RSA NETWITNESS® SUITE

Konfigurationsleitfaden Workbench

für Version 11.0

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

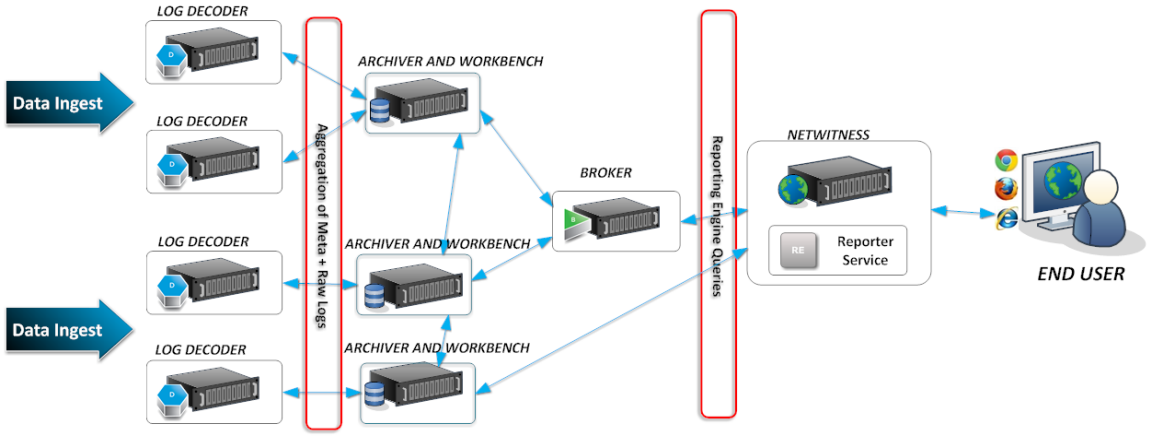
Februar 2018

Inhalt

Workbench – Übersicht

Der NetWitness Suite Workbench-Service ermöglicht das Erstellen von Sammlungen aus offline von einem Archiver gespeicherten wiederhergestellten Daten. Nachdem die Daten kopiert und in eine Sammlung gespeichert wurden, können Sie in Investigation und Reporting analysiert werden.

Das folgende Diagramm stellt die Architektur eines NetWitness Suite-Netzwerks dar, in dem die Workbench implementiert ist.

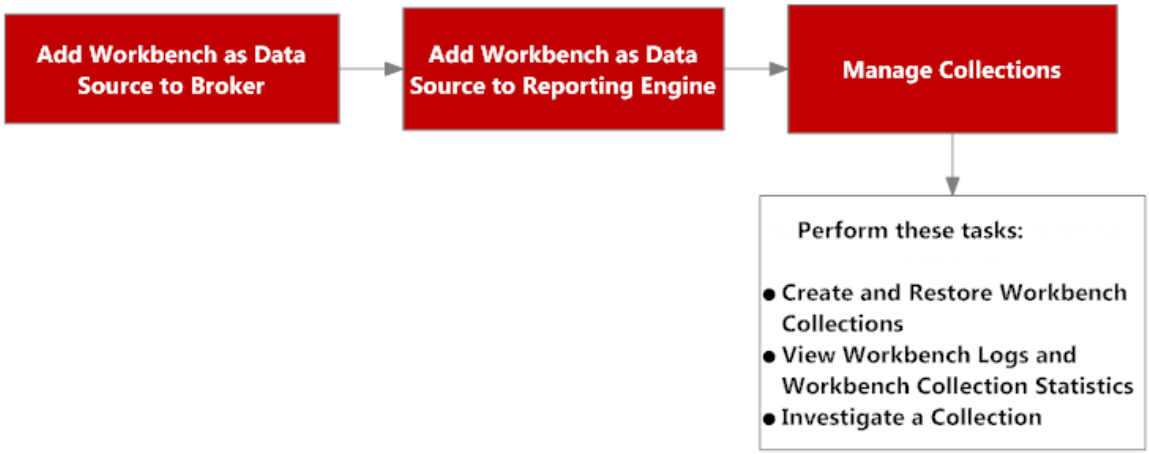


Workbench-Konfigurationsverfahren

Hinweis: Während NetWitness Suite 11.0.0.0 weiterhin Workbench unterstützt und einige Kunden möglicherweise Workbench zur Wiederherstellung von Daten konfiguriert haben, ist die Best Practice zur Wiederherstellung von Daten die Verwendung von Archiver. Anweisungen zur Archivierung und Wiederherstellung von Daten finden Sie im *Konfigurationsleitfaden Archiver*.

Workflow

Hierbei handelt es sich um die grundlegenden Schritte für die Konfiguration und das Management eines Workbench-Services.



1. Fügen Sie einen Workbench-Service als Datenquelle zu Broker hinzu (siehe Hinzufügen von Workbench Service als eine Datenquelle zu Broker).

2. Fügen Sie einen Workbench-Service als Datenquelle zur Reporting Engine hinzu (siehe Hinzufügen der Workbench als Datenquelle zur Reporting Engine

3. Verwalten Sie Sammlungen auf einem Workbench-Service (siehe Managen von Sammlungen).

4. Untersuchen Sie eine Workbench (siehe Managen von Sammlungen).

Voraussetzungen

Vor der Konfiguration des Workbench-Services müssen Sie folgende Aktionen ausführen:

- Fügen Sie den NetWitness Suite-Workbench-Service dem Host in Ihrer Netzwerkumgebung hinzu. (Weitere Informationen finden Sie unter Workbench – Übersicht.)
- Installieren Sie den NetWitness Suite-Workbench-Host in Ihrer Netzwerkumgebung. Weitere Informationen finden Sie im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Die Schritte zum Konfigurieren der Workbench-Services sind:

1. Hinzufügen von Workbench Service als eine Datenquelle zu Broker
2. Hinzufügen der Workbench als Datenquelle zur Reporting Engine

Wenn die Konfiguration abgeschlossen ist, können Sie Sammlungen erstellen und managen. Informationen dazu finden Sie unter Managen von Sammlungen.

Hinzufügen von Workbench Service als eine Datenquelle zu Broker

Voraussetzungen

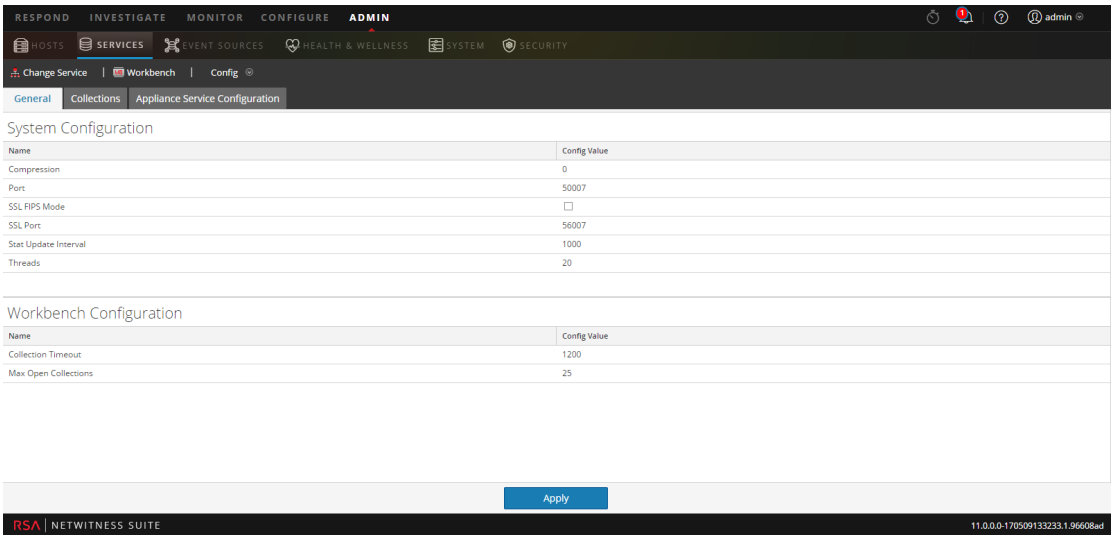
Bevor Sie den Workbench-Service hinzufügen, müssen Sie folgende Aktionen ausführen:

- Installieren des Workbench-Services auf der Archiver-Appliance
- Hinzufügen einer Sammlung zum Workbench-Service

So fügen Sie den Workbench-Service als Datenquelle auf dem Broker hinzu:

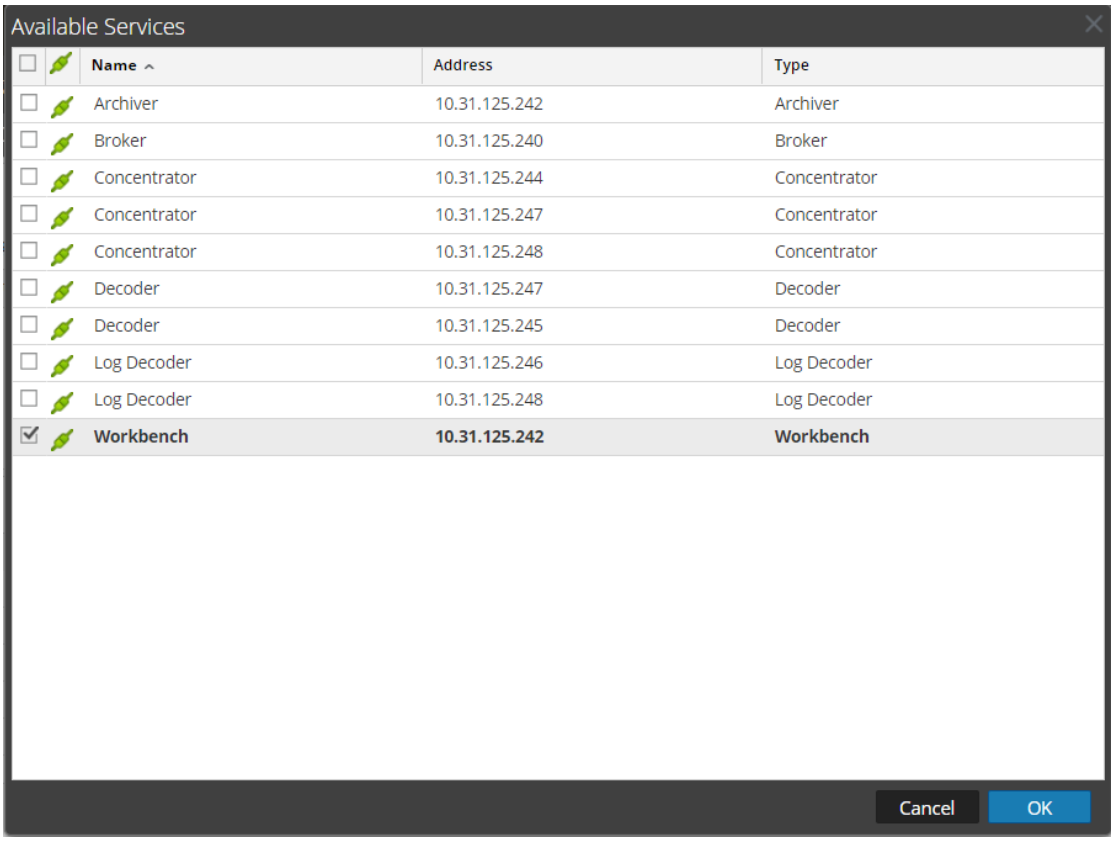
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie einen Broker-Service und dann  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Service-Konfiguration“ wird angezeigt.

