RSA NETWITNESS® SUITE

Konfigurationsleitfaden Reporting Engine

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

Funktionsweise der Reporting Engine

NetWitness Reporting Engine ist ein Service auf dem NetWitness-Administrationsserver und erleichtert die Extraktion von Daten aus verschiedenen Datenquellen, um Berichte für die Compliance und Analysen zu erzeugen. Reporting Engine speichert die Definitionen der Diagramme, Regeln, Berichte und Warnmeldungen, die zum Generieren von Berichten, Diagrammen und Warnmeldungen verwendet werden.

Die Reporting Engine-Konfiguration umfasst die Konfiguration der Datenquellen, der Definitionen von Ausgaben oder Benachrichtigungen und der Parameter, um die Performance der Datenextraktion und der Erzeugung von Berichten, Diagrammen und Warnmeldungen zu verbessern.

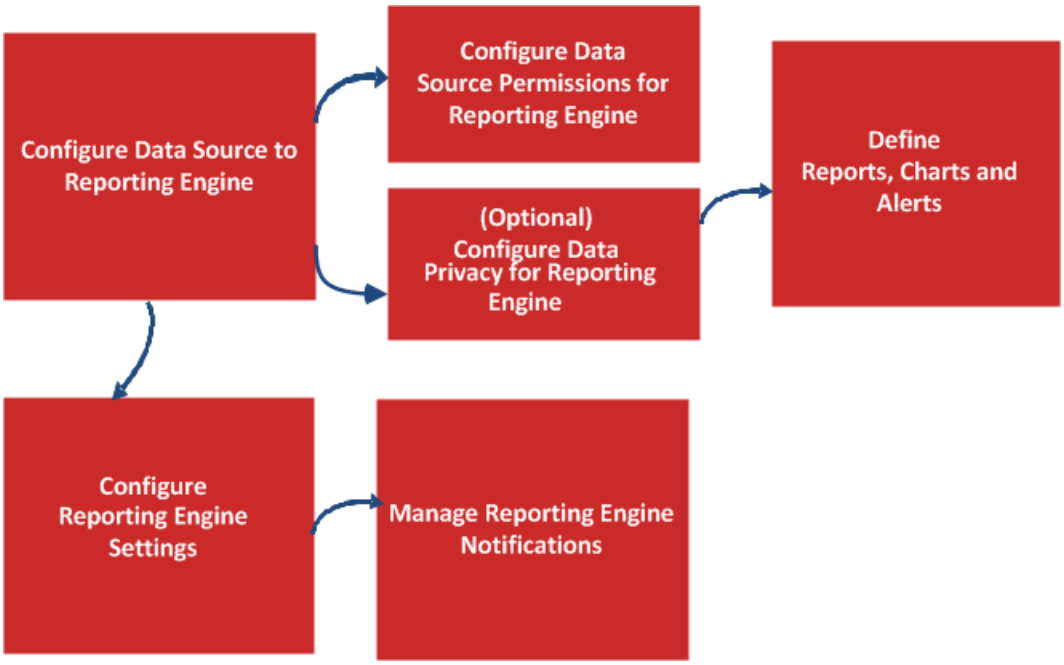
Bei der Installation der NetWitness Suite wird Reporting Engine automatisch als Service installiert. Hierdurch können die Berichte, Diagramme und Warnmeldungen in der RSA NetWitness Suite verwaltet werden und stehen zur Ansicht zur Verfügung. Des Weiteren können Berichte im PDF- oder CSV-Format und Diagramme im PDF-Format heruntergeladen und als Dashlets hinzugefügt werden.

Damit die Reporting Engine Berichte und Warnmeldungen anhand der aus einer Datenquelle abgerufenen Daten ausführen kann, müssen Sie einer Reporting Engine eine Datenquelle bzw. mehrere Datenquellen zuordnen. Es gibt drei Typen von Datenquellen:

- NWDB-Datenquellen: Die NWDB-Datenquellen (NetWitness Database) sind Decoder, Log Decoder, Broker, Concentrators, Archiver und Collection. Die Erzeugung von Berichten, Warnmeldungen und Diagrammen für NWDB-Datenquellen wird in der Reporting Engine unterstützt.
- Warehouse-Datenquellen: Die Warehouse-Datenquellen sind Horton Works und MapR, die Informationen vom Warehouse Connector sammeln und Berichte und Warnmeldungen erzeugen. Diese Datenquelle erzeugt nur Berichte.
- Respond-Datenquellen: Respond wird zum Erzeugen von Berichten für Warnmeldungen und Incidents verwendet. Diese Datenquelle erzeugt nur Berichte.

Workflow

Der folgende Workflow stellt eine Übersicht über die Reporting Engine-Konfiguration dar, die es dem Benutzer ermöglicht, Berichte, Diagramme und Warnmeldungen zu erzeugen.


Configure Data Source to Reporting Engine
Configure Data Source Permissions for Reporting Engine
(Optional) Configure Data Privacy for Reporting Engine
Define Reports, Charts and Alerts
Configure Reporting Engine Settings
Manage Reporting Engine Notifications

Konfigurieren der Reporting Engine

Bei der Installation des NetWitness-Servers ist der Reporting Engine-Service automatisch verfügbar und einige Parameter werden mit Standardwerten ausgefüllt, um optimale Ergebnisse zu erzielen.

Sie müssen außerdem sicherstellen, dass die Datenquellen in NetWitness Suite bereitgestellt und konfiguriert sind. Weitere Informationen finden Sie im Thema zum Dialogfeld „Service hinzufügen“ oder „Service bearbeiten“ im *Leitfaden zur Host- und Service-Konfiguration*.

Hier können Sie folgende Aufgaben ausführen:

- Prüfen Sie Live auf den neuesten Datenquellen-Inhalt. Führen Sie diese Überprüfung regelmäßig durch. (Weitere Informationen finden Sie im Thema „Managen von Live-Ressourcen“ im *Handbuch Live-Services*.)
- (Optional)Hinzufügen von zusätzlichem Speicherplatz für große Berichte.

Konfigurieren der Datenquellen

Datenquellen wie beispielsweise NWDB, Warehouse oder Respond müssen konfiguriert werden. Sie können NWDB, Warehouse und Respond konfigurieren, um Berichte, Diagramme und Warnmeldungen zu erzeugen. Optional können Sie auch Archiver-, Sammlungs- und Workbench-Datenquellen konfigurieren.

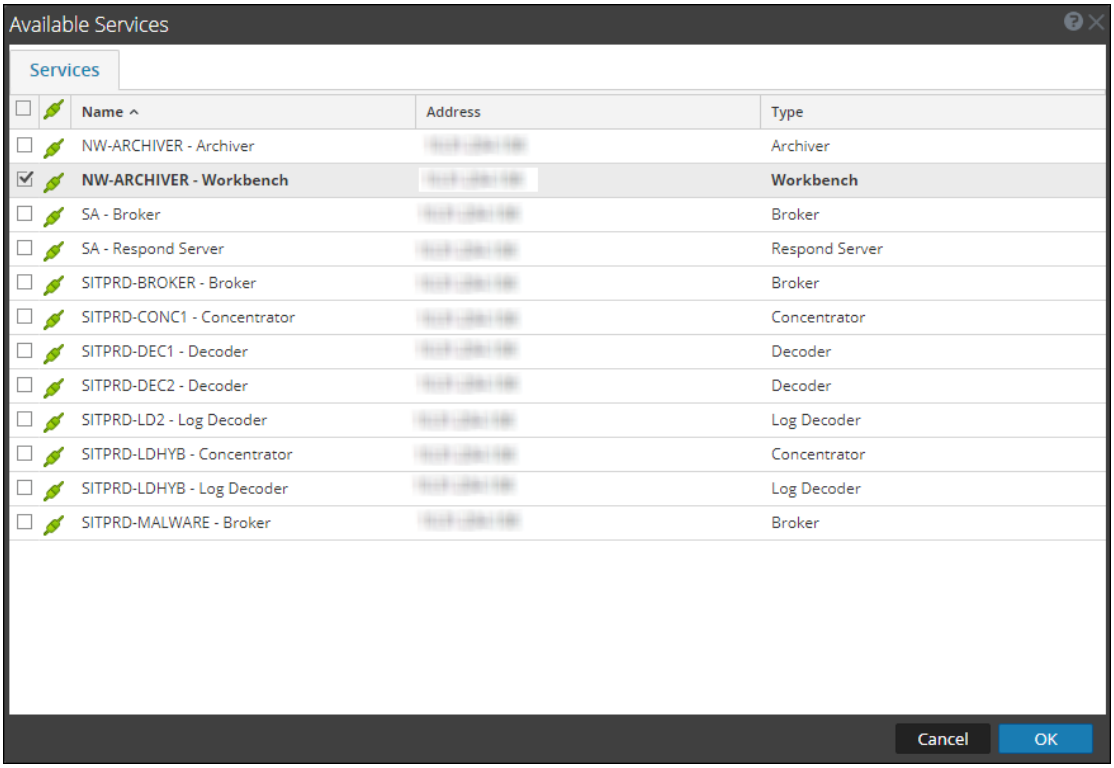
Konfigurieren einer NWDB-Datenquelle

So fügen Sie eine NWDB-Datenquelle hinzu:

1. Navigieren Sie zu **ADMIN** > **Services**.
2. Wählen Sie im Bereich **Services** den **Reporting Engine**-Service aus.
3. Klicken Sie auf  > **Ansicht** > **Konfiguration**.

