **Aktionen** die Optionen **Ansicht > Protokolle** aus.

   Die Serviceprotokollansicht wird mit geöffneter Registerkarte Echtzeit angezeigt.
4. Klicken Sie auf die Registerkarte **Historisch**.

   Eine Liste von Verlaufsprotokollen für den ausgewählten Service wird angezeigt.



Suchen von Protokolleinträgen

So durchsuchen Sie die Ergebnisse in der Registerkarte **Verlauf**:

1. (Optional) Wählen Sie ein **Startdatum** und ein **Enddatum** aus. Wählen Sie optional eine **Startzeit** und eine **Endzeit** aus.
2. (Optional) Wählen Sie für System- und Serviceprotokolle eine **Protokollebene** und/oder ein **Schlüsselwort** aus. Systemprotokolle haben sieben Protokollebenen. Serviceprotokolle haben nur sechs Protokollebenen, da sie nicht über die Ebene **TRACE** verfügen. Der Standardwert ist **ALLE** Protokolleinträge.
3. (Optional) Wählen Sie für Serviceprotokolle den Service aus: Host oder Service.

4. Klicken Sie auf **Suchen**.

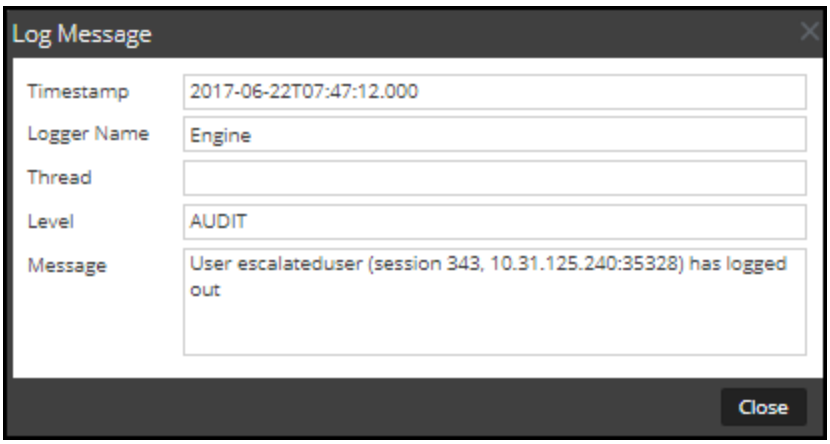
   Die Ansicht wird mit den letzten 10 Einträgen aktualisiert, die mit dem Filter übereinstimmen. Wenn neue übereinstimmende Protokolleinträge verfügbar werden, wird die Ansicht mit diesen Einträgen aktualisiert.

Anzeigen von Details zu einem Protokolleintrag

Jede Zeile des Protokollrasters auf der Registerkarte **Verlauf** bietet zusammenfassende Informationen zu einem Protokolleintrag. So zeigen Sie alle Details zu einer Protokollmeldung an:

1. Doppelklicken Sie auf einen Protokolleintrag.

   Das Dialogfeld **Protokollmeldung**, das den Zeitstempel, den Protokollierungsnamen, den Thread, die Ebene und die Meldung enthält, wird angezeigt.



2. Klicken Sie nach dem Betrachten auf **Schließen**.

   Das Dialogfeld wird geschlossen.

Blättern durch Protokolleinträge

Verwenden Sie zur Überprüfung der verschiedenen Seiten des Rasters die Seitenauswahlsteuerungen unter dem Raster wie folgt:

- Verwenden Sie die Navigationsschaltflächen.
- Geben Sie die Nummer der Seite, die Sie anzeigen möchten, manuell ein und drücken Sie die **EINGABETASTE**.

Exportieren einer Protokolldatei

So exportieren Sie die Protokolle in der aktuellen Ansicht:

Klicken Sie auf **Exportieren** und wählen Sie eine der Drop-down-Optionen aus: **CSV-Format** oder **Tabulator-Trennzeichen**.

Die Datei wird mit einem Dateinamen heruntergeladen, der den Protokolltyp und das Feldtrennzeichen ausweist. Beispiel: Ein NetWitness Suite-Systemprotokoll, das mit Komma getrennten Werten exportiert wurde, heißt **UAP_log_export_CSV.txt** und ein Hostprotokoll, das mit Tabulator getrennten Werten exportiert wurde, heißt **APPLIANCE_log_export_TAB.txt**.

Verwalten von Abfragen mithilfe der URL-Integration

Eine URL-Integration ist eine Methode zur Darstellung der Breadcrumbs oder Abfragepfade, die Sie beim aktiven Ermitteln eines Services in der Navigationsansicht nutzen. Diese Objekte müssen nicht häufig angezeigt und bearbeitet werden.

Eine URL-Integration stellt eine Zuordnung zu einer eindeutigen ID her, die automatisch erstellt wird, wenn Sie in der Navigationsansicht auf einen Navigationslink klicken, um einen Drill-down zu Daten durchzuführen. Nach Abschluss des Drill-downs gibt die URL die Abfrage-IDs des aktuellen Drill-down-Punkts an. Der angezeigte Name wird im Breadcrumb in der Navigationsansicht angezeigt.

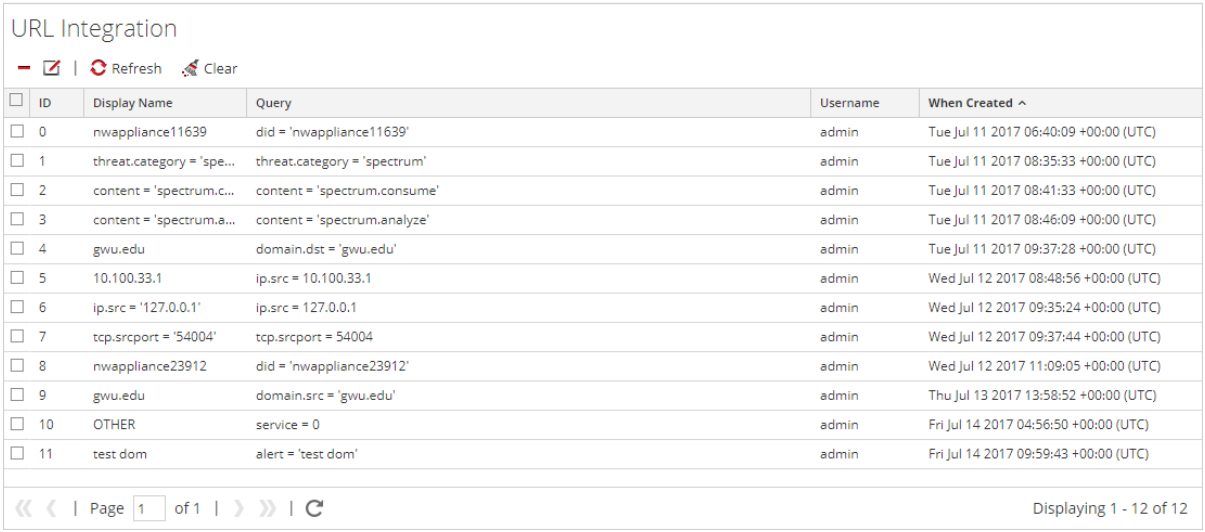
Im Bereich **URL-Integration** wird eine Liste der Abfragen angezeigt. Benutzer, die über die entsprechenden Berechtigungen verfügen, können diese zugrunde liegende Datenquelle ändern und die Abfragemuster anderer Benutzer des NetWitness Suite-Systems analysieren. In diesem Bereich können Sie:

- die Liste aktualisieren
- eine Abfrage bearbeiten
- eine Abfrage löschen
- alle Abfragen in der Liste löschen

Achtung: Nachdem eine Abfrage aus dem System entfernt wurde, werden alle Ermittlungs-URLs, die die ID dieser Abfrage enthalten, nicht länger funktionieren.

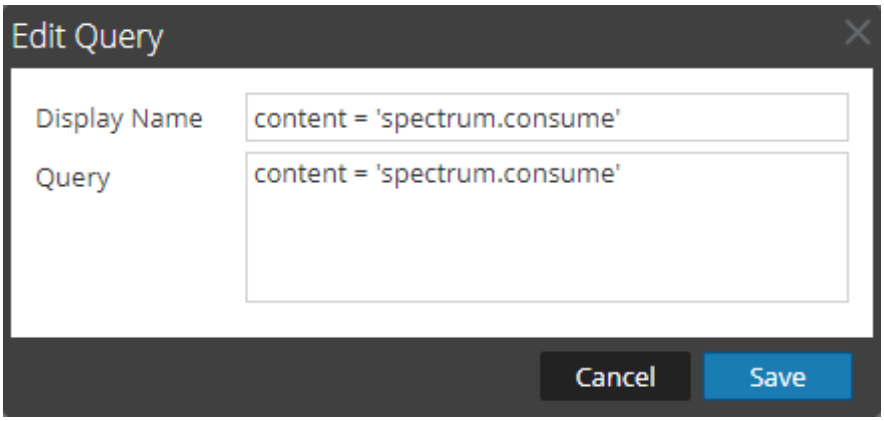
Bearbeiten einer Abfrage

1. Navigieren Sie zu **ADMINISTRATION > System**.
2. Wählen Sie im Bereich Optionen **URL-Integration** aus.



3. Wählen Sie die Zeile im Raster aus und doppelklicken Sie dann entweder auf die Zeile oder klicken Sie auf .

   Das Dialogfeld **Abfrage bearbeiten** wird angezeigt.



4. Bearbeiten Sie den **Angezeigten Namen** und die **Abfrage**, lassen Sie jedoch keines der Felder leer.
5. Klicken Sie zum Speichern der Änderungen auf **Speichern**.

Löschen einer Abfrage

Achtung: Nachdem eine Abfrage aus dem System entfernt wurde, werden alle Ermittlungs-URLs, die die ID dieser Abfrage enthalten, nicht länger funktionieren.

So entfernen Sie eine Abfrage vollständig aus NetWitness Suite:

1. Wählen Sie eine Abfrage aus.
2. Klicken Sie auf

   Mit einem Dialogfeld werden Sie aufgefordert, das Löschen der Abfrage zu bestätigen.
3. Klicken Sie auf **Yes**.

Löschen aller Abfragen

So löschen Sie alle Abfragen in der Liste:

- Klicken Sie auf 

  Die gesamte Liste wird gelöscht.

Verwenden einer Abfrage in einer URI

Die URL-Integration erleichtert Integrationen mit Produkten von Drittanbietern, da das Durchsuchen der NetWitness Suite-Architektur ermöglicht wird. Wenn Sie eine Abfrage in einer URI verwenden, können Sie ausgehend von jedem Produkt, das benutzerdefinierte Links zulässt, zu einem bestimmten Drill-down-Punkt in der Ansicht „Investigation“ in NetWitness Suite einschwenken.

Das Format zur Eingabe einer URI mithilfe einer URL-kodierten Abfrage lautet:

http://<nw host:port>/investigation/<serviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
wobei Folgendes gilt:

- **<nw host: port>** ist die IP-Adresse oder DNS, mit oder ohne einen Port, soweit anwendbar (SSL oder nicht). Diese Bezeichnung ist nur erforderlich, wenn der Zugriff über einen nicht standardmäßigen Port über einen Proxy konfiguriert ist.
- **<serviceId>** ist die interne Service-ID in der NetWitness Suite-Instanz für den abzufragenden Service. Die Service-ID kann nur als ganze Zahl repräsentiert werden. Sie können die relevante Service-ID in der URL einsehen, wenn Sie in NetWitness Suite auf die Ansicht „Investigation“ zugreifen. Dieser Wert ändert sich abhängig von dem Service, mit dem zwecks Analyse eine Verbindung hergestellt wird.
- **<encoded query>** ist die URL-kodierte NetWitness Suite-Abfrage. Die Länge der Abfrage ist durch die HTML-URL-Begrenzungen begrenzt.
- **<start date>** und **<end date>** definieren den Datumsbereich der Abfrage. Das Format lautet <jjjj-mm-tt>T<hh:mm>. Start- und Enddatum sind erforderlich. Relative

Bereiche (zum Beispiel Letzte Stunde) werden in dieser Version nicht unterstützt. Alle Zeiten werden als UTC ausgeführt.

Beispiel:
http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00/2012-10-31T00:00

Beispiele

Dies sind Abfragebeispiele, bei denen der NetWitness-Server die IP-Adresse 192.168.1.10 hat und „serviceID“ als 2 erkannt wurde.

Alle Aktivitäten am 03/12/2013 zwischen 5:00 und 6:00 Uhr mit einem registrierten Hostnamen

- Angepasster Pivot: alias.host existiert
- https://192.168.1.10/investigation/2...13-03-12T06:00

Alle Aktivitäten am 03/12/2013 zwischen 17:00 und 17:10 Uhr mit Http-Datenverkehr zu und von der IP-Adresse 10.10.10.3

- Angepasster Pivot: service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- Kodierter Pivot analysiert:
  - service=80 => service&3D80
  - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
  - https://192.168.1.10/investigation/2...13-03-12T17:10

Weitere Hinweise

Einige Werte müssen eventuell nicht als Teil der Abfrage kodiert werden. Zum Beispiel werden normalerweise die IP src und dst für diesen Integrationspunkt verwendet. Wenn zur Integration dieser Funktion eine Drittanbieter-Anwendung genutzt wird, ist es möglich, diese Werte ohne angewandte Codierung zu referenzieren.

FIPS-Unterstützung

Im Lieferumfang von NetWitness Suite 11.0 sind FIPS-validierte 140-2-Kryptomodule enthalten, die sämtliche kryptografischen Vorgänge in NetWitness Suite unterstützen. NetWitness Suite nutzt zwei Module, die eine sichere Level-3-Entwicklung unterstützen:

- RSA BSAFE Crypto-J
- OpenSSL mit BSAFE (OWB)

Beide Module wurden mit einer Betriebsumgebung zertifiziert, die mit der NetWitness Suite-Standardkonfiguration vergleichbar ist.

Standardmäßig setzen die Kryptomodule die Nutzung der FIPS-zertifizierten Cipher Suites soweit möglich durch. Ausnahmen können Sie den unten stehenden Informationen und den Versionshinweisen entnehmen. Weitere Informationen zu den FIPS-Modulen finden Sie auf der Website http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Die Nummer des RSA BSAFE Crtypo-J FIPS-Zertifikats lautet 2468. Das OWB FIPS-Zertifikat ist in der RSA BSAFE Crypto-C Micro Edition mit der Zertifikatnummer 2300 enthalten.

In Version 11.0.0.0 ist FIPS für alle Services aktiviert, mit Ausnahme von Log Collector. Dies umfasst Log Decoder und Decoder, sofern diese Services in Version 10.6.4.x für FIPS aktiviert waren. FIPS kann nicht für Services deaktiviert werden, mit Ausnahme von Log Collector, Log Decoder und Decoder.

Hinweis: Bei einer Neuinstallation von Version 11.0.0.0 werden alle Core-Services standardmäßig für FIPS durchgesetzt, außer Log Collector und Log Decoder. FIPS kann nicht für Services deaktiviert werden, mit Ausnahme von Log Collector, Log Decoder und Packet Decoder.

Hinweis: Für Upgrades von Version 10.6.4.x auf 11.0.0.0 gelten die folgenden Bedingungen für den Log Collector-, Log Decoder- und Decoder-Service:
– Log Collector wurde nach dem Upgrade auf Version 11.0.0.0 nicht für FIPS aktiviert, selbst wenn FIPS in Version 10.6.4.x aktiviert war. Sie müssen die FIPS-Unterstützung nach dem Upgrade auf Version 11.0.0.0 aktivieren. Anweisungen dazu finden Sie unter FIPS-Unterstützung für Log Collector.
– Wenn FIPS in Version 10.6.4.x für den Log Decoder- und Packet Decoder-Service aktiviert war, ist FIPS auch in Version 11.0.0.0 aktiviert. Wenn Log Decoder und Packet Decoder jedoch in Version 10.6.4.x NICHT für FIPS aktiviert war, sind diese Services auch nicht in Version 11.0.0.0 aktiviert. Sie können FIPS für diese Services gegebenenfalls manuell aktivieren. Anweisungen dazu finden Sie unter FIPS-Unterstützung für Log Decoder und Decoder.

FIPS-Unterstützung für Log Collector

So aktivieren Sie FIPS für Log Collector:

1. Beenden Sie den Log Collector-Service.
2. Öffnen Sie die Datei `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Ändern Sie den Wert der folgenden Variable zu **off**, wie hier beschrieben:
   `Environment="OWB_ALLOW_NON_FIPS=on"`
   zu
   `Environment="OWB_ALLOW_NON_FIPS=off"`
4. Laden Sie den System-Daemon neu, indem Sie den folgenden Befehl ausführen:
   `systemctl daemon-reload`
5. Starten Sie den Log Collector-Service neu.
6. Stellen Sie den FIPS-Modus für den Log Collector-Service in der Benutzeroberfläche ein:

   Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie ein Upgrade von Version 10.6.4 auf 11.0.0.0 durchführen und FIPS in Version 10.6.4 aktiviert war.

   a. Navigieren Sie zu **ADMINISTRATION** > **Services**.
   b. Wählen Sie den Log Collector-Service aus und navigieren Sie zu **Ansicht** > **Konfiguration**.
   c. Aktivieren Sie im SSL FIPS-Modus das Kontrollkästchen im Bereich „Konfigurationswert“ und klicken Sie auf **Anwenden**.

FIPS-Unterstützung für Log Decoder und Decoder

So aktivieren Sie FIPS für Log Decoder und Decoder, für die FIPS in Version 10.6.4.x nicht aktiviert war:

1. Navigieren Sie zu **ADMINISTRATION** > **Services** und wählen Sie einen Log Decoder- oder Packet Decoder-Service aus.
2. Wählen Sie **Ansicht** > **Konfiguration** aus und aktivieren Sie im Bereich **Systemkonfiguration** die Option **SSL FIPS-Modus**, indem Sie in der Spalte **Konfigurationswert** das Kontrollkästchen aktivieren.
3. Starten Sie den Service neu.
4. Klicken Sie auf **Anwenden**.

Troubleshooting der NetWitness-Suite

Weitere Informationen über das Troubleshooting der NetWitness Suite finden Sie in den folgenden Themen:

Debugging-Informationen

NetWitness Suite-Protokolldateien

Die folgenden Dateien enthalten NetWitness Suite-Protokollinformationen.

Komponente	Datei
rabbitmq	/var/log/rabbitmq/nw@localhost.log /var/log/rabbitmq/nw@localhost-sasl.log
collectd	/var/log/messages
nwlogcollector	/var/log/messages
nwlogdecoder	/var/log/messages
sms	/opt/rsa/sms/wrapper.log
sms	/opt/rsa/sms/logs/sms.log
sms	/opt/rsa/sms/logs/audit/audit.log
NetWitness Suite	/var/lib/netwitness/uax/logs/nw.log
NetWitness Suite	/var/lib/netwitness/uax/logs/ audit/audit.log
NetWitness Suite	/opt/rsa/jetty9/logs

Interessierende Dateien

Die folgenden Dateien werden in wichtigen NetWitness Suite-Komponenten verwendet und können beim Eingrenzen verschiedener Probleme hilfreich sein.

Komponente	Datei	Beschreibung
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQ-Konfigurationsdatei. Diese Konfigurationsdatei steuert teilweise das Verhalten von RabbitMQ, insbesondere bezüglich Netzwerk-/SSL-Einstellungen.
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQ-Umgebungskonfigurationsdatei. In dieser Datei sind Name und Speicherort des RabbitMQ-Node der aktivierten Plug-in-Datei spezifiziert.
rabbit	/etc/rabbitmq/rsa_enabled_plugins	In dieser Datei ist die Liste aktivierter Plug-ins in RabbitMQ spezifiziert. Diese Datei wird vom RabbitMQ-Server über den Befehl „rabbitmq-plugins“ gemanagt. Die Datei überschreibt den Pfad „/etc/rabbitmq/enabled_plugins“, um Probleme beim Upgrade des Log Collector von früheren Versionen zu umgehen.

Komponente	Datei	Beschreibung
rabbit	/etc/rabbitmq/ssl/truststore.pem	Der RabbitMQ-Truststore. Diese Datei enthält eine Folge von PEM-kodierten X.509-Zertifikaten von vertrauenswürdigen Zertifizierungsstellen. Alle Clients, die eine Verbindung zu RabbitMQ herstellen und ein von einer Zertifizierungsstellen in dieser Liste signiertes Zertifikat vorlegen, werden als vertrauenswürdiger Client eingestuft.

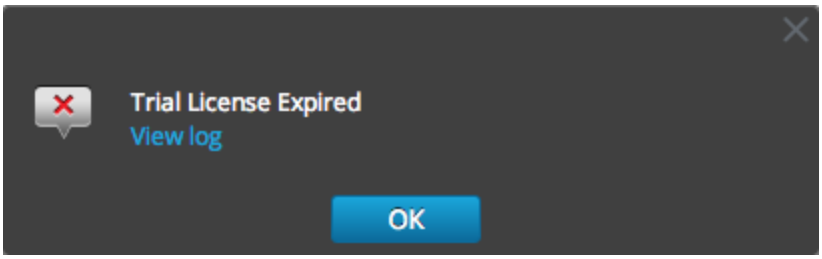
Komponente	Datei	Beschreibung
rabbit	/var/log/rabbitmq/mnesia/nw@localhost	Das RabbitMQ Mnesia-Verzeichnis. Mnesia ist die Erlang-/OTP-Datenbanktechnologie für die persistente Speicherung von Erlang-Objekten. RabbitMQ verwendet diese Technologie zum Speichern von Informationen wie dem aktuellen Policy-Satz, persistenten Austauschvorgängen und Warteschlangen usw. Wichtig ist, dass die Verzeichnisse msg_store_ persistent und msg_store_ transient sich dort befinden, wo RabbitMQ Meldungen speichert, die auf Festplatte gespoolt werden, z. B. wenn Meldungen als persistente Meldung weitergeleitet werden oder aufgrund von Speicherbeschränkungen auf Festplatte ausgelagert wurden. Beobachten Sie dieses Verzeichnis genau, wenn die Festplatten- oder Speicherwarnmeldungen in RabbitMQ ausgelöst wurden. **Achtung:** Löschen Sie diese

Komponente	Datei	Beschreibung
		Dateien nicht manuell. Verwenden Sie RabbitMQ-Tools, um Warteschlangen zu leeren oder zu löschen. Durch das manuelle Ändern dieser Dateien kann die Ausführung der RabbitMQ-Instanz unmöglich werden.

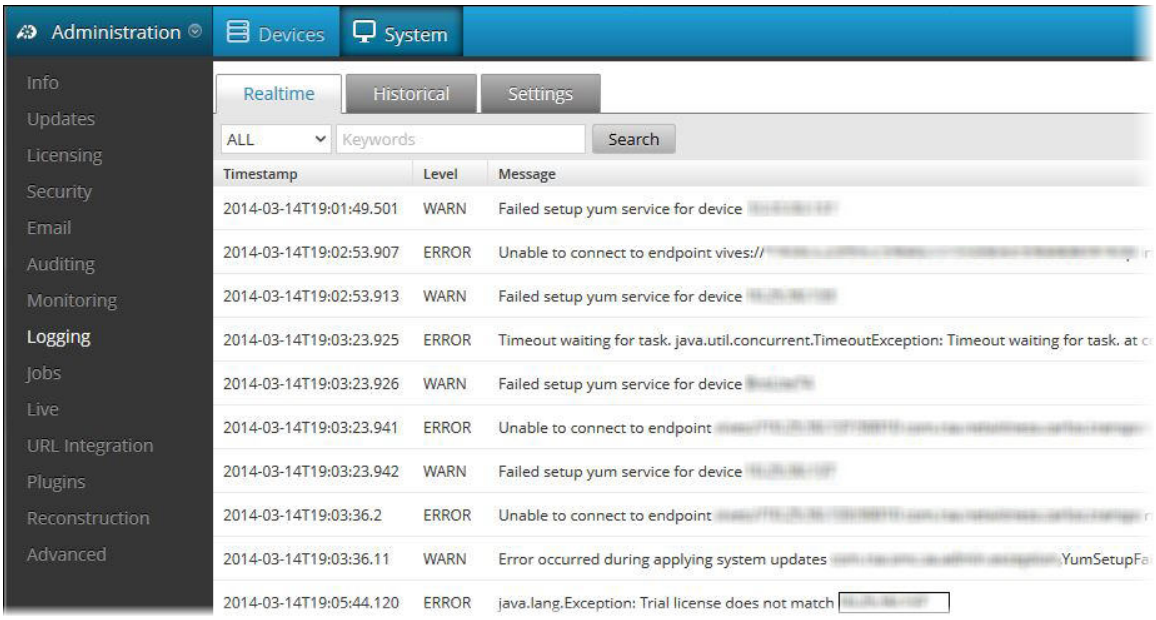
Fehlerbenachrichtigung

In NetWitness Suite sind verschiedene Arten von Fehlermeldungen unterschiedlichen Komponenten und Operationen zugeordnet. Die Rückmeldung von NetWitness Suite erfolgt in Form einer einfachen Fehlermeldung sowie eines Protokolleintrags.

Wenn ein Fehlermeldungsdialog angezeigt wird, haben Sie zwei Möglichkeiten: Bestätigen Sie die Meldung oder sehen Sie sich das Systemprotokoll an, um weitere Informationen zu erhalten.



Wenn Sie weitere Informationen zu einer Fehlermeldung im Systemprotokoll einsehen möchten, klicken Sie auf **Protokoll anzeigen**. Das Protokoll wird in der Ansicht **Administration** > **System** geöffnet und enthält eine Liste der Meldungen. Dazu werden Zeitstempel und Stufe der Meldung angegeben.



Verschiedene Tipps

Sicherheitsverstärkung für das Admin-Konto

Weitere Informationen hierzu finden Sie im Leitfaden zur STIG-Sicherheitsverstärkung in der NetWitness Suite-Dokumentation auf RSA Link (https://community.rsa.com/docs/DOC-64211).

Auditprotokollmeldungen

Es kann hilfreich sein, zu prüfen, welche Benutzeraktionen zu welchem Protokollmeldungstyp in der Datei **/var/log/messages** führt.

Im Arbeitsblatt mit Ereigniskategorien, das im Protokollparserpaket im Archiv der Datei „NetWitness Suite Parser v2.0.zip“ enthalten ist, sind die Ereigniskategorien und Ereignisparserzeilen aufgelistet, um Sie bei der Erstellung von Berichten, Warnmeldungen und Abfragen zu unterstützen.

NwConsole für "Integrität und Zustand"

RSA hat eine Befehlsoption mit der Bezeichnung **logParse** zu **NwConsole** hinzugefügt. Die neue Befehlsoption unterstützt das Protokollparsing, eine praktische Methode zur Überprüfung der Protokollparser, ohne das gesamte System für Protokollparsing einzurichten. Um weitere Informationen zum Befehl **logParse** zu erhalten, geben Sie in die Befehlszeile den Befehl `help logParse` ein.

Thick-Clientfehler: Remoteinhaltsgeräte-Eintrag nicht gefunden

Fehler: Für eine auf einen Concentrator angewendete Korrelationsregel wird *„Der Remoteinhaltsgeräte-Eintrag wurde nicht gefunden“* ausgegeben.

Problem: Wenn Sie in Investigation im Warnmeldungs-Metaschlüssel auf den Metawert `correlation-rule-name` klicken, werden keine Sitzungsinformationen angezeigt.

Lösung: Verwenden Sie auf Decodern und Concentrators ESA-Regeln statt Korrelationsregeln. Die ESA-Regeln zeichnen die Korellationssitzungen auf, die der ESA-Regel entsprechen.

Anzeigen von Beispielparsern

Da Flex- und Lua-Parser verschlüsselt sind, wenn Sie von Live bereitgestellt werden, können Sie deren Inhalt nicht leicht einsehen.

Es sind jedoch einige Beispiele in Klartext unter folgender URL verfügbar: **https://community.emc.com/docs/DOC-41108**.

Konfigurieren von WinRM-Ereignisquellen

Der folgende Inside EMC-Artikel enthält ein Video, das Sie durch den Einrichtungsprozess der Windows RM-Sammlung (Remote Management) führt: **https://inside.emc.com/docs/DOC-122732**.

Darüber hinaus enthält er zwei Skripte zur beschleunigten Durchführung der im „Konfigurationsleitfaden für Windows-Ereignisquellen“ beschriebenen Verfahren.