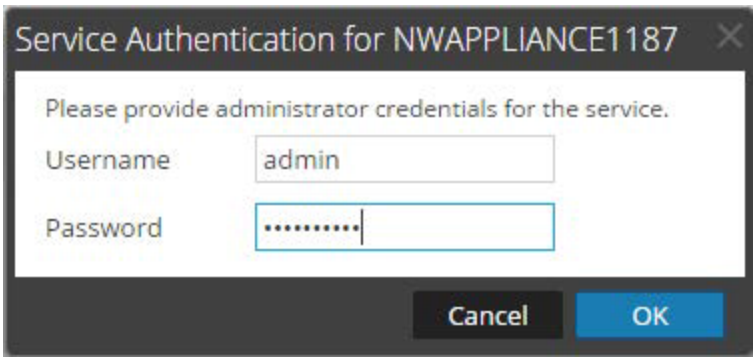


3. Wählen Sie die Registerkarte **Allgemein** aus.
4. Klicken Sie auf  und wählen Sie **Verfügbare Services** aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.

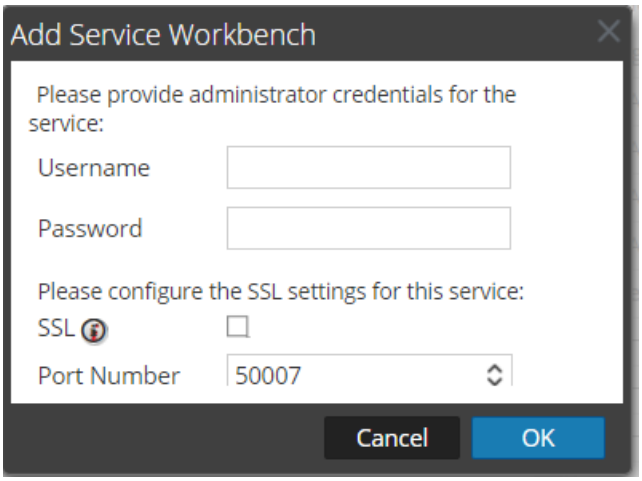


5. Wählen Sie den Workbench-Service aus und klicken Sie auf **OK**.
6. Wenn der Workbench-Service ein Vertrauensmodell verwendet, wird ein Dialogfeld zur Serviceauthentifizierung für den ausgewählten Service angezeigt.



7. Geben Sie den Benutzernamen und das Passwort der Administratorzugangsdaten für den Service ein, und klicken Sie auf **OK**.

   Das Dialogfeld „Hinzufügen eines Workbench-Services“ wird angezeigt.



8. Geben Sie den Benutzernamen und das Passwort der Administratorzugangsdaten für den Service ein, und klicken Sie auf **OK**.

   Der Workbench-Service wird nun als Datenquelle zum Broker hinzugefügt und erscheint in der NWDATA-Quellenliste.

Hinweis: Dieses Verfahren muss für jede Sammlung durchgeführt werden.

Hinzufügen der Workbench als Datenquelle zur Reporting Engine

Voraussetzungen

Folgende Aufgaben sind vor dem Hinzufügen von Workbench als Datenquelle zu Reporting obligatorisch:

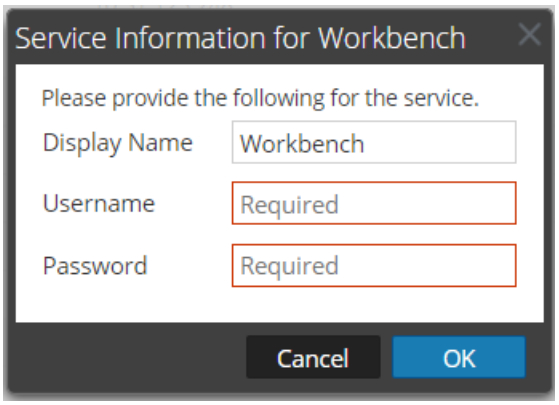
1. Sie haben die Reporting Engine als Service zu Ihrer NetWitness Suite-Bereitstellung hinzugefügt.
2. Sie haben Workbench als Service zu Ihrem NetWitness Suite Archiver-Host hinzugefügt (falls noch nicht installiert).

Hinweis: Für das Hinzufügen von Workbench-Sammlungen als Datenquelle zur Reporting Engine ist eine vertrauenswürdige Verbindung erforderlich. Wenn die Workbench mit einer vertrauenswürdigen Verbindung eingerichtet wurde, sollten Sie Workbench-Sammlungen manuell als Quelle zur Reporting Engine hinzufügen.

So verknüpfen Sie eine Workbench-Datenquelle mit der Reporting Engine:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ die Option **Reporting Engine** aus. Wählen Sie  **Ansicht > Konfiguration** aus.
3. Wechseln Sie zur Registerkarte **Quellen**.
4. Wählen Sie  .
5. Wählen Sie **Verfügbare Services** aus. Wählen Sie im Dialogfeld „Verfügbare Services“ einen Workbench-Service aus.
6. Klicken Sie auf **OK**.

   Das Dialogfeld „Serviceinformationen“ wird angezeigt.



7. Geben Sie den Benutzernamen und das Kennwort ein.
   - Erforderlich, wenn der Workbench-Service „Vertrauenswürdig“ ist.
   - Optional, wenn der Workbench-Service nicht vertrauenswürdig ist (manuell hinzugefügt).
8. Klicken Sie auf **OK**.
9. Wählen Sie im Workbench-Dialog unter „Eine Sammlung hinzufügen“ die Option **Sammlung** aus.
10. Klicken Sie auf **OK**.

Ergebnis

Sie können jetzt Berichte über die vom Workbench gesammelten Daten erstellen.

Managen von Sammlungen

Administratoren können Workbench-Sammlungen erstellen und löschen und Workbench-Statistiken und -Protokolle anzeigen. Dieses Thema enthält alle diese Verfahren und ein Beispiel für die Vorgehensweise zum Wiederherstellen einer Sammlung für Reporting und Investigation.

- Mounten von Archiver-Verzeichnissen
- Erstellen einer Sammlung
- Löschen einer Sammlung
- Untersuchen einer Sammlung
- Anzeigen von Workbench-Sammlungsstatistiken
- Anzeigen von Workbench-Protokollen

Mounten von Archiver-Verzeichnissen

Wenn sich Daten in einem Offlinespeicher oder Cold-Tier-Speicher befinden, müssen Sie die Archiver-Verzeichnisse mounten, um die Daten für Berichts- und Ermittlungszwecke wiederherzustellen:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ einen **Archiver** aus und wählen Sie  **> Ansicht > Durchsuchen** aus.
   Die Ansicht „Explorer“ für den Archiver wird angezeigt.
3. Klicken Sie im linken Strukturbaum mit der rechten Maustaste auf den Node **Datenbank** und wählen Sie **Datenbankeigenschaften** aus, um diese im rechten Bereich zu öffnen.
4. Führen Sie den Befehl **manifest** für den Zeitraum vom 1. April 2017 bis 10. April 2017 aus.
   Die Suche gibt alle Dateien zurück, die für die ausgewählte Abfrage wiederhergestellt werden müssen.

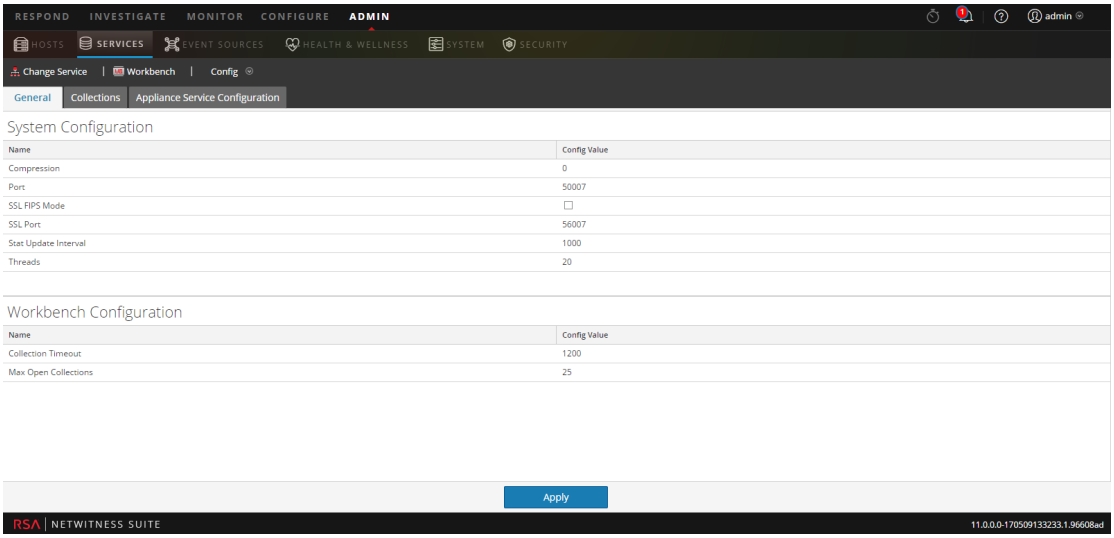
Erstellen einer Sammlung

Administratoren können Sammlungen aus wiederhergestellten Daten aus einem Backup oder einem vorhandenen Datensatz erstellen.