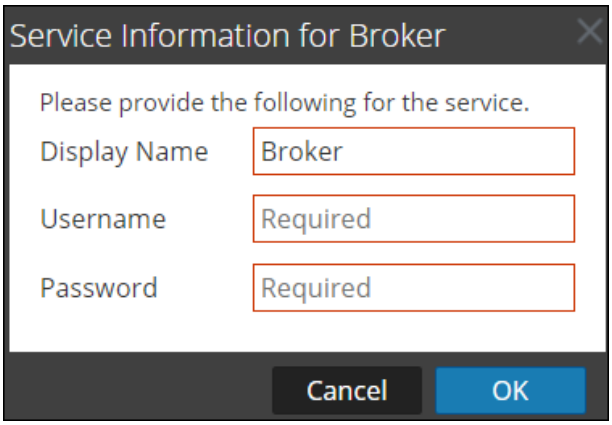
   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Klicken Sie auf der Registerkarte **Quellen** auf  > **Verfügbare Services**.

   Das Dialogfeld **Verfügbare Services** wird angezeigt.

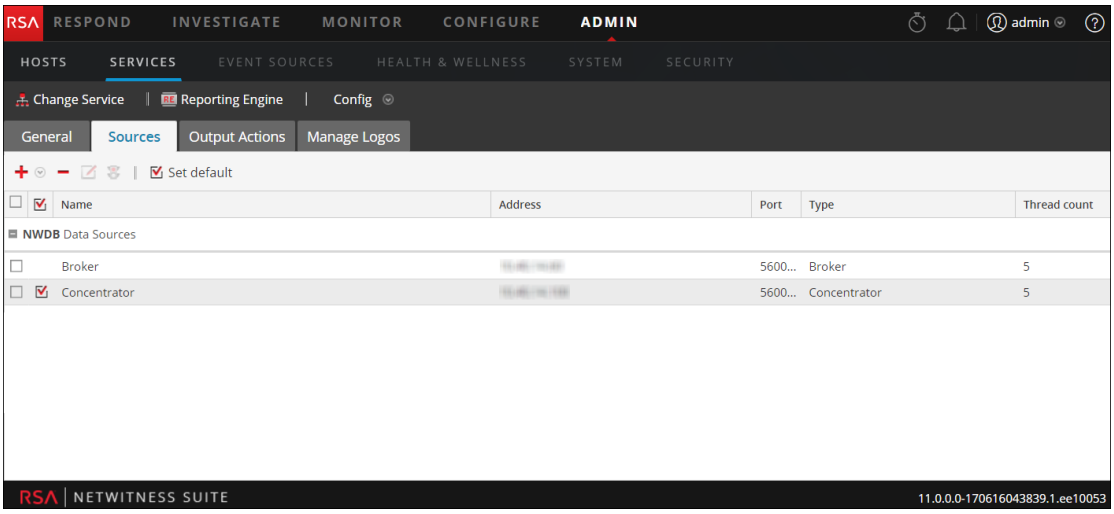


5. Wählen Sie einen NWDB-Service aus, den Sie hinzufügen möchten, und klicken Sie auf **OK**.

6. Geben Sie im Dialogfeld „Serviceinformationen für Broker“ die Serviceinformationen für den Service ein und klicken Sie auf **OK**. In diesem Beispiel wird ein Broker-Service hinzugefügt.



7. Wenn der Service erfolgreich hinzugefügt wurde, wird er auf der Registerkarte „Quellen“ angezeigt.



Hinweis: Die Services mit aktiviertem Trust-Modell müssen einzeln hinzugefügt werden. Sie werden aufgefordert, einen Benutzernamen und ein Passwort für den ausgewählten Service einzugeben.

Konfigurieren einer Warehouse-Datenquelle

Sie können die Warehouse-Datenquelle zu Reporting Engine hinzufügen, sodass Sie die Daten aus den erforderlichen Services extrahieren, in MapR oder Horton Works speichern sowie Berichte und Warnmeldungen erzeugen können. Das Verfahren zum Konfigurieren von Warehouse als Datenquelle ist unterschiedlich. Zum Extrahieren von Daten aus einer Warehouse-Datenquelle müssen Sie diese anhand des folgenden Verfahrens konfigurieren.

Hinweis: Warehouse Analytics wird in NetWitness Suite 11.0 nicht unterstützt.

Voraussetzung

Führen Sie folgende Aufgaben aus und stellen Sie Folgendes sicher:

- Hinzufügen einer Warehouse-Datenquelle zur Reporting Engine
- Einstellen einer Warehouse-Datenquelle als Standardquelle
- Der HIVE-Server befindet sich auf allen Warehouse-Nodes im Ausführungsstatus.
  Verwenden Sie den folgenden Befehl, um den Status des HIVE-Servers zu prüfen:
  `status hive2` *(MapR deployments)*
  `service hive-server2 status` *(Horton Works deployments)*
- Warehouse Connector ist so konfiguriert, dass Daten in die Warehouse-Bereitstellungen geschrieben werden.
- Wenn die Kerberos-Authentifizierung für HiveServer2 aktiviert ist, vergewissern Sie sich, dass die Keytab-Datei in das Verzeichnis `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/` auf dem Reporting Engine-Host kopiert wurde.

  Hinweis: Der Benutzer **rsasoc** muss über Leseberechtigungen für die Keytab-Datei verfügen. Weitere Informationen erhalten Sie unter Konfigurieren von Datenquellenberechtigungen.

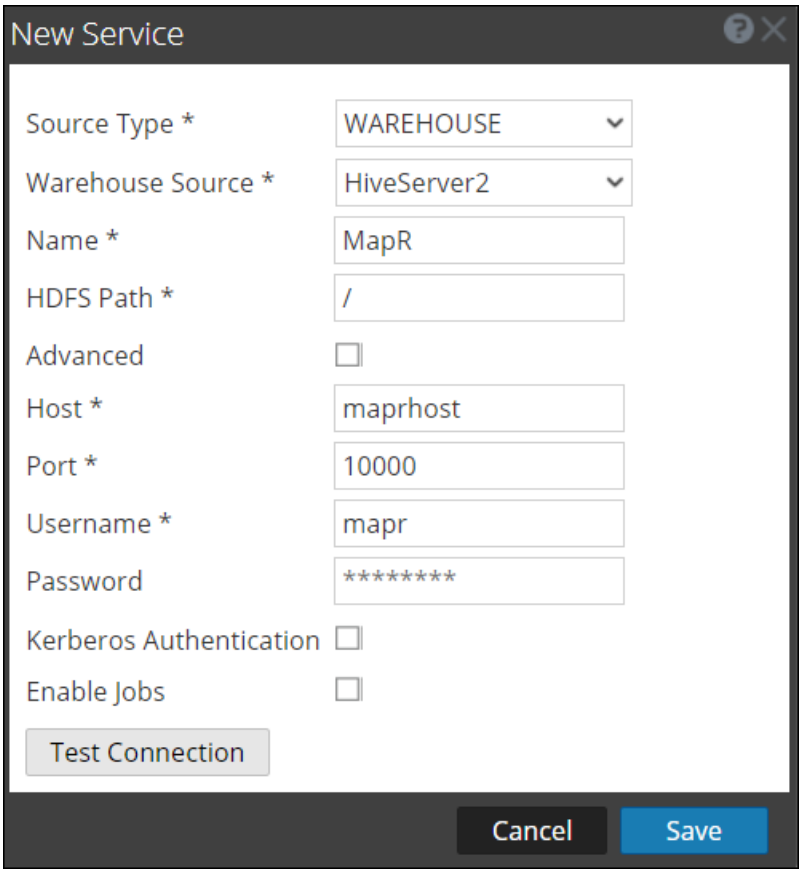
  Außerdem müssen Sie den Speicherort der Keytab-Datei im Parameter **Kerberos-Keytab-Datei** in der Ansicht „Services > Konfiguration“ der Reporting Engine aktualisieren. Weitere Informationen finden Sie unter Registerkarte „Allgemein“.

So fügen Sie die Warehouse-Datenquelle für MapR hinzu:

1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie in der Liste **Services** den **Reporting Engine**-Service aus.
3. Klicken Sie auf  > **Ansicht** > **Konfiguration**.
4. Klicken Sie auf die Registerkarte **Quellen**.

   Die Ansicht **Service-Konfiguration** wird mit geöffneter Registerkarte **Quellen** in der Reporting Engine angezeigt.
5. Klicken Sie auf  und wählen Sie **Neuer Service** aus.

   Das Dialogfeld Neuer Service wird angezeigt.



6. Wählen Sie im Drop-down-Menü **Quelltyp** die Option **WAREHOUSE** aus.
7. Wählen Sie aus dem Drop-down-Menü **Warehouse-Quelle** die Warehouse-Datenquelle aus.
8. Geben Sie im Feld **Name** den Hostnamen für die Warehouse-Datenquelle ein.
9. Geben Sie im Feld **HDFS-Pfad** den HDFS-Stammpfad ein, in den der Warehouse Connector die Daten schreibt.

   Beispiel:
   Wenn **/saw** der lokale Mount-Punkt für HDFS ist, den Sie beim Mounten von NFS (Network File System) auf dem Gerät konfiguriert haben und wenn der Warehouse Connector-Service zum Schreiben von Daten nach SAW installiert ist, finden Sie weitere Informationen hierzu im Thema „Mounten des Warehouse auf dem Warehouse Connector“ im *Konfigurationsleitfaden für RSA NetWitness Warehouse (MapR)*.

   Wenn Sie ein Verzeichnis namens **Ionsaw01** unter **/saw** erstellt und den entsprechenden lokalen Mount-Pfad als **/saw/Ionsaw01** angegeben haben, lautet der entsprechende HDFS-Stammpfad **/Ionsaw01**.