NwLogPlayer

Bei NwLogPlayer handelt es sich um ein Dienstprogramm, das syslog-Datenverkehr simuliert. In der gehosteten Umgebung ist `NwLogPlayer.exe` ein Befehlszeilendienstprogramm auf dem RSA NetWitness® Suite-Clientcomputer und befindet sich im folgenden Verzeichnis:

```
C:\Program Files\NetWitness\NetWitness 9.8
```

NwLogPlayer befindet sich außerdem auf dem Log Decoder-Host im Verzeichnis `/usr/bin`.

Nutzung

Geben Sie in der Befehlszeile `nwlogplayer.exe -h` ein, um die verfügbaren Optionen wie hier reproduziert aufzulisten:

`--priority arg`	set log priority level
`-h [ --help ]`	show this message

`-f [ --file ] arg (=stdin)`	input message; defaults to **stdin**
`-d [dir ] arg`	input directory
`-s [ --server ] arg (=localhost)`	remote server; defaults to **localhost**
`-p [ --port ] arg (=514)`	remote port; defaults to **514**
`-r [ --raw ] arg (=0)`	Determines raw mode. • 0 = add priority mark (default) • 1= File contents will be copied line by line to the server. • 3 = auto detect • 4 = enVision stream • 5 = binary object
`-m [ --memory ] arg`	Speed test mode. Read up to 1 Megabyte of messages from the file content and replays.
`--rate arg`	Number of events per second. This argument has no effect if **rate** > eps that the program can achieve in continuous mode.
`--maxcnt arg`	maximum number of messages to be sent
`-c [ --multiconn ]`	multiple connection
`-t [ --time ] arg`	simulate time stamp time; format is `yyyy-m-d-hh:mm:ss`
`-v [ --verbose ]`	If **true**, output is verbose
`--ip arg`	simulate an IP tag
`--ssl`	use SSL to connect
`--certdir arg`	OpenSSL certificate authority directory
`--clientcert arg`	use this PEM-encoded SSL client certificate
`--udp`	send in UDP

Troubleshooting bei Feeds

Überblick

Der Zweck des Feedgenerators ist das Erzeugen der Zuordnung einer Ereignisquelle zu einer Gruppenliste, zu der sie gehört.

Wenn es eine Ereignisquelle gibt, aus der Sie Meldungen sammeln, und diese nicht in den korrekten Ereignisquellengruppen angezeigt wird, dann finden Sie in diesem Thema Hintergründe und Informationen, die Ihnen helfen, das Problem zu identifizieren.

Details

Der ESM-Feed ordnet mehrere Schlüssel einem einzigen Wert zu. Er ordnet die Attribute DeviceAddress, Forwarder und DeviceType dem Wert groupName zu.

Der Zweck des ESM-Feeds ist es, die Ereignisquellen-Metadaten mit dem auf dem Log Decoder gesammelten groupName zu versehen.

Funktionsweise

Der Feedgenerator wird planmäßig jede Minute aktualisiert. Er wird jedoch nur ausgelöst, wenn Änderungen (Erstellen, Aktualisieren oder Löschen) in Ereignisquellen oder -gruppen auftreten.

Er erzeugt eine einzige Feeddatei mit Zuordnungen von Ereignisquellen zu Gruppen und verteilt denselben Feed an alle Log Decoder, die mit NetWitness Suite verbunden sind.

Nachdem die Feeddatei auf die Log Decoders hochgeladen wurde, wird den Metadaten für jedes neue Ereignis der groupName hinzugefügt und dieser groupName wird an logstats angehängt.

Sobald der „groupName“ in logstats enthalten ist, gruppiert der ESM-Aggregator Informationen und sendet Sie an ESM. Zu diesem Zeitpunkt sollte in der Registerkarte **Ereignisquellenüberwachung** die Spalte **Gruppenname** angezeigt werden.

Der gesamte Vorgang kann einige Zeit in Anspruch nehmen. Daher kann es nach dem Hinzufügen einer Gruppe oder einer Ereignisquelle einige Sekunden dauern, bevor der Gruppenname angezeigt wird.

Hinweis: Wird das Attribut für die Ereignisquellentyp geändert, wenn der Feed aktualisiert wird, fügt NetWitness Suite einen neuen Eintrag in der „logstats“-Datei hinzu, statt den vorhandenen Eintrag zu ändern. Daher existieren in logdecoder zwei verschiedenen logstats-Einträge. Zuvor vorhandene Meldungen werden unter dem vorherigen Typ aufgeführt und alle neuen Meldungen werden für den neuen Ereignisquellentyp protokolliert.

Feeddatei

Die Feeddatei ist wie folgt formatiert:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

`DeviceAddress` ist entweder `ipv4, ipv6` oder `hostname`, je nachdem, welcher Typ für die Ereignisquelle definiert wurde.

Im Folgenden ist ein Beispiel der Feeddatei dargestellt:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apachegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"

"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","Apache
grp"
```

Troubleshooting

Sie können die folgenden Elemente überprüfen, um einzugrenzen, wo das Problem auftritt.

Vorhandene Feeddatei

Vergewissern Sie sich, dass das Feed-ZIP-Archiv an folgendem Speicherort vorhanden ist:
`/opt/rsa/sms/esmfeed.zip`

Ändern Sie diese Datei nicht.

Gruppenmetadaten auf LD ausgefüllt

Überprüfen Sie, ob die Gruppenmetadaten auf dem Log Decoder ausgefüllt sind. Navigieren Sie zum Log Decoder-REST und überprüfen Sie die logstats-Datei:

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

Die ist ein Beispiel für eine logstats-Datei mit Gruppeninformationen:

```
device=apache  forwarder=NWAPPLIANCE10304  source=1.2.3.4  count=338
lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat  forwarder=NWAPPLIANCE10304  source=5.6.7.8
count=1301  lastSeenTime=2015-Feb-04 22:30:19  lastUpdatedTime=2015-Feb-
04 22:30:19  groups=AllOtherGroup,ApacheTomcatGroup
```

Im Text oben sind die Gruppeninformationen **fett** gedruckt.

Gerätegruppenmetadaten auf dem Concentrator

Vergewissern Sie sich, dass der Metawert **Gerätegruppe** auf dem Concentrator vorhanden ist und dass die Ereignisse Werte für das Feld `device.group` aufweisen.

SMS-Protokolldatei

Überprüfen Sie die SMS-Protokolldatei an dem folgenden Speicherort, um Informations- und Fehlermeldungen anzuzeigen: `/opt/rsa/sms/logs/sms.log`

Im Folgenden finden Sie Beispiele für Informationsmeldungen:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

Im Folgenden finden Sie Beispiele für Fehlermeldungen:

```
Error creating CSV File : <reason>Unable to push the ESM Feed: Unable to
create feed zip archive.
```

```
Failed to add Group in CSV: GroupName: <groupName> : Error: <error>
Unable to push the ESM Feed: CSV file is empty, make sure you have al-
least on group with al-least one eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on LogDecoder-
<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error: The zip
archive "/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not be
opened
Unable to push the ESM Feed: <reason>
```

Überprüfen, ob logstats-Daten von ESMReader und ESMAggregator gelesen und weitergeleitet werden

Diese Schritte dienen der Überprüfung, ob die logstats-Daten von **collectd** gesammelt und an das Ereignisquellenmanagement weitergeleitet werden.

ESMReader

1. Fügen Sie auf den Log Decodern den Flag **debug "true"** in die Datei **/etc/collectd.d/NwLogDecoder_ESM.conf** ein:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>        </stats>    </Module>    <Module
"NgEsmReader" "update">        port      "56002"
        ssl       "yes"
```

```
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>        </stats>    </Module></Plugin>
```

2. Führen Sie den Befehl
   `collectd service restart` aus.
3. Führen Sie den folgenden Befehl aus:
   `tail –f /var/log/messages | grep collectd`
   Vergewissern Sie sich, dass ESMReader die „logstats“ liest und keine Fehler vorhanden sind. Wenn Probleme beim Lesen vorliegen, werden Fehlermeldungen ähnlich der folgenden angezeigt:

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. Kommentieren Sie in NetWitness Suite das Flag „verbose“ in **/etc/collectd.d/ESMAggregator.conf** aus:

```
        # ESMAggregator module collectd.conf configuration file
        #
        # Copyright (c) 2014 RSA The Security Divsion of EMC
        #

        <Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"

        <Module "ESMAggregator">
                verbose 1
                interval "60"
                cache_save_interval "600"
```

```
                persistence_dir "/var/lib/netwitness/collectd"
        </Module>    </Plugin>
```

2. Führen Sie folgenden Befehl aus:
   `collectd service restart`.
3. Führen Sie den folgenden
   -Befehl aus:`run "tail -f /var/log/messages | grep ESMA`
   Suchen Sie nach ESMAggregator-Daten und stellen Sie sicher, dass Ihr „logstats"-Eintrag in Protokollen verfügbar ist.