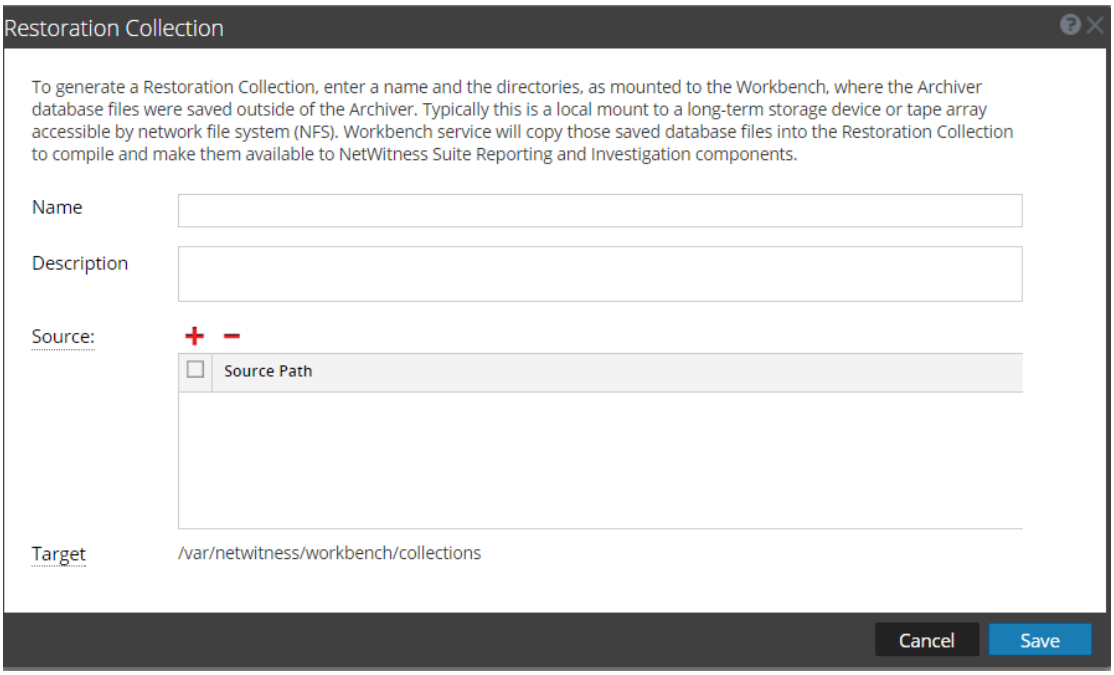
Hinweis: Als Quellpfad können Sie den Speicherort der Datenbankdateien angeben. Mit dem Befehl zum Wiederherstellen werden diese dann auf die Workbench kopiert. Bevor eine Wiederherstellungssammlung erstellt werden kann, müssen Sie diese Verzeichnisse in dem Archiver mounten, in dem die Workbench installiert ist.

So erstellen Sie eine Sammlung mithilfe von Daten, die aus den gesicherten Daten oder einer bestehenden Teilmenge der Daten wiederhergestellt wurden:

1. Navigieren Sie zu **ADMIN > Services.**
2. Wählen Sie in der Ansicht „Services“ eine **Workbench** und wählen Sie dann  > **Ansicht > Konfiguration** aus.
   Die Ansicht „Services-Konfiguration“ wird mit geöffneter Registerkarte „Allgemein“ angezeigt.



3. Klicken Sie auf die Registerkarte **Sammlungen**.
   Das Raster „Sammlungen“ wird angezeigt.
4. Klicken Sie in der Symbolleiste auf  .
   Das Dialogfeld **Wiederherstellungssammlung** wird angezeigt.



5. Stellen Sie folgende Informationen bereit:

   - **Name:** Der Name der Workbench-Sammlung, die Sie wiederherstellen möchten.
   - **Quelle:** Der Speicherort, an den die Archiver-Datenbankdateien aus dem Cold-Speicher verschoben wurden.

   Hinweis: Ziel ist der Speicherort, an dem die Sammlung erstellt wird.

6. Klicken Sie auf **Speichern**, um die Sammlung wiederherzustellen.

   Hinweis: Wenn der Quellpfad, der für die Erstellung der Wiederherstellungssammlung angegeben wurde, nicht vorhanden ist, wird die folgende Fehlermeldung angezeigt:
   `The source path does not exist '/xxx/xxx/'.`

   Wenn nicht genügend Speicherplatz vorhanden ist, um Ihre Sammlung wiederherzustellen, wird die folgende Fehlermeldung angezeigt:
   `Error during disk space checking. Insufficient disk space in location '/xxx/xxx'.`

   Das Dialogfeld „Job planen“ wird mit der folgenden Meldung angezeigt:
   `Restoring data into a new collection. Check the jobs page for progress.`

7. Klicken Sie in der NetWitness Suite-Symbolleiste auf das Symbol **Jobs**  , um die Liste der Jobs zur Wiederherstellungssammlung mit dem jeweiligen aktuellen Status anzuzeigen.

Hinweis: Das Wiederherstellen einer Sammlung, die größer als 550 GB ist, kann mehrere Stunden dauern.

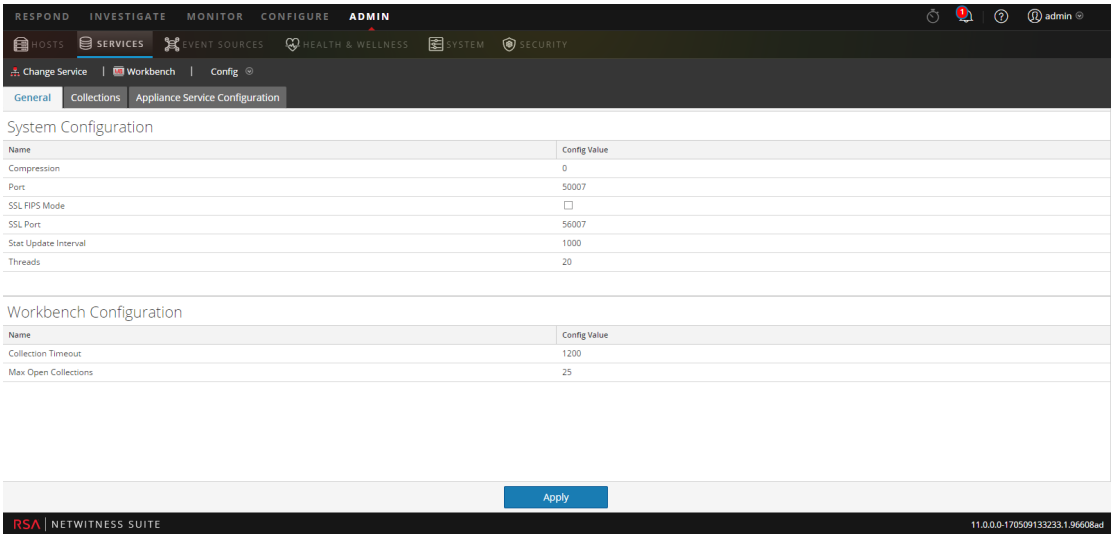
Löschen einer Sammlung

Administratoren können Sammlungen aus dem Workbench-Service löschen.

Führen Sie die folgenden Schritte aus, um eine Sammlung zu löschen:

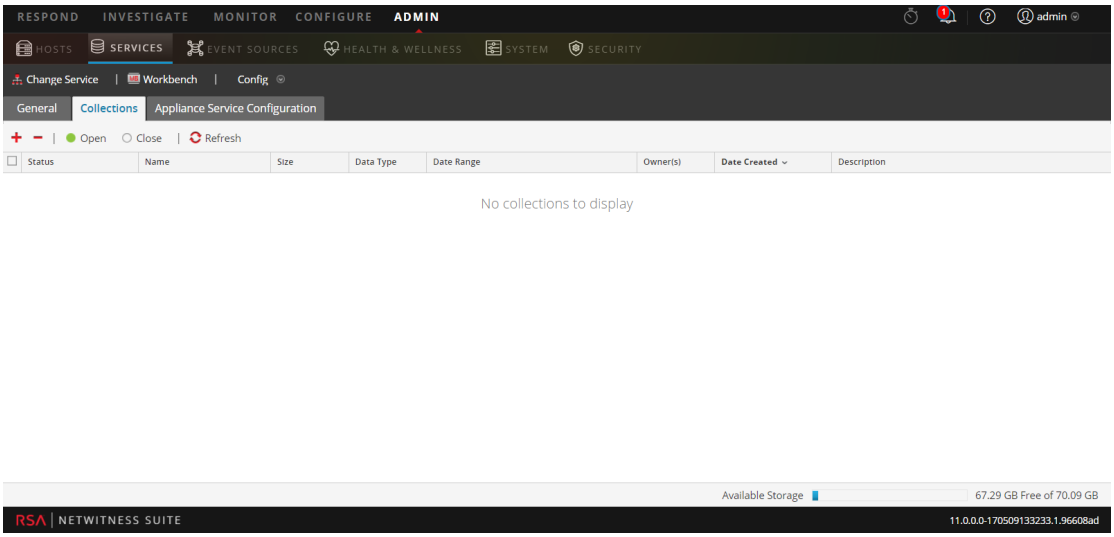
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht Services eine **Workbench** aus und klicken Sie auf  > **Ansicht > Konfiguration**.