   Der Mount-Punkt **/saw** impliziert / als Stammpfad für HDFS. Der Warehouse Connector schreibt die Daten von **/Ionsaw01** in HDFS. Wenn in diesem Pfad keine Daten verfügbar sind, wird die folgende Fehlermeldung angezeigt:

`"No data available. Check HDFS path"`

Stellen Sie sicher, dass **/lonsaw01/rsasoc/v1/sessions/meta** AVRO-Dateien der Metadaten enthält, bevor Sie einen Verbindungstest durchführen.

10. Aktivieren Sie das Kontrollkästchen **Erweitert**, um die erweiterten Einstellungen zu verwenden, und geben Sie die **Datenbank-URL** mit der vollständigen JDBC-URL ein, um eine Verbindung mit dem HiveServer2 herzustellen.

    Beispiel:
    Wenn Kerberos in HIVE aktiviert ist, lautet die JDBC-URL wie folgt:

    `jdbc:hive2://<host>:<port>/<db>;principal=<Kerberos serverprincipal>`

    Wenn SSL in Hive aktiviert ist, lautet die JDBC-URL wie folgt:

    `jdbc:hive2://<host>:<port>/<db>;ssl=true;sslTrustStore=<trust_store_path>;trustStorePassword=<trust_store_password>`

    Weitere Informationen zu HIVE-Serverclients finden Sie unter https://cwiki.apache.org/confluence/display/hive/HiveServer2+Clients.

11. Wenn Sie die erweiterten Einstellungen nicht verwenden, geben Sie die Werte für **Host** und **Port** ein.

    - Geben Sie in das Feld **Host** die IP-Adresse des Hosts ein, auf dem HiveServer2 gehostet ist.

      Hinweis: Sie können die virtuelle IP-Adresse von MapR nur dann verwenden, wenn HiveServer2 auf allen Nodes im Cluster ausgeführt wird.

    - Geben Sie in das Feld **Port** den HiveServer2-Port der Warehouse-Datenquelle ein. Die Standardportnummer ist **10000**.

12. Geben Sie in die Felder **Benutzername** und **Passwort** die JDBC-Anmeldedaten für den Zugriff auf HiveServer2 ein.

    Hinweis: Sie können auch den LDAP-Modus der Authentifizierung mithilfe von Active Directory verwenden. Anweisungen zum Aktivieren des LDAP-Authentifizierungsmodus finden Sie unter Aktivieren der LDAP-Authentifizierung.

13. Zum Ausführen von Warehouse Analytics-Berichten finden Sie weitere Informationen unter Aktivieren von Jobs im Thema Konfigurieren von Datenquellen für Reporting.

14. Zum Aktivieren der Kerberos-Authentifizierung finden Sie weitere Informationen unter Aktivieren der Kerberos-Authentifizierung im Thema Konfigurieren von Datenquellen für Reporting.

15. Wenn Sie die hinzugefügte Warehouse-Datenquelle als Standardquelle für die Reporting Engine festlegen möchten, wählen Sie sie aus und klicken Sie auf Set default.

So fügen Sie die Warehouse-Datenquelle für Horton Works (HDP) hinzu:

Hinweis: Achten Sie darauf, die Datei `hive-jdbc-1.2.1-with-full-dependencies.jar` herunterzuladen. Diese JAR-Datei enthält die Treiberdatei von HIVE 1.2.1, die für Hive 1.2.1 Hiveserver2 über RSA Link (https://community.rsa.com/docs/DOC-67251) eine Verbindung zur Reporting Engine herstellt.

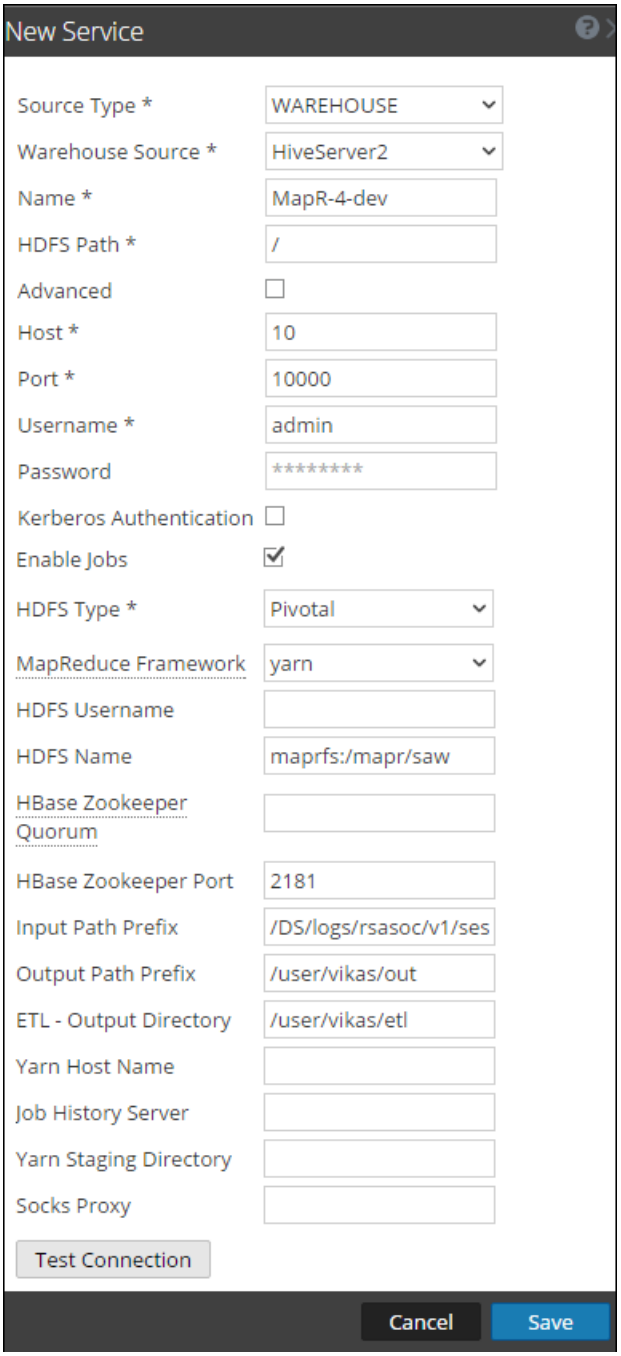
1. Stellen Sie über SSH eine Verbindung mit dem NetWitness Suite-Server her.
2. Erstellen Sie im Ordner `/opt/rsa/soc/reporting-engine/plugins/` ein Backup der folgenden JAR-Datei:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` oder `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
3. Entfernen Sie die folgende JAR-Datei:
   `hive-jdbc-0.12.0-with-full-dependencies.jar` oder `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
4. Kopieren Sie im Ordner „/opt/rsa/soc/reporting-engine/plugins“ mithilfe von WinSCP die folgende JAR-Datei:
   `hive-jdbc-1.2.1-with-full-dependencies.jar`
5. Starten Sie den Reporting Engine-Service neu.
6. Melden Sie sich bei der NetWitness Suite-Benutzeroberfläche an.
7. Wählen Sie den **Reporting Engine**-Service und dann  > **Ansicht** > **Durchsuchen** aus.
8. Stellen Sie in der Datei **hiveConfig** den Parameter **EnableSmallSplitBasedSchemaLiteralCreation** auf **true** ein.

Jobs aktivieren

Hinweis: Warehouse Analytics wird in NetWitness Suite 11.0 nicht unterstützt.

Führen Sie zum Ausführen von Warehouse Analytics-Berichten das folgende Verfahren aus.

1. Aktivieren Sie das Kontrollkästchen **Jobs aktivieren**.



Hinweis: Wählen Sie im Feld „HDFS-Typ“ nicht „Pivotal“ aus, da diese Option nicht für diese Version unterstützt wird.

2. Geben Sie die folgenden Details ein:

a. Wählen Sie im Drop-down-Menü **HDFS-Typ** den HDFS-Typ aus.

- Wenn Sie den HDFS-Typ „Horton Works“ auswählen, geben Sie die folgenden Informationen ein:

Feld	Beschreibung
HDFS-Benutzername	Geben Sie den Benutzernamen ein, den die Reporting Engine beim Herstellen einer Verbindung mit Horton Works beanspruchen soll. Für Horton Works DCA-Standardcluster lautet dieser „gpadmin“.
HDFS-Name	Geben Sie die URL für den Zugriff auf HDFS ein. Beispiel: hdfs://hdm1.gphd.local:8020.
HBase Zookeeper Quorum	Geben Sie die Liste der Hostnamen (durch Kommas getrennt) ein, auf denen die ZooKeeper-Server ausgeführt werden.
HBase Zookeeper-Port	Geben Sie die Portnummer für die ZooKeeper-Server ein. Der Standardport ist 2181.
Eingabepfadpräfix	Geben Sie den Ausgabepfad für den Warehouse Connector (`/sftp/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) bis zum Verzeichnis für das Jahr ein. Beispiel: `/sftp/rsasoc/v1/sessions/data/`.
Ausgabepfadpräfix	Geben Sie den Speicherort ein, an dem die Ergebnisse des Data Science-Jobs in HDFS gespeichert sind.
Yarn-Hostname	Geben Sie den Hostnamen des Hadoop-Yarn-Ressourcenmanagers im DCA-Cluster ein. Beispiel: **hdm3.gphd.local**.
Jobverlaufsserver	Geben Sie die Adresse des Hadoop-Jobverlaufsservers im DCA-Cluster ein. Beispiel: **hdm3.gphd.local:10020**.
Yarn-Staging-Verzeichnis	Geben Sie das Staging-Verzeichnis für YARN im DCA-Cluster ein. Beispiel: `/user`.