Beispielausgabe:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
```

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Konfigurieren des Jobintervalls des JMX-Feedgenerators

Obwohl der Feedgeneratorjob so geplant ist, dass er standardmäßig jede Minute ausgeführt wird, können Sie dies bei Bedarf mit `jconsole` ändern.

So ändern Sie das Jobintervall des Feedgenerators:

1. Öffnen Sie **jconsole** für den SMS-Service.
2. Navigieren Sie in der Registerkarte „MBeans“ zu **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attribute**.
3. Ändern Sie den Wert für die Eigenschaft **FeedGeneratorJobIntervalInMinutes**.
4. Wechseln Sie in derselben Navigationsstruktur zu **Vorgänge** und klicken Sie auf **commit()**. Dadurch wird der neue Wert in der zugehörigen json-Datei unter **/opt/rsa/sms/conf** persistent und der Wert wird verwendet, wenn SMS neu gestartet wird.

Durch das Festlegen eines neuen Wertes wir der Feedgeneratorjob auf das neue Intervall umgeplant.

Referenzen

Dieser Abschnitt beschreibt die Ansichten der NetWitness Suite-Benutzeroberfläche, in der Sie Systemwartungsaufgaben durchführen können. Sie können diese Benutzeroberfläche für folgende Aufgaben verwenden:

- Überwachen und Verwalten von Services (Einstellungen, Statistiken, Befehls- und Nachrichtensyntax, REST API, RSA-Konsolendienstprogramm und die in NetWitness Suite unterstützten Protokolle).
- Anzeigen der aktuellen NetWitness Suite-Version und des Lizenzstatus.
- Managen Ihres lokalen Update-Repository, aus dem Sie Softwareversionsaktualisierungen auf Hosts anwenden.

Die folgenden Themen beschreiben jede Schnittstelle im Detail:

- Ansicht „Integrität und Zustand“
- Ansicht „System“ – Bereich „Systeminfo“

Ansicht „Integrität und Zustand“

Mithilfe der Einstellungen für Integrität und Zustand können Sie Alarme einstellen und anzeigen, Ereignisse überwachen und Policies und Systemstatistiken anzeigen. Weitere Informationen über jedes dieser Themen finden Sie unter:

- Ansicht „Integrität und Zustand“ – Ansicht „Alarme“
- Ansicht „Ereignisquellenüberwachung“
- Verlaufsdiagramme für „Integrität und Zustand“
- Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Archiver
- Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Ereignisquellen
- Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Warehouse Connector
- Ansicht „Überwachung“
- Ansicht „Richtlinien“
- Ansicht „Systemstatistikbrowser“

Ansicht „Integrität und Zustand“ – Ansicht „Alarme“

Sie können Hosts und Services überwachen, um zu bestimmen, wann benutzerdefinierte Grenzwerte erreicht wurden, indem Sie alle aktiven Alarme anzeigen. Die Alarme werden durch Richtlinienregeln ausgelöst, die Sie in der **Registerkarte „Richtlinien“** definieren bzw. den Hosts und Services zuordnen. Sie können:

- alle Alarme anzeigen, die derzeit für all Ihre Systeme und Services aktiv sind
- einen Alarm auswählen und die entsprechenden Details anzeigen

Was möchten Sie tun?

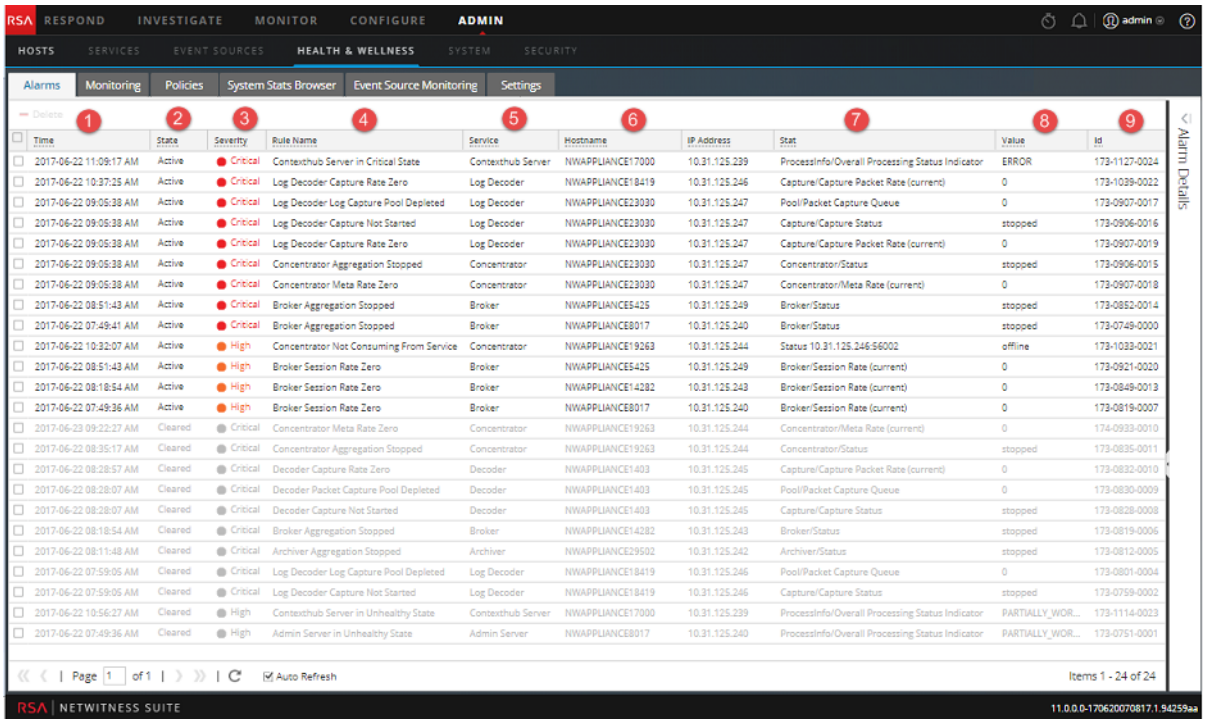
Rolle	Ziel	Details anzeigen
Administrator	Anzeigen des Alarmstatus von NetWitness-Servers und Services	Überwachen von Alarmen
Administrator	Anzeigen detaillierter Informationen über einen bestimmte Alarm	Überwachen von Alarmen

Verwandte Themen

Richtlinien managen

Überblick

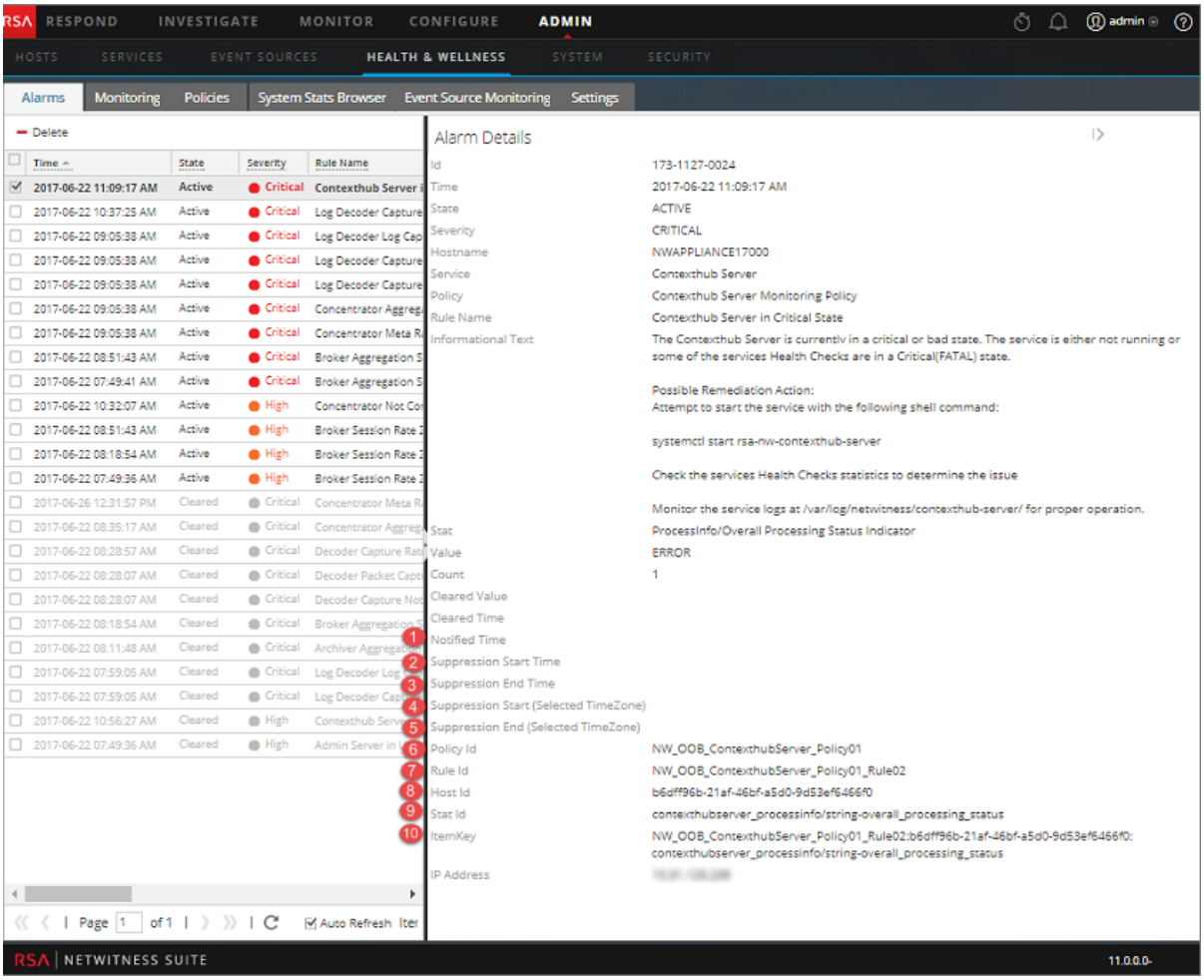
Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist **Services managen**. Navigieren Sie zu **Admin** > **Integrität und Zustand**, um auf die Ansicht „Alarme“ zuzugreifen. Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt. Die Registerkarte „Alarme“ enthält eine Liste der Alarme sowie den Bereich „Alarmattribute“.



1	Der Zeitpunkt, zu dem der Alarm ausgelöst wurde.
2	Der Status des Alarms: • **Aktiv**: Der Statistikschwellenwert wurde überschritten, wodurch der Alarm ausgelöst wurde. • **Gelöscht**: Der Löschschwellenwert wurde überschritten und der Alarm deaktiviert.
3	Der Schweregrad, der diesem Alarm zugeordnet wurde: • **Kritisch** • **High** • **Mittel** • **Niedrig**
4	Der Name der Regel, die den Alarm ausgelöst hat.
5	Der in der Regel definierte Service.
6	Der Host, auf dem der Alarm ausgelöst wird.
7	Die ausgewählte Statistik in der Regel, die den Alarm ausgelöst hat.
8	Der Statistikwert, der den Alarm ausgelöst hat.
9	Die ID-Nummer des Alarms.

Hinweis: NetWitness Suite sortiert die Alarme in zeitlicher Reihenfolge. Sie können die relevanten Parameter in auf- oder absteigender Reihenfolge sortieren.

Diese Abbildung zeigt die Registerkarte „Alarme“ mit eingeblendetem Bereich „Alarmattribute“.



Bereich „Alarmattribute“

Im Bereich „Alarmattribute“ werden Informationen über den in der Liste der Alarme ausgewählten Alarm angezeigt. Er enthält alle Informationen in der Liste der Alarme sowie die folgenden Felder.

1	Benachrichtigungszeitpunkt des Alarms
2	Startzeit für Unterdrückung
3	Endzeit für Unterdrückung
4	Start der Unterdrückung (ausgewählte Zeitzone)
5	Ende der Unterdrückung (ausgewählte Zeitzone)

6	Die Richtlinien-ID
7	Die Regel-ID
8	Die Host-ID
9	Die Statistik-ID
10	Elementschlüssel

Ansicht „Ereignisquellenüberwachung“

Hinweis: Informationen über das Management von Ereignisquellen erhalten Sie unter „Informationen über Ereignisquellenmanagement“ im *NetWitness Suite Leitfaden für das Ereignisquellenmanagement*.

NetWitness Suite bietet die Möglichkeit, die Statistiken für die verschiedenen Ereignisquellen in der Benutzeroberfläche überwachen. Die angezeigten Informationen sind Verlaufsdaten und stammen aus Log Decoder. Die Ansicht kann angepasst werden, indem Parameter zum Filtern der Daten ausgewählt werden.

So greifen Sie auf die Ansicht „Ereignisquellenüberwachung“ zu:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Klicken Sie auf **Ereignisquellenüberwachung**.

Was möchten Sie tun?

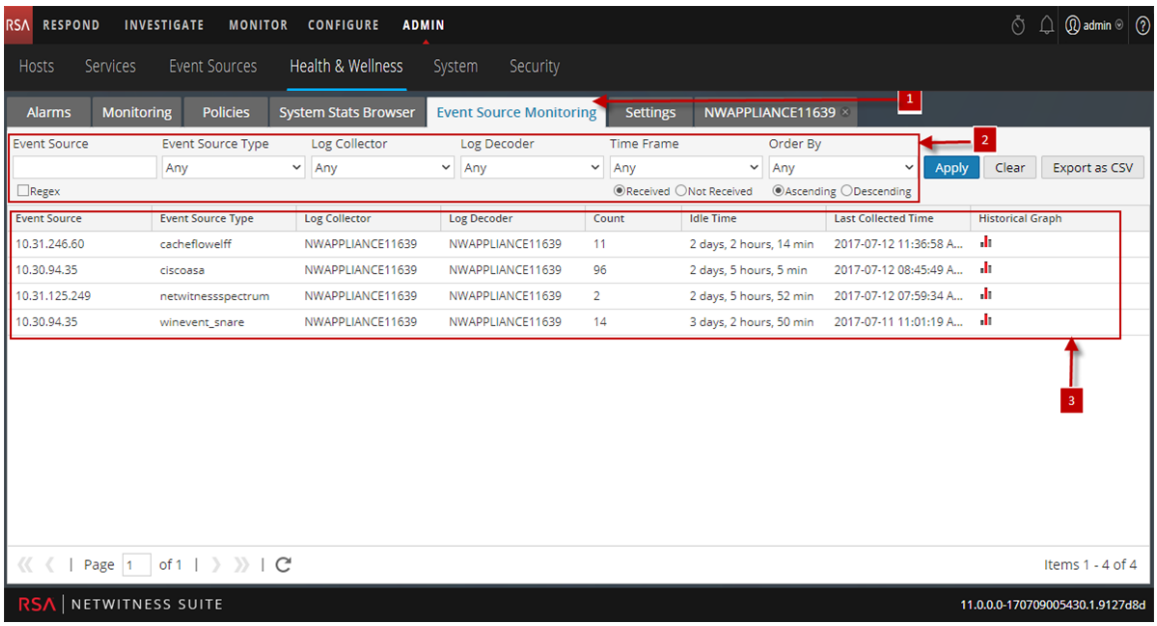
Rolle	Ziel	Details anzeigen
Administrator	Anzeigen der aus einer Ereignisquelle erfassten Ereignisse	Verlaufsdiagrammansicht für erfasste Ereignisse aus einer Ereignisquelle

Verwandte Themen

- Überwachen von Ereignisquellen
- Filtern von Ereignisquellen
- Anzeigen eines Verlaufsdiagramms für die für eine Ereignisquelle erfassten Ereignisse

Überblick

Die Ansicht Ereignisquellenüberwachung wird angezeigt.



1. Zeigt die Registerkarte „Ereignisquellenüberwachung“ an.
2. Symbolleiste zum Filtern und Anpassen der Registerkarte „Ereignisquellenüberwachung“.
3. Zeigt den Bereich „Ereignisquellendaten“ an.

Filter

Diese Tabelle enthält die verschiedenen Parameter, mit denen Sie die Ansicht „Ereignisquellenüberwachung“ filtern und anpassen können.

Parameter	Beschreibung
Ereignisquelle	Geben Sie den Namen der Ereignisquelle ein, die Sie überwachen möchten. Wählen Sie Regex aus, um den Regex-Filter zu aktivieren. Der Text wird nach einem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Wenn „Regex“ nicht ausgewählt ist, wird Globbing per Musterzuordnung unterstützt.
Ereignisquelltyp	Wählen Sie einen Ereignisquelltyp für die ausgewählte Ereignisquelle aus.
Log Collector	Wählen Sie die Protokollsammlung aus, um die Daten anzuzeigen, die von der angegebenen Protokollsammlung gesammelt wurden.
Log Decoder	Wählen Sie einen Log Decoder aus, um die Daten anzuzeigen, die vom angegebenen Log Decoder gesammelt wurden.

Parameter	Beschreibung
Zeitrahmen	Wählen Sie den Zeitraum aus, für den die Daten angezeigt werden sollen. Wählen Sie die Option **Empfangen** aus, wenn die Abfrageergebnisse nur die Ereignisquellen enthalten sollen, für die Protokolle im ausgewählten Zeitraum empfangen wurden. oder Wählen Sie die Option **Nicht empfangen** aus, wenn die Abfrageergebnisse nur die Ereignisquellen enthalten sollen, für die im ausgewählten Zeitraum keine Protokolle empfangen wurden.
Sortieren nach	Wählen Sie die Reihenfolge aus, in der die Liste gefiltert werden muss. Wählen Sie die Option „Aufsteigend“ aus, wenn die Liste in aufsteigender Reihenfolge sortiert werden soll.
Anwenden	Klicken Sie hierauf, um die ausgewählten Filter anzuwenden und die Liste entsprechend anzuzeigen.
Clear	Klicken Sie hierauf, um die ausgewählten Filter zu löschen.
Als CSV-Datei exportieren	Klicken Sie hierauf, um die Informationen als CSV-Datei zu exportieren.

Anzeige der Ereignisquellendaten

Parameter	Beschreibung
Ereignisquelle	Zeigt den Namen der Ereignisquelle an.
Ereignisquelltyp	Zeigt den Ereignisquelltyp an.
Log Collector	Zeigt die Protokollsammlung an, von der die Ereignisse ursprünglich erfasst wurden.
Log Decoder	Zeigt den Log Decoder an, über den die Ereignisse verarbeitet werden.
Count	Zeigt die Anzahl der Ereignisse an, die seit der letzten Zurücksetzung des Anzahlwerts von Log Decoder empfangen wurden.

Parameter	Beschreibung
Inaktivitätsdauer	Zeigt an, wie viel Zeit seit der letzten Datenerfassung verstrichen ist.
Letzte Sammlungszeit	Zeigt die Zeit an, zu der Log Decoder zuletzt ein Ereignis für die Ereignisquelle verarbeitet hat.
Verlaufsdiagramm	Klicken Sie auf , um das Verlaufsdiagramm mit den Daten anzuzeigen, die für die Ereignisquelle gesammelt wurden.

Verlaufsdiagramme für „Integrität und Zustand“

Durch Konfigurieren der Archiver-Überwachung können Sie automatisch Benachrichtigungen erzeugen, wenn kritische Schwellenwerte bezüglich der Aggregation und des Speichers von Archiver erreicht wurden. Die Ansicht „Verlaufsdiagramm“ bietet eine visuelle Darstellung von Verlaufsdaten.

Weitere Details finden Sie in den folgenden Themen:

- Verlaufsdiagrammansicht für erfasste Ereignisse aus einer Ereignisquelle
- Verlaufsdiagramm für Systemstatistiken

Verlaufsdiagrammansicht für erfasste Ereignisse aus einer Ereignisquelle

Die Ansicht „Verlaufsdiagramme“ für Ereignisse, die aus einer Ereignisquelle gesammelt wurden, bietet eine visuelle Darstellung von Verlaufsdaten. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.

   Die Ansicht Integrität und Zustand wird mit geöffneter Registerkarte Überwachung angezeigt.

2. Klicken Sie auf **Ereignisquellenüberwachung**.

   Die Ansicht Ereignisquellenüberwachung wird angezeigt.

3. Wählen Sie in der Spalte **Verlaufsdiagramm** aus.

   Das Verlaufsdiagramm des ausgewählten Ereignisquellentyps wird in einem Pop-up-Fenster angezeigt.

   In der Abbildung werden die aus dem Ereignisquellentyp **winevent_snare** gesammelten

Ereignisse angezeigt.

Sie können das Diagramm wie gewünscht anpassen. Die Tabelle zeigt die verschiedenen Parameter, mit denen das Verlaufsdiagramm angepasst werden kann.

Parameter	Beschreibung
Zeitrahmen	Wählen Sie den Zeitrahmen aus, dessen Verlaufsdaten Sie anzeigen möchten. Folgende Optionen sind verfügbar: Aktueller Tag, Aktuelle Woche, Aktueller Monat.
Von <Datum> bis <Datum>	Wählen Sie den Datumsbereich aus, dessen Verlaufsdaten Sie anzeigen möchten.

Wenn Sie sich die Daten im Verlaufsdiagramm genauer anschauen möchten, können Sie Vergrößerungsfunktionen verwenden.

Vergrößerungsfunktion 1 und 2

Sie können einen der Werte auswählen, um die Verlaufsdaten für den ausgewählten Wert anzuzeigen. Die Abbildung unten zeigt ein Beispiel für einen 6-stündigen Zeitraum, der für die Vergrößerung ausgewählt wurde. Der Schieberegler unten rechts wird auch an das 6-stündige Zeitfenster angepasst.

Alternativ können Sie den Schieberegler rechts unten bewegen, um die Ansicht eines bestimmten Zeitraums zu vergrößern.

Vergrößerungsfunktion 3

Sie können im Plotbereich auch auf eine Zeit klicken und mit der Maus ziehen, um die Ansicht eines bestimmten Zeitraums zu vergrößern.

Verlaufsdiagramm für Systemstatistiken

So greifen Sie auf das Verlaufsdiagramm für die Systemstatistiken zu:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.

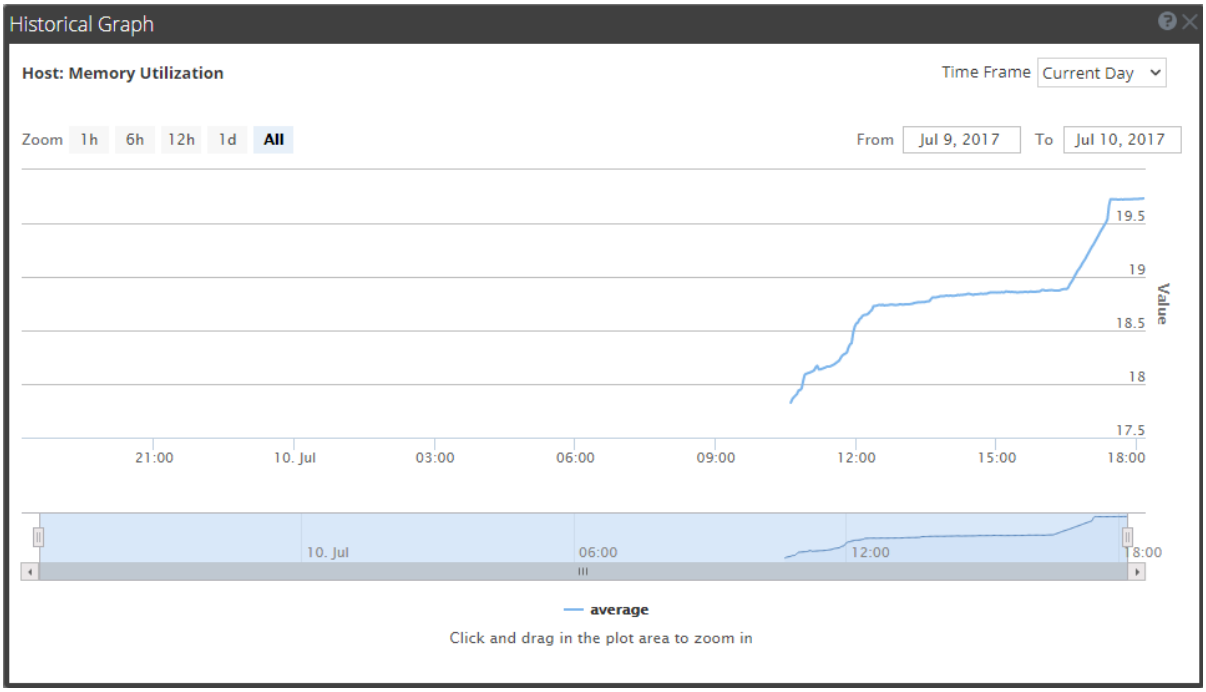
2. Klicken Sie auf die Registerkarte **Systemstatistikbrowser**.

   Die Registerkarte Systemstatistikbrowser wird angezeigt.

3. Wählen Sie in der Spalte **Verlaufsdiagramm** aus.

   Das Verlaufsdiagramm mit der ausgewählten Statistik für einen Host wird angezeigt.

   In der Abbildung wird die Ansicht „Systemstatistiken“ für die Nutzungsstatistiken des Arbeitsspeichers angezeigt.



Parameter

Sie können die Diagrammansicht wie gewünscht anpassen. Die Tabelle zeigt die verschiedenen Parameter, mit denen die Verlaufsdiagrammansicht angepasst werden kann.

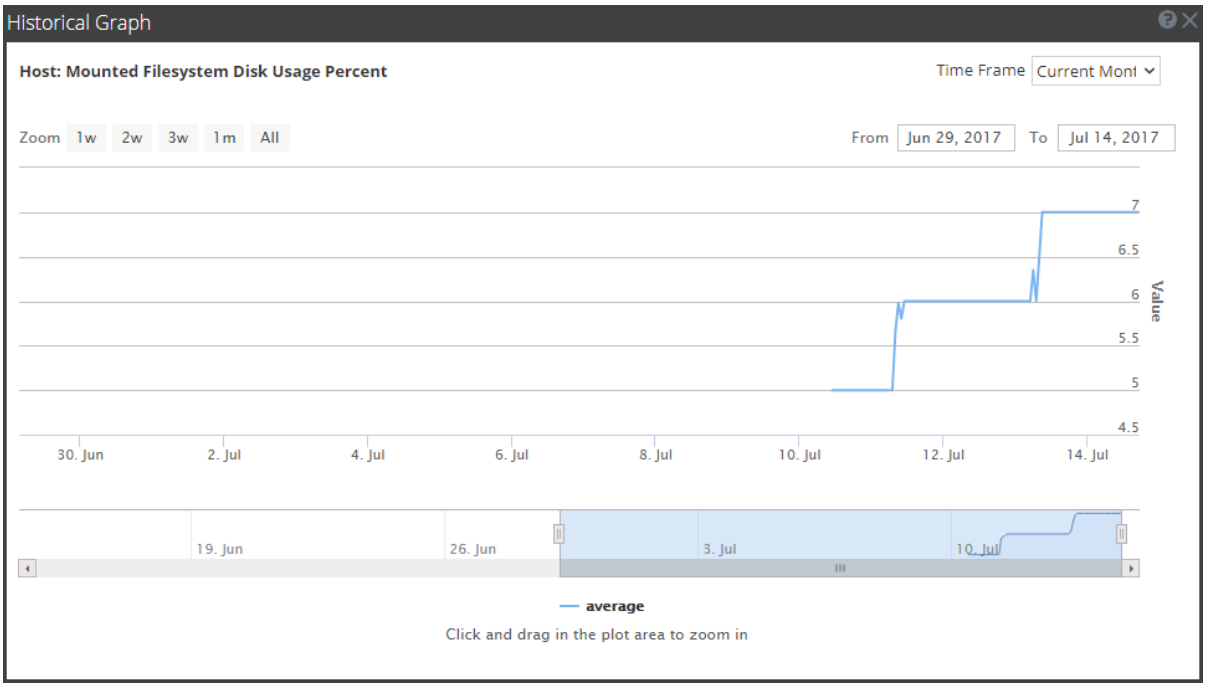
Parameter	Beschreibung
Zeitrahmen	Wählen Sie den Zeitrahmen aus, dessen Verlaufsdaten Sie anzeigen möchten. Folgende Optionen sind verfügbar: **Aktueller Tag**, **Aktuelle Woche**, **Aktueller Monat** und **Aktuelles Jahr**.
Von <Datum> bis <Datum>	Wählen Sie den Datumsbereich aus, dessen Verlaufsdaten Sie anzeigen möchten.

Wenn Sie sich die Daten im Verlaufsdiagramm genauer anschauen möchten, können Sie Vergrößerungsfunktionen verwenden.

Vergrößerungsfunktion 1 und 2:

Sie können einen der Werte auswählen, um die Verlaufsdaten für den ausgewählten Wert anzuzeigen. Die Abbildung unten zeigt ein Beispiel für einen 6-stündigen Zeitraum, der für die Vergrößerung ausgewählt wurde. Der Schieberegler unten rechts wird auch an das 6-stündige Zeitfenster angepasst.

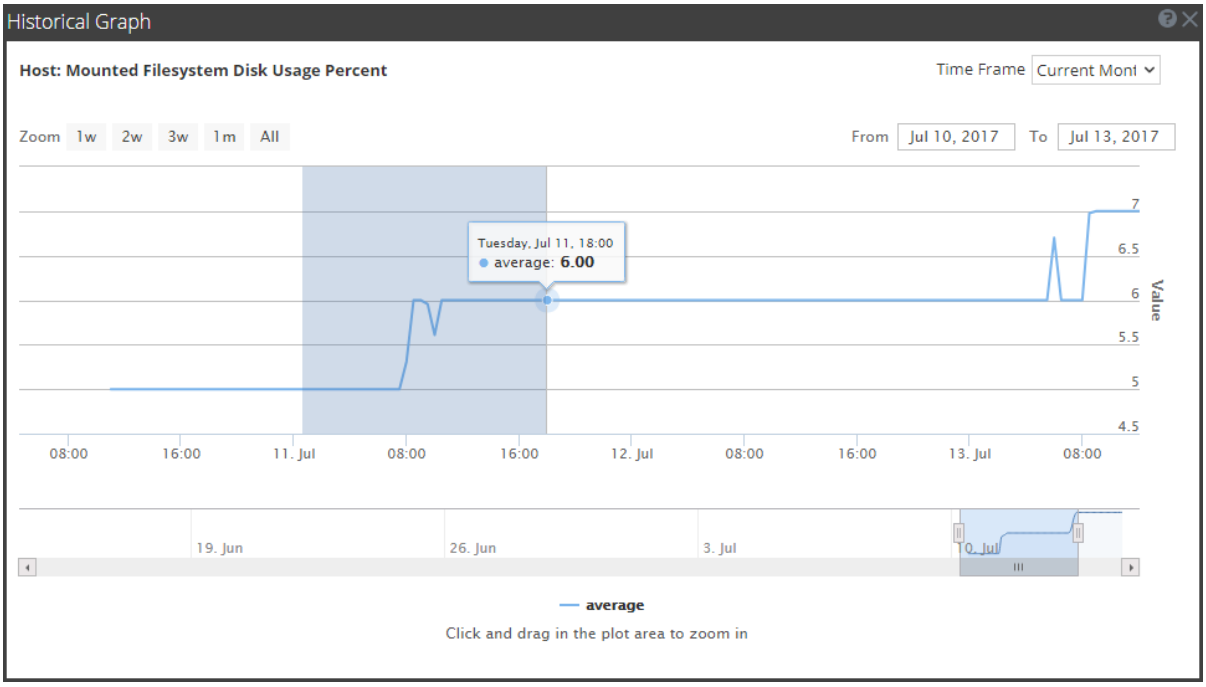
Alternativ können Sie den Schieberegler rechts unten bewegen, um die Ansicht eines bestimmten Zeitraums zu vergrößern.



Vergrößerungsfunktion 3:

Sie können im Plotbereich auch auf eine Zeit klicken und mit der Maus ziehen, um die Ansicht eines bestimmten Zeitraums zu vergrößern.

Die Abbildung unten zeigt ein Beispiel, wie das Diagramm angezeigt wird, während Sie klicken und ziehen.



Ansicht „Einstellungen" der Benutzeroberfläche „Integrität und Zustand" – Archiver

Hinweis: Informationen zum Überwachen von Archiver und Warehouse Connector finden Sie unter Integritätsrichtlinie.

So greifen Sie auf die Ansicht Überwachung in Archiver zu:

1. Navigieren Sie zu **Administration > Integrität und Zustand**.
2. Wählen Sie **Einstellungen > Archiver** aus.

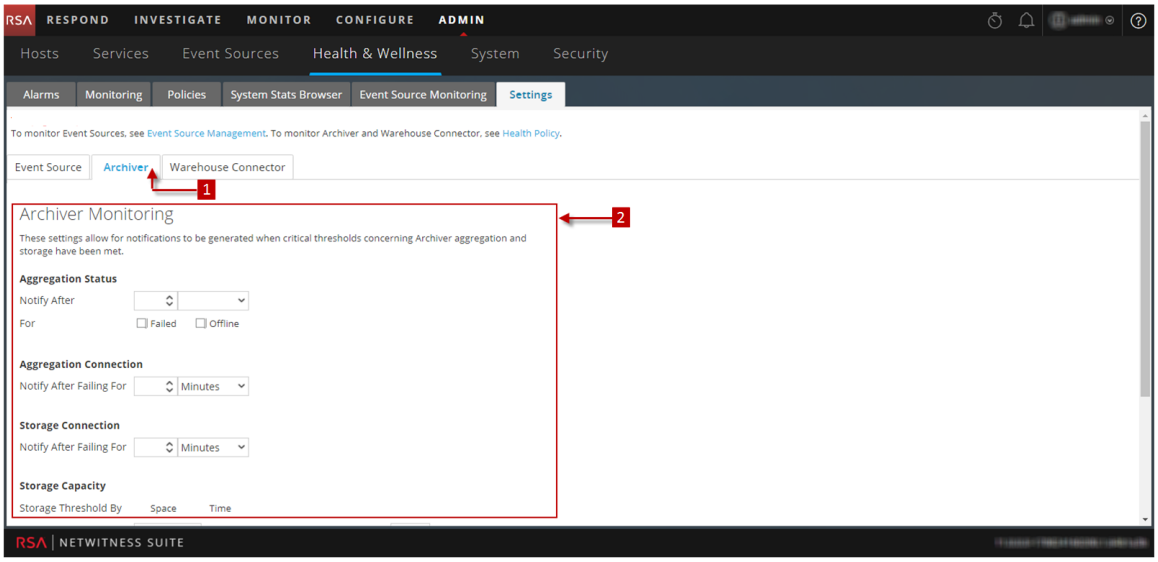
Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Überwachen von Servicedetails von Archiver	Überwachen von Servicedetails

Verwandte Themen

Überwachen von Servicedetails

Überblick



1	Zeigt den Bereich „Archiver-Überwachung“ an.
2	Konfiguriert den Bereich „Archiver-Überwachung“ zur automatischen Benachrichtigung.

Funktionen

In der folgenden Tabelle werden die Parameter aufgelistet, die benötigt werden, um den Archiver so zu konfigurieren, dass beim Erreichen kritischer Schwellenwerte automatisch Benachrichtigungen erzeugt werden.

Parameter	Wert	Beschreibung
Aggregationsstatus	Benachrichtigen nach	Anzahl der Minuten oder Stunden, nach denen Sie über den Aggregationsstatus informiert werden
	Für	Fehlgeschlagen: Wenn diese Option aktiviert ist, werden Sie benachrichtigt, wenn der Aggregationsstatus des Archiver für die definierte Anzahl von Minuten oder Stunden „Fehlgeschlagen“ lautet. Offline: Wenn diese Option aktiviert ist, werden Sie benachrichtigt, wenn der Aggregationsstatus des Archiver für die definierte Anzahl von Minuten oder Stunden „Offline“ lautet.