   Die Ansicht „Services-Konfiguration“ wird mit geöffneter Registerkarte Allgemein angezeigt.



3. Wählen Sie die Registerkarte **Sammlungen** aus.

   Das Raster „Sammlungen“ wird angezeigt.



4. Wählen Sie im Raster „Sammlungen“ die Sammlung aus, die Sie löschen möchten.
5. Klicken Sie in der Symbolleiste auf .

   In einem Warnmeldungsdialogfeld werden Sie zur Bestätigung aufgefordert.
6. Wenn Sie die Sammlung löschen möchten, klicken Sie auf **Ja**.

   Die Sammlung wird aus dem Workbench-Service gelöscht.

Beispiel für die Vorgehensweise: Wiederherstellung einer Sammlung für Berichts- und Ermittlungszwecke

Die folgenden Schritte veranschaulichen, wie Daten, die sich in einem Offlinespeicher oder einem Cold-Tier-Speicher befinden, für Berichts- und Ermittlungszwecke wiederhergestellt werden können. Im folgenden Beispiel werden Daten für den Zeitraum zwischen dem 1. April 2015 und dem 10. April 2015 wiederhergestellt.

So stellen Sie Daten für Berichts- und Ermittlungszwecke wieder her:

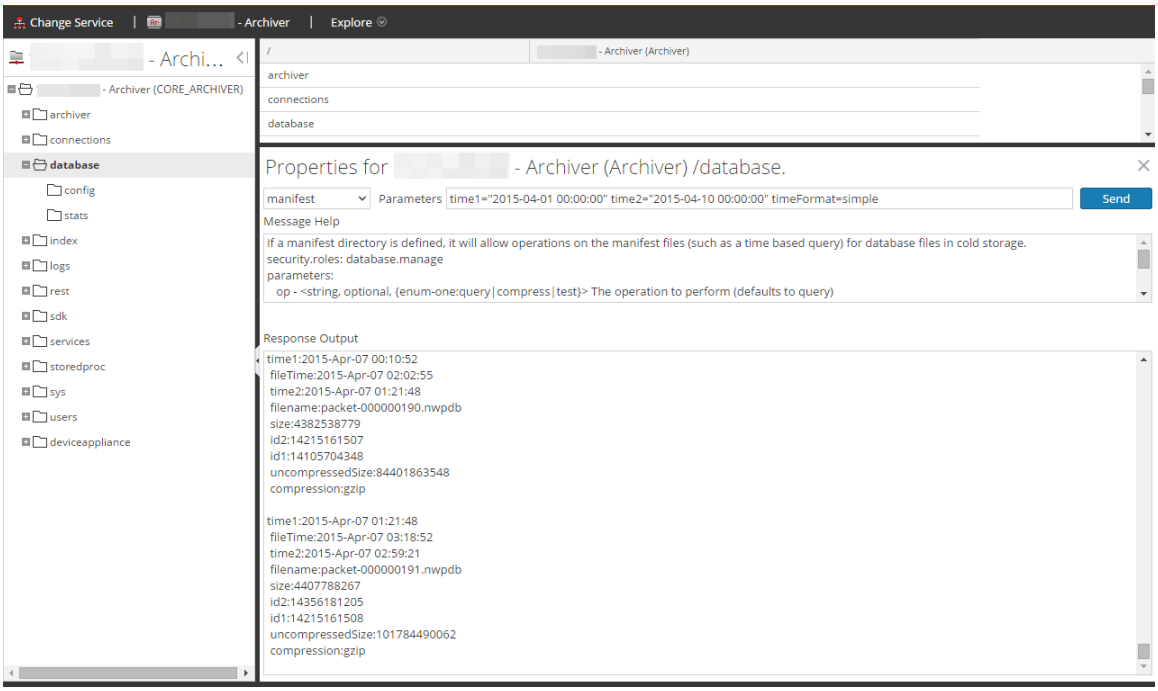
1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie im Raster „Services“ den **Archiver** aus.
3. Navigieren Sie zur Ansicht „Explorer“ der Archiver-Appliance, indem Sie > **Ansicht > Durchsuchen** auswählen.

   Die Ansicht „Explorer“ für den Archiver wird angezeigt.
4. Klicken Sie im linken Strukturbaum mit der rechten Maustaste auf den Node **Datenbank** und wählen Sie **Datenbankeigenschaften** aus, um diese im rechten Bereich zu öffnen.

5. Führen Sie den Befehl **manifest** für den ausgewählten Zeitraum vom 1. April 2015 bis 10. April 2015 aus.
   Die Suche gibt alle Dateien zurück, die für die ausgewählte Abfrage wiederhergestellt werden müssen.

Suchbeispiel:

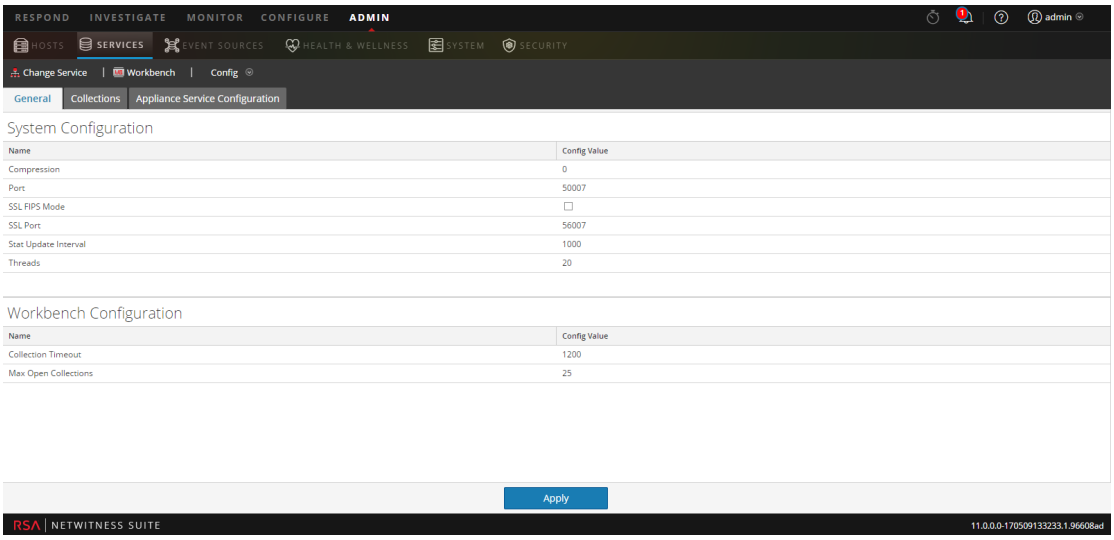
```
time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
timeFormat=simple
```



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

7. Wählen Sie in der Ansicht „Services“ eine **Workbench** und wählen Sie dann  **> Ansicht > Konfiguration** aus.

   Die Ansicht „Services-Konfiguration“ wird mit geöffneter Registerkarte Allgemein angezeigt.

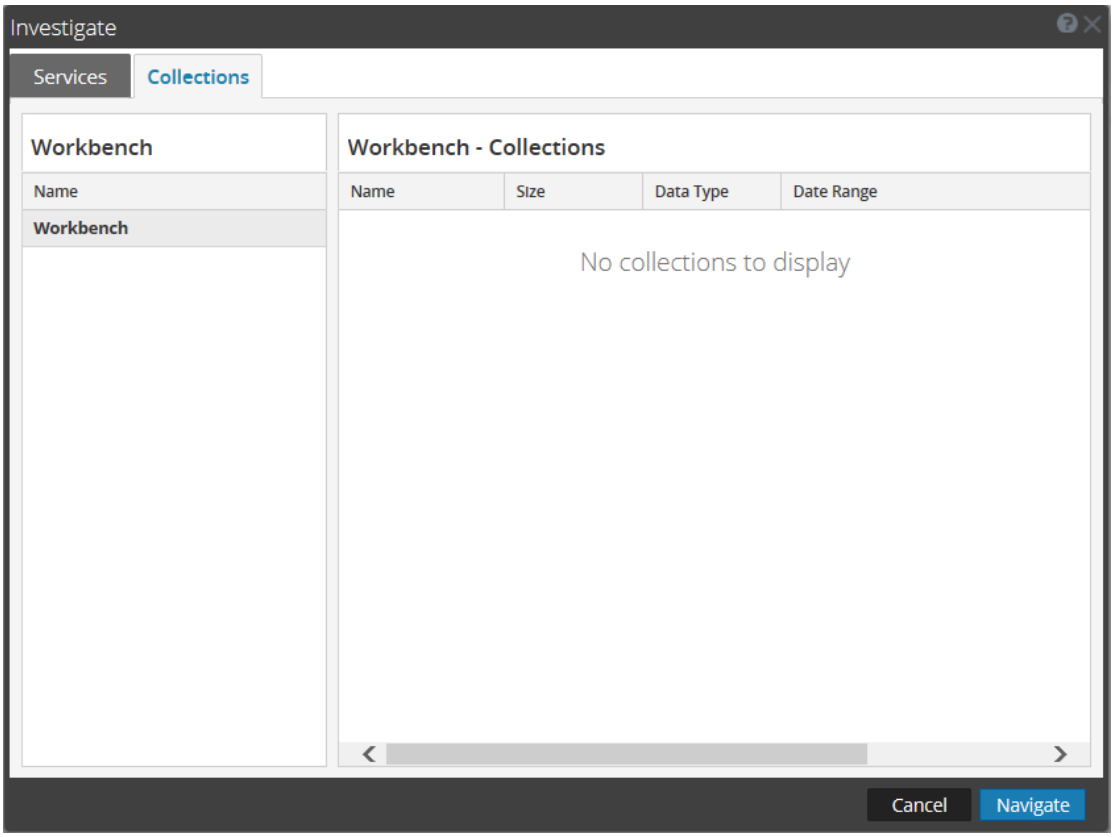


8. Wählen Sie die Registerkarte **Sammlungen aus.**
9. Erstellen Sie eine Wiederherstellungssammlung mit dem Quellpfad, der auf die in der Ausgabe des Befehls „manifest“ aufgeführten Dateien verweist.
10. Speichern Sie die Sammlung.
    Nach der erfolgreichen Erstellung einer Sammlung können Sie diese für Berichts- und Ermittlungszwecke verwenden.