Feld	Beschreibung
Socks-Proxy	Wenn Sie das Standard-DCA-Cluster verwenden, werden die meisten der Hadoop-Services in einem lokalen privaten Netzwerk ausgeführt, das nicht von der Reporting Engine erreichbar ist. Dann müssen Sie eine SOCKS-Proxy in dem DCA-Cluster ausführen und den Zugriff von außerhalb des Clusters erlauben. Beispiel: **mdw.netwitness.local:1080**.

- Wenn Sie den Typ MapR HDFS auswählen, geben Sie die folgenden Informationen ein:

Feld	Beschreibung
MapR-Hostname	Der Benutzer kann die öffentliche IP-Adresse mit einem beliebigen der MapR-Warehouse-Hosts ausfüllen.
MapR-Hostbenutzer	Geben Sie den UNIX-Benutzernamen im entsprechenden Host ein, der Zugriff auf die Ausführung der Map-Reduzierungsjobs im Cluster hat. Der Standardwert ist „mapr“.
MapR-Hostpasswort	(Optional) Kopieren Sie zum Einrichten einer Authentifizierung ohne Passwort den öffentlichen Schlüssel des Benutzers „rsasoc“ von **/home/rsasoc/.ssh/id_rsa.pub** in die Datei „authorized_keys“ des Warehouse-Hosts in **/home/mapr/.ssh/authorized_keys** unter der Annahme, dass „mapr“ der Remote-UNIX-Benutzer ist.
MapR-Hostarbeitsverzeichnis	Geben Sie einen Pfad ein, für den der entsprechende UNIX-Benutzer (z. B. „mapr“) über Schreibberechtigung verfügt. **Hinweis:** Das Arbeitsverzeichnis wird von der Reporting Engine verwendet, um die Warehouse Analytics-jar-Dateien remote zu kopieren und die Jobs von dem gegebenen Hostnamen aus zu starten. Sie dürfen „/tmp“ nicht verwenden, um ein Auffüllen des temporären Systemspeichers zu vermeiden.Das angegebene Arbeitsverzeichnis wird von der Reporting Engine remote gemanagt.

Feld	Beschreibung
HDFS-Name	Geben Sie die URL für den Zugriff auf HDFS ein. Für den Zugriff auf ein bestimmtes Cluster ist dies z. B. „maprfs:/mapr/<Clustername>“.
HBase Zookeeper-Port	Geben Sie die Portnummer für die ZooKeeper-Server ein. Der Standardport ist 5181.
Eingabepfadpräfix	Geben Sie den Ausgabepfad (`/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) bis zum Verzeichnis für das Jahr ein. Beispiel: `/rsasoc/v1/sessions/data/`.
Eingabedateiname	Geben Sie den Dateinamenfilter für avro-Dateien ein. Beispiel: **sessions-warehouseconnector**.
Ausgabepfadpräfix	Geben Sie den Speicherort ein, an dem die Ergebnisse des Data Science-Jobs in HDFS gespeichert sind.

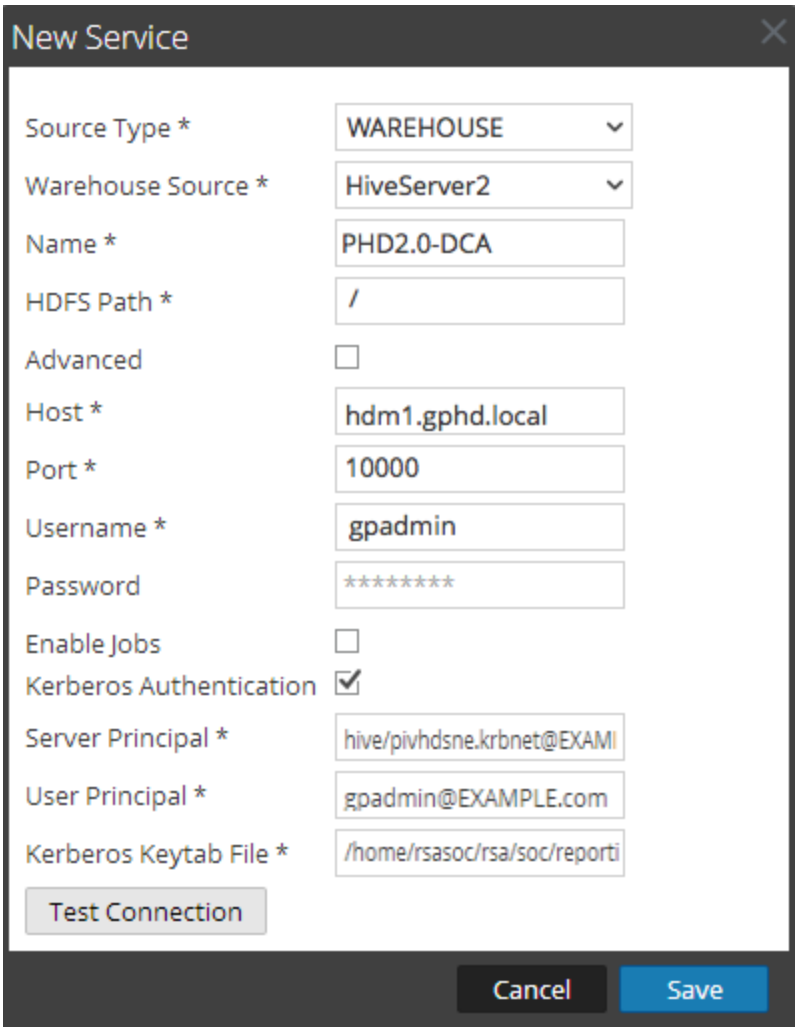
b. Wählen Sie das MapReduce-Framework gemäß HDFS-Typ aus.

Hinweis: Für den HDFS-Typ „MapR“ wählen Sie das MapReduce-Framework als „Klassisch“ aus. Für den HDFS-Typ „Horton Works“ wählen Sie das MapReduce-Framework als „Yarn“ aus.

Aktivieren Sie dann die Kerberos-Authentifizierung.

Aktivieren der Kerberos-Authentifizierung

1. Aktivieren Sie das Kontrollkästchen **Kerberos-Authentifizierung**, wenn Warehouse über einen Kerberos-fähigen Hive-Server verfügt.



2. Füllen Sie die Felder wie folgt aus:

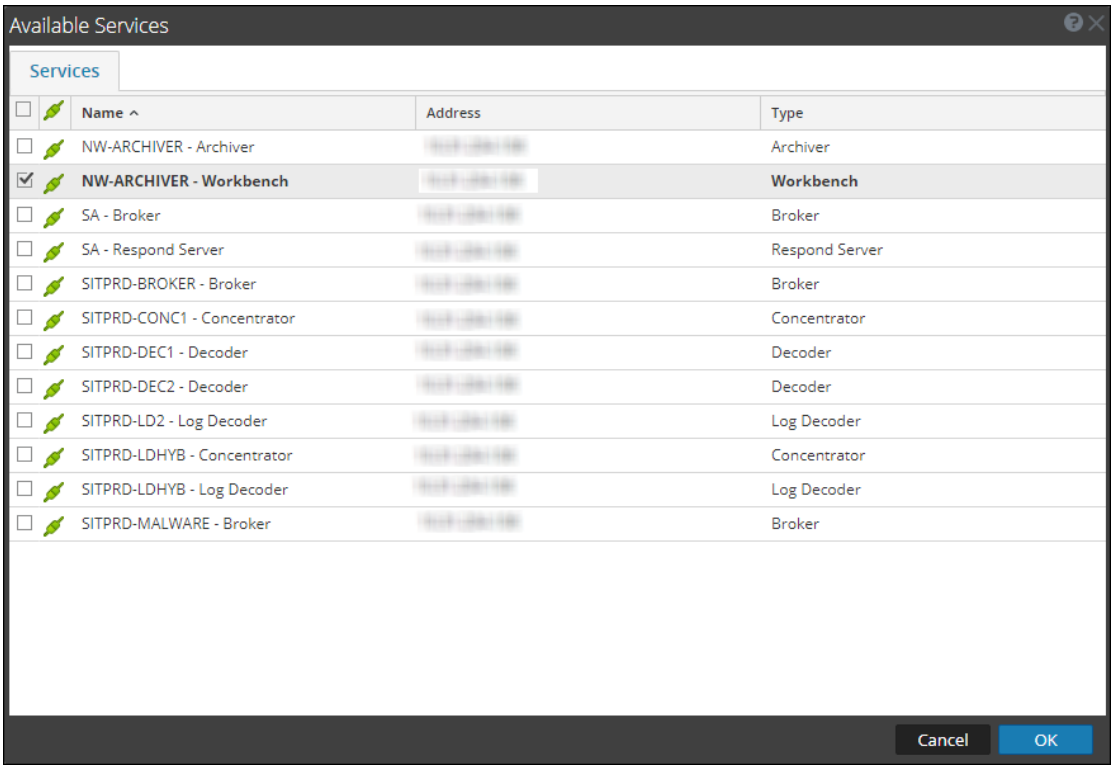
Feld	Beschreibung
Serverprinzipal	Geben Sie den Prinzipal ein, mit dem der Hive-Server beim KDC-Server (Key Distribution Center) authentifiziert wird.
Benutzerprinzipal	Geben Sie den Prinzipal ein, den der HIVE-JDBC-Client für die Authentifizierung beim KDC-Server verwendet, um eine Verbindung mit dem HIVE-Server herzustellen. Beispiel: **gpadmin@EXAMPLE.COM**.

Feld	Beschreibung
Kerberos-Keytab-Datei	Sehen Sie sich den Speicherort der Kerberos-Keytab-Datei an, der im Bereich „HIVE-Konfiguration“ auf der Reporting Engine-Registerkarte „Allgemein“ konfiguriert ist. **Hinweis:** Die Reporting Engine unterstützt nur die Datenquellen, die mit den gleichen Kerberos-Anmeldedaten konfiguriert wurden wie Benutzerprinzipal und Schlüsseltabellendatei.