Aggregationsverbindung	Benachrichtigen nach Ausfall für	Anzahl der Minuten oder Stunden, nach denen Sie benachrichtigt werden, wenn die Aggregationsverbindung des Archiver fehlschlägt.
Speicherverbindung	Benachrichtigen nach Ausfall für	Anzahl der Minuten oder Stunden, nach denen Sie benachrichtigt werden, wenn die Speicherverbindung des Archiver fehlschlägt.

Parameter	Wert	Beschreibung
Speicherkapazität	Speicherschwellenwert nach	Wählen Sie **Speicherplatz**, wenn Sie benachrichtigt werden möchten, wenn die Speicherkapazität des Archiver den im Feld **Bei einer Speichergröße von** definierten Prozentsatz überschreitet. Wählen Sie **Zeit** aus, wenn Sie benachrichtigt werden möchten, wenn die im Archiver gespeicherten Dateien die im Feld **Bei einer ältesten Speicherdatei von** definierte Anzahl von Tagen überschreiten.
	Bei einer Speichergröße von	Geben Sie an, zu wieviel Prozent die Speichergröße voll sein soll, wenn Sie eine Benachrichtigung erhalten möchten.
	Bei einer Warmspeichergröße von	Geben Sie an, zu wieviel Prozent die Warmspeichergröße voll sein soll, wenn Sie eine Benachrichtigung erhalten möchten.

Parameter	Wert	Beschreibung
Benachrichtigungstyp	Konfigurieren von E-Mails oder Verteilerlisten	Klicken Sie hierauf, um eine E-Mail zu konfigurieren, damit Sie in NetWitness Suite Benachrichtigungen empfangen können.
	Konfigurieren von Syslog- und SNMP-Trap-Servern	Klicken Sie hierauf, um Auditprotokolle zu konfigurieren.
	NW-Konsole, E-Mail, Syslog-Benachrichtigung, SNMP-Trap-Benachrichtigung	Aktivieren der NW-Konsole zum Empfangen von Benachrichtigungen in der Benachrichtigungssymbolleiste der NetWitness Suite-Benutzeroberfläche Aktivieren von E-Mail zum Empfangen von E-Mail-Benachrichtigungen Aktivieren von Syslog-Benachrichtigung zum Erzeugen von Syslog-Ereignissen Aktivieren der SNMP-Trap-Benachrichtigung zum Abrufen von Auditereignissen als SNMP-Traps

Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Ereignisquellen

Hinweis: Informationen über das Management von Ereignisquellen erhalten Sie unter **Informationen über Ereignisquellenmanagement** im *RSA NetWitness Suite-Leitfaden für das Ereignisquellenmanagement*.

Die Ansicht „Ereignisquellenüberwachung“ besteht aus dem Bereich „Ereignisquelle“, dem Dialogfeld „Quellüberwachung hinzufügen oder bearbeiten“, dem Bereich „Außerbetriebnahme“ und dem Dialogfeld „Außerbetriebnahme“. In dieser Ansicht können Sie Folgendes konfigurieren:

- Erzeugen von Benachrichtigungen für Ereignisquellen, von denen die Protokollsammlung keine Protokolle mehr erhält
- Bedingungen für das Versenden dieser Benachrichtigungen
- Außerbetriebnehmen einer Protokollsammlung, wenn ein Remote Collector und der Local Collector einen Failover zu einem Stand-by Log Decoder durchführen

Die erforderliche Rolle für den Zugriff auf diese Ansicht ist **Managen von NW-Auditing**. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Admin > Integrität und Zustand**.
2. Wählen Sie **Einstellungen > Ereignisquelle** aus.

Was möchten Sie tun?

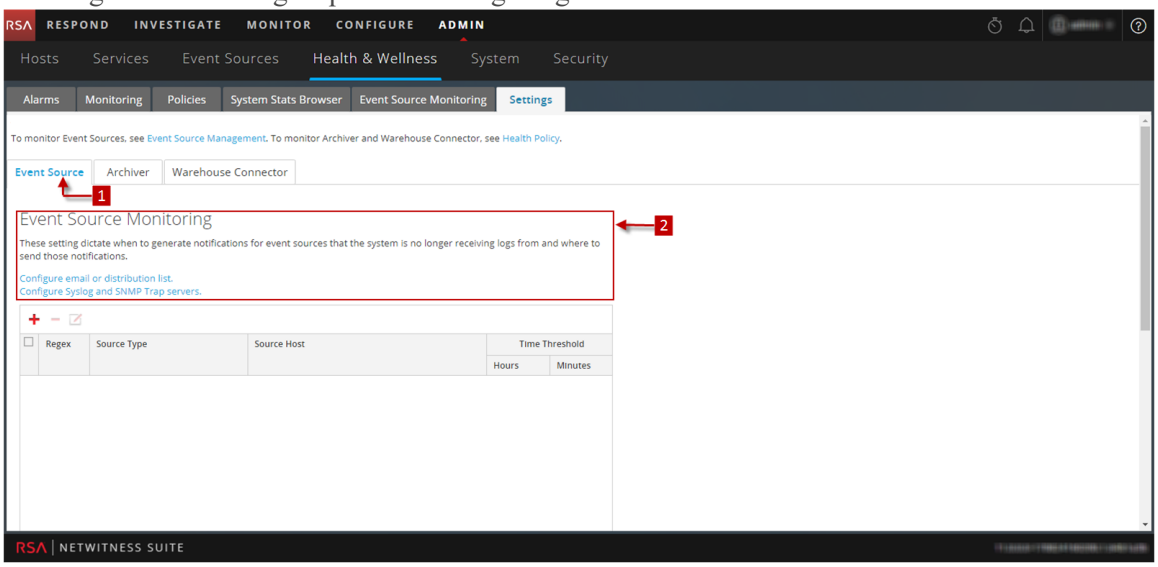
Rolle	Ziel	Details anzeigen
Administrator	Anzeigen der Funktion der Ereignisquellenüberwachung	Überwachen von Ereignisquellen

Verwandte Themen

Konfigurieren der Ereignisquellenüberwachung

Überblick

Die Registerkarte Ereignisquelle wird angezeigt.



1	Zeigt den Bereich „Ereignisquellenüberwachung“ an.
2	Konfiguriert den Bereich „Ereignisquellenüberwachung“ zum Empfang von Benachrichtigungen.

Bereich „Ereignisquellenüberwachung“

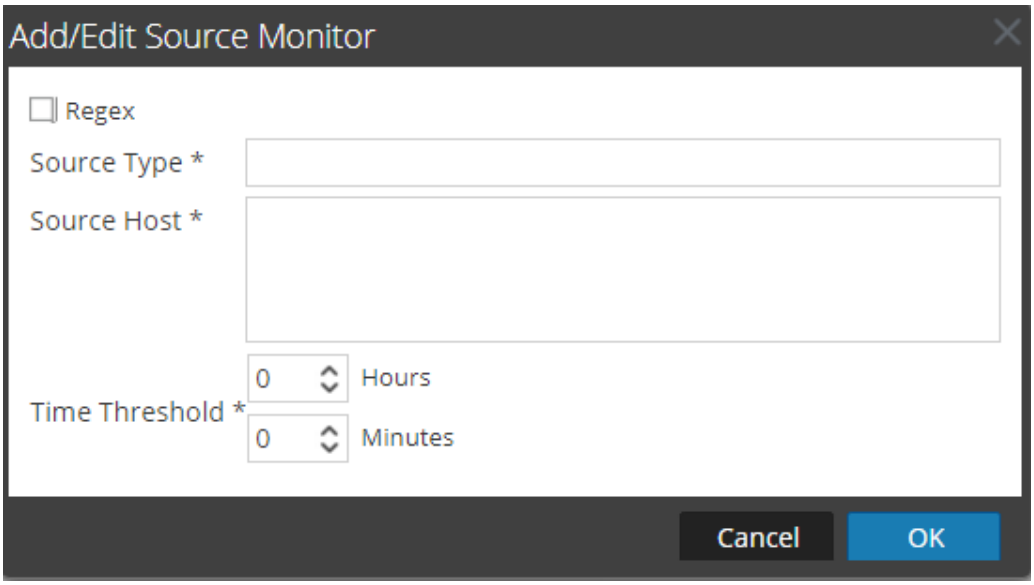
Funktion	Beschreibung
E-Mails oder Verteilerlisten konfigurieren	Öffnet die Ansicht **Administration** > **System** > E-Mail, in der Sie den E-Mail-Versand für die Ausgabe der Ereignisquellenüberwachung festlegen können, sofern erforderlich.
Syslog- und SNMP-Trap-Server konfigurieren	Öffnet die Ansicht **Administration** > **System** > Auditing, in der Sie die Syslog- und SNMP-Trap-Verteilung für die Ausgabe der Ereignisquellenüberwachung festlegen können, sofern erforderlich.
	Zeigt das Dialogfeld „Quellüberwachung hinzufügen oder bearbeiten“ an, in dem Sie zu überwachende Ereignisquellen hinzufügen oder ändern können.
	Löscht die ausgewählten Ereignisquellen aus der Überwachung.
	Wählt eine Ereignisquelle aus.
Quelltyp	Zeigt den Quelltyp der Ereignisquelle an.
Quellhost	Zeigt den Quellhost der Ereignisquelle an.
Zeitschwellenwert	Zeigt die Zeitdauer an, nach deren Ablauf NetWitness Suite keine Benachrichtigungen mehr versendet (Zeitschwellenwert).
Anwenden	Wendet alle Ergänzungen, Löschungen oder Änderungen an. Diese werden sofort wirksam.
Abbrechen	Bricht alle Hinzufügungen, Löschungen oder Änderungen ab.

Bereich Außerbetriebnahme

Funktion	Beschreibung
	Zeigt das Dialogfeld „Außerbetriebnahme“ an, in dem Sie außer Betrieb zu nehmende Ereignisquellen hinzufügen oder ändern können.

Funktion	Beschreibung
	Löscht die ausgewählten Ereignisquellen aus der Außerbetriebnahme.
	Wählt eine Ereignisquelle aus.
Regex	Zeigt an, ob Sie die Verwendung von regulären Ausdrücken aktiviert haben.
Quelltyp	Zeigt den Quelltyp der außer Betrieb genommenen Ereignisquelle an.
Quellhost	Zeigt den Quellhost der außer Betrieb genommenen Ereignisquelle an.
Anwenden	Wendet alle Ergänzungen, Löschungen oder Änderungen an. Diese werden sofort wirksam.
Abbrechen	Bricht alle Hinzufügungen, Löschungen oder Änderungen ab.

Dialogfeld „Quellüberwachung hinzufügen oder bearbeiten“



Im Dialogfeld **Quellüberwachung hinzufügen oder bearbeiten** können Sie zu überwachende Ereignisquellen hinzufügen oder ändern. Die beiden Parameter, die eine Ereignisquelle identifizieren, sind **Quelltyp** und **Quellhost**. Sie können **Globbing** (Musterabgleich und Platzhalter) verwenden, um den Quelltyp und Quellhost von Ereignisquellen anzugeben, wie im folgenden Beispiel gezeigt:

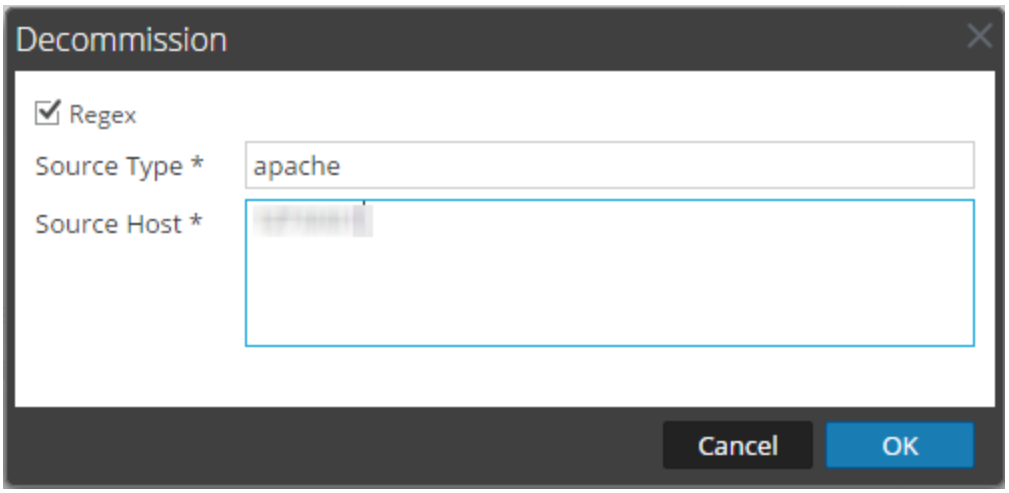
Quelltyp	Quellhost
ciscopix	**1.1.1.1**
*	**1.1.1.1**
*	*
*	**1.1.1.1|1.1.1.2**
*	**1.1.1.[1|2]**
*	**1.1.1.[123]**
*	**1.1.1.[0-9]**
*	**1.1.1.11[0-5]**
*	**1.1.1.1,1.1.1.2**
*	**1.1.1.[0-9]|1.1.1.11[0-5]**
*	**1.1.1.[0-9]|1.1.1.11[0-5],10.31.204.20**
*	**1.1.1.***
*	**1.1.1.[0-9]{1,3}**

Funktionen

Funktion	Beschreibung
Regex	Aktivieren Sie das Kontrollkästchen, wenn Sie reguläre Ausdrücke verwenden möchten.
Quelltyp	Der Quelltyp der Ereignisquelle. Sie müssen den Wert verwenden, den Sie für die Ereignisquelle auf der Registerkarte **Ereignisquellen** in der Ansicht **Administration** > **Services** > Log Collector-Service > **Ansicht** > **Konfiguration** konfiguriert haben.

Funktion	Beschreibung
Quellhost	Der Hostname bzw. die IP-Adresse der Ereignisquelle. Sie müssen den Wert verwenden, den Sie für die Ereignisquelle auf der Registerkarte **Ereignisquellen** in der Ansicht **Administration** > **Services** > Log Collector-Gerät > **Ansicht** > **Konfiguration** konfiguriert haben.
Zeitschwellenwert	Die Zeitspanne, nach deren Ablauf von NetWitness Suite Benachrichtigungen versendet werden.
Abbrechen	Schließt das Dialogfeld, ohne die Ereignisquelle dem Bereich Ereignisquellenüberwachung hinzuzufügen oder die Ereignisquelle zu ändern.
OK	Fügt die Ereignisquelle dem Bereich Ereignisquellenüberwachung hinzu.

Dialogfeld „Außerbetriebnahme“



Funktion	Beschreibung
Quelltyp	Der Quelltyp der Ereignisquelle. Sie müssen den Wert verwenden, den Sie für die Ereignisquelle auf der Registerkarte **Ereignisquellen** in der Ansicht **Administration** > **Services** > Log Collector-Gerät > **Ansicht** > **Konfiguration** konfiguriert haben.

Funktion	Beschreibung
Quellhost	Der Hostname bzw. die IP-Adresse der Ereignisquelle. Sie müssen den Wert verwenden, den Sie für die Ereignisquelle auf der Registerkarte **Ereignisquellen** in der Ansicht **Administration** > **Services** > Log Collector-Service > **Ansicht** > **Konfiguration** konfiguriert haben.
Abbrechen	Schließt das Dialogfeld, ohne Hinzufügungen, Löschungen oder Änderungen an der Ereignisquelle im Bereich Außerbetriebnahme zu speichern.
OK	Übernimmt alle Hinzufügungen, Löschungen oder Änderungen an den Ereignisquellen im Bereich Außerbetriebnahme.

Ansicht „Einstellungen“ der Benutzeroberfläche „Integrität und Zustand“ – Warehouse Connector

Hinweis: Informationen zum Überwachen von Archiver und Warehouse Connector finden Sie unter Integritätsrichtlinie.

Durch das Konfigurieren der Warehouse Connector-Überwachung können automatisch Benachrichtigungen erzeugt werden, wenn kritische Schwellenwerte in Bezug auf Warehouse Connector und Speicherplatz erreicht werden.

Zugreifen auf die Ansicht „Warehouse Connector-Überwachung“

1. Navigieren Sie zu **Admin > Integrität und Zustand**.
2. Wählen Sie **Einstellungen > Warehouse Connector**.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Anzeigen von Details für Warehouse Connector	Ansicht „Details für Warehouse Connector“

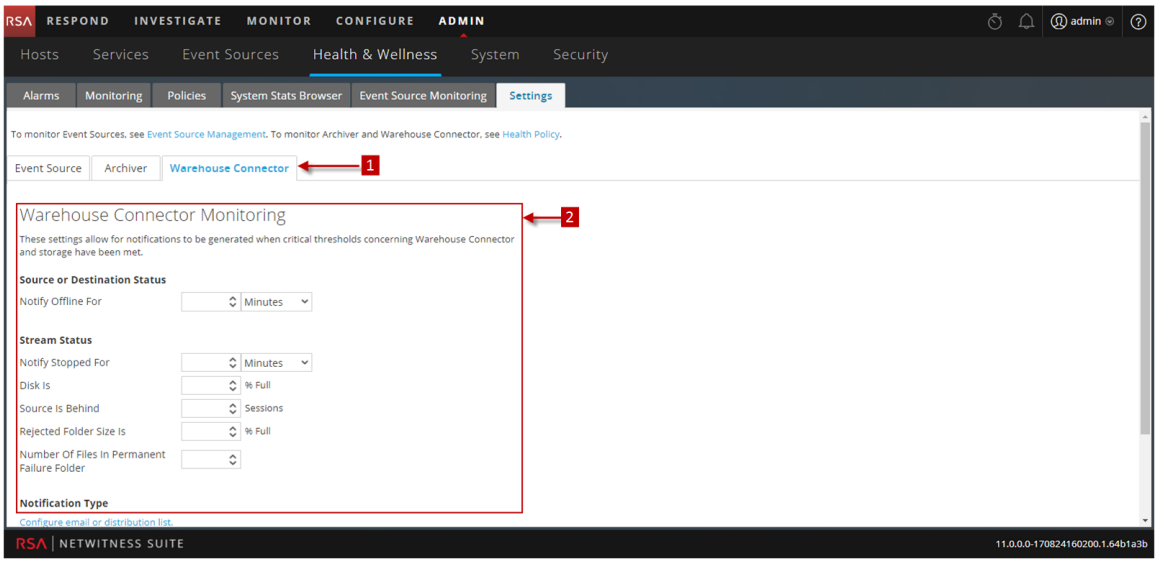
Verwandte Themen

Ansicht „Details für Warehouse Connector“

Überwachen von Servicedetails

Überblick

Die Ansicht „Warehouse Connector-Überwachung“ wird angezeigt.



1 Zeigt die Ansicht „Warehouse Connector-Überwachung“ an.

2 Ermöglicht die Konfiguration der Parameter für die Warehouse Connector-Überwachung.

Parameter für die Warehouse Connector-Überwachung

In der folgenden Tabelle werden die Parameter aufgeführt, die zum Konfigurieren von Warehouse Connector für die automatische Erzeugung von Benachrichtigungen beim Erreichen kritischer Schwellenwerte erforderlich sind.

Parameter	Wert	Beschreibung
Quell- oder Zielstatus	Benachrichtigung bei offline für	Anzahl der Minuten oder Stunden, nach deren Ablauf Sie eine Benachrichtigung erhalten, falls die Quell- oder Zielverbindung fehlgeschlagen ist.
Streamstatus	Benachrichtigung bei beendet für	Anzahl der Minuten oder Stunden, nach deren Ablauf Sie eine Benachrichtigung erhalten, falls der Stream offline ist.
	Festplatte ist	Der Prozentwert an belegtem Festplattenspeicherplatz, bei dessen Erreichen Sie eine Benachrichtigung erhalten.

Parameter	Wert	Beschreibung
	Quelle ist zurück	Anzahl an Sitzungen, bei denen eine Benachrichtigung ausgelöst wird, sofern die Quelle diese definierte Anzahl an Sitzungen nicht erfüllt.
	Größe des Ablehnungsordners ist	Der Prozentwert an belegtem Ordnerspeicherplatz, bei dessen Erreichen Sie eine Benachrichtigung erhalten.
	Anzahl der Dateien im Ordner für permanente Fehler	Anzahl der Dateien im Ordner für permanente Fehler, bei deren Erreichen Sie eine Benachrichtigung erhalten.
Benachrichtigungstyp	Konfigurieren von E-Mails oder Verteilerlisten	Klicken Sie hierauf, um eine E-Mail zu konfigurieren, damit Sie in NetWitness Suite Benachrichtigungen empfangen können.
	Konfigurieren von Syslog- und SNMP-Trap-Servern	Klicken Sie hierauf, um Auditprotokolle zu konfigurieren.

Parameter	Wert	Beschreibung
	NW-Konsole, E-Mail, Syslog-Benachrichtigung, SNMP-Trap-Benachrichtigung	Aktivieren der NW-Konsole zum Empfangen von Benachrichtigungen in der Benachrichtigungssymbolleiste der NetWitness Suite-Benutzeroberfläche Aktivieren von E-Mail zum Empfangen von E-Mail-Benachrichtigungen Aktivieren von Syslog-Benachrichtigung zum Erzeugen von Syslog-Ereignissen Aktivieren der SNMP-Trap-Benachrichtigung zum Abrufen von Auditereignissen als SNMP-Traps

Ansicht „Überwachung“

Die Detailansichten in NetWitness Suite enthalten detaillierte Statistiken und andere Informationen zum Host und zu den einzelnen NetWitness Suite-Services. Sie können die derzeitige Integrität aller Hosts, sämtliche auf den Hosts ausgeführten Services, verschiedene Aspekte der Integrität der Hosts sowie Details von Hosts und Services in der Ansicht Überwachung anzeigen.

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Überwachung**.

Was möchten Sie tun?

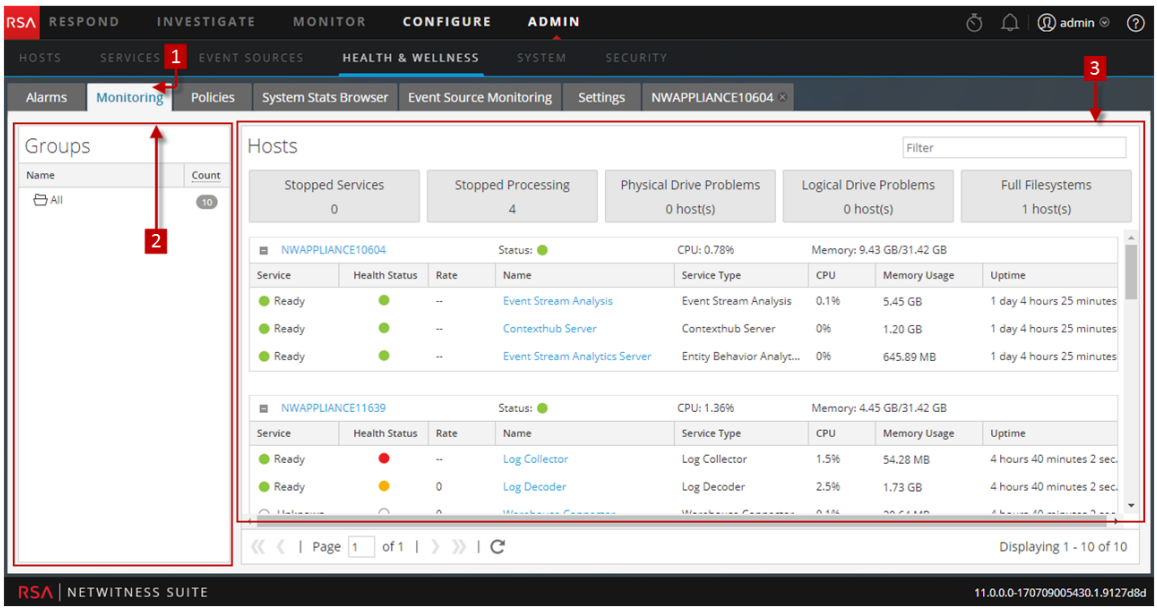
Rolle	Ziel	Details anzeigen
Administrator	Anzeigen und Durchführen von Verfahren	Überwachen von Hosts und Services

Verwandte Themen

- Überwachen von Hosts und Services

Überblick

Die
-Ansicht „Überwachung“ wird angezeigt.



1 Zeigt die Registerkarte „Überwachung“ an.

2 Im Bereich „Gruppen“ können Sie eine Gruppe auswählen.

3 Im Bereich Hosts werden betriebliche Statistiken angezeigt.

Bereich „Gruppen“

Im Bereich „Gruppen“ werden alle verfügbaren Gruppen von Hosts aufgelistet. Wenn Sie eine Gruppe auswählen, wird der zugehörige Inhalt im Bereich „Hosts“ angezeigt.

Hinweis: Wenn die gesamte **Anzahl** der Hosts im Bereich **Gruppen** niedriger ist als die tatsächliche Anzahl der Hosts, die im Bereich **Hosts** angezeigt wird, finden Sie mögliche Ursachen und empfohlene Lösungen für dieses Problem unter dem Thema Troubleshooting von Integrität und Zustand.

Bereich „Hosts“

Im Bereich „Hosts“ werden betriebliche Statistiken für Hosts und die Services angezeigt, die auf jedem Host ausgeführt werden.

Parameter	Beschreibung
Filter	Geben Sie den Namen eines Hosts oder eines Services in das Feld „Suche“ ein, um die entsprechenden Hosts und Services im Bereich „Hosts“ anzeigen zu lassen.

Parameter	Beschreibung
Beendete Services	Klicken Sie auf **Beendete Services**, um eine Liste aller beendeten Services anzeigen zu lassen. Hier wird auch der Host angezeigt, auf dem der Service installiert ist.
Beendete Verarbeitung	Klicken Sie auf **Beendete Verarbeitung**, um eine Liste aller Hosts anzuzeigen, auf denen Services mit dem Status „Beendete Verarbeitung“ installiert sind.
Probleme mit physischem Laufwerk <#> Host(s)	Klicken Sie hier, um Hosts anzuzeigen, bei denen es Probleme mit dem physischen Laufwerk gibt.
Probleme mit logischem Laufwerk <#> Host(s)	Klicken Sie hier, um Hosts anzuzeigen, bei denen es Probleme mit dem logischen Laufwerk gibt.
Volle Dateisysteme <#> Host(s)	Klicken Sie hier, um Hosts anzuzeigen, deren Dateisysteme voll sind.

Hinweis: Die Zusammenfassungsinformationen in den Feldern oben zeigen die Systemstatistiken für alle in NetWitness Suite konfigurierten Hosts an, sie ändern sich nicht beim Anwenden von Hostfiltern auf Gruppen.

Im oberen Bereich folgt eine Liste von Hosts, den darauf installierten Services und Informationen zu den Hosts und Services.

Parameter	Beschreibung
Hostname	Zeigt den Hostnamen an. Wenn auf einem Host ein Service installiert ist, sehen Sie vor dem Hostnamen das Präfix ⊞. Klicken Sie auf ⊞, um alle auf einem Host installierten Services anzuzeigen.

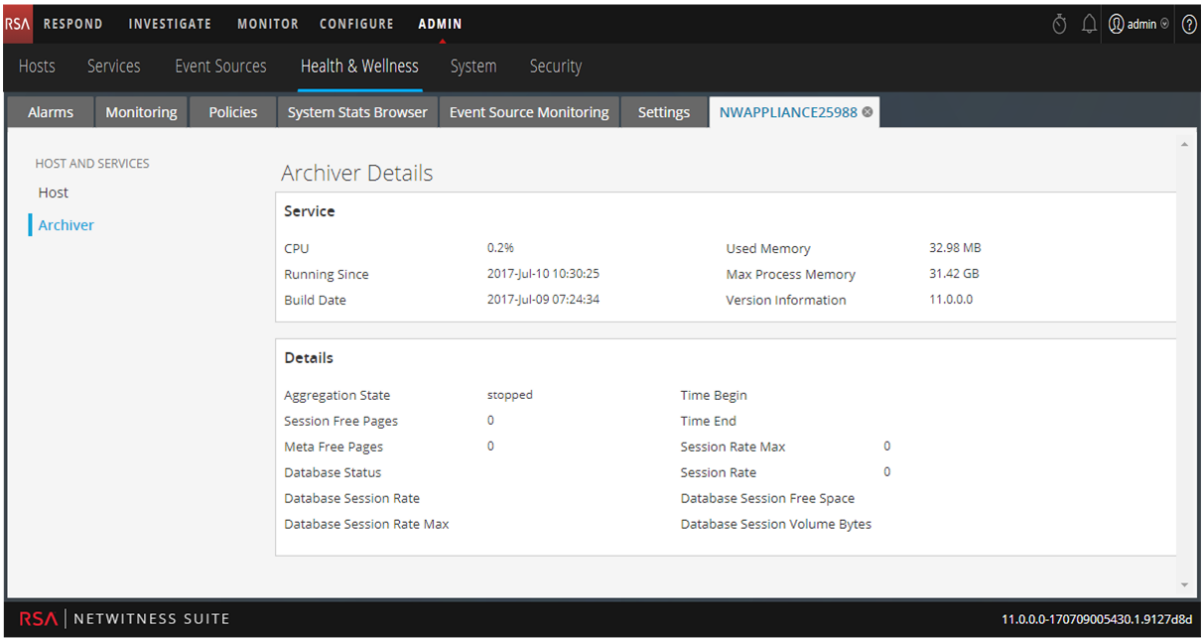
Parameter	Beschreibung
Status	Zeigt den aktuellen Status des Hosts an. ● – zeigt an, dass der Host aktiv ist und ausgeführt wird. ● – gibt an, dass der Host die Verarbeitung beendet hat oder noch nicht damit begonnen hat.
CPU	Zeigt die aktuelle CPU-Auslastung des Hosts an.
Memory	Zeigt den von dem Host verwendeten Arbeitsspeicher an.

Wenn Sie auf ⊞ vor dem Hostnamen klicken, wird eine Liste aller auf dem Host installierten Services angezeigt. In der folgenden Tabelle sind die unterschiedlichen Parameter aufgeführt, die für einen Service angezeigt werden, sowie die zugehörigen Beschreibungen.