Untersuchen einer Sammlung

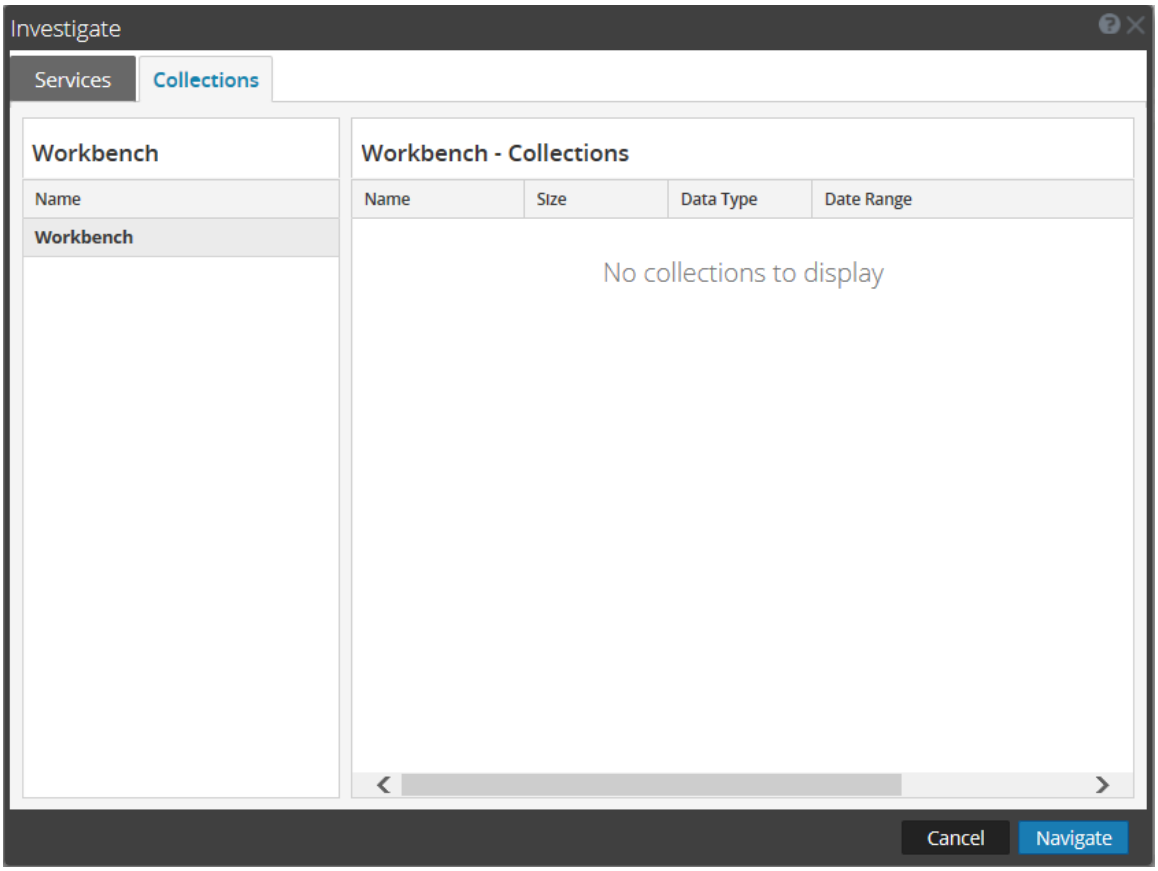
So führen Sie eine Untersuchung an einer Workbench-Sammlung durch:

1. Wählen Sie **Untersuchen** aus.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Klicken Sie auf der Registerkarte **Sammlungen** auf das Dialogfeld „Untersuchen“.
3. Wählen Sie im linken Bereich einen Workbench-Service aus.
4. Wählen Sie im rechten Bereich die Sammlung aus, die Sie untersuchen möchten.
5. Klicken Sie auf **Navigieren**.

Die Ansicht „Navigieren“ wird mit Daten in Bezug auf die ausgewählte Workbench-Sammlung angezeigt.



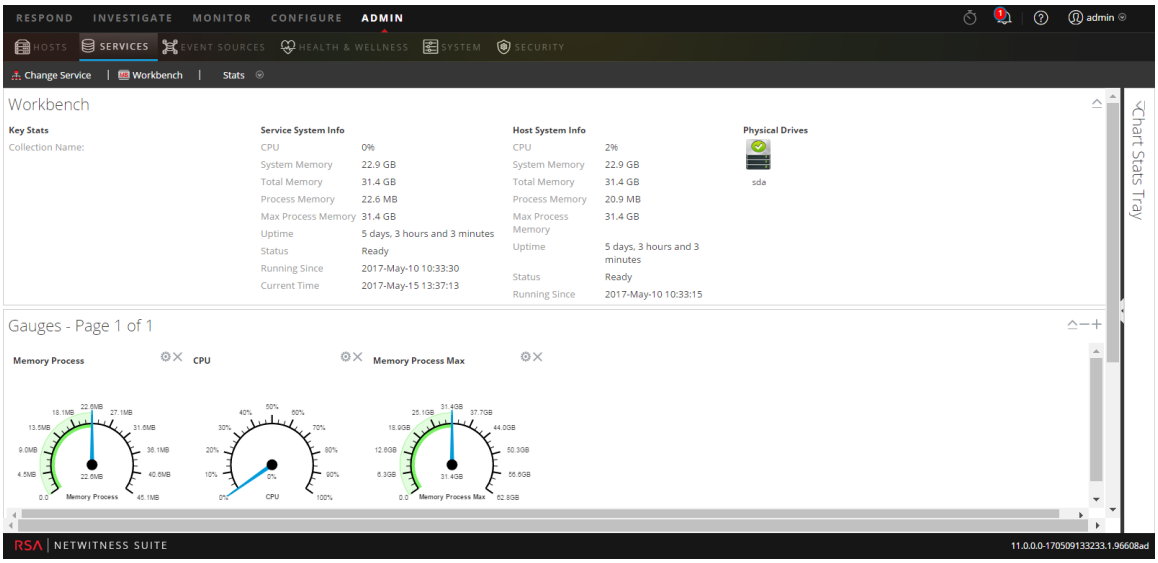
Hinweis: Detaillierte Informationen zur Verwendung von Investigation finden Sie im *Leitfaden Investigation und Malware Analysis*.

Anzeigen von Workbench-Sammlungsstatistiken

Für den Workbench-Service sind dieselben Statistiken verfügbar wie für andere Services. In der Ansicht „Services“ > „Statistik“ werden wichtige Statistiken und Systeminformationen im Zusammenhang mit dem ausgewählten Workbench-Service angezeigt. Die Informationen werden in mehreren verschiedenen Abschnitten innerhalb der Ansicht Statistik angezeigt: Workbench, Messdiagramme, Zeitachsendiagramm und Diagrammstatistikbereich. Im Diagrammstatistikbereich werden alle verfügbaren Statistiken für die Workbench aufgelistet. Jede Statistik im Diagrammstatistikbereich kann in einem Messdiagramm oder in einem Zeitplandiagramm angezeigt werden.

Führen Sie zum Anzeigen von Workbench-Statistiken folgende Schritte durch:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ eine **Workbench** und wählen Sie dann  > **Ansicht > Statistiken** aus.
   Die Ansicht „Services-Statistik“ wird angezeigt.



Hinweis: Weitere Informationen über Workbench-Statistiken finden Sie im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Anzeigen von Workbench-Protokollen

Führen Sie zum Anzeigen von Protokollen zu einem Workbench-Service folgende Schritte durch:

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ eine **Workbench** und wählen Sie dann  > **Ansicht > Protokolle** aus.
   Das Raster „Serviceprotokolle“ wird angezeigt.

Hinweis: Weitere Informationen zum Anzeigen und Konfigurieren von Auditprotokollen erhalten Sie in den Themen **Konfigurieren der globalen Auditprotokollierung** im *Systemkonfigurationsleitfaden*.

Referenzen

Workbench-Referenzthemen:

- Ansicht „Service-Konfiguration“ – Workbench
- Ansicht „Service-Konfiguration“ – Registerkarte „Sammlungen“
- Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“

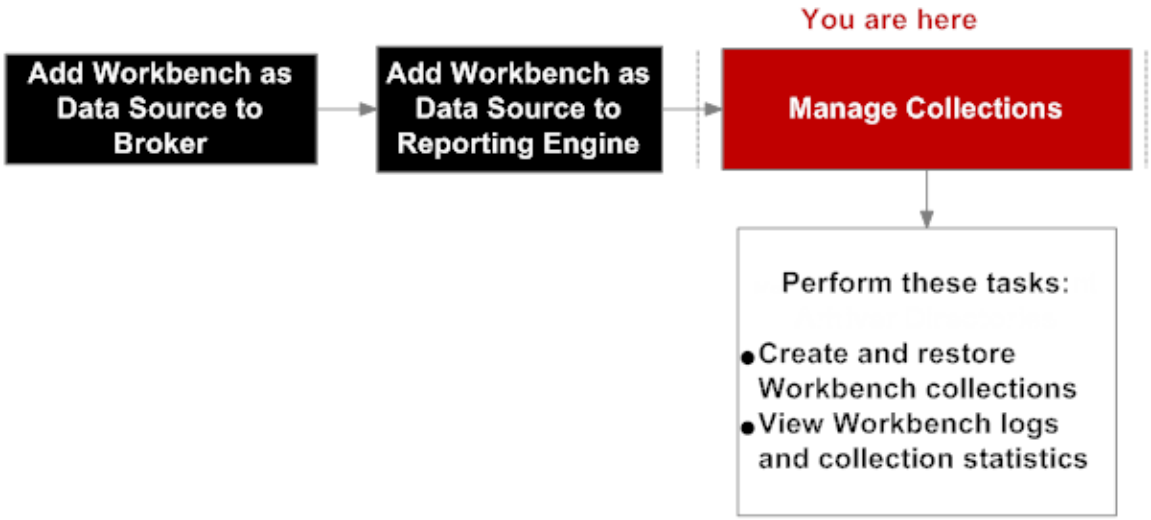
Ansicht „Service-Konfiguration“ – Workbench

In der Ansicht „Service-Konfiguration“ für Workbench sind einige der Parameter identisch mit anderen NetWitness Suite-Services, während andere spezifisch für den Workbench-Service sind.