3. Klicken Sie auf **Verbindung testen**, um die Verbindung mit den eingegebenen Werten zu testen.
4. Klicken Sie auf **Speichern**.

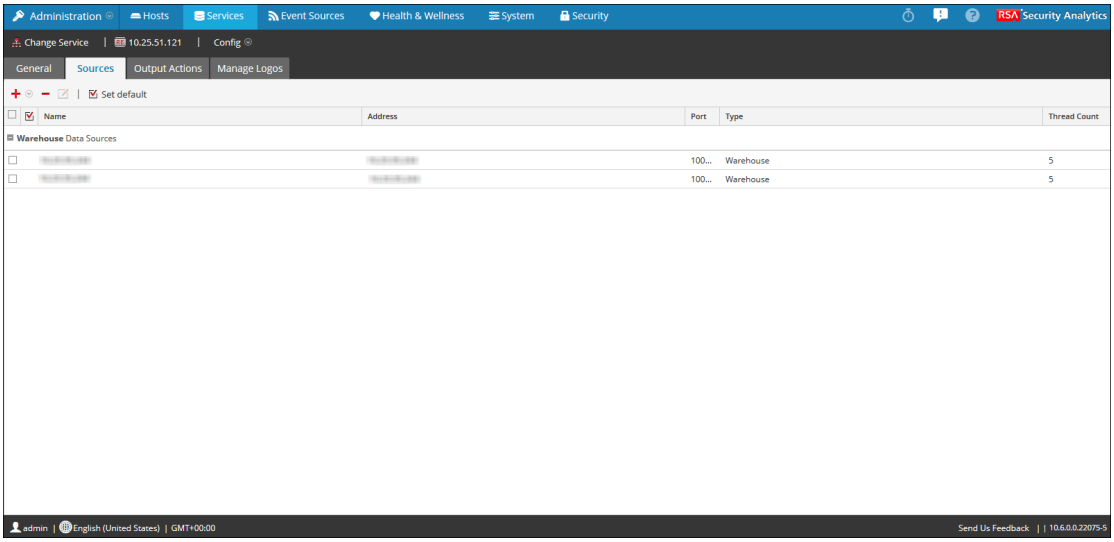
   Die hinzugefügte Warehouse-Datenquelle wird auf der Reporting Engine-Registerkarte „Quellen“ angezeigt.
5. Klicken Sie auf > **Verfügbare Services**.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



6. Wählen Sie im Dialogfeld „Verfügbare Services“ den Service aus, den Sie als Datenquelle zur Reporting Engine hinzufügen möchten, und klicken Sie auf **OK**.

NetWitness Suite fügt diesen Service als Datenquelle hinzu, die für Berichte und Warnmeldungen in dieser Reporting Engine verfügbar ist.



Hinweis: Dieser Schritt ist nur für ein nicht vertrauenswürdiges Modell maßgeblich.

Einstellen einer Datenquelle als Standardquelle

So legen Sie beim Erstellen von Berichten und Warnmeldungen eine Datenquelle als Standardquelle fest:

1. Navigieren Sie zu **Dashboard** > **Administration** > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Wählen Sie > **Ansicht** > **Konfiguration** aus.

   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.

   Die **Servicekonfigurationsansicht** wird mit geöffneter Registerkarte „Reporting Engine-Quellen“ angezeigt.
5. Wählen Sie die Quelle aus, die Sie als Standardquelle festlegen möchten, z. B. „Broker“.
6. Aktivieren Sie das Kontrollkästchen **Als Standard festlegen**.

   NetWitness Suite verwendet diese Datenquelle als Standard, wenn Sie Berichte und Warnmeldungen für diese Reporting Engine erstellen.

(Optional) Hinzufügen einer Workbench als Datenquelle

Sie müssen die folgenden Workbench-Konfigurationen ausführen, damit Sie Daten aus der Workbench-Datenquelle zum Erzeugen von Berichte und Warnmeldungen verwenden können. In diesem Thema erhalten Sie folgende Anweisungen zum Hinzufügen des Workbench-Services als Datenquelle zur Reporting Engine, um einen Bericht für die durch Workbench gesammelten Daten zu erzeugen.

Voraussetzungen

Vergewissern Sie sich, dass Sie:

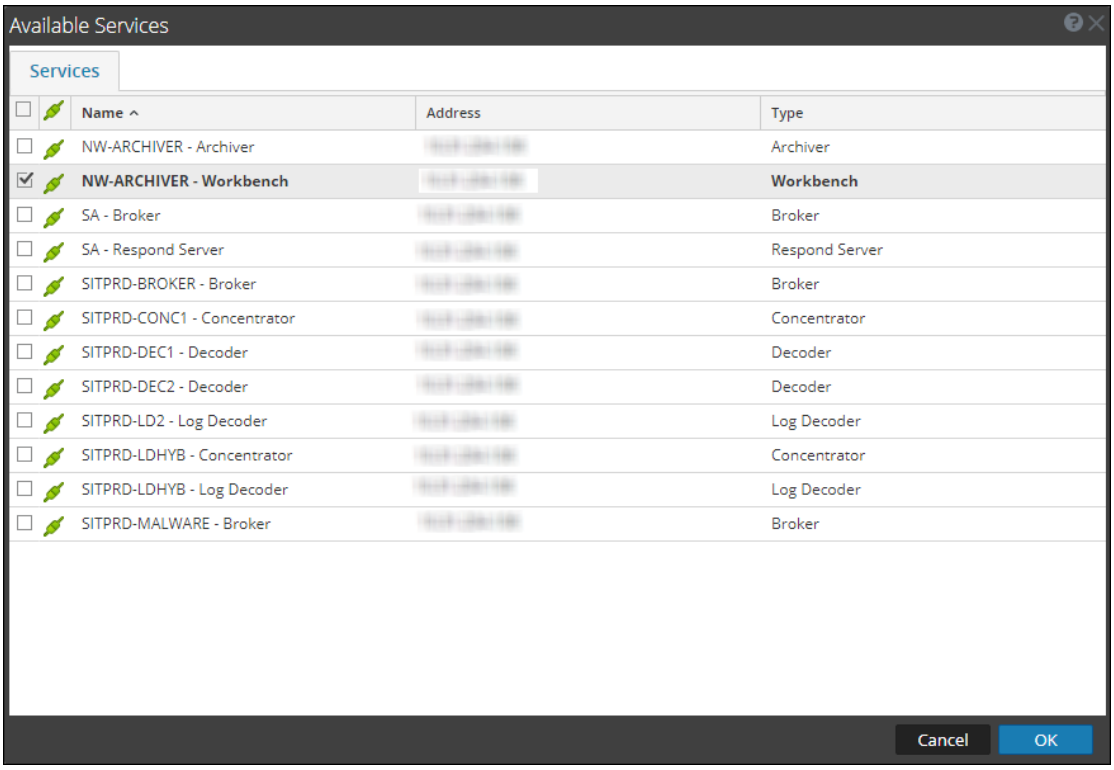
1. Workbench als Service zu Ihrer NetWitness Suite-Bereitstellung hinzugefügt haben. Weitere Informationen finden Sie im *Konfigurationsleitfaden Archiver*.
2. Eine Sammlung wurde zum Workbench-Service hinzugefügt.

So fügen Sie Workbench als Datenquelle zur Reporting Engine hinzu:

1. Navigieren Sie zu ADMIN > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Wählen Sie  > **Ansicht** > **Konfiguration** aus.

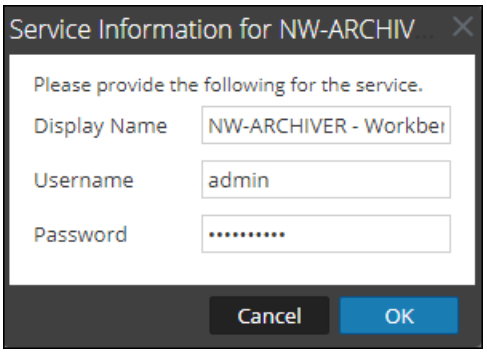
   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.
5. Klicken Sie auf  und wählen Sie **Verfügbare Services** aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.

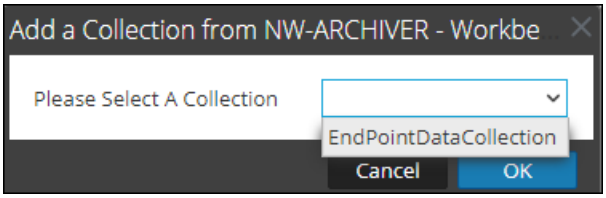


6. Wählen Sie den Workbench-Service aus und klicken Sie auf **OK**.
   Eine Liste der Sammlungen wird angezeigt.

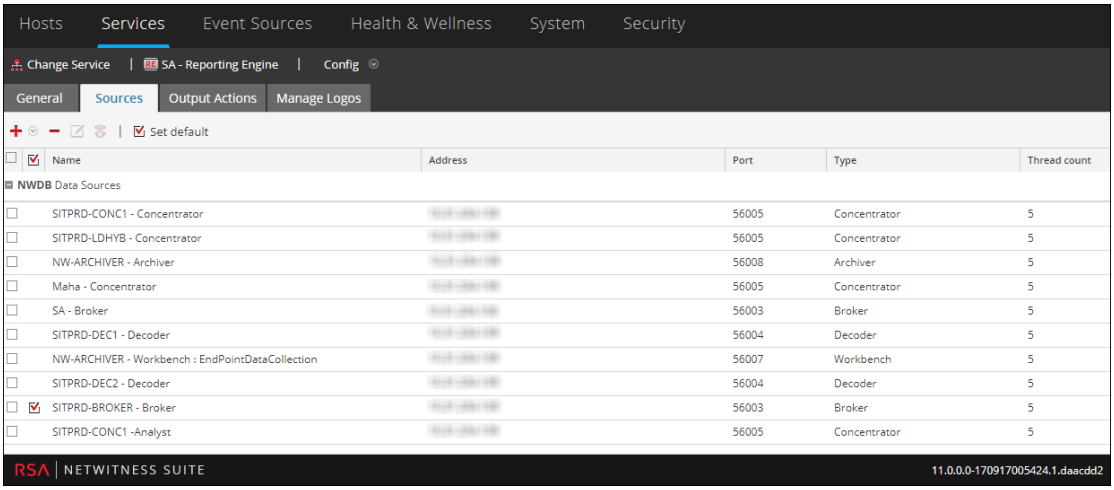
7. Geben Sie die Serviceinformationen ein und klicken Sie auf **OK**.