Parameter	Beschreibung
Service	Zeigt den aktuellen Status des Services an. ● Bereit – zeigt an, dass der Service aktiv ist und ausgeführt wird. ● Gestoppt – zeigt an, dass der Service die Verarbeitung beendet hat oder noch nicht damit begonnen hat.
Integritätsstatus	Zeigt den Verarbeitungsstatus des Services an. ● – zeigt an, dass der Prozess ausgeführt wird und die Daten mit einer Rate größer Null verarbeitet werden. ● – zeigt an, dass die Verarbeitung beendet wurde. ●- zeigt an, dass die Verarbeitung aktiviert wurde, die Daten aber nicht verarbeitet werden.
Rate	Gibt die Rate an, mit der die Daten verarbeitet werden.
Name	Der Name des Service.
Servicetyp	Gibt den Namen des Servicetyps an.
CPU	Zeigt die aktuelle CPU-Auslastung des Services an.
Speichernutzung	Zeigt den vom Service verwendeten Arbeitsspeicher an.
Uptime	Zeigt die Laufzeit des Services an.

Ansicht „Details für Archiver“

Die Ansicht „Details für Archiver“ enthält Informationen über den Archiver. Die folgende Abbildung zeigt die Ansicht „Details für Archiver“.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

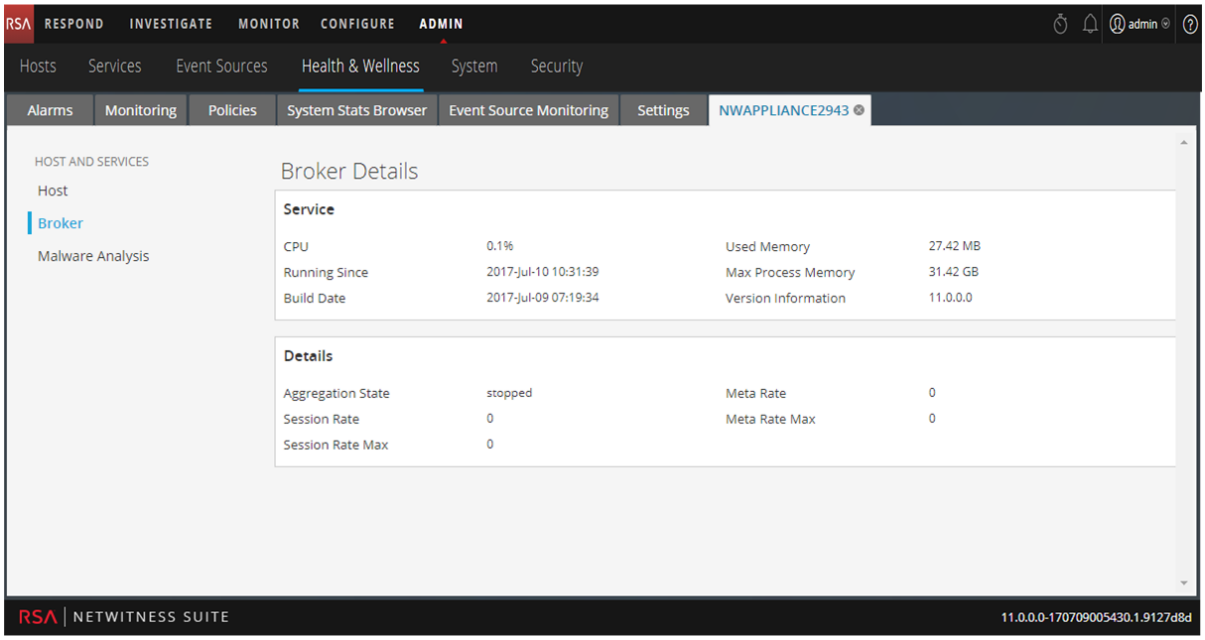
In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den Service angezeigt.

Statistik	Beschreibung
Aggregationszustand	Status der Datenaggregation
Zeit Anfang	Der Zeitpunkt (UTC), zu dem die erste Sitzung vom Index nachverfolgt wurde.
Sitzung - Freie Seiten	Die für die Aggregation verfügbaren Seiten der Sitzung
Zeit Ende	Zeitpunkt (UTC), zu dem die letzte Sitzung vom Index nachverfolgt wurde
Meta - Freie Seiten	Die für die Aggregation verfügbaren Seiten
Sitzungsrate max.	Maximale Rate der Sitzungen pro Sekunde

Statistik	Beschreibung
Database Status	Status der Datenbanken Gültige Werte: • **closed:** Die Datenbank steht für QUERY und UPDATE nicht zur Verfügung (die Datenbanken werden initialisiert). Dieser Wert ist selten zu sehen. • **opened:** Die Datenbank steht für QUERY und UPDATE zur Verfügung. • **failure**: Die Datenbank konnte nicht geöffnet werden. Das kann viele verschiedene Gründe haben. Sie können das überprüfen, wenn die Erfassung nicht startet oder wenn Abfragen keine Daten zurückgeben. Dies passiert normalerweise aufgrund einer beschädigten Datenbank.
Sitzungsrate	Rate der Sitzungen pro Sekunde
Datenbanksitzungsrate	Rate pro Sekunde, mit der der Service Sitzungen in die Datenbank schreibt
Freier Speicherplatz in Datenbanksitzung	Freier Speicherplatz in der Sitzung, der für die Aggregation verfügbar ist
Max. Datenbanksitzungsrate	Maximale Rate pro Sekunde, mit der der Service Sitzungen in die Datenbank schreibt
Datenbanksitzung-Volumenbyte	Die Anzahl der Sitzungsbyte in der Datenbank

Ansicht „Details für Broker“

Die Ansicht „Details für Broker“ enthält Informationen für den Broker. Die folgende Abbildung zeigt die Ansicht „Details für Broker“.



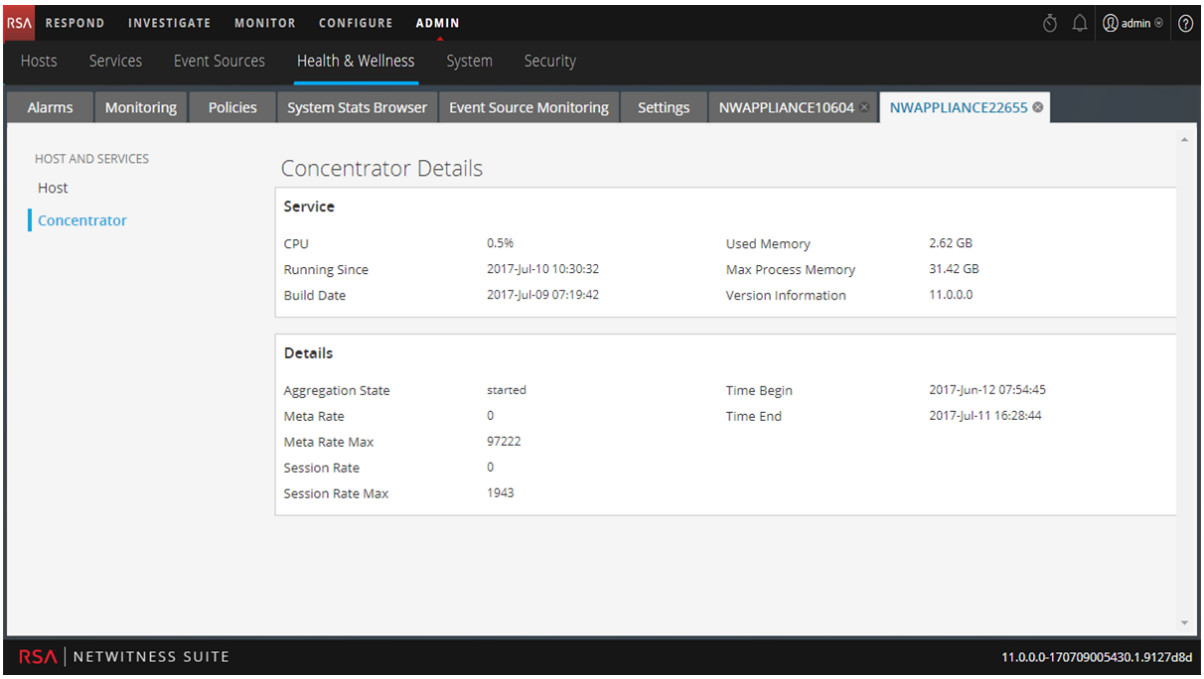
Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den Service angezeigt.

Statistik	Beschreibung
Aggregationszustand	Status der Datenaggregation
Metarate	Rate der Metadatenobjekte pro Sekunde
Sitzungsrate	Rate der Sitzungen pro Sekunde
Metarate max.	Maximale Rate der Metadatenobjekte pro Sekunde
Sitzungsrate max.	Maximale Rate der Sitzungen pro Sekunde

Ansicht „Details für Concentrator“

Die Ansicht „Details für Concentrator“ enthält Informationen für den Concentrator. Die folgende Abbildung zeigt die Ansicht „Details für Concentrator“.



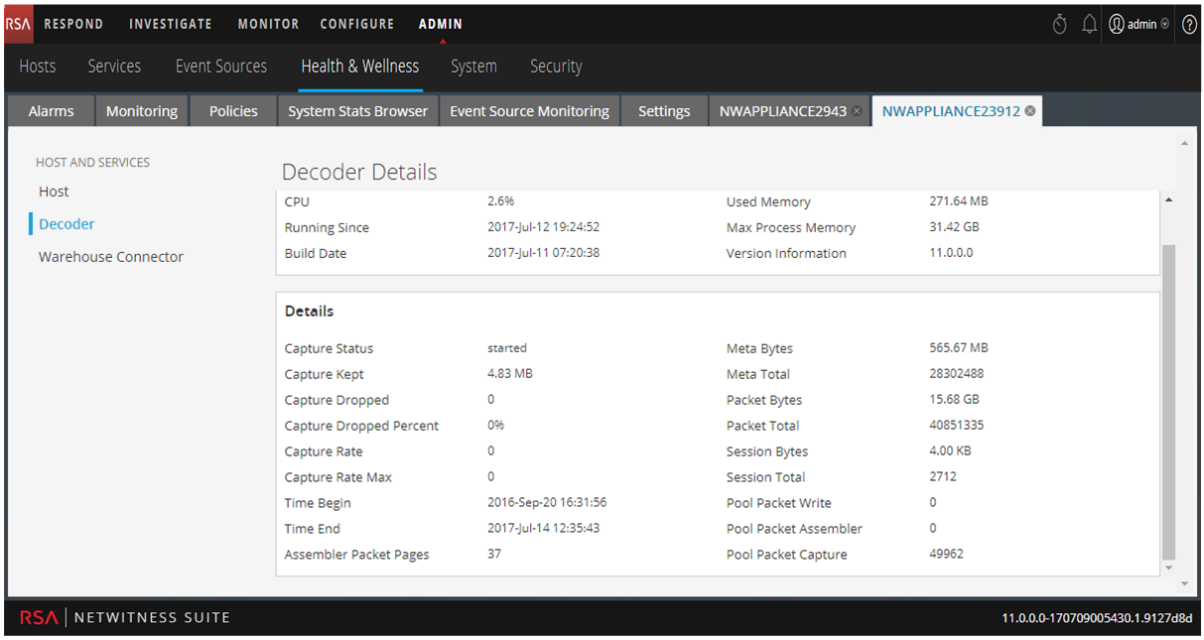
Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den Service dargestellt.

Statistik	Beschreibung
Aggregationszustand	Status der Datenaggregation
Zeit Anfang	Der Zeitpunkt (UTC), zu dem die erste Sitzung vom Index nachverfolgt wurde.
Metarate	Rate der Metadatenobjekte pro Sekunde
Zeit Ende	Zeitpunkt (UTC), zu dem die letzte Sitzung vom Index nachverfolgt wurde
Metarate max.	Maximale Rate der Metadatenobjekte pro Sekunde
Sitzungsrate	Rate der Sitzungen pro Sekunde
Sitzungsrate max.	Maximale Rate der Sitzungen pro Sekunde

Ansicht Details für Decoder

Die Ansicht „Details für Decoder“ enthält Informationen für den Decoder. Die folgende Abbildung zeigt die Ansicht „Details für Decoder“.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den Service angezeigt.

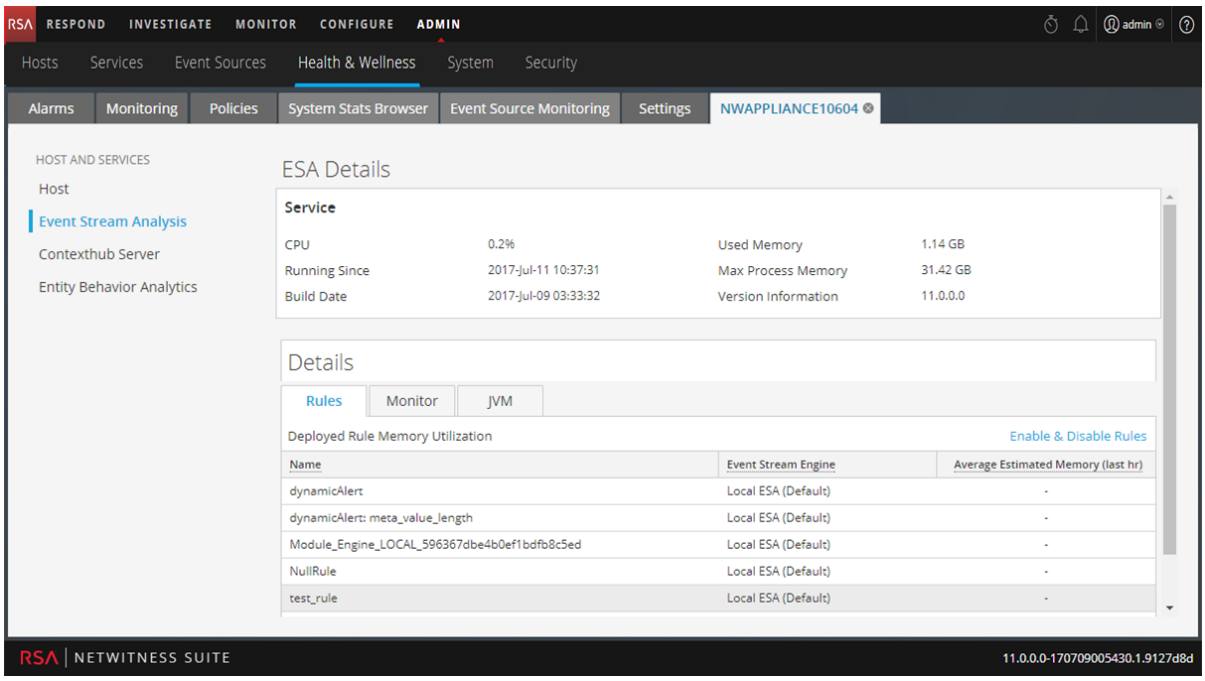
Statistik	Beschreibung
Erfassungsstatus	Status der Datenerfassung. Gültige Werte: • **Wird gestartet**: Datenerfassung wird gestartet (Daten werden noch nicht erfasst). • **Gestartet**: Daten werden erfasst. • **Wird beendet**: Datenerfassung wird beendet (Anforderung zum Beenden der Datenerfassung erhalten, aber die Datenerfassung wurde noch nicht beendet). • **Beendet**: Daten werden nicht erfasst. • **Deaktiviert**: Nicht als Decoder-Service konfiguriert.
Metabyte	Anzahl der Metabyte in der Datenbank.

Statistik	Beschreibung
Erfassung aufbewahrt	Anzahl an Paketen, die während der Erfassung beibehalten werden.
Meta insgesamt	Anzahl der Metadaten in der Datenbank.
Erfassung gelöscht	Anzahl der Pakete, die von der Netzwerkkarte als verloren gegangen gemeldet wurden. Nachdem die Datenerfassung beendet wurde, wird die Rate auf null zurückgesetzt.
Paketbyte	Anzahl der Paketbyte in der Datenbank.
Erfassung gelöscht (Prozent)	Anzahl der Pakete, die von der Netzwerkkarte als verloren gegangen gemeldet wurden, in Prozent.
Pakete insgesamt	Anzahl der Paketobjekte auf, die in der Paketdatenbank gehalten werden. Die Gesamtzahl wird kleiner, wenn die Datenbank Dateien aufgrund von Größenbeschränkungen nacheinander löscht. Die Zahl wird nicht zurückgesetzt, nachdem die Datenerfassung des Services beendet wurde.
Erfassungsrate	Rate der Datenerfassung durch den Service in Megabit pro Sekunde. Die Rate ist ein gleitender Durchschnittswert für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Datenerfassung beendet wurde, wird die Rate auf null zurückgesetzt.
Sitzungsbyte	Die Anzahl der Sitzungsbyte in der Datenbank
Erfassungsrate max.	Maximale Rate der Datenerfassung durch den Service in Megabit pro Sekunde. Die Rate ist ein gleitender Durchschnittswert für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Datenerfassung durch den Service beendet wurde, wird die maximale Rate während der Datenerfassung angezeigt.

Statistik	Beschreibung
Sitzungen insgesamt	Anzahl der Sitzungen in der Sitzungsdatenbank. Dieser Wert wird kleiner, wenn die Datenbank Dateien aufgrund von Größenbeschränkungen nacheinander löscht. Die Zahl wird nicht zurückgesetzt, nachdem die Datenerfassung des Services beendet wurde.
Zeit Anfang	Zeitpunkt, zu dem das erste Paket erfasst wurde (Zeitpunkt, zu dem das erste Paket in der Paketdatenbank gespeichert wurde). Der Wert für diesen Zeitpunkt erhöht sich, wenn Pakete aus der Paketdatenbank gelöscht werden.
Pool-Paket-Schreibvorgänge	Anzahl der Paketseiten, die sich zurzeit in der PCS-Pipeline befinden und in die Datenbank geschrieben werden müssen.
Zeit Ende	Zeitpunkt, zu dem das letzte Paket erfasst wurde (Zeitpunkt, zu dem das Paket in die Datenbank geschrieben wurde). Der Wert für diesen Zeitpunkt erhöht sich, wenn neue Pakete erfasst werden.
Pool-Paket-Assembler	Anzahl der Paketseiten, die darauf warten, zusammengesetzt zu werden.
Assembler-Paketseiten	Anzahl der Paketseiten, die darauf warten, zusammengesetzt zu werden.
Pool-Paket-Erfassungen	Anzahl der Paketseiten, die für die Erfassung zur Verfügung stehen.

Ansicht Details für Event Stream Analysis (ESA)

Die Ansicht „Details für Event Stream Analysis“ enthält Informationen für ESA. In der folgenden Abbildung sind die Details für Event Stream Analysis dargestellt.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken und Regelinformationen für den Service angezeigt. Er enthält die Registerkarten **Regeln**, **Überwachung** und **JVM** (Java Virtual Machine), auf denen Regeln und zusätzliche Statistiken zu Event Stream Analysis angezeigt werden.

Registerkarte „Überwachung“

Zeigt die folgenden allgemeinen statistischen Informationen für den Event Stream Analysis-Service an:

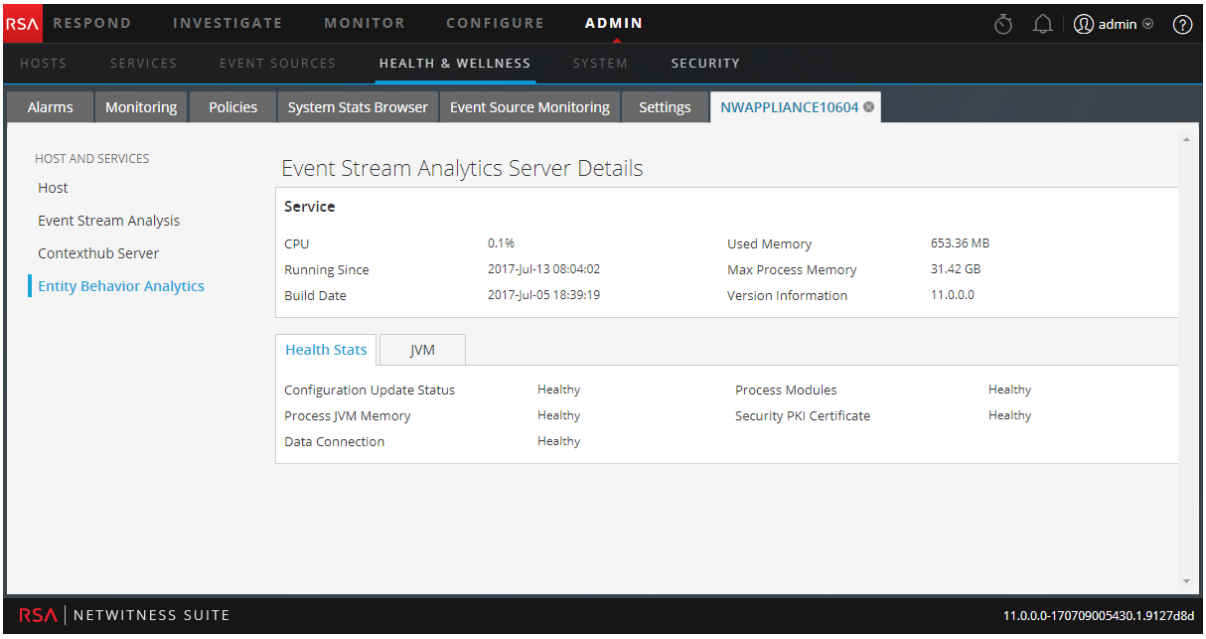
- Durchschnittliche empfangene Anzahl von Bytes pro Ereignismeldungsfeld
- Durchschnittliche empfangene Anzahl von Bytes pro Ereignismeldung
- Gesamtanzahl von empfangenen Bytes
- Gesamtanzahl von empfangenen Feldern
- Anzahl bereitgestellter Regeln im ESA-Service. Die Summe der aktivierten und deaktivierten Regeln muss mit der Anzahl bereitgestellter Regeln übereinstimmen.
- Gesamtanzahl der Ereignisse, die mit allen Regeln im ESA-Service übereinstimmen
- Gesamtanzahl von Ereignissen, die vom ESA-Service seit dem letzten Servicestart analysiert wurden

- Gesamtanzahl von Warnmeldungen, die auf Basis von allen Regeln im ESA-Service ausgelöst wurden
- Gesamtanzahl – als verspätet gelöscht
- Gesamtanzahl – pünktlich zugeliefert
- Gesamtanzahl – vorzeitig beendet
- Sekunden zwischen Feeds
- Zeitspanne im Fenster
- Ereignisse im Fenster insgesamt
- Verbrauchter Prozentsatz des Fensters
- Quellarbeitseinheiten insgesamt
- Gelöschter Bus nach Nutzdaten insgesamt
- Gelöschter Bus nach Ereignissen insgesamt
- Gelöschter Bus nach Feldern insgesamt
- Gesamtanzahl von Warnmeldungen, die an den Nachrichtenbus gesendet wurden
- Gesamtanzahl von Busereignissen
- Gesamtanzahl von Busarbeitseinheiten
- Erfasste Endpunkte insgesamt
- Verlorene Endpunkte insgesamt
- Gesamtzahl fehlgeschlagene Clients
- Gesamtzahl erfolgreiche Clients
- Gesamtzahl erfolgreiche Server
- Minuten seit letztem Erfolg
- Anzahl, wie oft Proxys angefordert und gewährt wurden
- Gesamtzahl erfolgreicher Anforderungen
- Anzahl, wie oft Proxys angefordert und nicht gewährt wurden
- Gesamtzahl nicht erfolgreicher Anforderungen

Ansicht „Details für ESA Analytics“

Die Ansicht „Details für ESA Analytics bietet Informationen zum Integritätsstatus des ausgewählten Analytics ESA-Services. Analytics ESA-Services verarbeiten die Daten für die automatisierte Bedrohungserkennung. Es ist wichtig, dass Sie jedes Element angehen, das einen anderen Status als Grün (in Ordnung) anzeigt, damit die Datenverarbeitung nicht unterbrochen wird und kritische Events nicht übersehen werden.

Die folgende Abbildung zeigt ein Beispiel für die Ansicht „Details für ESA Analytics“.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

Details für ESA Analytics

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den ausgewählten ESA Analytics-Service angezeigt.

Integritätsstatus

Im Abschnitt „Integritätsstatus“ wird die Integrität der folgenden Elemente für den ausgewählten ESA Analytics-Service angezeigt:

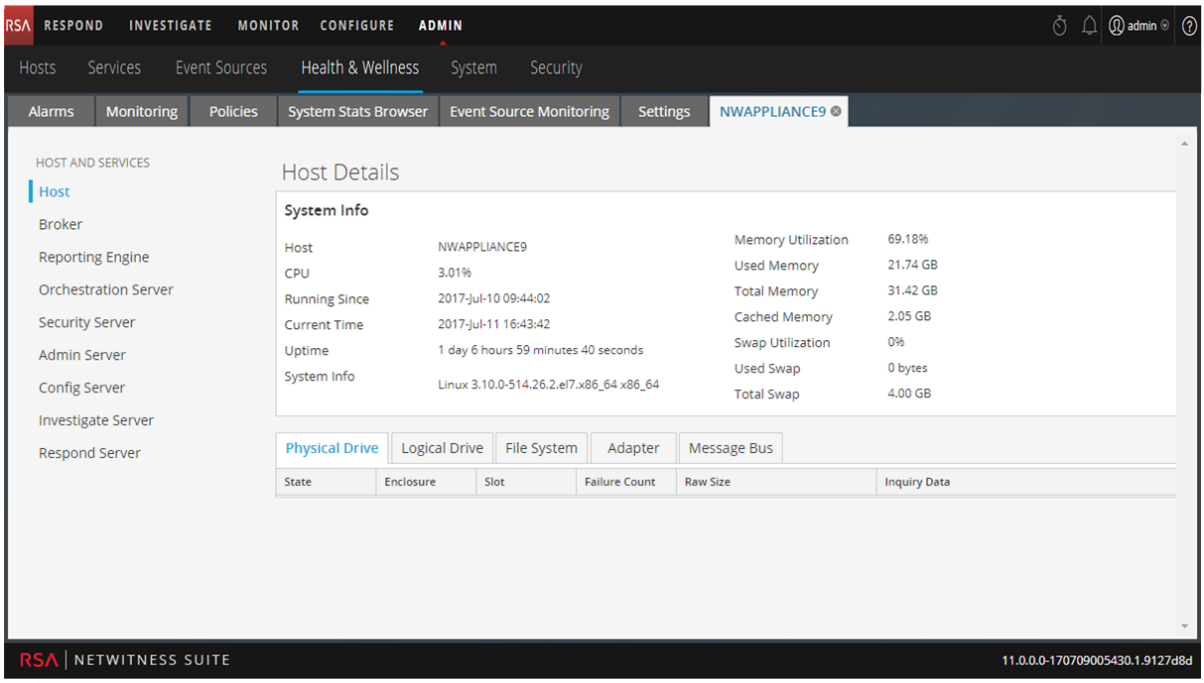
- Mongo
- Java Virtual Machine (JVM)
- Festplattenspeicher
- Modul „Verdächtige Domains“
- Modul „User Behavior Analytics“

In der folgenden Tabelle wird die Bedeutung der einzelnen Integritätsstatus beschrieben.

Integritätsstatus	Beschreibung
Grün	In Ordnung
Gelb	Nicht ordnungsgemäß
Rot	Kritisch; sofortige Aufmerksamkeit erforderlich
- -	Nicht zutreffend

Ansicht „Details zum Host“

Die Ansicht „Details zum Host“ enthält Informationen über einen Host. Die folgende Abbildung zeigt die Ansicht „Details zum Host“.



Im Bereich „Optionen“ auf der linken Seite werden der Host und die auf dem Host installierten Services angezeigt. Sie können für den jeweiligen Service auf Host klicken, um die Statistiken und andere zugehörige Informationen für diesen Host oder Service anzuzeigen.

Im Bereich „Details“ werden Informationen über den Host sowie zusätzliche Informationen über die Hardware des Hosts angezeigt.

Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuelle Performance, die aktuelle Kapazität und die Verlaufsstatistiken des Hosts angezeigt.

Parameter	Beschreibung
Host	Hostname:
CPU	Die aktuelle CPU-Auslastung des Hosts.
Ausgeführt seit	Der Zeitpunkt, an dem der Host gestartet wurde.
Aktuelle Zeit	Die aktuelle Zeit auf dem Host.
Betriebszeit	Die Zeit, in der der Host aktiv war.
Systeminfo	Die auf dem Host installierte Betriebssystemversion.
Arbeitsspeicherauslastung	Der Prozentsatz des vom Host genutzten Speichers.
Belegter Arbeitsspeicher	Der belegte Arbeitsspeicher in GB.
Gesamtspeicher	Die Kapazität des im System installierten Speichers.
Cache	Arbeitsspeicher, der auf die Festplatte zwischengespeichert wird in GB.
Swap-Auslastung	Prozentsatz der System-Swap verwendet.
Swap verwendet	Verwendeter Swap in GB.
Swap insgesamt	Die Kapazität des im System installierten Swap.

Im unteren Abschnitt werden die aktuellen allgemeinen Statistiken für den Host auf den Registerkarten angezeigt, die in der folgenden Tabelle beschrieben werden.

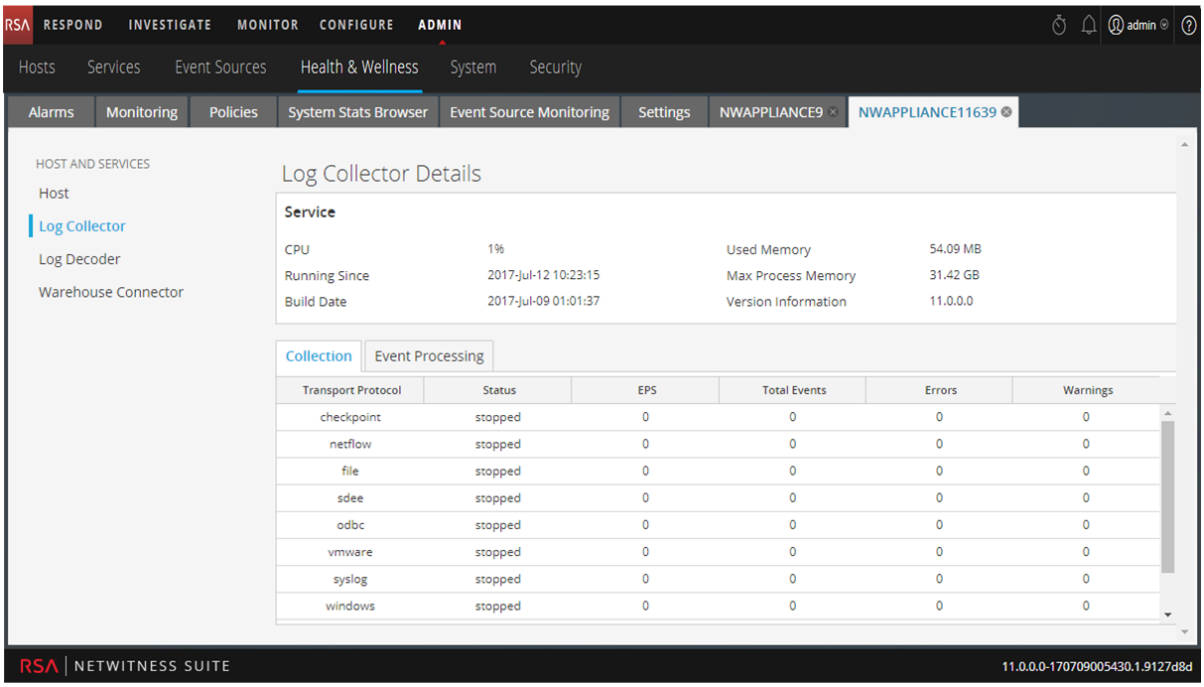
Registerkarte	Beschreibung
Physisches Laufwerk	Die Art des physischen Laufwerks auf dem Host sowie dessen Auslastung und zusätzliche Informationen.
Logisches Laufwerk	Das logische Laufwerk auf dem Host.
Dateisystem	Informationen zum Dateisystem, zur Größe, zur aktuellen Nutzung und zur verfügbaren Kapazität auf dem Host.
Adapter	Der auf dem Host verwendete Adapter.

Registerkarte	Beschreibung
Nachrichtenbus	**Veröffentlichungsrate**: Rate, in der eingehende Nachrichten in die Warteschlange des Nachrichtenbusses gestellt werden. **Summe der Nachrichten in Warteschlange**: Anzahl der Nachrichten in der Nachrichtenwarteschlange. **Genutzter Arbeitsspeicher**: Vom Nachrichtenbus genutzter Arbeitsspeicher (in Bytes). **Freier Festplattenplatz**: Freier Speicherplatz auf der Festplatte, der für den Nachrichtenbus verfügbar ist (in Bytes). **Speichergrenzwert**: Das Limit des Systemspeichers. Wenn die Speichernutzung diesen Wert überschreitet, wird der **Speicheralarm** ausgelöst und Security Analytics empfängt keine Nachrichten mehr. **Grenzwert für freien Festplattenplatz**: Freier Speicherplatz auf der Festplatte, der für den Nachrichtenbus verfügbar ist. Wenn der verfügbare Speicherplatz diesen Wert unterschreitet, wird der **Alarm für freien Festplattenplatz** ausgelöst und Security Analytics empfängt keine Nachrichten mehr. **Speichergrenzwert verfügbar**: Verfügbarer Speicherplatz auf dem Arbeitsspeicher für diesen Message Broker (in Bytes). Wenn dieser Wert erreicht wird, wird der **Alarm für verwendeten Arbeitsspeicher** ausgelöst. **Festplattengrenzwert verfügbar**: Freier Speicherplatz auf der Festplatte, der für diesen Message Broker verfügbar ist (in Bytes). Wenn dieser Wert erreicht wird, wird der **Alarm für Grenzwert für freien Festplattenplatz** ausgelöst. **Alarm für freien Festplattenplatz**: **True** oder **False**. **True** gibt an, dass der verfügbare Festplattenspeicher unter dem Wert liegt, der im Feld **Grenzwert für freien Festplattenplatz** festgelegt wurde, und dass Security Analytics keine Nachrichten mehr empfängt. **Speicheralarm**: **True** oder **False**. **True** gibt an, dass der verfügbare Arbeitsspeicher unter dem Wert liegt, der im Feld **Speichergrenzwert** festgelegt wurde, und dass Security Analytics keine Nachrichten mehr

Registerkarte	Beschreibung
	empfängt.

Ansicht „Details für Log Collector“