Über die Ansicht „Services-Konfiguration – Workbench“ (ADMIN > Services > Workbench-Service und Ansicht > Konfiguration auswählen) können Sie einen Workbench-Service konfigurieren.

Workflow

Hierbei handelt es sich um die grundlegenden Schritte für die Konfiguration und das Management eines Workbench-Services.



Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Hinzufügen von Workbench als eine Datenquelle zu Broker	Hinzufügen von Workbench Service als eine Datenquelle zu Broker
Administrator	Hinzufügen der Workbench als Datenquelle zur Reporting Engine	Hinzufügen der Workbench als Datenquelle zur Reporting Engine
Administrator	*Erstellen oder Löschen einer Sammlung	Managen von Sammlungen

Rolle	Ziel	Details anzeigen
Administrator	*Ansicht „Workbench-Statistiken und -Protokolle“	Managen von Sammlungen
Administrator	Anzeigen von Informationen zur Konfiguration von Appliances, die mit dem Workbench-Service verbunden sind	Wählen Sie die Registerkarte **Appliance-Servicekonfiguration** aus. Die Registerkarte Appliance-Servicekonfiguration ist für alle NetWitness Suite-Services identisch. Sie bietet Informationen zur Konfiguration von Appliances, die mit dem Workbench-Service verbunden sind. Informationen über die Registerkarte **Appliance-Servicekonfiguration** finden Sie unter **Registerkarte „Appliance-Servicekonfiguration“** im *Leitfaden für die ersten Schritte mit Hosts und Services*.

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

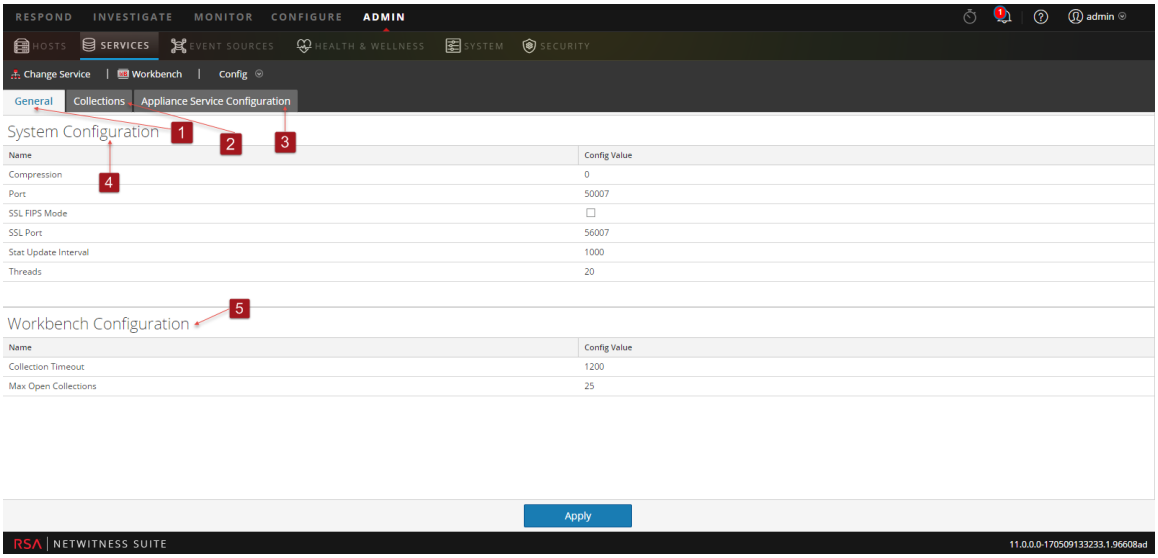
- Managen von Sammlungen
- Fehlerbehebung:

Überblick

Der Workbench-Service verfügt über drei Registerkarten und zwei Bereiche in der Ansicht „Konfiguration“:

- Registerkarte „Allgemein“
- Registerkarte „Sammlungen“

- Registerkarte „Appliance-Servicekonfiguration“
- Bereich „Systemkonfiguration“
- Bereich „Workbench-Konfiguration“



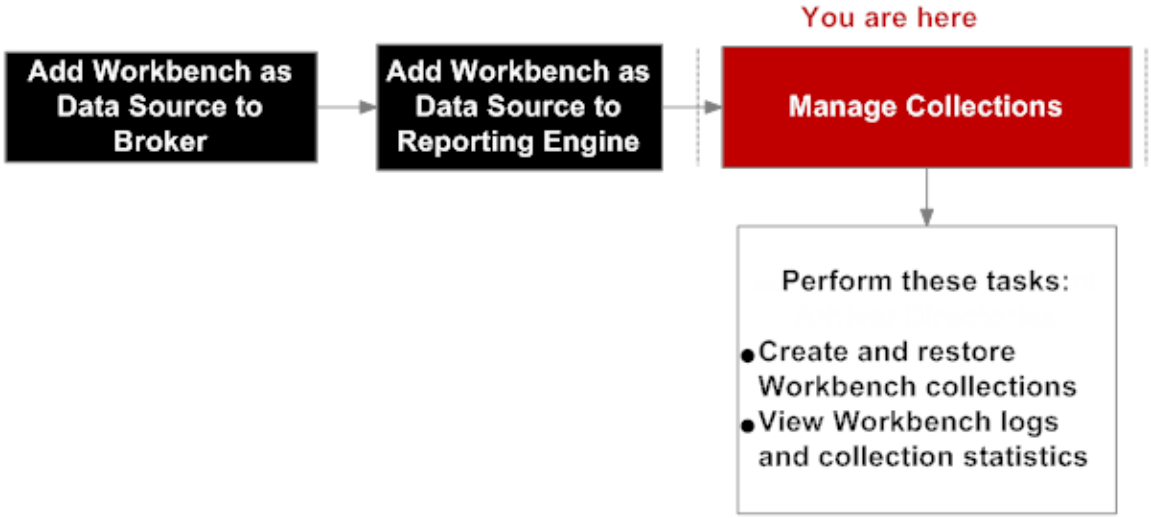
1	Die Registerkarte „Allgemein“ bietet eine Möglichkeit für das Management der grundlegenden Workbench-Servicekonfiguration.
2	Die Registerkarte „Sammlungen“ bietet eine Möglichkeit für das Management von Sammlungen auf einem Workbench-Service.
3	Die Registerkarte „Appliance-Servicekonfiguration“ bietet eine Möglichkeit zum Konfigurieren eines Workbench-Services.
4	Der Bereich „Systemkonfiguration“ bietet eine Möglichkeit für das Management der Servicekonfiguration für einen Workbench-Service.
5	Der Bereich „Workbench-Konfiguration“ bietet eine Möglichkeit zum Starten und Stoppen eines Workbench-Service.

Ansicht „Service-Konfiguration“ – Registerkarte „Sammlungen“

Die Registerkarte „Sammlungen“ für den Workbench-Service bietet eine Möglichkeit für das Management von Workbench-Sammlungen. Navigieren Sie zu ADMIN > Services, wählen Sie einen Workbench-Service aus, wählen Sie dann Ansicht > Konfiguration aus und wählen Sie die Registerkarte „Sammlungen“ aus, um auf die Registerkarte „Sammlungen“ zuzugreifen.

Workflow

Hierbei handelt es sich um die grundlegenden Schritte für die Konfiguration und das Management eines Workbench-Services.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	*Erstellen und Wiederherstellen der Workbench-Sammlungen	Managen von Sammlungen
Administrator	*Anzeigen von Protokollen Sammlungsstatistiken	Managen von Sammlungen

Rolle	Ziel	Dokumentation
Administrator	Anzeigen von Informationen zur Konfiguration von Appliances, die mit dem Workbench-Service verbunden sind	Wählen Sie die Registerkarte **Appliance-Servicekonfiguration** aus. Die Registerkarte Appliance-Servicekonfiguration ist für alle NetWitness Suite-Services identisch. Sie bietet Informationen zur Konfiguration von Appliances, die mit dem Workbench-Service verbunden sind. Informationen über die Registerkarte **Appliance-Servicekonfiguration** finden Sie unter **Registerkarte „Appliance-Servicekonfiguration“** im *Leitfaden für die ersten Schritte mit Hosts und Services*.

*Sie können diese Aufgabe hier durchführen.