8. Wählen Sie eine Sammlung in der Drop-down-Liste aus.



9. Die Datenquelle wird auf der Registerkarte „Quellen“ angezeigt.



Der Workbench-Service wird jetzt als Datenquelle zur Reporting Engine hinzugefügt.

Hinweis: Die Services mit aktiviertem Trust-Modell müssen einzeln hinzugefügt werden. Sie werden aufgefordert, einen Benutzernamen und ein Passwort für den ausgewählten Service einzugeben.

(Optional) Hinzufügen von Archiver als Datenquelle

Sie müssen die folgenden Archiver-Konfigurationen ausführen, um Daten aus der Archiver-Datenquelle zum Erzeugen von Berichte und Warnmeldungen verwenden zu können:

Voraussetzungen

Vergewissern Sie sich, dass Folgendes zutrifft:

1. Sie haben den NetWitness Suite Archiver-Host in Ihrer Netzwerkumgebung installiert. Weitere Informationen erhalten Sie im *Leitfaden für die ersten Schritte mit Hosts und Services*.
2. Sie haben den Log Decoder in Ihrer Netzwerkumgebung installiert und konfiguriert. Weitere Informationen finden Sie unter „Hinzufügen von Log Decoder als Datenquelle zu Archiver“ im *Konfigurationsleitfaden Archiver*.
3. Reporting Engine ist als Service in Ihrer NetWitness Suite-Bereitstellung verfügbar.
4. Sie haben Archiver als Service zu Ihrer NetWitness Suite-Bereitstellung hinzugefügt. Weitere Informationen finden Sie unter „Hinzufügen des Archiver-Services“ im

Konfigurationsleitfaden Archiver.

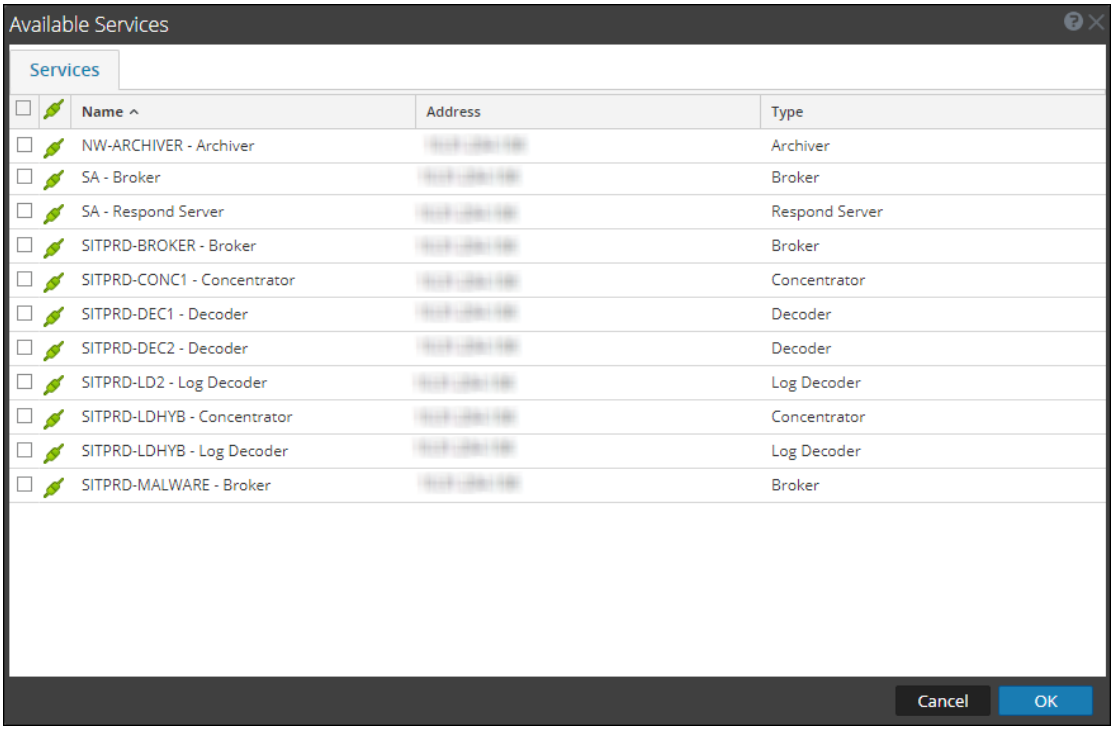
5. Sie haben eine Lizenz für den Archiver-Service angewendet.

So fügen Sie die Archiver-Datenquelle zur Reporting Engine hinzu:

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Wählen Sie in der Liste **Services** den **Reporting Engine**-Service aus.
3. Klicken Sie auf  **> Ansicht > Konfiguration**.

   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.
5. Klicken Sie auf  und wählen Sie **Verfügbare Services** aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



6. Wählen Sie den Archiver-Service aus und klicken Sie auf **OK**.

   Das Dialogfeld für die Serviceauthentifizierung wird angezeigt.

   Hinweis: Die Services mit aktiviertem Trust-Modell müssen einzeln hinzugefügt werden. Sie werden aufgefordert, einen Benutzernamen und ein Passwort für den ausgewählten Service einzugeben.

7. Geben Sie den Benutzernamen und das Passwort für Archiver ein.

8. Klicken Sie auf **OK**.

   Der ausgewählte Archiver wird im Bereich Services aggregieren aufgeführt.

(Optional) Integrieren von Endpunktinformationen in Berichte

Sie können die Endpunktdaten verwenden, indem Sie anhand der folgenden Anweisungen die Endpunktinformationen zu Berichten hinzufügen. Der *Leitfaden zur RSA Endpunktintegration* bietet einen Überblick über die Endpunktintegration in RSA NetWitness Suite.

Voraussetzungen

Achten Sie auf Folgendes:

- Sie müssen die Endpunktwarnmeldungen über Syslog für einen Log Decoder konfiguriert haben. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Endpunktwarnmeldungen über Syslog für einen Log Decoder“ im *Leitfaden zur RSA Endpunktintegration*.

So integrieren Sie Endpunktinformationen in Berichte:

1. Wählen Sie in **Reporting Engine** die Optionen **Ansicht** > **Konfiguration** > **Quellen** aus.
2. Fügen Sie den Concentrator, der Daten vom Log Decoder nutzt, als Datenquelle hinzu. Die Endpunktmetadaten werden in die Reporting Engine geladen.
3. Führen Sie Berichte aus, indem Sie die gewünschten Metadaten auswählen.

(Optional) Hinzufügen einer Sammlung als Datenquelle zur Reporting Engine

Sie müssen die folgenden Konfigurationen für eine Sammlung ausführen, damit Sie Daten aus der Datenquelle der Sammlung zum Erzeugen von Berichte, Diagrammen und Warnmeldungen verwenden können:

Voraussetzungen

Vergewissern Sie sich, dass Sie:

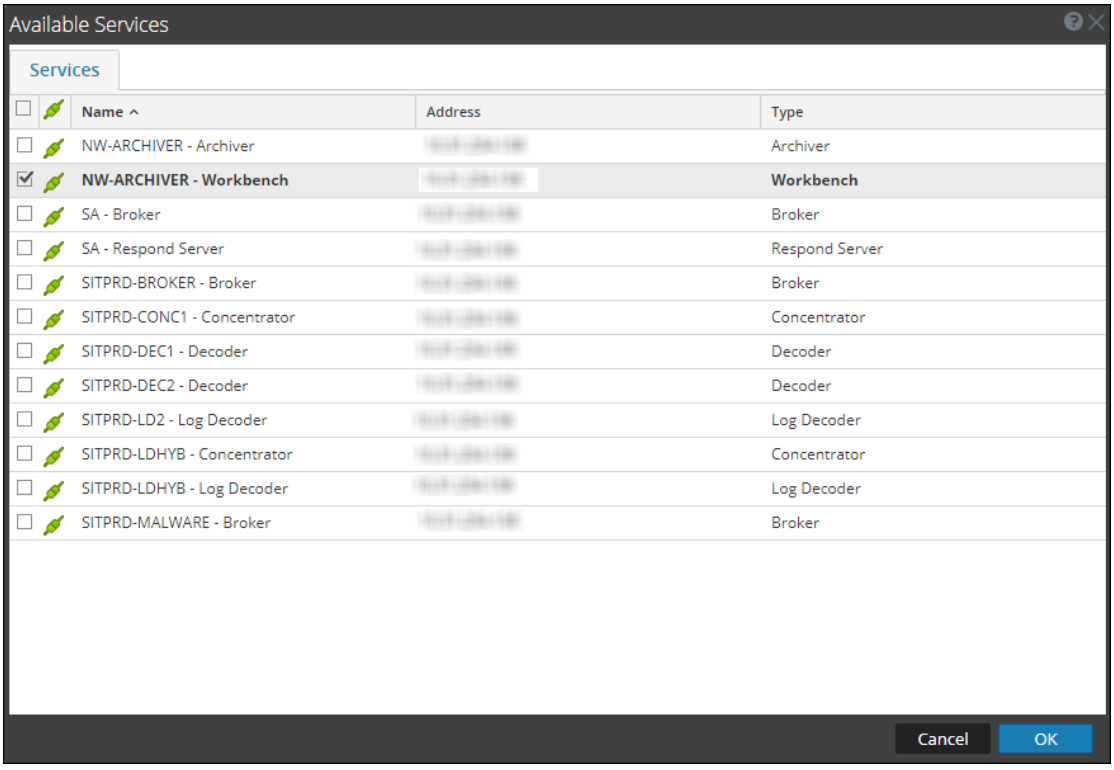
- Sie haben einen Workbench-Service auf einem Reporting Engine-Host installiert.
- Sie haben Daten an einem bekannten Speicherort auf Ihrem lokalen Host gesichert, wenn Sie eine Sammlung hinzufügen möchten, für die aus der Sicherung wiederhergestellte Daten verwendet werden sollen.