Die Ansicht „Details für Log Collector“ enthält Informationen für den Log Collector. Die folgende Abbildung zeigt die Ansicht „Details für Log Collector“.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

Der untere Abschnitt besteht aus den Registerkarten **Sammlung** und **Ereignis wird verarbeitet**, die allgemeine Statistiken für den Service anzeigen.

Registerkarte „Sammlung“

Zeigt die Ereignissammlungsstatistik für jedes Log Collection-Protokoll an, das Sie in NetWitness Suite implementiert haben (siehe den ***Leitfaden für die ersten Schritte mit der Protokollsammlung*** in den ***Leitfäden zur Protokollsammlung***).

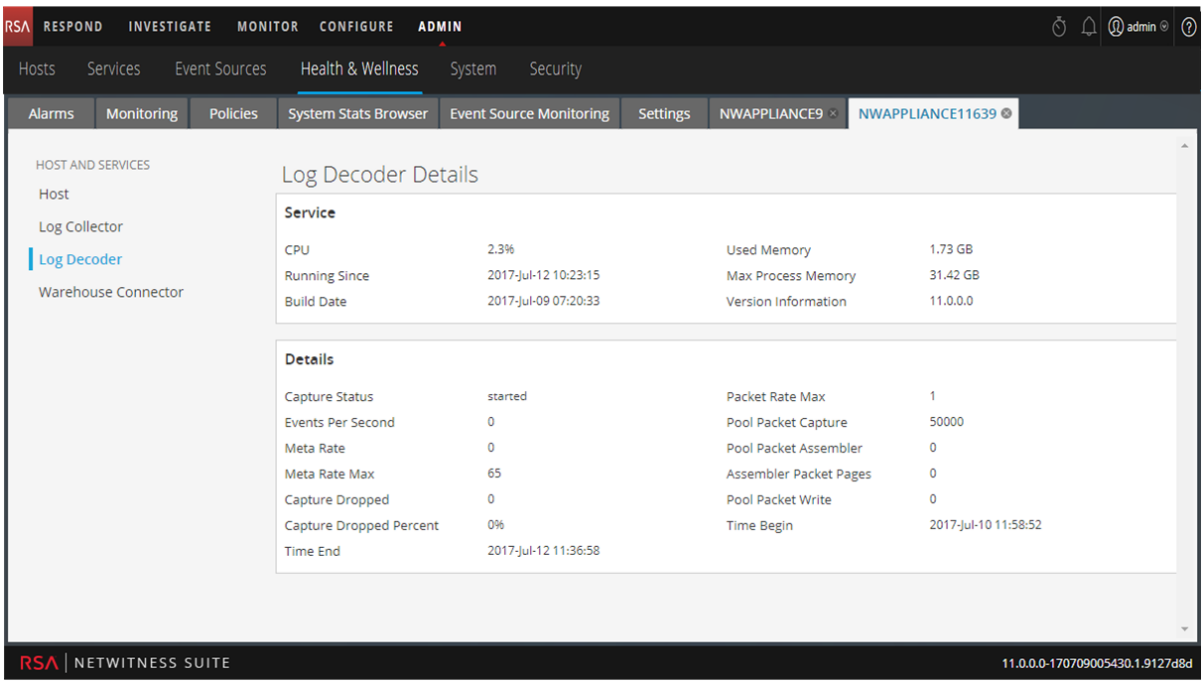
Registerkarte „Ereignis wird verarbeitet“

Zeigt Statistiken für das interne NetWitness Suite-Ereignisverarbeitungsprotokoll (d. h. den Log Decoder) für Log Collection an.

Parameter	Beschreibung
Transportprotokoll	NetWitness Suite-Protokollverwendung für Protokollsammlungen (d. h. der Log Decoder).
Status	Status des Log Decoder. Gültige Werte: • **Wird gestartet**: Datenerfassung wird gestartet (Daten werden noch nicht erfasst). • **Gestartet**: Daten werden erfasst. • **Wird beendet**: Datenerfassung wird beendet (Anforderung zum Beenden der Datenerfassung erhalten, aber die Datenerfassung wurde noch nicht beendet). • **Beendet**: Daten werden nicht erfasst. • **Deaktiviert**: Nicht als Decoder-Service konfiguriert.
EPS	Rate (Ereignisse pro Sekunde), mit der der Log Decoder Ereignisse vom Log Collector verarbeitet.
Ereignisse insgesamt	Gesamtzahl der vom Log Decoder verarbeiteten Ereignisse
Errors	Anzahl der gefundenen Fehler
Warnungen	Anzahl der gefundenen Warnungen
Byterate	Aktueller Durchsatz in Byte pro Sekunde

Ansicht Details für Log Decoder

Die Ansicht „Details für Log Decoder“ enthält Informationen für den Log Decoder. In der folgenden Abbildung sind die Details für Log Decoder dargestellt.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

In diesem Abschnitt werden die aktuellen allgemeinen Statistiken für den Service angezeigt.

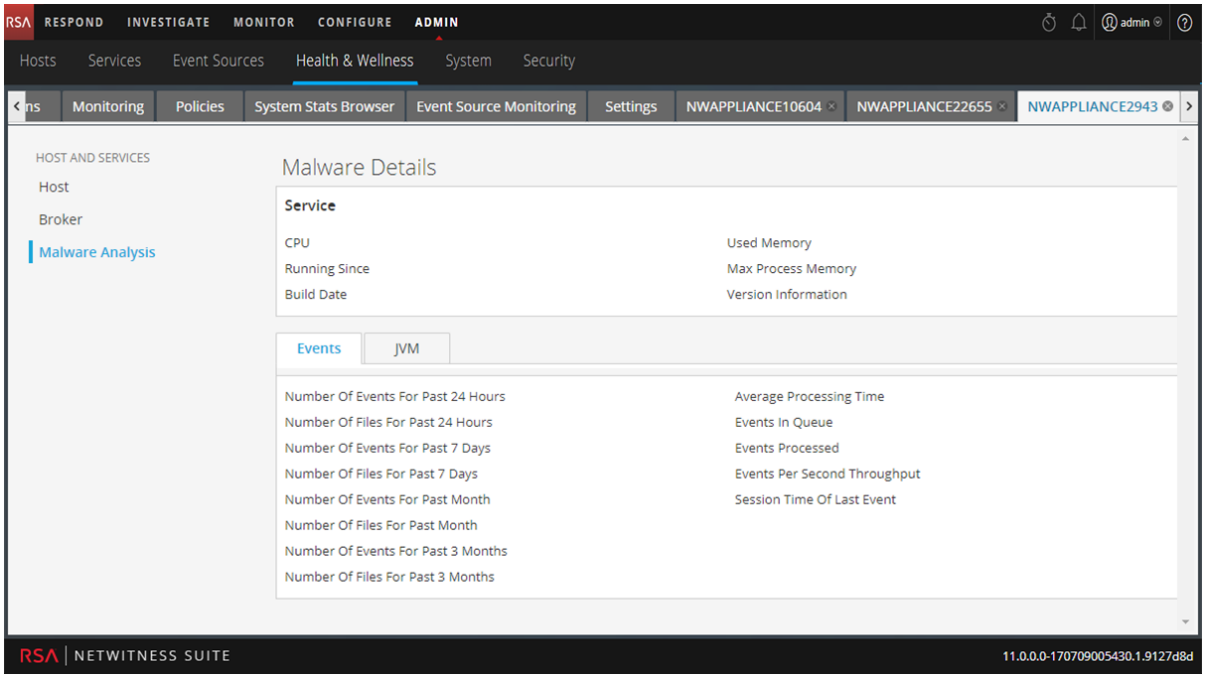
Statistik	Beschreibung
Erfassungsstatus	Status der Datenerfassung. Gültige Werte: • **Wird gestartet**: Datenerfassung wird gestartet (die Daten werden noch nicht erfasst). • **Gestartet**: Daten werden erfasst. • **Wird beendet**: Datenerfassung wird beendet (Anforderung zum Beenden der Datenerfassung erhalten, aber die Datenerfassung wurde noch nicht beendet). • **Beendet**: Daten werden nicht erfasst. • **Deaktiviert**: Nicht konfiguriert als ein Log Decoder-Service.
Max. Paketrate	Maximale Rate pro Sekunde, mit der der Service Pakete in die Datenbank schreibt. Die Rate ist ein gleitender Durchschnittswert für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Datenerfassung durch den Service beendet wurde, wird die maximale Rate während der Datenerfassung angezeigt.

Statistik	Beschreibung
Ereignisse pro Sekunde	Rate (Ereignisse pro Sekunde), mit der der Log Decoder Ereignisse vom Log Collector verarbeitet
Pool-Paket-Erfassungen	Anzahl der Paketseiten, die für die Erfassung zur Verfügung stehen.
Metarate	Rate pro Sekunde, mit der der Service Metadatenobjekte in die Datenbank schreibt. Die Rate ist ein gleitender Durchschnittswert für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Datenerfassung beendet wurde, wird die Rate auf null zurückgesetzt.
Pool-Paket-Assembler	Anzahl der Paketseiten, die darauf warten, zusammengesetzt zu werden.
Metarate max.	Maximale Rate pro Sekunde, mit der der Service Metadatenobjekte in die Datenbank schreibt. Die Rate ist ein gleitender Durchschnittswert für Stichproben über eine kurze Zeitdauer (10 Sekunden). Nachdem die Datenerfassung beendet wurde, wird die maximal erreichte Rate während der Datenerfassung angezeigt.
Assembler-Paketseiten	Anzahl der Paketseiten, die darauf warten, zusammengesetzt zu werden.
Erfassung gelöscht	Anzahl der Pakete, die von der Netzwerkkarte als verloren gegangen gemeldet wurden. Nachdem die Datenerfassung beendet wurde, wird die Rate auf null zurückgesetzt.
Pool-Paket-Schreibvorgänge	Anzahl der Paketseiten, die sich in der PCS-Pipeline befinden und in die Datenbank geschrieben werden müssen.
Erfassung gelöscht (Prozent)	Anzahl der Pakete, die von der Netzwerkkarte als verloren gegangen gemeldet wurden, in Prozent.

Statistik	Beschreibung
Zeit Anfang	Zeitpunkt, zu dem das erste Paket erfasst wurde (Zeitpunkt, zu dem das erste Paket in der Paketdatenbank gespeichert wurde). Der Wert für diesen Zeitpunkt erhöht sich, wenn Pakete aus der Paketdatenbank gelöscht werden.
Zeit Ende	Zeitpunkt, zu dem das letzte Paket erfasst wurde (Zeitpunkt, zu dem das Paket in die Datenbank geschrieben wurde). Der Wert für diesen Zeitpunkt erhöht sich, wenn neue Pakete erfasst werden.

Ansicht „Details für Malware“

Die Ansicht „Details für Malware“ enthält Informationen für Malware Analysis. In der folgenden Abbildung sind die Details für Malware dargestellt.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

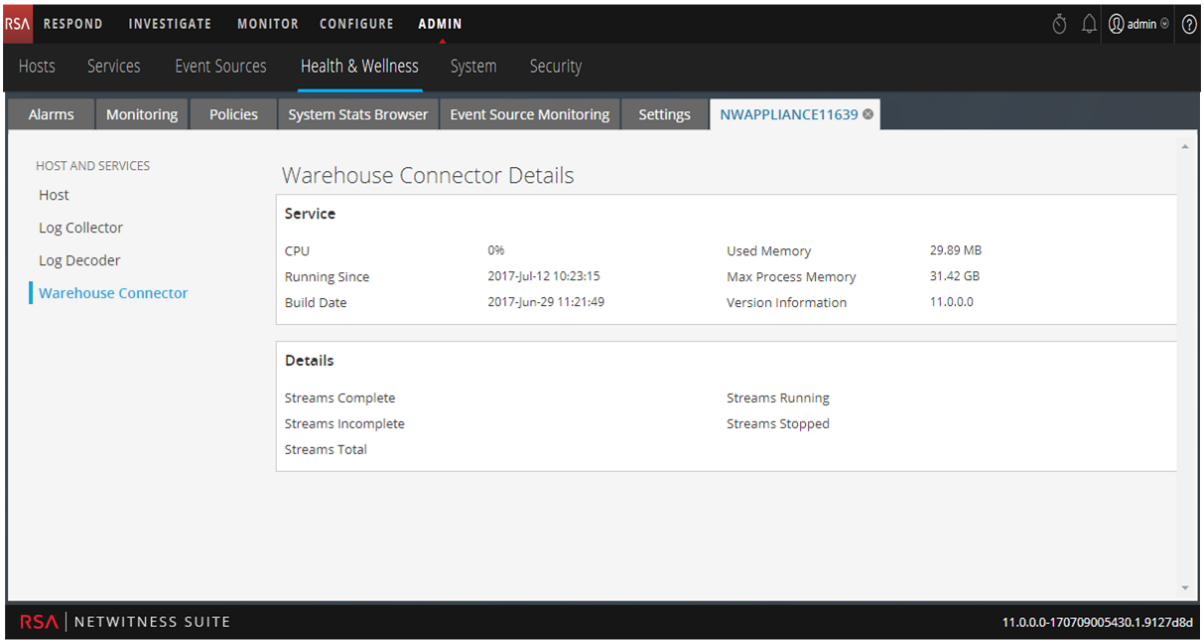
Zeigt die folgende ereignisbezogene statistische Information für den Malware Analysis-Service an.

- Anzahl der Ereignisse in den letzten 24 Stunden
- Durchschn. Verarbeitungszeit
- Anzahl der Dateien in den letzten 24 Stunden

- Ereignisse in Warteschlange
- Anzahl der Ereignisse in den letzten 7 Tagen
- Verarbeitete Ereignisse
- Anzahl der Ereignisse in den letzten 7 Tagen
- Durchsatz von Ereignissen pro Sekunde
- Anzahl der Ereignisse im letzten Monat
- Sitzungszeit des letzten Ereignisses
- Anzahl der Dateien im letzten Monat
- Anzahl der Ereignisse in den letzten 3 Monaten
- Anzahl der Dateien in den letzten 3 Monaten

Ansicht „Details für Warehouse Connector“

Die Registerkarte „Details für Warehouse Connector“ enthält Informationen für den Warehouse Connector, z. B. das Datum der Erstellung, CPU und Versionsinformationen. In der folgenden Abbildung sind die Details für Warehouse Connector dargestellt.



Das entsprechende Verfahren finden Sie unter Überwachen von Servicedetails.

Ansicht „Richtlinien“

Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist **Services managen**.

Was möchten Sie tun?

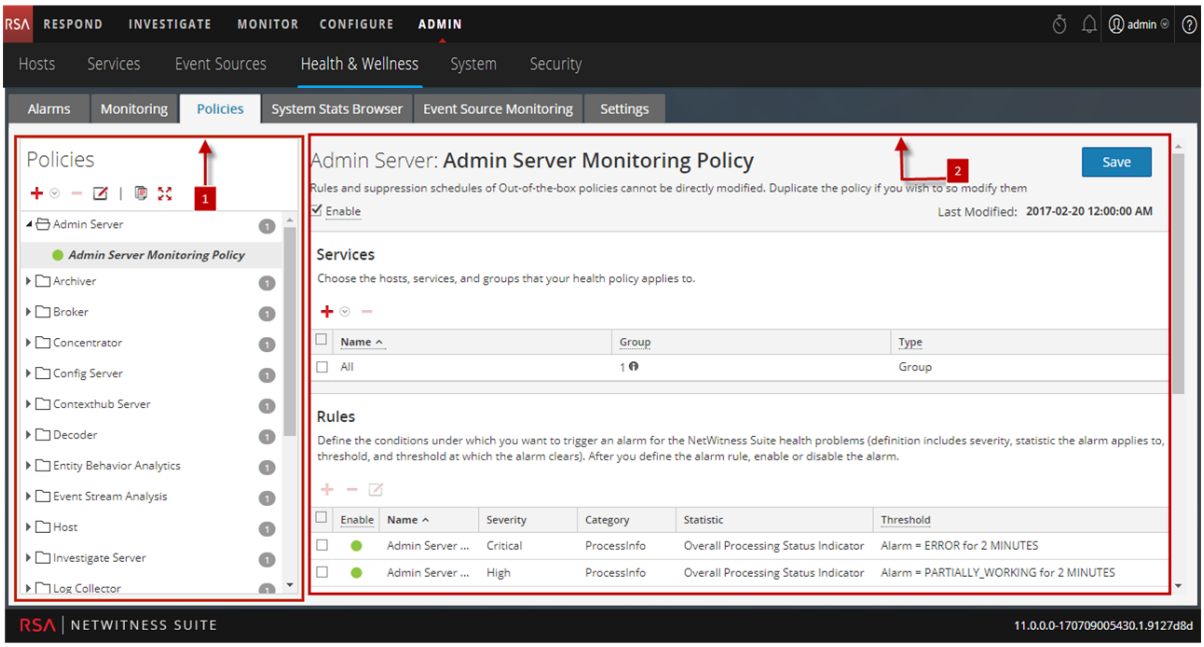
Rolle	Ziel	Details anzeigen
Administrator	Anzeigen der Richtlinien NetWitness-Server und Services	Richtlinien managen
Administrator	Hinzufügen, Bearbeiten, Duplizieren und Löschen von Richtlinien	Richtlinien managen

Verwandte Themen

Richtlinien managen

Überblick

In dieser Abbildung ist die Ansicht „Richtlinien“ zu sehen.



1 Bereich „Richtlinien“

2 Bereich „Richtliniendetails“

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.

Bereich Richtlinien

Im Bereich Richtlinien können Sie Richtlinien für Hosts und Services in diesem Bereich hinzufügen oder löschen.

Funktion	Beschreibung
	Zeigt die für die Erstellung einer neuen Richtlinie verfügbaren Servicetypen an. Wählen Sie einen Typ aus, um hierfür eine oder mehrere Richtlinien zu erstellen.
	Hiermit wird die ausgewählte Richtlinie aus dem Bereich „Richtlinien“ gelöscht. Sie können jeweils nur eine Richtlinie löschen.
	Hiermit können Sie den Namen der Richtlinie ändern.
	Erstellt eine Kopie der ausgewählten Richtlinie. Wenn Sie zum Beispiel **Erste Richtlinie** auswählen und danach auf  klicken, erstellt NetWitness Suite eine Kopie dieser Richtlinie und benennt sie mit „Erste Richtlinie (1)“.
	Erweitert die Liste der unter den Services und Hosts aufgeführten Richtlinien im Bereich **Richtlinien**.
	Verkürzt die Liste der unter den Services und Hosts aufgeführten Richtlinien im Bereich **Richtlinien**.
	Liste der • Services und Hosts, für die Sie Richtlinien erstellt haben • Standardrichtlinien von RSA, die Sie für Hosts und Services anwenden können.

Bereich Richtliniendetails

Im Bereich **Richtliniendetails** wird die im Bereich „Richtlinien“ ausgewählte Richtlinie angezeigt.

Funktion	Beschreibung
Speichern	Speichert alle in diesem Bereich eingegebenen Änderungen.
Policy-Typ	Zeigt den Typ der ausgewählten Richtlinie an.

Funktion	Beschreibung
Änderungsdatum	Zeigt das Datum an, an dem diese Richtlinie zuletzt geändert wurde.
☐ Aktivieren	Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, um die Richtlinie zu aktivieren bzw. zu deaktivieren.
Services	
	Zeigt ein Menü, in dem Sie Folgendes auswählen können: • **Gruppen**, um das Dialogfeld **Gruppen** anzuzeigen, in dem Sie die Servicegruppen für diese Richtlinie auswählen können • **Service/Host**, um das Dialogfeld **Services/Hosts** auszuwählen, in dem Sie die Services auswählen können, die zu dieser Richtlinie hinzugefügt werden sollen Lautet der Policy-Typ **Host**, steht im Menü entsprechend **Host** statt **Service**. Sie können Services anhand des Policy-Typs auswählen.
	Löscht den ausgewählten Service oder die ausgewählte Gruppe aus dieser Richtlinie.
Regeln	
	Zeigt das Dialogfeld „Regel hinzufügen“ an, in dem Sie eine Regel für diese Richtlinie definieren können.
	Löscht die ausgewählte Regel aus dieser Richtlinie.
	Zeigt das Dialogfeld „Regel bearbeiten“ für die ausgewählte Regel an.
Richtlinienunterdrückung	
	Fügt eine Zeile für den Zeitraum der Unterdrückung einer Richtlinie hinzu.

Funktion	Beschreibung
−	Löscht die ausgewählte Zeile für den Zeitbereich der Unterdrückung einer Richtlinie.
Zeitzone	Wählen Sie die Zeitzone für die Richtlinie aus der Drop-down-Liste aus. Diese Zeitzone gilt für die Unterdrückung von sowohl Richtlinien als auch Regeln.
☐	Aktivieren Sie das Kontrollkästchen, um eine Zeile für den Zeitbereich einer Richtlinienunterdrückung auszuwählen.
Tage	Wochentage, an denen die Richtlinie im jeweils angegebenen Zeitraum unterdrückt werden soll. Wählen Sie den Wochentag aus, an dem Sie die Richtlinie unterdrücken möchten. Es können beliebige Tage kombiniert oder auch alle Tage ausgewählt werden.
Zeitbereich	Zeitbereich, in dem die Richtlinie für die ausgewählten Tage unterdrückt ist.
Benachrichtigungen	
+	Fügt eine E-MAIL-Benachrichtigungszeile hinzu.
−	Löscht die ausgewählte Zeile für den Zeitbereich der Unterdrückung einer Richtlinie.
Benachrichtigungseinstellungen	Öffnet die Ansicht Benachrichtigungsserver, in der Sie die Einstellungen für E-Mail-Benachrichtigungen vornehmen können.
☐	Durch Aktivieren des Kontrollkästchens wird eine Zeile für den Zeitbereich einer Richtlinienunterdrückung ausgewählt.
Ausgabe	Der Typ der Benachrichtigung, der auf der Seite „Globale Benachrichtigungen“ festgelegt wird. Dieser kann E-Mail, SNMP, Syslog oder Skript sein.

Funktion	Beschreibung
Empfänger	Name der Person, die die Benachrichtigung erhält
Benachrichtigungsserver	Wählen Sie den E-MAIL-Benachrichtigungsserver aus. Unter „Konfigurieren von Benachrichtigungsservern“ im *Systemkonfigurationsleitfaden* finden Sie die Quelle der in dieser Drop-down-Liste enthaltenen Werte.
Vorlage	Wählen Sie die Vorlage für diese E-MAIL-Benachrichtigung aus. RSA stellt sowohl die SMTP-Standardvorlage für Integrität und Zustand als auch die Vorlage für Alarmmeldungen bereit. Unter **Konfigurieren von Benachrichtigungsvorlagen** im *Systemkonfigurationsleitfaden* finden Sie die Quelle der anderen in dieser Drop-down-Liste enthaltenen Werte. **Hinweis:** Wenn Sie in Ihren E-Mail-Benachrichtigungen zu Integrität und Zustand für die angegebenen Empfänger die Standardbetreffzeile aus der Vorlage „Integrität und Zustand“ verwenden möchten, lesen Sie die Informationen unter Einbeziehen der Standardbetreffzeile für E-Mails.

Dialogfeld „Gruppen“

Funktion	Beschreibung
Bereich **Gruppen**	
Name	Zeigt die Servicegruppen an, die Sie definiert haben. Zur Auswahl stehen: • **Alle**, um alle vorhandenen Services im Bereich **Services** anzuzeigen • Eine Gruppe zum Anzeigen der Services, die in dieser Gruppe im Bereich **Services** enthalten sind
Bereich **Services**	
Name	Zeigt den Namen des Services an.
Host	Zeigt den Host an, auf dem der Service ausgeführt wird.
Typ	Zeigt den Servicetyp an.

Dialogfeld „Regeln“

Funktion	Beschreibung
☐ Aktivieren	Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, um die Regel für diese Richtlinie zu aktivieren bzw. zu deaktivieren.
Name	Geben Sie den Namen der Regel ein.
Beschreibung	Geben Sie die Beschreibung der Regel ein. RSA empfiehlt, dass Sie folgende Informationen in dieses Feld aufnehmen. • Informationsbeschreibung: Zweck der Regel und welches Problem sie überwacht. • Korrektur: Schritte zur Behebung der Bedingung, die den Alarm für diese Regel auslöst.
Schweregrad	Wählen Sie den Schweregrad der Regel aus. Gültige Werte: • Kritisch • High • Mittel • Niedrig
Statistik	Wählen Sie die Statistik aus, die Sie mit dieser Regel überprüfen können. Zur Auswahl stehen: • statistische Kategorie aus der linken Drop-down-Liste • Statistik aus der rechten Drop-down-Liste **Hinweis:** Wählen Sie für die Richtlinie zur Public Key Infrastructure (PKI) die Kategorie PKI und eine der folgenden Statistiken aus: - NetWitness-Server PKI-Zertifikat – Ablaufdatum: Zeigt die Zeit vor dem Ablauf des Zertifikats an. - NetWitness-Server PKI CRL – Ablaufdatum: Zeigt die Zeit vor dem Ablauf der Zertifikatrückrufliste an. - NetWitness-Server PKI CRL – Status: Zeigt den aktuellen Status der CRL an. Der Ansicht „Systemstatistikbrowser“ können Sie Beispiele zu den Statistiken entnehmen, die Sie mit einer Regel überprüfen möchten.

Funktion	Beschreibung
Alarmschwellenwert	Legen Sie den Schwellenwert für die Regel fest, der den Richtlinienalarm auslöst: • Menge **Hinweis:** Das für das CRL-Ablaufdatum unterstützte Format lautet ddddhhmm, z. B.: - 10000 steht für 1 Tag -2359 steht für 23 Stunden und 59 Minuten -10023 steht für 1 Tag und 23 Minuten -3650100 steht für 365 Tage und 1 Stunde • Zeit in Minuten

Recovery	Legt fest, wann der Schwellenwert der Regel gelöscht werden soll:
	• Operator:
	  • Für NetWitness Suite 10.5 (=, !=, <, <=, > oder >=)
	  • Für NetWitness Suite 10.5.0.1 und höher (siehe Schwellenwertoperatoren)
	• Menge
	• Zeit in Minuten

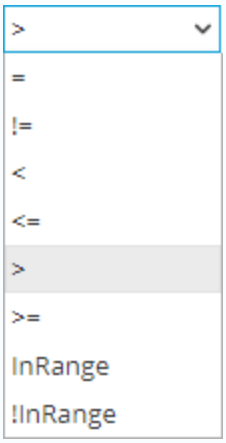
Regelunterdrückung	
+	Durch Auswahl dieser Option können Sie eine Zeile für den Zeitbereich der Regelunterdrückung hinzufügen.
−	Durch Auswahl dieser Option können Sie die ausgewählte Zeile für den Zeitbereich der Regelunterdrückung löschen.
☐	Durch Auswahl des Kontrollkästchens können Sie eine Zeile für den Zeitbereich der Regelunterdrückung auswählen.
Zeitzone: *Zeitzone*	Zeigt die Zeitzone der Richtlinie an. Legen Sie im Bereich Richtlinienunterdrückung die Zeitzone für eine Richtlinie fest.

Funktion	Beschreibung
Tage	Wochentage, an denen die Regel im jeweils angegebenen Zeitbereich unterdrückt werden soll. Wählen Sie den Wochentag aus, an dem Sie die Regel unterdrücken möchten. Es können beliebige Tage kombiniert oder auch alle Tage ausgewählt werden.
Zeitbereich	Zeitbereich, in dem die Regel für die ausgewählten Tage unterdrückt ist.

Schwellenwertoperatoren

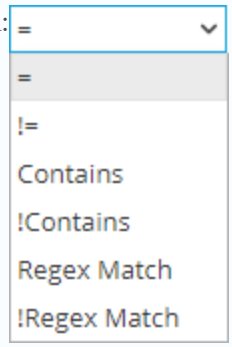