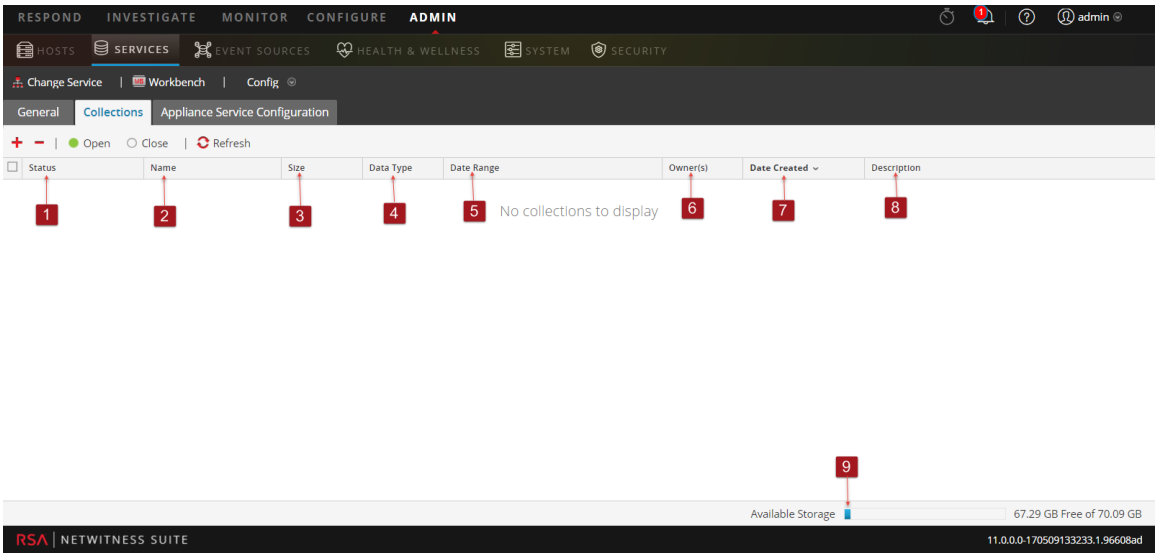
Verwandte Themen

- Managen von Sammlungen

Überblick

Die Registerkarte „Sammlungen“ enthält eine Symbolleiste und ein Raster, in dem die relevanten Informationen über die Workbench-Sammlungen aufgeführt sind.

Diefolgende Abbildung ist ein Beispiel für das Raster Sammlungen.



1	Status der Wiederherstellungssammlung: • **Daten werden wiederhergestellt**: Die Datenwiederherstellung läuft. • **Geschlossen**: Daten werden wiederhergestellt. • **Wird geöffnet**: Daten werden indexiert. • **Bereit**: Indexierung ist abgeschlossen. • **Wird geschlossen**: Die Sammlung wird geschlossen.
2	**Name**: Name der Datei, die wiederhergestellt wird.
3	**Größe**: Sammlungsgröße.
4	**Datentyp**: Protokolle
5	**Datumsbereich**: Listet Datumsbereich auf, in dem die Sammlung wiederhergestellt wird.
6	**Eigentümer**: Zeigt den Ersteller der Sammlung an
7	**Erstellungsdatum**: Zeigt das Datum an, an dem die Sammlung erstellt wurde.
8	**Beschreibung**: Beschreibt die Wiederherstellungssammlung.
9	**Anzeige für verfügbaren Speicher**: Zeigt den verfügbaren Festplattenspeicher in GB (Gigabyte) an. Wenn versucht wird, eine Wiederherstellungssammlung zu erstellen, führt die Workbench eine Validierung durch, um zu überprüfen, ob genug Speicherplatz verfügbar ist.

Symbolleiste

Dies sind die Optionen der Symbolleiste:

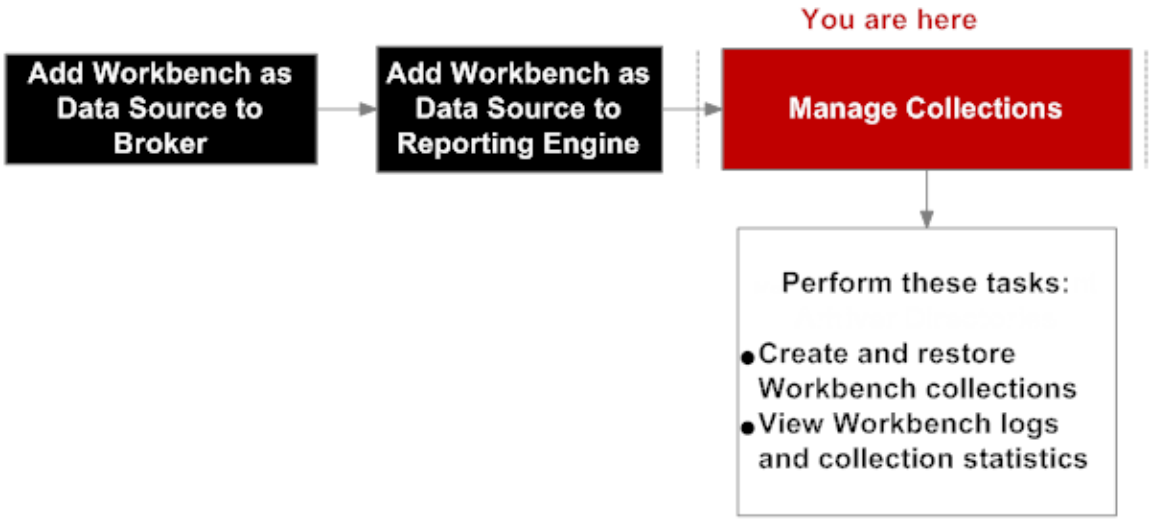
Parameter	Beschreibung
	Erstellt eine neue Wiederherstellungssammlung.
	Löscht die ausgewählte Workbench-Sammlung.
Öffnen und Schließen: Bezieht sich auf den Status der Wiederherstellungssammlung.	Öffnen: Macht die Sammlung für Investigation und Reporting verfügbar. Schließen: Die Sammlung ist nicht für Investigation und Reporting verfügbar; die Ressourcen bleiben erhalten.
	Aktualisiert die Liste der Workbench-Sammlungen.

Ansicht „Service-Konfiguration“ – Registerkarte „Allgemein“

Die Registerkarte „Allgemein“ für den Workbench-Service bietet eine Möglichkeit für das Management der grundlegenden Servicekonfiguration. Um auf die Registerkarte „Allgemein“ zuzugreifen, navigieren Sie zu Admin > Services und wählen Sie einen  **> Ansicht > Konfiguration** aus.

Workflow

Hierbei handelt es sich um die grundlegenden Schritte für die Konfiguration und das Management eines Workbench-Services.



Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Administrator	Erstellen und Wiederherstellen der Workbench-Servicesammlungen	Managen von Sammlungen
Administrator	Anzeigen von Protokollen Sammlungsstatistiken	Managen von Sammlungen
Administrator	Verarbeiten von Workbench-Sammlungen zu verarbeiten.	Managen von Sammlungen

Verwandte Themen

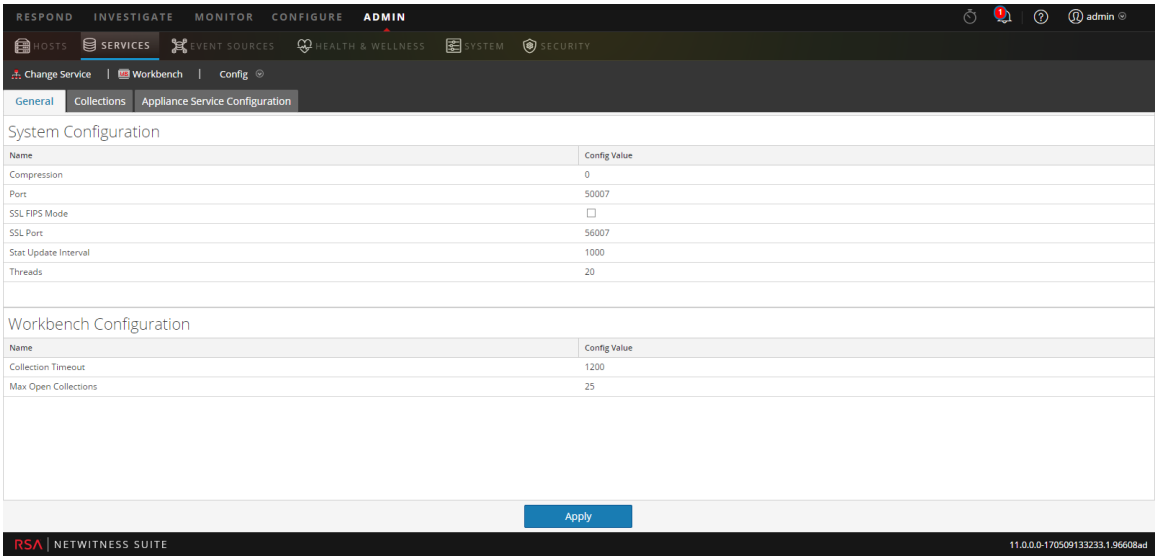
- Workbench-Konfigurationsverfahren

Überblick

Die Registerkarte Allgemein umfasst zwei Bereiche:

- Systemkonfiguration
- Workbench-Konfiguration

In der folgenden Abbildung ist ein Beispiel der Registerkarte Allgemein gezeigt.



Bereich „Systemkonfiguration“

Im Bereich „Systemkonfiguration“ werden Konfigurationsparameter für den Workbench-Service angezeigt. In der folgenden Tabelle werden die Funktionen des Bereichs Systemkonfiguration beschrieben.

Parameter	Beschreibung
Komprimierung	Bei Einstellung auf einen positiven Wert die Mindestanzahl an Byte, bevor eine Meldung komprimiert wird. **0** bedeutet keine Komprimierung von Meldungen. Die Änderung wird bei den folgenden Verbindungen wirksam.
Port	Der unverschlüsselte Port, den der Service abhört. **0** bedeutet deaktiviert. Die Änderung wirkt sich beim Serviceneustart aus.

Parameter	Beschreibung
SSL FIPS-Modus	Bestimmt, ob die OpenSSL-Bibliothek in den FIPS-Modus übergeht. Die Änderung wirkt sich beim Serviceneustart aus.
SSL-Port	SSL-Port, den der Service abhört. **0** bedeutet deaktiviert. Die Änderung wirkt sich beim Serviceneustart aus.
Statistikaktualisierungsintervall	Legt fest, wie oft (in Millisekunden) Statistik-Nodes im System aktualisiert werden Die Änderung wird sofort wirksam.
Threads	Die Anzahl der Threads im Threadpool für die Verarbeitung eingehender Anforderungen. Die Änderung wird sofort wirksam.

Bereich Workbench-Konfiguration

Im Bereich Workbench-Konfiguration werden Konfigurationsparameter für die Workbench-Sammlungen angezeigt. In der folgenden Tabelle sind die Funktionen des Bereichs Workbench-Konfiguration beschrieben.