So verknüpfen Sie eine Sammlung als Datenquelle mit Reporting Engine:

1. Navigieren Sie zu **ADMIN** > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Klicken Sie auf  > **Ansicht** > **Konfiguration**.

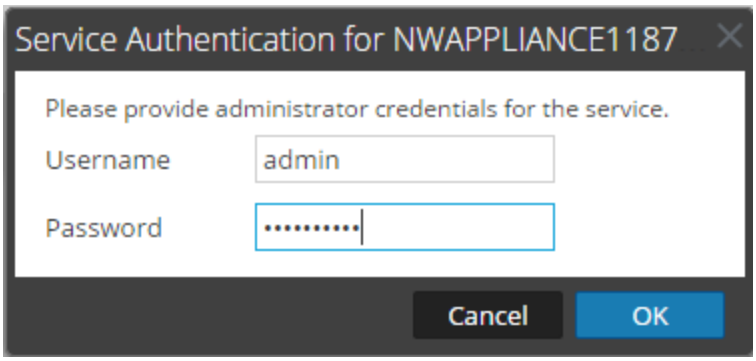
   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.
5. Klicken Sie auf  und wählen Sie **Verfügbare Services** aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt.



6. Wählen Sie den Workbench-Service aus und klicken Sie auf **OK**.

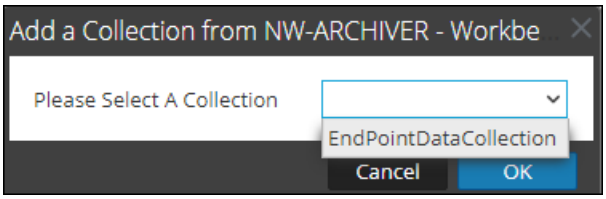
   Das Dialogfeld „Serviceauthentifizierung“ für den ausgewählten Service wird angezeigt.



Hinweis: Die Services mit aktiviertem Trust-Modell müssen einzeln hinzugefügt werden. Sie werden aufgefordert, einen Benutzernamen und ein Passwort für den ausgewählten Service einzugeben.

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

   Das Dialogfeld zum Hinzufügen einer Sammlung wird angezeigt.



9. Wählen Sie eine Sammlung aus der Drop-down-Liste aus und klicken Sie auf **OK**.

   Der Workbench-Service wird jetzt als Datenquelle zur Reporting Engine hinzugefügt.

Konfigurieren des Datenschutzes für die Reporting Engine

Sie können den Datenschutz für alle Datenquellen der Reporting Engine mithilfe der Registerkarte „Quellen“ in der Ansicht „Services > Ansicht > Konfiguration“ konfigurieren.

Aufgrund der neuen Datenschutzfunktion in NetWitness Suite 11.0 und höher kann der Zugriff auf vertrauliche Metadaten in NetWitness Suite Core-Services durch das Konfigurieren separater Datenquellen für DPO-Benutzer (Data Privacy Officer) und Nicht-DPO-Benutzer sowie durch das Beschränken des Zugriffs auf diese Datenquellen mithilfe entsprechender Berechtigungen eingeschränkt werden.

In der Ansicht Services > Konfiguration können Sie jeden Core-Service als zwei separate Datenquellen hinzufügen: einmal mit einem Servicekonto mit Berechtigungen, die denen eines DPO entsprechen, und einmal mit einem Servicekonto mit Berechtigungen, die denen eines beliebigen anderen Benutzers entsprechen. Dann können Sie zur rollenbasierten Beschränkung des Zugriffs auf diese Datenquellen individuellen Rollen Lesezugriff oder keinen Zugriff auf diese Datenquellen zuweisen. Zum Beschränken des Zugriffs auf Warehouse-Datenquellen können Sie ebenso vorgehen.

Weitere Informationen erhalten Sie unter Konfigurieren von Datenquellenberechtigungen.

Hinweis: Ein Benutzer, dem die Rolle `Data_Privacy_Officers` (oder eine entsprechende benutzerdefinierte Rolle) zugewiesen wurde, kann einen Bericht, ein Diagramm und eine Warnmeldung erstellen. Sie können außerdem einen Bericht oder eine Warnmeldungs-Ausgabeaktionen im Reporting-Modul konfigurieren. In einer Umgebung, in der Datenschutzfunktionen von NetWitness Suite aktiviert sind und mindestens ein Metaschlüssel als geschützt konfiguriert ist, kann dies folgende Auswirkungen haben:
- Wenn von einem DPO-Benutzer ein Alarm erstellt wird, sind alle von der Warnmeldung betroffenen geschützten oder vertraulichen Metadaten automatisch in Respond verfügbar. Dadurch können unbeabsichtigt alle Benutzer des Respond-Moduls unabhängig von ihren Rollen Zugriff auf die vertraulichen Metawerte erhalten. Eine Möglichkeit, dies zu verhindern, besteht darin, die Veröffentlichung in Respond aus Reporting zu deaktivieren.
- Wenn von einem DPO-Benutzer eine Ausgabeaktion konfiguriert wird, können vertrauliche Metawerte oder Berichte mit vertraulichen Metawerten oder beides für die Zielbenutzer dieser Ausgabeaktion verfügbar werden, unabhängig davon, welche Rolle den Zielbenutzern zugewiesen wurde.

Es wird dringend empfohlen, dass DPO-Benutzer es vermeiden, Warnmeldungen zu erstellen oder Ausgabeaktionen für einen Bericht oder eine Warnmeldung im Reporting-Modul zu konfigurieren. Wenn sie eine solche Konfiguration vornehmen, müssen die obigen Auswirkungen sorgsam bedacht werden.

NetWitness Suite Core-Services (z. B. Concentrator, Broker oder Archiver) unterstützen die Möglichkeit zur Beschränkung von Metadaten basierend auf der konfigurierten Benutzerrolle. Um die Datenschutzfunktionen für Reporting Engine zu verwenden, können Sie zwei separate Servicekonten für Core konfigurieren: ein Servicekonto für das allgemeine Reporting, das keine sensiblen Daten umfasst, und ein weiteres Konto für Benutzer mit den nötigen Berechtigungen für den Zugriff auf alle Daten einschließlich sensibler Daten. Der Zugriff auf beschränkte Metadaten für die beiden Servicekonten wird im Rahmen des Datenschutzplans auf jedem Core-Service konfiguriert.

In Reporting Engine können Sie jeden Core-Service als zwei separate Datenquellen hinzufügen (einmal als reguläre Datenquelle und einmal als privilegierte Datenquelle), indem Sie zwei separate Servicekonten verwenden. Sie können Reporting Engine so konfigurieren, dass nur Benutzer mit privilegierten Rollen Zugriff auf die sensible Datenquelle haben. Folglich kann Reporting Engine auf zwei Wegen eine Verbindung zu einer NWDB-Datenquelle herstellen:

- Über ein Servicekonto mit DPO-Rolle
- Über ein Servicekonto ohne DPO-Rolle

Hinweis: Außerdem können Sie für denselben Core-Service zwei oder mehrere Datenquellen hinzufügen.

Nachdem demselben Core-Service zwei Datenquellen mit verschiedenen Servicekonten hinzugefügt wurden, können Sie Datenquellenberechtigungen konfigurieren, um den Zugriff auf diese Datenquellen zu managen. Weitere Informationen erhalten Sie unter Konfigurieren von Datenquellenberechtigungen.

Hinweis: Wenn der Inhalt für die Verwendung des transformierten Metaschlüssels geändert wird, wird der Hash-Wert der ursprünglichen Metadaten an dessen Stelle in Berichten, Diagrammen und Warnmeldungen angezeigt.