In den Feldern **Alarmschwellenwert** und **Recovery-Schwellenwert** im Dialogfeld **Regeln** müssen Sie entweder numerische Operatoren oder Zeichenfolgenoperatoren eingeben, die auf den von Ihnen angegebenen Statistikkriterien basieren.

Drop-down-Menü für numerische Operatoren:



=
!=
<
<=
>
>=
InRange
!InRange

Drop-down-Menü für Zeichenfolgenoperatoren:

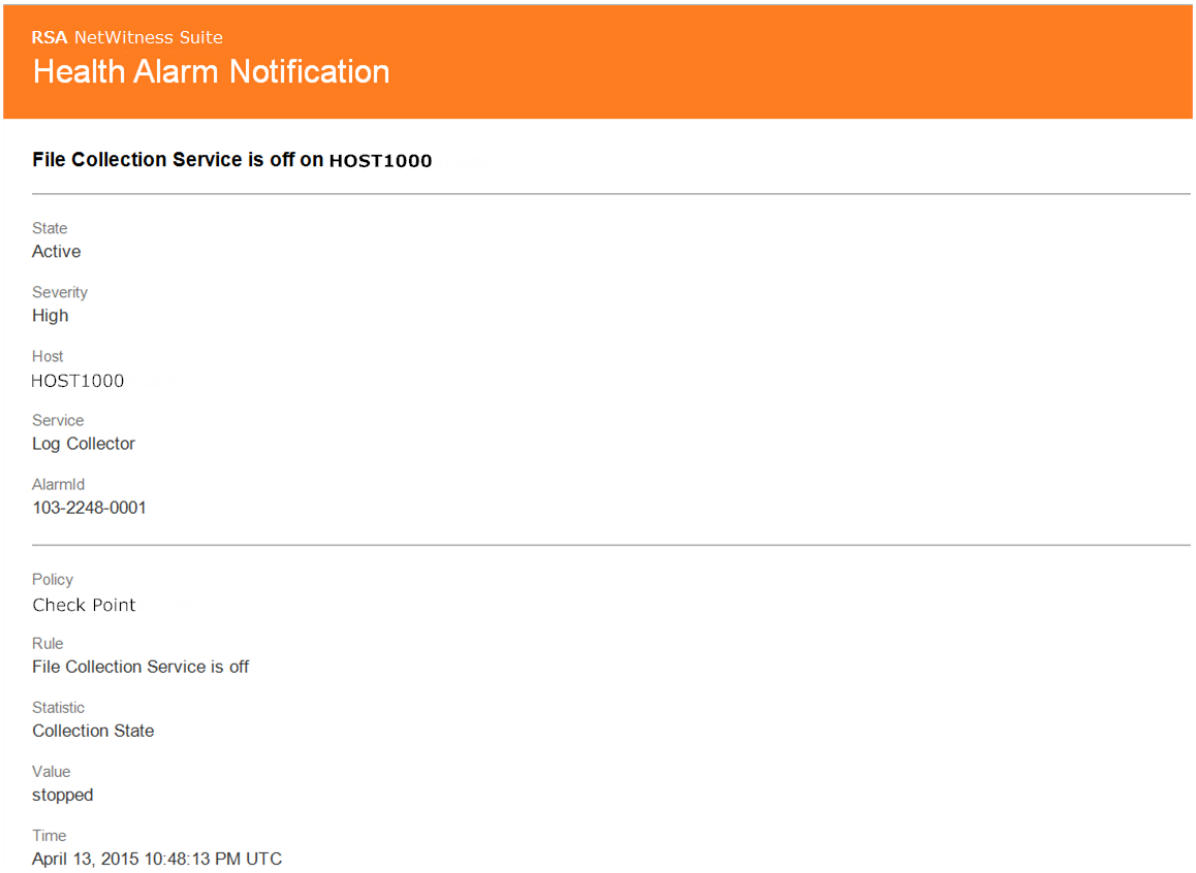


=
!=
Contains
!Contains
Regex Match
!Regex Match

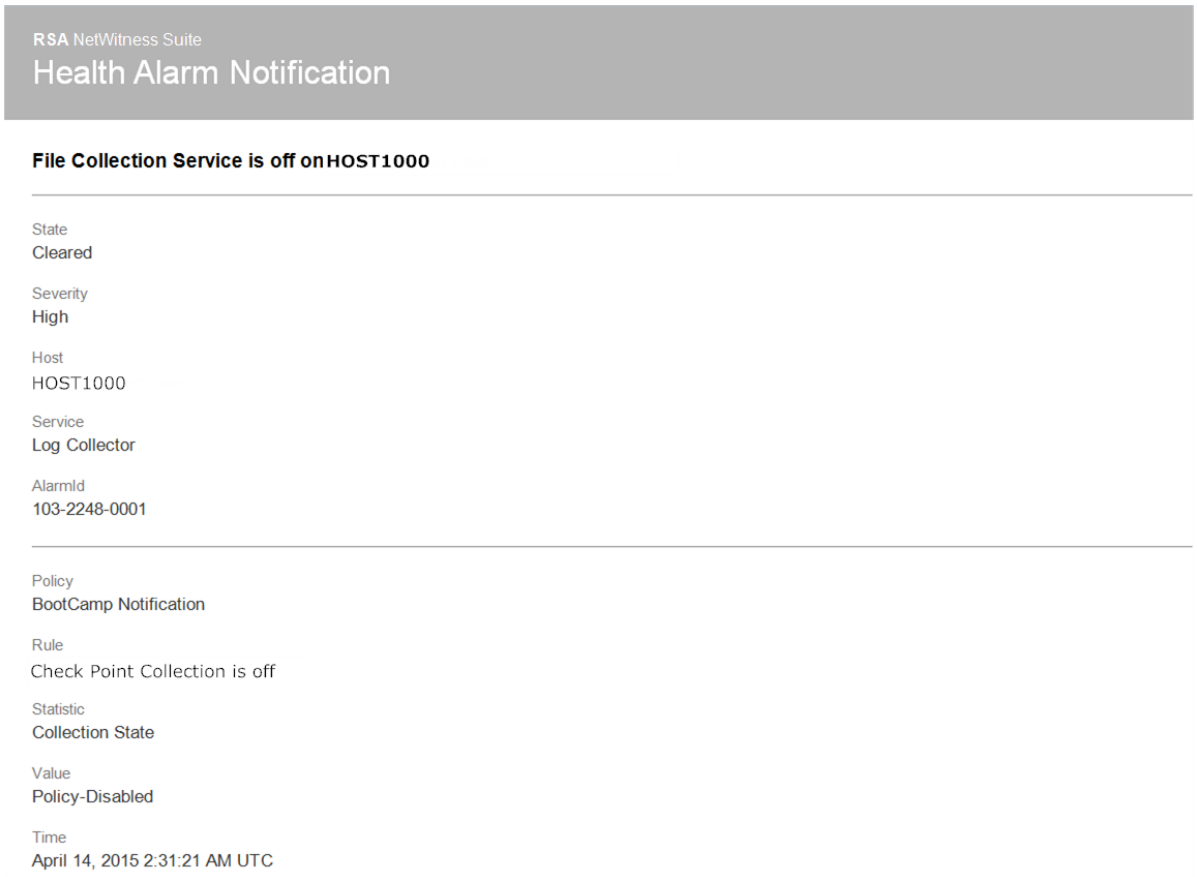
E-Mail-Vorlagen für RSA Integrität und Zustand

Hinweis: Wenn Sie in Ihren E-Mail-Benachrichtigungen zu Integrität und Zustand für die angegebenen Empfänger die Standardbetreffzeile aus der Vorlage „Integrität und Zustand“ verwenden möchten, lesen Sie die Informationen unter Einbeziehen der Standardbetreffzeile für E-Mails.

Standard-SMTP-Vorlage für Integrität und Zustand



Vorlage für Alarmmeldungen



Vordefinierte Richtlinien für NetWitness Suite

In der folgenden Tabelle sind die vordefinierten NetWitness Suite-Richtlinien mit den für die einzelnen Richtlinien definierten Regeln aufgeführt.

Auf dieser Registerkarte können Sie folgende Aufgaben für diese Richtlinien ausführen:

- Ändern der Service-/Gruppenzuweisungen
- Aktivieren/Deaktivieren der Zuweisungen

Folgende Aufgaben können Sie nicht für diese Richtlinien ausführen:

- Löschen der Richtlinien
- Bearbeiten der Richtliniennamen

Hinweis: Weitere Informationen über die vordefinierten Richtlinien finden Sie in der Benutzeroberfläche unter „
Integrität und Zustand“ > „Richtlinien“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
	Ausfall der Kommunikation zwischen dem Security Analytics-Masterhost und einem Remotehost	Mindestens 10 Minuten lang ist der Host nicht verfügbar, das Netzwerk ist nicht bereit, Message Broker wird heruntergefahren oder Sicherheitszertifikate sind ungültig oder fehlen.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness-Server Überwachungsrichtlinie	Kritische Nutzung des Rabbitmq Message Broker-Dateisystems	Für `var/lib/rabbitmq` übersteigt die Datenträgernutzung des gemounteten Dateisystems 75 %.
	Dateisystem ist ausgelastet.	Die gesamte Datenträgernutzung des gemounteten Dateisystems erreicht 100 %.
	Hohe Nutzung des Dateisystems	Die gesamte Datenträgernutzung des gemounteten Dateisystems übersteigt 95 %.
	Hohe Nutzung des System-Swap	Die Swap-Nutzung liegt mindestens 5 Minuten lang unter 5 %.
	Hohe Nutzung des Rabbitmq Message Broker-Dateisystems	Datenträgernutzung des gemounteten Dateisystems für `var/lib/rabbitmq` übersteigt 60 %.
	Host nicht erreichbar	Der Host wird nicht ausgeführt.
	Status des LogCollector-Ereignisprozessors mit Exchange-Bindungen	Es gibt mindestens 10 Minuten lange Probleme mit der Message Broker-Warteschlange für die Protokollsammlung.
	Warteschlange des LogCollector-Ereignisprozessors ohne Bindungen	Es gibt mindestens 10 Minuten lange Probleme mit der Message Broker-Warteschlange für die Protokollsammlung.

Richtlinienname	Name der Regel	Ausgelöster Alarm
	Warteschlange des LogCollector-Ereignisprozessors ohne Verbraucher	Es gibt mindestens 10 Minuten lange Probleme mit der Message Broker-Warteschlange für die Protokollsammlung.
	Netzteil-Ausfall	Der Host ist nicht eingeschaltet.
	Logisches RAID-Laufwerk heruntergestuft	Der Laufwerksstatus für ein logisches RAID-Laufwerk lautet „Heruntergestuft“ oder „Teilweise heruntergestuft“.
	Fehler am logischen RAID-Laufwerk	Der Laufwerksstatus für ein logisches RAID-Laufwerk ist „Offline“, „Fehlgeschlagen“ oder „Unbekannt“.
	Erneuter Aufbau des logischen RAID-Laufwerks	Der Laufwerksstatus für ein logisches RAID-Laufwerk ist „Erneuter Aufbau“.
	Fehler am physischen RAID-Laufwerk	Der Status das physischen RAID-Laufwerks ist nicht „Online“, „Online, Spun Up“ oder „HotSpare“.
	Vorhergesagter Fehler am physischen RAID-Laufwerk	Der Zähler für vorhergesagte Fehler am phyischen RAID-Laufwerk ist größer 1.
	Erneuter Aufbau des physischen RAID-Laufwerks	Der Laufwerksstatus für ein physisches RAID-Laufwerk ist „Erneuter Aufbau“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
	Nicht konfiguriertes physisches RAID-Laufwerk	Der Laufwerksstatus des physischen RAID-Laufwerks ist „Unconfigured (good)“.
	Fehler an SD-Karte	Der Status der SD-Karte ist nicht „OK“.
NetWitness SuiteRichtlinie für die Überwachung von Archiver	Archiver-Aggregation beendet	Der Status von Archiver lautet nicht „gestartet“.
	Archiver-Datenbank(en) nicht geöffnet	Der Datenbankstatus lautet nicht „geöffnet“.
	Archiver nutzt den Service nicht	Der Gerätestatus lautet nicht „wird genutzt“.
	Archiver-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Archiver-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness SuiteRichtlinie für die Überwachung von Broker	Broker >5 anstehende Abfragen	10 Minuten lang sind mindestens 5 Abfragen ausstehend.
	Broker-Aggregation beendet	Der Status von Broker lautet nicht „gestartet“.
	Broker nutzt den Service nicht	Der Gerätestatus lautet nicht „wird genutzt“.
	Broker-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Broker-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	Broker-Sitzungsrate gleich null	Die (derzeitige) Sitzungsrate beträgt mindestens eine Minute lang 0.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Concentrator	Concentrator >5 anstehende Abfragen	10 Minuten lang sind mindestens 5 Abfragen ausstehend.
	Concentrator-Aggregation >100K Sitzungen zurück	Gerätesitzungen sind mindestens 1 Minute lang größer oder gleich 100.000 Sitzungen zurück.
	Concentrator-Aggregation >1M Sitzungen zurück	Gerätesitzungen sind mindestens 1 Minute lang größer oder gleich 1.000.000 Sitzungen zurück
	Concentrator-Aggregation >50M Sitzungen zurück	Gerätesitzungen sind mindestens 1 Minute lang größer oder gleich 50.000.000.Sitzungen zurück
	Concentrator-Aggregation beendet	Der Status von Broker lautet nicht „gestartet“.
	Concentrator-Datenbank(en) nicht geöffnet	Der Datenbankstatus lautet nicht „geöffnet“.
	Concentrator-Metarate Null	Die (aktuelle) Metarate von Concentrator beträgt mindestens 2 Minuten lang 0.
	Concentrator nutzt den Service nicht	Der Gerätestatus lautet nicht „wird genutzt“.
	Concentrator-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Concentrator-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness SuiteRichtlinie für die Überwachung von Decoder	Erfassung durch Decoder nicht gestartet	Der Erfassungsstatus lautet nicht „gestartet“.
	Erfassungsrate Decoder Null	Die (aktuelle) Erfassungsrate beträgt mindestens 2 Minuten lang 0.
	Decoder-Datenbank nicht geöffnet	Der Datenbankstatus lautet nicht „geöffnet“.
	Decoder hat >1 % der Pakete abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 1 %.
	Decoder hat >10 % der Pakete abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 10 %.
	Decoder hat >5 % der Pakete abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 5 %.
	Der Erfassungspaketpool von Decoder ist erschöpft	Die Warteschlage für die Paketerfassung ist mindestens 2 Minuten lang 0.
	Decoder-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Decoder-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Event Stream Analysis	ESA-Gesamtspeicherauslastung > 85 %	Die gesamte prozentuale Speichernutzung durch ESA ist größer oder gleich 85 %.
	ESA-Gesamtspeicherauslastung > 95 %	Die gesamte prozentuale Speichernutzung durch ESA ist größer oder gleich 95 %.
	ESA-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	ESA-Testregeln deaktiviert	Der Status der Testregeln lautet nicht „aktiviert“.
NetWitness Suite Richtlinie für die Überwachung von IPDB Extractor	IPDB Extractor-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	IPDB Extractor-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
NetWitness Suite Richtlinie für die Überwachung von Incident-Management	Incident Management-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Log Collector	Log Collector-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	Log Decoder-Ereignisquelle >50 % voll	Die Anzahl der derzeit in der Warteschlange vorhandenen Ereignisse nutzt mindestens 50 % der Warteschlange.
	Log Decoder-Ereignisquelle >80 % voll	Die Anzahl der derzeit in der Warteschlange vorhandenen Ereignisse nutzt mindestens 80 % der Warteschlange.
	Log Collector-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness SuiteRichtlinie für die Überwachung von Log Decoder	Decoder hat > 10 % der Pakete abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 10 %.
	Protokollerfassung nicht gestartet	Der Erfassungsstatus lautet nicht „gestartet“.
	Erfassungsrate Log Decoder Null	Die (aktuelle) Erfassungsrate beträgt mindestens 2 Minuten lang 0.
	Log Decoder-Datenbank nicht geöffnet	Der Datenbankstatus lautet nicht „geöffnet“.
	Log Decoder hat >1 % der Protokolle abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 1 %.
	Log Decoder hat >5 % der Protokolle abgelegt	Der Prozentsatz der abgelegten Erfassungspakete ist (derzeit) größer oder gleich 5 %.
	Der Erfassungspaketpool von Log Decoder ist erschöpft	Die Warteschlage für die Paketerfassung ist mindestens 2 Minuten lang 0.
	Log Decoder-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	Log Decoder-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Malware Analysis	Malware Analysis-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Reporting Engine	Kritische Verwendung von Reporting Engine-Warnmeldungen	Es werden mindestens 5 Minuten lang größer oder gleich 10 Warnmeldungen verwendet.
	Verfügbarer Datenträgerplatz für Reporting Engine <10 %	Der verfügbare Speicherplatz auf dem Datenträger beträgt weniger als 10 %.
	Verfügbarer Datenträgerplatz für Reporting Engine <5 %	Der verfügbare Speicherplatz auf dem Datenträger beträgt weniger als 5 %.
	Kritische Verwendung von Reporting Engine-Diagrammen	Es werden mindestens 5 Minuten lang größer oder gleich 10 Diagramme verwendet.
	Kritische Verwendung von Reporting Engine-Regeln	Es werden mindestens 5 Minuten lang größer oder gleich 10 Regeln verwendet.
	Kritische Verwendung von Reporting Engine-Pools für geplante Aufgaben	Es werden mindestens 15 Minuten lang größer oder gleich 10 Pools für geplante Aufgaben verwendet.
	Reporting Engine-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	Kritische Verwendung von freigegebenen Aufgaben in Reporting Engine	Es werden mindestens 5 Minuten lang größer oder gleich 10 Pools für freigebene Aufgaben verwendet.

Richtlinienname	Name der Regel	Ausgelöster Alarm
NetWitness Suite Richtlinie für die Überwachung von Warehouse Connector	Warehouse Connector-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Warehouse Connector-Service angehalten	Der Serverstatus lautet nicht „gestartet“.
	Warehouse Connector-Stream zurück	Der Stream ist größer oder gleich 2000000 zurück.
	Warehouse Connector-Stream Datenträgernutzung > 75 %	Die Datenträgernutzung des Stream (Anstehende Ziellast) ist größer oder gleich 75.
	Warehouse Connector-Stream in schlechtem Zustand	Der Streamstatus zeigt mindestens 10 Minuten lang keine Nutzung oder ist nicht online
	Permanent durch den Warehouse Connector-Stream abgelehnte Dateien > 300	Die Anzahl der permanent abgelehnten Daten beträgt größer oder gleich 300.
	Permanent durch den Warehouse Connector-Stream abgelehnte Ordner > 75 % voll	Die Nutzung durch abgelehnte Ordner ist größer oder gleich 75 %.
NetWitness Suite Richtlinie für die Überwachung von Workbench	Workbench-Service in schlechtem Zustand	Der Status des Services lautet nicht „gestartet“ oder „bereit“.
	Workbench-Service angehalten	Der Serverstatus lautet nicht „gestartet“.

Ansicht „Systemstatistikbrowser“

NetWitness Suite bietet die Möglichkeit, den Status und den Betrieb der Hosts und Services zu überwachen. Die Registerkarte Systemstatistikbrowser zeigt wichtige Statistiken, Servicesysteminformationen und Hostsysteminformationen für einen Host oder Service an.

Sie können die Statistikansicht abhängig von dem zur Filterung der Daten ausgewählten Parameter anpassen.

So greifen Sie auf die Ansicht „Systemstatistikbrowser“ zu:

1. Navigieren Sie zu **ADMIN > Integrität und Zustand**.

   Die Ansicht „Integrität und Zustand“ wird mit geöffneter Registerkarte „Alarme“ angezeigt.
2. Klicken Sie auf die Registerkarte **Systemstatistikbrowser**.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Anzeigen des Verlaufsdiagramms für Systemstatistiken	Verlaufsdiagramm für Systemstatistiken

Verwandte Themen

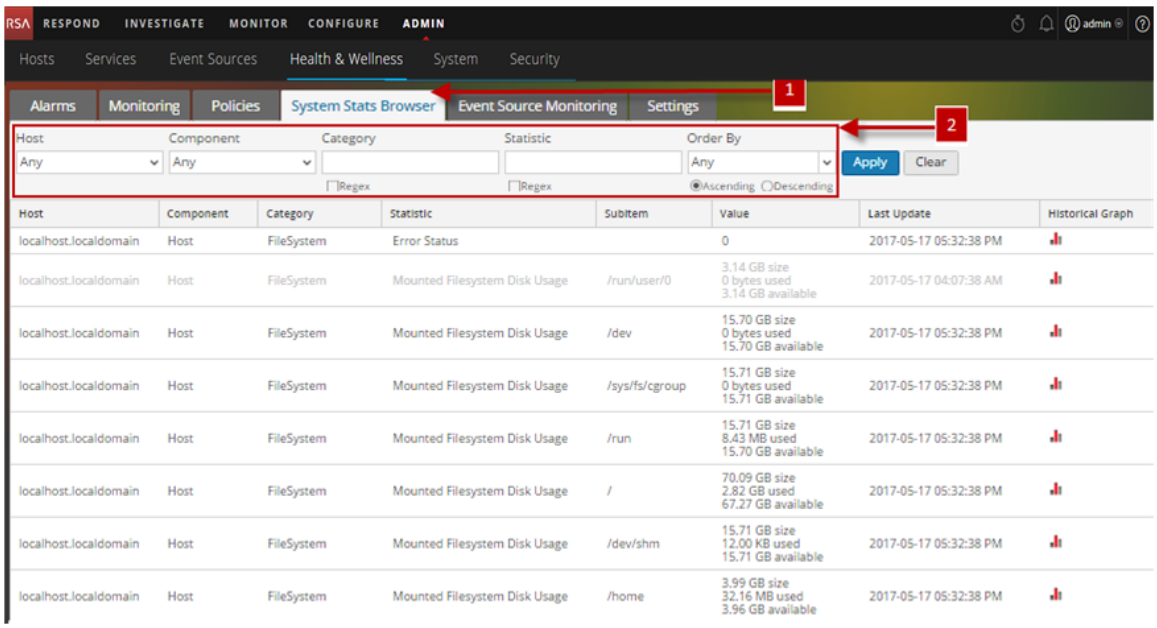
Überwachen von Servicestatistiken

Filtersystemstatistiken

Anzeigen eines Verlaufsdiagramms für Systemstatistiken

Überblick

Die Ansicht „Systemstatistikbrowser“ wird angezeigt.



1 Zeigt die Ansicht „Systemstatistikbrowser“ an.

2 Die Symbolleiste können Sie zum Filtern und Anpassen der Ansicht „Systemstatistikbrowser“ verwenden.

Filter

In dieser Tabelle werden die verschiedenen Parameter aufgeführt, die Sie verwenden können, um die Ansicht „Systemstatistiken“ zu filtern und anzupassen.

Parameter	Beschreibung
Host	Wählen Sie einen Host aus dem Drop-down-Menü aus, um die Statistiken des ausgewählten Hosts anzuzeigen. Wählen Sie **Jede**, um alle verfügbaren Hosts aufzulisten.
Komponente	Wählen Sie eine Komponente aus dem Drop-down-Menü aus, um die Statistiken der ausgewählten Komponente anzuzeigen. Wählen Sie **Jede** aus, um alle Komponenten auf einem ausgewählten Host aufzulisten.

Parameter	Beschreibung
Kategorie	Geben Sie die Kategorie ein, um die Statistiken für die erforderliche Kategorie anzuzeigen. Wählen Sie Regex aus, um den Regex-Filter zu aktivieren. Der Text wird nach einem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Wenn „Regex“ nicht ausgewählt ist, wird Globbing per Musterzuordnung unterstützt.
Statistik	Geben Sie die Statistik ein, um die erforderliche Statistik auf allen Hosts oder Komponenten anzuzeigen. Wählen Sie Regex aus, um den Regex-Filter zu aktivieren. Der Text wird nach einem regulären Ausdruck durchsucht und die angegebene Kategorie wird aufgelistet. Wenn „Regex“ nicht ausgewählt ist, wird Globbing per Musterzuordnung unterstützt.
Sortieren nach	Wählen Sie die Reihenfolge aus, in der die Liste gefiltert werden muss. Wählen Sie Aufsteigend aus, um die Liste in aufsteigender Reihenfolge zu filtern.

Befehle

Befehl	Aktion
Anwenden	Klicken Sie hierauf, um die ausgewählten Filter anzuwenden und die Liste entsprechend anzuzeigen.
Clear	Klicken Sie hierauf, um die ausgewählten Filter zu löschen.

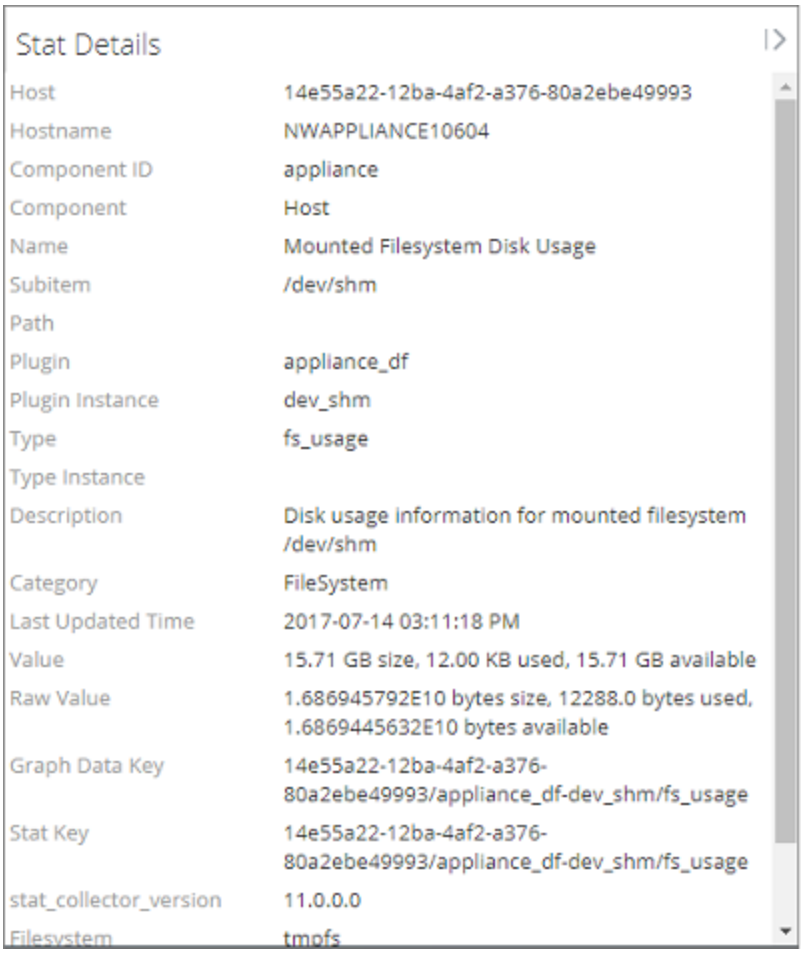
Ansicht „Systemstatistik“

Zeigt Statistiken, Servicesysteminformationen und Hostsysteminformationen für einen Host oder Service an.

Zugreifen auf Statistikdetails

Wählen Sie eine der Statistiken aus und klicken Sie auf **Statistikdetails** auf der rechten Seite des Bereichs.

Der Bereich „Statistikdetails“ wird mit Details der ausgewählten Statistiken geöffnet.



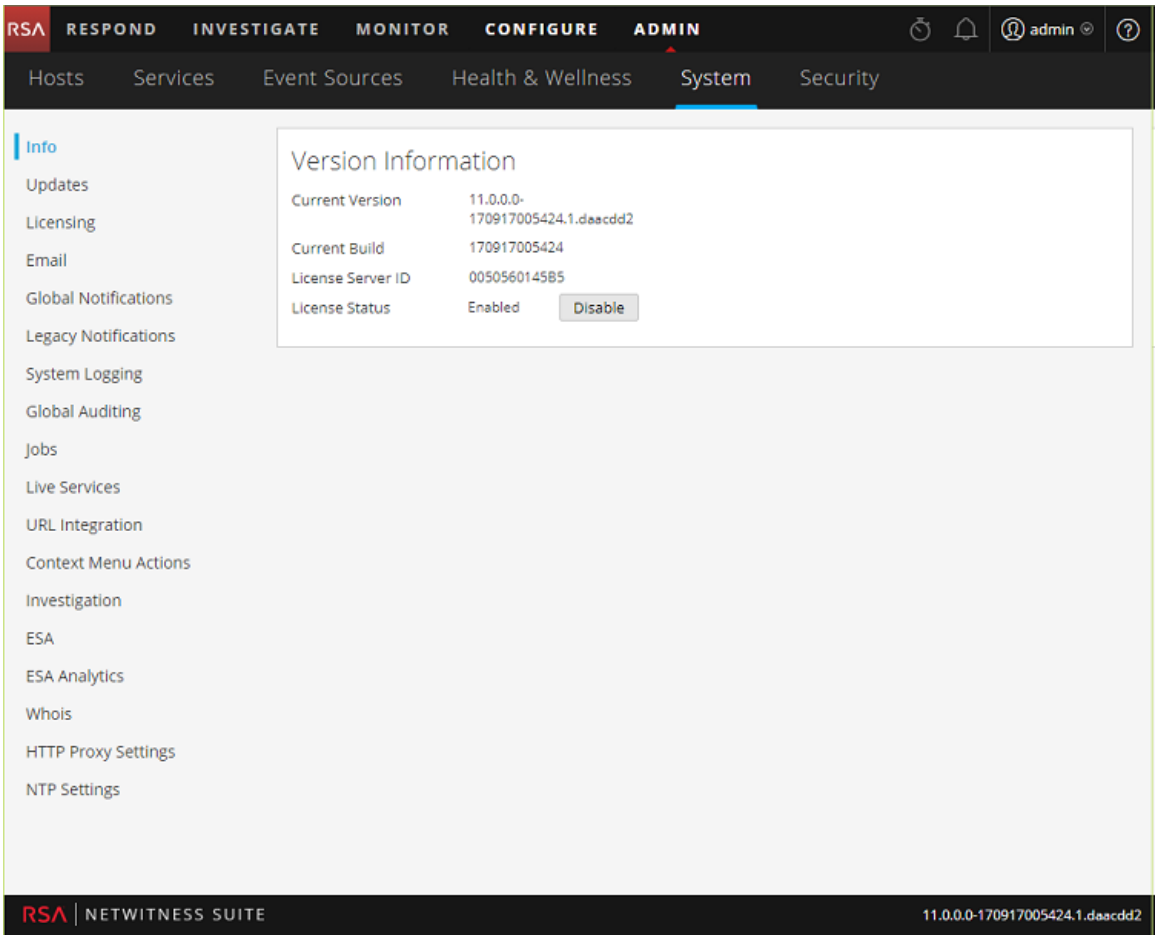
Ansicht „System“ – Bereich „Systeminfo“

In diesem Thema wird der Bereich „Systeminformationen“ erläutert, in dem Informationen über die Systemversion und den Lizenzstatus angezeigt werden.