Parameter	Beschreibung
Sammlungs-Timeout	Anzahl an Sekunden, bevor eine inaktive Sammlung automatisch beendet wird
Max. geöffnete Sammlungen	Anzahl an Sammlungen, die gleichzeitig geöffnet sein können. Mit dem Wert 0 wird die Begrenzung deaktiviert.
Anwenden	Aktualisiert die geänderten Konfigurationen im Bereich

Fehlerbehebung:

NetWitness Suite benachrichtigt Benutzer über Probleme mithilfe von Pop-up-Benachrichtigungen.

NetWitness Suite Workbench gibt die folgenden Arten von Fehlermeldungen aus, die in der untenstehenden Tabelle erklärt werden.

Problem	Mögliche Ursachen	Lösungen

Es konnte keine Verbindung zum Workbench-Service von der Administrationsseite der NetWitness Suite-**Benutzeroberflächeh ergestellt werden.**	NetWitness Suite-Service wird nicht ausgeführt.	Stellen Sie sicher, dass der NetWitness Suite-Service ausgeführt wird. Melden Sie sich bei Ihrem NetWitness-Server an und führen Sie den folgenden Befehl aus:
		`status nwworkbench`
		Firewall-Regeln sollten Verbindungen von 50007, 50607 und 50107 zulassen.
		Überprüfen Sie Ihre Verbindung, indem Sie den folgenden Befehl ausführen:
		`service iptables status`
		Stellen Sie sicher, dass Sie REST starten können. Führen Sie folgenden Befehl für Ihre Appliance aus:
		`https://<IPAddress>:50107 service`
		Wenn Sie den REST-Service für Ihre Appliance starten können, können Sie bestätigen, dass es kein Problem mit der Appliance gibt. Navigieren Sie zur NetWitness Suite-Website, um weitere Ermittlungen durchzuführen:
		• Aktivieren Sie den Debug-Modus und achten Sie auf sa.log-Fehler unter:
		`/var/lib/netwitness/uax/logs`
		• Aktivieren Sie Entwicklertools mithilfe der Tastenkombination `Ctrl+Shift+I` für Chrome und überprüfen Sie die

Problem	Mögliche Ursachen	Lösungen
		Vorschau und Antwort auf die Anforderung.
Die Registerkarte Appliance-Servicekonfiguration für die im SSL-Modus ausgeführte Workbench-Appliance konnte nicht angezeigt werden.		Aktivieren Sie SSL für den Appliance-Service und starten Sie den Appliance-Service von Neuem.

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, Metadaten zu laden, um einen Bericht über eine Workbench-Sammlung zu erstellen: „Beim Versuch, Metadaten zu laden, konnte kein Schema von der Datenquelle abgerufen werden.“		Laden Sie Metadaten für die Appliance von der Regelbibliothek der NetWitness Suite-Benutzeroberfläche und achten Sie auf Fehlermeldungen im Reporting Engine-Protokoll unter:
		`/home/rsasoc/rsa/soc/reporting-engine/logs`
		Starten Sie REST für das Gerät und achten Sie auf jede Fehlermeldung, wenn Sie die folgende Abfrage ausführen.
		`/sdk?msg=language&force-content-type=text/plain&expiry=600&size=10`

Problem	Mögliche Ursachen	Lösungen
Es werden keine Ergebnisse angezeigt, nachdem eine Abfrage von der NetWitness Suite-Benutzeroberfläche über die Reporting Engine ausgeführt wurde.		Führen Sie die Abfrage auf der Reporting Engine aus und achten Sie auf `/var/log/messages` auf der Datenquelle. Suchen Sie nach einer Abfrage, die der Datenquelle genau entspricht. **TIPP:** Suchen Sie nach `[SDK-Query]` in der Protokolldatei. Kopieren Sie die Abfrage genau und führen Sie sie von REST SDK aus, um zu sehen, ob Sie Ergebnisse erhalten. `REST Query: /sdk?msg=query&force-contenttype=text/plain&expiry=600&query=select%20user.dst&size=10`
Die Workbench-Anzeige des verfügbaren Speichers auf der Registerkarte „Workbench-Sammlungen“ ist nicht genau.	Die Anzeige des verfügbaren Speichers in der Benutzeroberfläche zeigt das Standardsammlungsverzeichnis an, wie unten angezeigt: `/VAR/NETWITNESS/WORKBENCH/COLLECTIONS`	Keine.
Es können keine neuen Sammlungen geöffnet werden, nachdem bestehende Sammlungen geöffnet wurden.	Es gibt eine Workbench-Konfiguration namens „Max. geöffnete Sammlungen“, die standardmäßig auf 25 eingestellt ist. Diese Konfiguration bestimmt die Anzahl der Sammlungen, die gleichzeitig geöffnet sein können.	Sie können diesen Wert ändern. Mit dem Wert Null wird der Grenzwert für maximal geöffnete Sammlungen deaktiviert.

Problem	Mögliche Ursachen	Lösungen
Es wurde eine Sammlung erfolgreich geöffnet, die in den Status „Ready“ gelangte. Aber nach einiger Zeit wechselte die Sammlung automatisch in den Status „Closed“.	Es gibt eine Workbench-Konfiguration namens „collection.timeout“, die standardmäßig auf 1.200 Sekunden eingestellt ist. Diese Konfiguration bestimmt die Anzahl Sekunden, bevor eine inaktive Sammlung automatisch geschlossen wird. Die maximal zulässige Zeitdauer, bevor es zum Timeout kommt, ist 86.400 Sekunden (24 Stunden).	Mit dem Wert Null wird der Timeout deaktiviert.
Die Abfrage eines Zeitbereichs mithilfe des Befehls `/database manifest` gab eine leere Ausgabe zurück.	Eine leere Ausgabe zeigt an, dass keine **nwdb**-Dateien für den Zeitbereich verfügbar sind.	Keine
Die Sammlung wurde erstellt, aber der Sammlungsstatus ist in Jobs nicht verfügbar und die Sammlung wird auf der Registerkarte „Sammlungen“ der Workbench nicht angezeigt.	Möglicherweise läuft Ihre Umgebung in einem gemischten Modus, etwa wenn eine Sammlung auf einer 10.4.x-Version von Workbench von einer 10.5 NetWitness Suite-Benutzeroberfläche aus erstellt wird.	Die Sammlung wird auf der Registerkarte „Sammlungen“ der Workbench angezeigt, nachdem die Seite erneut geladen wurde.

Problem	Mögliche Ursachen	Lösungen
Die Felder Datenbereich und Erstellungsdatum für Sammlungen sind leer.	Alle Sammlungen zeigen die Felder „Datenbereich“ und „Erstellungsdatum leer an.	Werte für Datenbereich und Erstellungsdatum werden nach Durchführung des Upgrades auf 10.5 angezeigt.
Diskrepantes Verhalten beim Hinzufügen von Workbench-Sammlungen als Datenquelle zu Reporting Engine.	Dieses Verhalten hängt davon ab, ob Sie eine vertrauenswürdige Verbindung haben oder nicht.	Wenn Ihr Workbench-Service mit einer vertrauenswürdigen Verbindung eingerichtet wurde, sollten Sie Workbench-Sammlungen manuell als eine Quelle zu Reporting Engine hinzufügen. Wenn Ihr Workbench-Service nicht mit einer vertrauenswürdigen Verbindung eingerichtet wurde, als die Workbench-Wiederherstellungssammlung erstellt wurde, sendet er automatisch eine Nachricht an die Reporting Engine, um ihn als eine Quelle in der Reporting Engine hinzuzufügen.

Problem	Mögliche Ursachen	Lösungen
Sammlungsattribute (Größe, Datenbereich und Erstellungsdatum) werden nicht angezeigt.	Der Datenbereich für eine Sammlung wird nicht angezeigt, wenn der Jetty-Service von Neuem gestartet wird, während die Wiederherstellung läuft. Wiederherstellungssammlungen, die von einer Explorer-Ansicht erstellt wurden, zeigen einen leeren Datenbereich an. Alle Sammlungen, die auf einer 10.4 Workbench erstellt wurden, zeigen leere Werte für Datenbereich und Erstellungsdatum nach Durchführung des Upgrades auf 10.5 an. In einer Umgebung mit gemischtem Modus (10.5 NetWitness-Server und 10.4.x Workbench) werden Größe, Datenbereich und Erstellungsdatum nicht angezeigt.	Keine.
Ein Ausnahmefehler oder eine leere Seite wird angezeigt, wenn ein Drill-down in eine Workbench-Sammlung durchgeführt wird.	Sammlung wurde geschlossen, weil sie das Sammlungs-Timeout überschritten hat.	Untersuchen Sie die Sammlung von Beginn an.
Leere Sammlung wurde erstellt.	Leere Sammlung wird angezeigt, wenn die Wiederherstellung fehlschlägt, weil der Workbench-Service während der Erstellung der Sammlung von Neuem gestartet wurde.	Keine

Problem	Mögliche Ursachen	Lösungen
Service fährt plötzlich herunter.		Führen Sie den Service von der Befehlszeile aus und achten Sie auf jede Fehlermeldung. Wenn Sie ein Beispiel sehen möchten, führen Sie den Befehl von der Serverkonsole `/usr/sbin/NwWorkbench` für Workbench aus.
REST-Anforderung verweigert.		Überprüfen Sie die Konfiguration „user.agent.whitelist“ unter `/rest/config/`. Wenn sie nicht leer ist, sollte dies ein Regex-Ausdruck sein, der gültigen HTTP-Benutzeragenten entspricht. Wenn der regex-Ausdruck nicht passt, werden alle REST-Anforderungen verweigert (siehe allow.missing.user.agent für die potenzielle Ausnahme). Wenn er leer ist, werden alle Anforderungen zugelassen.
Abfragen mit Rohmetadaten geben leere Werte für das Feld „Roh“ zurück.		Überprüfen Sie, ob Sie über eine relevante **`packet db`** verfügen.