Die erforderliche Rolle für den Zugriff auf diese Ansicht ist **Managen von Systemeinstellungen**.

Um auf diese Ansicht zuzugreifen, führen Sie einen der folgenden Schritte aus:

- Navigieren Sie zu **ADMIN > System**.
  Der Bereich „Systeminformationen“ wird standardmäßig angezeigt.
- Wenn im Benachrichtigungsbereich die Benachrichtigung eingeblendet wird, dass eine neue Version von NetWitness Suite verfügbar ist, klicken Sie auf **Anzeigen**.



Im Abschnitt „Versionsinformationen“ werden Versionsinformationen zur derzeit installierten NetWitness Suite-Version angezeigt. In der folgenden Tabelle sind die Funktionen des Abschnitts Versionsinformationen beschrieben.

Name	Beschreibung
Vorhandene Version	Gibt an, welche Version von Security Analytics derzeit ausgeführt wird. Das Format der Version lautet *major-relase.minor-release.stability-id.build-number*. Mögliche Werte für *stability-id* sind: • 1 - Entwicklung • 2 - Alpha • 3 - Beta • 4 - RC • 5 - Gold

Name	Beschreibung
Aktueller Build	Gibt die aktuelle Buildversion zum Troubleshooting an.
Lizenzserver-ID	Jeder Clienthost wird mit installiertem Local Licensing Server (LLS) zum Managen der Hostlizenzen ausgeliefert. Dieses Feld gibt an, ob der LLS für diese Instanz von Security Analytics installiert ist. • Wenn der LLS installiert ist, wird die Lizenzierungsserver-ID angezeigt. • **Unbekannt** gibt an, dass der LLS nicht installiert ist.
Lizenzstatus	Gibt an, ob die Lizenz aktiviert ist. Ist die Lizenz • aktiviert, so wird **Aktiviert** in diesem Feld angezeigt. Mit der Schaltfläche **Deaktivieren** rechts davon kann sie deaktiviert werden. • deaktiviert, so wird **Deaktiviert** in diesem Feld angezeigt. Mit der Schaltfläche **Aktivieren** rechts davon kann sie aktiviert werden.

Bereich „Systemaktualisierungen“ – Registerkarte „Einstellungen“

In der Registerkarte „Systemaktualisierungseinstellungen“ wird die Benutzeroberfläche beschrieben, die Sie zum Herstellen einer Verbindung mit dem Live-Update-Repository verwenden. Diese Einstellungen gewährleisten, dass NetWitness Suite das Live-Update-Repository erreichen und mit Ihrem lokalen Update-Repository synchronisieren kann.

Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist **Systemupdates anwenden**.

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie **Updates**.

Was möchten Sie tun?

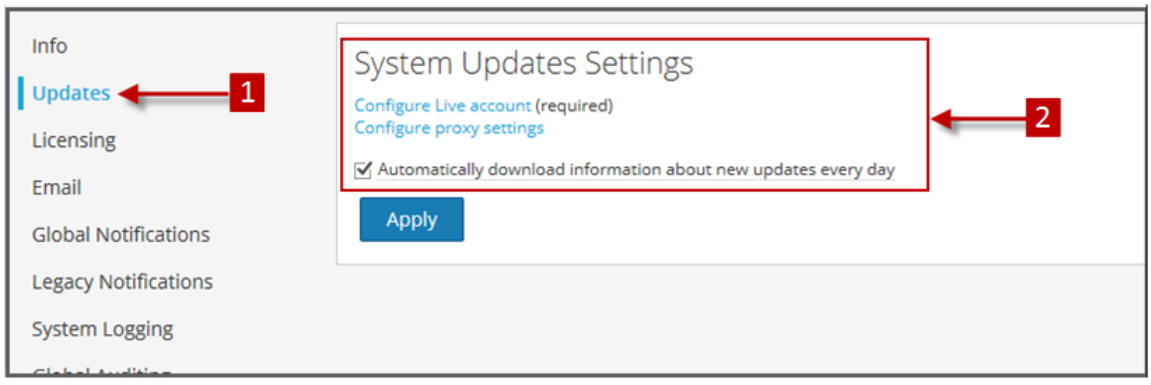
Rolle	Ziel	Details anzeigen
Administrator	Automatischer Herunterladen von Aktualisierungen	Automatische Synchronisation mit dem RSA-Update-Repository aktivieren

Verwandte Themen

Managen von NetWitness Suite-Aktualisierungen

Überblick

Der Bereich „Systemaktualisierungseinstellungen“ wird angezeigt.



1	Zeigt die Registerkarte „Einstellungen Systemaktualisierungen“ an.
2	Konfiguriert das Konto und die Einstellung für automatische Updates.

Funktionen

In dieser Tabelle werden die Funktionen der Registerkarte „Systemaktualisierungseinstellungen“ beschrieben.

Funktion	Beschreibung
Live-Konto konfigurieren	Zeigt den Bereich **ADMIN** > **System** > **Live-Services** an, in dem Sie Ihre Anmeldedaten des Live-Kontos konfigurieren können, sofern diese nicht konfiguriert sind.
Konfigurieren von Proxyeinstellungen	Zeigt den Bereich Administration **ADMIN** > **System** > **HTTP-Proxyeinstellungen** an, in dem Sie einen HTTP-Proxy konfigurieren können, sofern dieser nicht konfiguriert ist.
Informationen über neue Aktualisierungen täglich automatisch herunterladen	Wählen Sie diese Option, um die automatische Synchronisation mit dem RSA-Update-Repository zu aktivieren. Wenn Aktualisierungen verfügbar sind, wird dies automatisch im Bereich **ADMIN** > **HOSTS** angezeigt.
Anwenden	Wendet die Einstellungen dieser Registerkarte an.

Systemprotokollierung – Ansicht „Einstellungen“

Über die RSA NetWitness Suite-Ansicht „Einstellungen“ des Bereichs „Systemprotokollierung“ werden die Größe der Protokolldateien, die Anzahl der aufbewahrten Backupprotokolldateien sowie die standardmäßigen Protokollierungsebenen für die Pakete in NetWitness Suite konfiguriert. Das Thema **Konfigurieren von Protokolldateieinstellungen** im *Systemkonfigurationsleitfaden*enthält ausführliche Verfahren.

So rufen Sie die Registerkarte „Einstellungen“ auf:

1. Navigieren Sie zu **ADMIN > System**.
2. Wählen Sie im Bereich „Optionen“ die Option **Systemprotokollierung** aus.
   Der Bereich „Systemprotokollierung“ wird standardmäßig mit angezeigter Registerkarte „Echtzeit“ geöffnet.
3. Klicken Sie auf die Registerkarte **Einstellungen**.

Was möchten Sie tun?

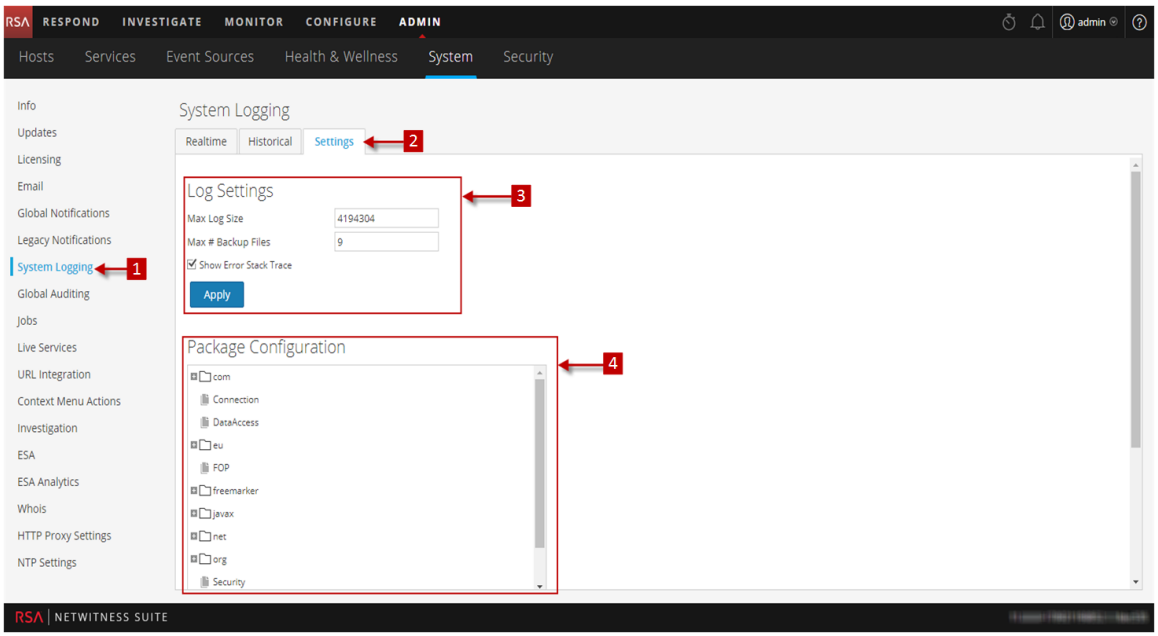
Rolle	Ziel	Details anzeigen
Administrator	Konfigurieren der Größe der Protokolldateien	Einrichten der Symbolleiste „Protokolleinstellungen“

Verwandte Themen

Systemprotokollierung – Registerkarte „Verlauf“

Systemprotokollierung – Registerkarte „Echtzeit“

Überblick



1	Zeigt den Bereich „Systemprotokollierung“ an.
2	Zeigt die Registerkarte „Einstellungen“ an.
3	In diesem Abschnitt kann der Benutzer Protokolleinstellungen konfigurieren.

4 In diesem Abschnitt kann der Benutzer das Paket konfigurieren.

Funktionen

Die Registerkarte **Einstellungen** besteht aus zwei Abschnitten: Protokolleinstellungen und Paketkonfiguration.

Protokolleinstellungen

Im Abschnitt „Protokolleinstellungen“ können die Größe der NetWitness Suite-Protokolldateien und die Anzahl der von NetWitness Suite aufbewahrten Backupprotokolle konfiguriert werden.

Funktion	Beschreibung
Max. Protokollgröße	Konfiguriert die maximale Größe für jede Protokolldatei in Byte. Der Mindestwert für diese Einstellung beträgt **4096**.
Max. Anzahl Backupdateien	Gibt an, wie viele Backupprotokolldateien 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.
Fehlerstapelüberwachung anzeigen	Aktivieren Sie das Kontrollkästchen, um die Protokollmeldungen ERROR, STACK und TRACE anzuzeigen.
Anwenden	Wendet die Einstellungen sofort auf alle zukünftigen Protokolle an.

Paketkonfiguration

Der Abschnitt Paketkonfiguration zeigt die NetWitness Suite-Pakete in einer Baumstruktur an.

Feature	Beschreibung
Paketstruktur	Die Struktur umfasst alle Pakete, die in NetWitness Suite verwendet werden. Sie können einen Drill-down in die Struktur durchführen, um die Protokollebenen jedes Pakets anzuzeigen. Die Protokollebene **root** ist die standardmäßige Protokollebene für alle Pakete, für die keine Ebene explizit festgelegt wird. Die root-Ebene ist auf **INFO** gesetzt.

Feature	Beschreibung
Feld Paket	In dieses Feld wird der Name des ausgewählten Pakets eingetragen, das Sie in der **Paketstruktur** ausgewählt haben.
Protokollebene	Wenn für das ausgewählte Paket eine Protokollebene festgelegt wurde, wird der Wert im Feld **Protokollebene** angezeigt.
Rekursiv zurücksetzen	Aktivieren Sie das Kontrollkästchen, um das Protokoll rekursiv zurückzusetzen.
Anwenden	Wendet die Einstellungen sofort auf alle zukünftigen Protokolle an.
Zurücksetzen	Über diese Schaltfläche wird das ausgewählte Paket auf die Protokollebene **root** zurückgesetzt.

Systemprotokollierung – Registerkarte „Echtzeit“

In diesem Thema werden die Funktionen unter Systemprotokollierung auf der Registerkarte Echtzeit sowie in der Ansicht Serviceprotokolle auf der Registerkarte Echtzeit beschrieben.

Auf der Registerkarte **Echtzeit** befindet sich eine Ansicht des NetWitness Suite-Protokolls bzw. eines Serviceprotokolls. Wenn die Ansicht neu geladen wird, enthält sie die letzten 10 Protokolleinträge. Werden neue Einträge verfügbar, wird die Ansicht mit diesen Einträgen aktualisiert.

So greifen Sie auf Registerkarte Echtzeit zu:

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

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Anzeigen von Details zu einem Protokolleintrag	Anzeigen von System- und Serviceprotokollen

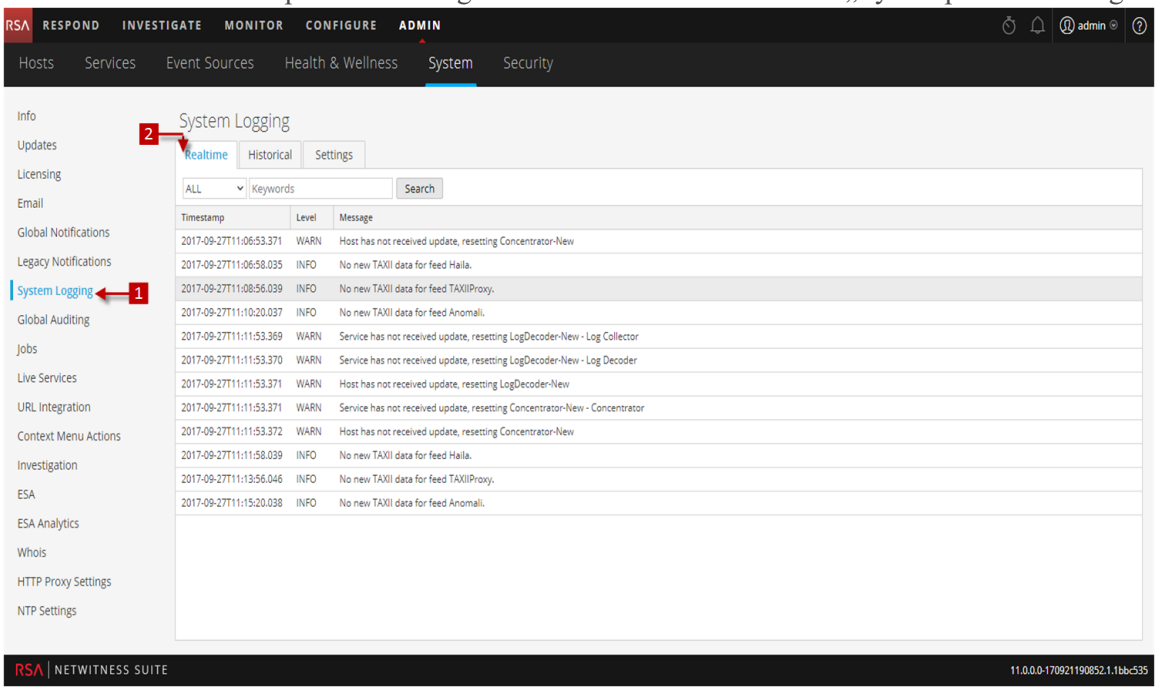
Verwandte Themen

Systemprotokollierung – Ansicht „Einstellungen“

Systemprotokollierung – Registerkarte „Verlauf“

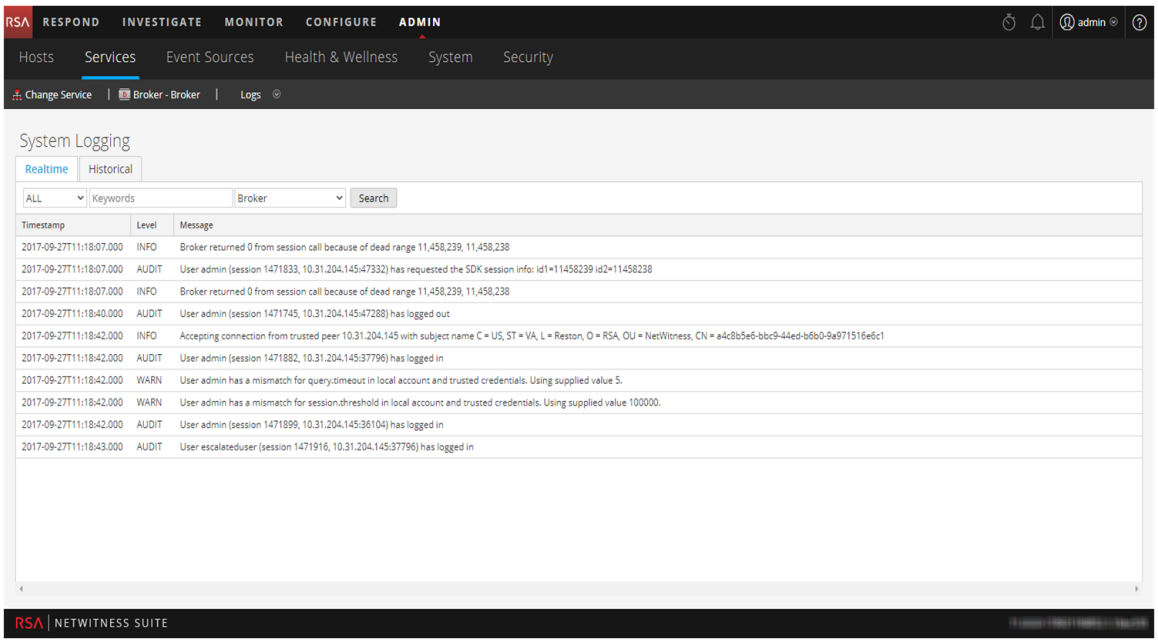
Überblick

Hier sehen Sie ein Beispiel für die Registerkarte **Echtzeit** im Bereich „Systemprotokollierung“.



1	Zeigt den Bereich „Systemprotokollierung“ an.
2	Zeigt die Registerkarte „Echtzeit“ an.

Hier sehen Sie ein Beispiel für die Registerkarte **Echtzeit** in der Ansicht „Serviceprotokolle“, die sehr ähnlich ist.



Funktionen

Auf der Registerkarte **Echtzeit** befindet sich eine Symbolleiste mit Eingabefeldern, über die Sie die Einträge filtern können. Unterhalb der Symbolleiste sehen Sie das Raster mit den Protokolleinträgen.

Symbolleiste

Funktion	Beschreibung
Drop-down-Menü „Protokollebene“ 	Wählt die Protokollebene für Einträge aus, die im Raster angezeigt werden. Das Drop-down-Menü **Protokollebene** zeigt die verfügbaren Protokollebenen für das System oder den Service an. • Systemprotokolle haben sieben Protokollebenen. • Serviceprotokolle haben nur sechs Protokollebenen, da sie nicht über die Ebene **TRACE** verfügen. • Der Standardwert ist **ALLE** Protokolleinträge.

Funktion	Beschreibung
Feld Schlüsselwörter	Gibt ein Schlüsselwort für das Filtern von Einträgen vor. Dieses Feld ist bei der System- und Servicefilterung identisch.
Feld Service (nur Serviceprotokolle)	Gibt den bei der Filterung von Serviceprotokolleinträgen zu verwendenden Servicetyp an. Mögliche Werte sind der Host oder der Service.
Schaltfläche Filter	Über diese Schaltfläche aktivieren Sie den Filter nach Protokollebene, Schlüsselwörtern und Serviceauswahl.

Spalten im Protokollraster

Spalte	Beschreibung
Timestamp	Dies ist der Zeitstempel für den Eintrag.
Level	Dies ist die Protokollebene für die Meldung.
Meldung	Dies ist der Text des Protokolleintrags.

Systemprotokollierung – Registerkarte „Verlauf“

Die Registerkarte „Verlauf“ bietet eine durchsuchbare Ansicht des NetWitness Suite-Protokolls oder des Serviceprotokolls in einer Seitenansicht. Wenn es erstmals geladen wird, wird im Raster die letzte Seite der Protokolleinträge für das System angezeigt.

So greifen Sie auf die Registerkarte „Verlauf“ zu:

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

   Der Bereich „Systemprotokollierung“ wird standardmäßig mit angezeigter Registerkarte **Echtzeit** geöffnet.
3. Klicken Sie auf die Registerkarte **Historisch**.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Anzeigen des Verlaufsdiagramms	Verlaufsdiagramm für Systemstatistiken

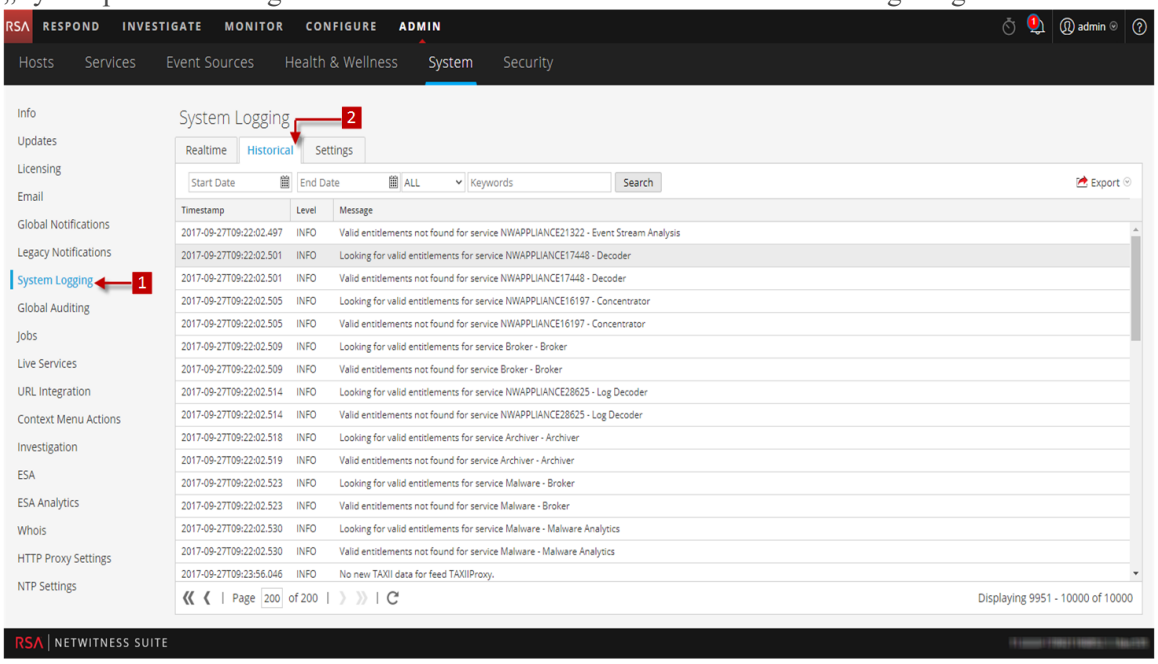
Verwandte Themen

Systemprotokollierung – Registerkarte „Echtzeit“

Systemprotokollierung – Ansicht „Einstellungen“

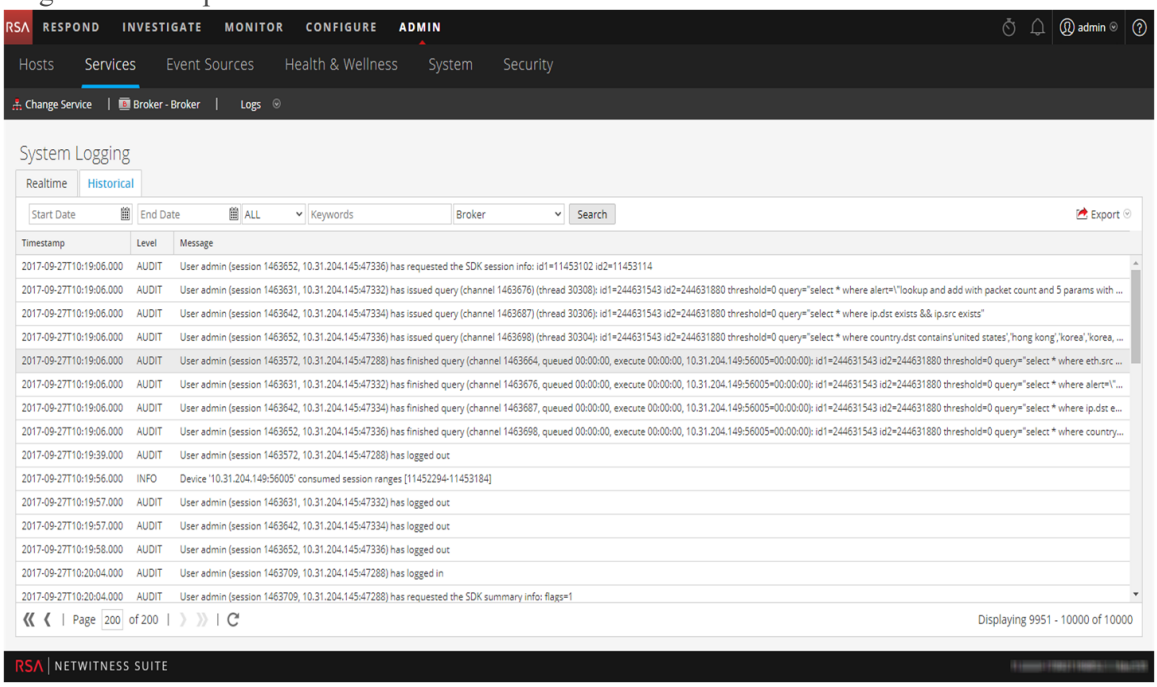
Überblick

Im Folgenden finden Sie ein Beispiel für die Registerkarte **Verlauf** im Bereich „Systemprotokollierung“. Hier werden die NetWitness Suite-Protokolle angezeigt.



1	Zeigt die Registerkarte „Systemprotokollierung“
2	Zeigt die Registerkarte „Verlauf“

Das Folgende ist ein Beispiel für die Registerkarte **Verlauf** in der Serviceprotokollansicht. Es zeigt die Serviceprotokolle.



Funktionen

Die Registerkarte **Verlauf** hat eine Symbolleiste mit Eingabefeldern, um das Filtern der Einträge zu erlauben, ein Raster, das die Protokolleinträge enthält und Paginierungstools.

Funktion	Beschreibung
Startdatum und **Enddatum**	Die Bereichssuchoptionen **Startdatum** und **Enddatum** begrenzen die Protokolleinträge auf einen Zeitpunkt. Wenn sie verwendet werden, müssen Sie sowohl ein Start- als auch ein Enddatum angeben. Die Zeiten sind optional. Der Datumsbereich wird validiert, um sicherzustellen, dass das Enddatum nicht vor dem Startdatum liegt.

Funktion	Beschreibung
Drop-down-Menü Protokollebene 	Wählt die Protokollebene für Einträge aus, die im Raster angezeigt werden. Das Drop-down-Menü **Protokollebene** zeigt die verfügbaren Protokollebenen für das System oder den Service an. • Systemprotokolle haben sieben Protokollebenen. • Serviceprotokolle haben nur sechs Protokollebenen, da sie nicht über die Ebene **TRACE** verfügen. • Der Standardwert ist **ALLE** Protokolleinträge.
Schlüsselwortfeld	Gibt ein Schlüsselwort für das Filtern von Einträgen vor. Dieses Feld ist bei der System- und Servicefilterung identisch.
Feld „Service“ (nur Serviceprotokolle)	Gibt den bei der Filterung von Serviceprotokolleinträgen zu verwendenden Servicetyp an. Mögliche Werte sind der Host oder der Service.
Schaltfläche „Suchen“	Klicken Sie hierauf, um eine Suche zu aktivieren, basierend auf Start- und Enddatum, Protokollebene, Schlüsselwort und Serviceauswahlen.
Export	Klicken Sie hierauf, um die aktuell angezeigten Rastereinträge in eine Textdatei zu exportieren. Sie können auswählen, ob die Einträge in der Datei mit Komma oder mit Tabulator getrennt werden.

Spalte	Beschreibung
Zeitstempel	Dies ist der Zeitstempel für den Eintrag.
Ebene	Dies ist die Protokollebene für die Meldung.
Meldung	Dies ist der Text des Protokolleintrags.

Mithilfe der Paginierungstools unter dem Raster können Sie durch die Seiten der Protokolleinträge navigieren.

Suchen von Protokolleinträgen

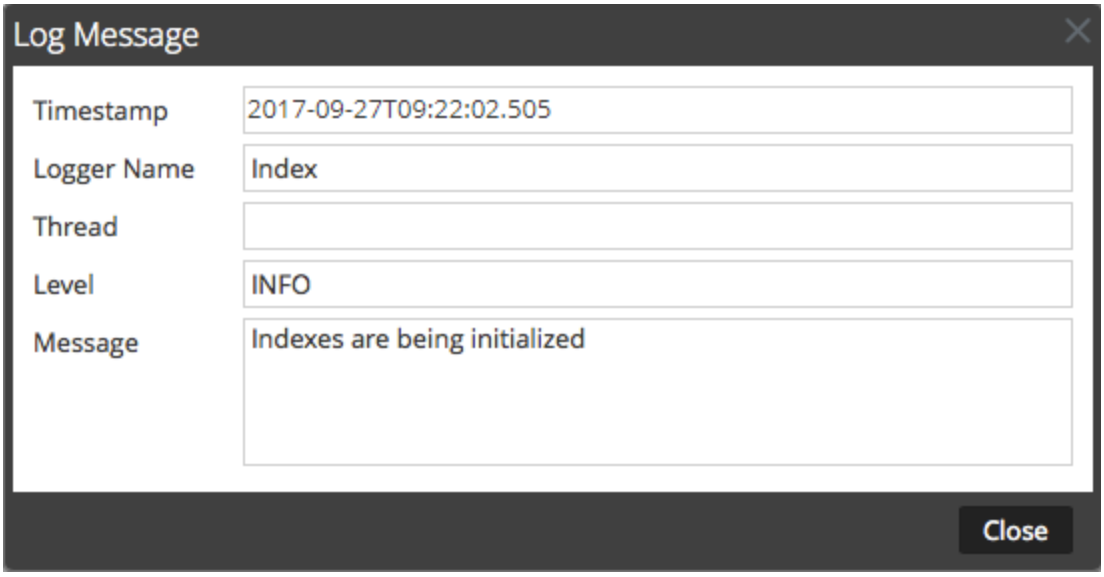
So durchsuchen Sie die Ergebnisse in der Registerkarte **Verlauf**:

1. (Optional) Wählen Sie ein **Startdatum** und ein **Enddatum** aus. Wählen Sie optional eine **Startzeit** und eine **Endzeit** aus.
2. (Optional) Wählen Sie für System- und Serviceprotokolle eine **Protokollebene** und/oder ein **Schlüsselwort** aus.
3. (Optional) Wählen Sie für Serviceprotokolle den **Service** aus: Host oder Service.
4. Klicken Sie auf **Suchen**.
   Die Ansicht wird mit den letzten 10 Einträgen aktualisiert, die mit dem Filter übereinstimmen. Wenn neue übereinstimmende Protokolleinträge verfügbar werden, wird die Ansicht mit diesen Einträgen aktualisiert.

Anzeigen von Details zu einem Protokolleintrag

Jede Zeile des Protokollrasters auf der Registerkarte **Verlauf** bietet zusammenfassende Informationen zu einem Protokolleintrag. So zeigen Sie alle Details an:

1. Doppelklicken Sie auf einen Protokolleintrag.
   Das Dialogfeld „Protokollmeldung“, das den Zeitstempel, den Protokollierungsnamen, den Thread, die Ebene und die Meldung enthält, wird angezeigt.



2. Klicken Sie nach dem Betrachten auf **Schließen**.

Blättern durch die Einträge

Verwenden Sie zur Anzeige der verschiedenen Seiten des Rasters die Seitenauswahlsteuerungen unter dem Raster wie folgt:

- Verwenden Sie die Navigationsschaltflächen.
- Geben Sie die Seite, die Sie anzeigen möchten, manuell ein und drücken Sie die **EINGABETASTE**.

Export

So exportieren Sie die Protokolle in der aktuellen Ansicht:

Klicken Sie auf **Exportieren** und wählen Sie eine der Drop-down-Optionen – **CSV-Format** oder **Tabulator-Trennzeichen** – aus.
Die Datei wird mit einem Dateinamen heruntergeladen, der den Protokolltyp und das Feldtrennzeichen ausweist. Beispiel: Ein NetWitness Suite-Systemprotokoll, das mit Komma-getrennten Werten exportiert wurde, heißt **UAP_log_export_CSV.txt**, und ein Appliance-Protokoll, das mit Tabulator-getrennten Werten exportiert wurde, heißt **APPLIANCE_log_export_TAB.txt**.