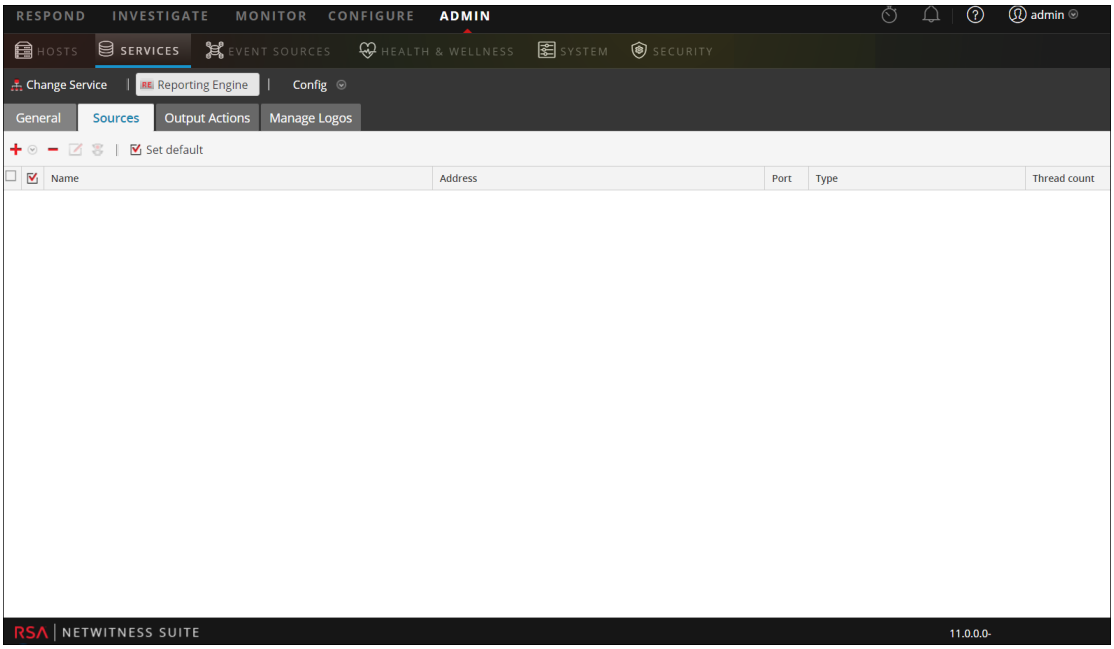
Hinzufügen einer NWDB-Datenquelle mit verschiedenen Servicekonten

So fügen Sie eine NWDB-Datenquelle hinzu:

1. Navigieren Sie zu **ADMIN** > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Klicken Sie auf  **Ansicht** > **Konfiguration**.

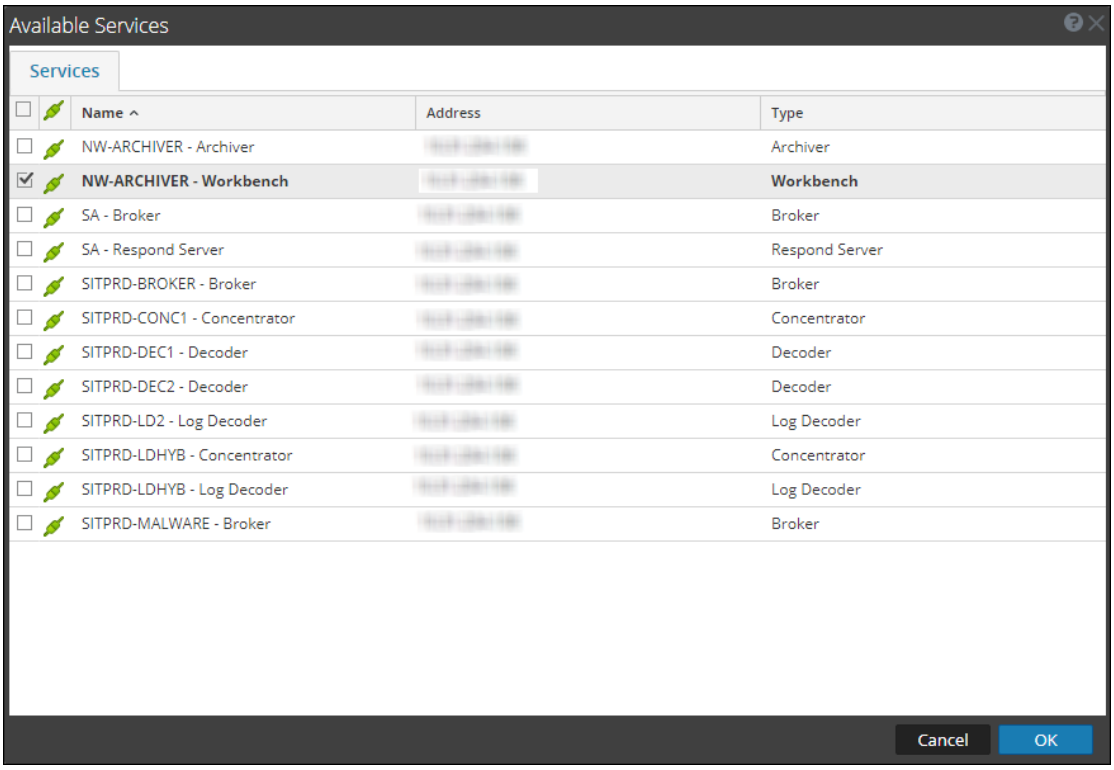
   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.

   Die Ansicht „Services > Konfiguration“ wird angezeigt.



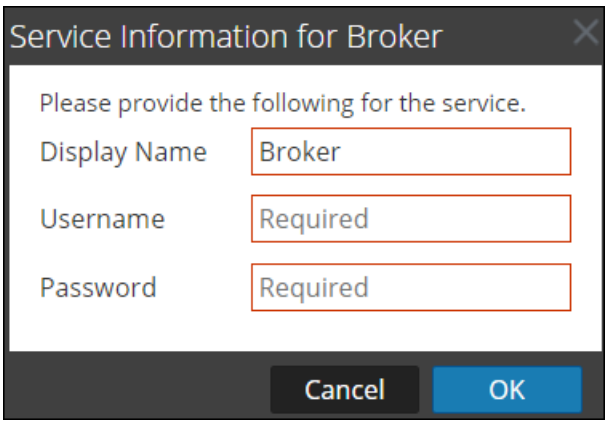
5. Klicken Sie auf + und wählen Sie „Verfügbare Services“ aus.

   Das Dialogfeld „Verfügbare Services“ wird angezeigt. Es werden alle Services aufgeführt, auch die bereits in Reporting Engine hinzugefügte Services.



6. Aktivieren Sie das Kontrollkästchen neben dem Service und klicken Sie auf **OK**.

Das Dialogfeld Serviceinformationen für den ausgewählten Service wird angezeigt.

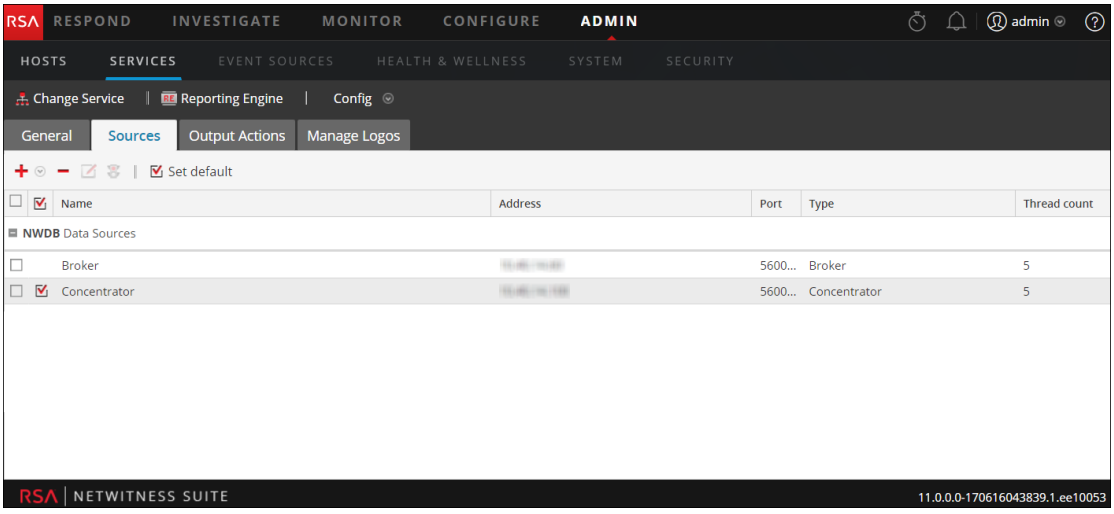


Hinweis: Sie werden von NetWitness Suite aufgefordert, einen Benutzernamen und ein Passwort für den ausgewählten Service einzugeben. Um den Zugriff auf sensible Daten zu beschränken, müssen DPO-Benutzer ihre Anmeldedaten statt der Administratoranmeldedaten verwenden, wenn Sie eine Quelle hinzufügen. Diese Anmeldeinformationen müssen auf den Host angewendet werden, auch wenn Sie vertrauenswürdige Verbindungen zwischen dem NetWitness Suite-Server und NetWitness Suite Core-Hosts verwenden.

Wiederholen Sie den Schritt für Nicht-DPO-Datenquellen.

7. Geben Sie den Benutzernamen und das Passwort für das gewünschte Servicekonto ein.
8. Klicken Sie auf **OK**.

Der gewünschte Service wird nun als Datenquelle zur Reporting Engine hinzugefügt. Zwei Datenquellen werden der Reporting Engine für dasselbe Core-Gerät hinzugefügt.



Konfigurieren von Datenquellenberechtigungen

Sie können Datenquellenberechtigungen auf der Registerkarte „Quellen“ der Ansicht „Services > Konfiguration“ für die Reporting Engine konfigurieren. Dies erleichtert es Ihnen, die Zugriffssteuerung für die Datenquellen zu managen, indem Sie die Datenquellenberechtigungen festlegen. Dank der Möglichkeit, einem Core-Service mehr als eine Datenquelle hinzuzufügen, können Sie nun verschiedene Berechtigungen für jede Datenquelle eines Core-Services konfigurieren. Beispielsweise können Datenschutzbeauftragte mit ihren Anmeldeinformationen eine Warehouse-Quelle erstellen. Dann dürfen sie Berichte am Warehouse ausführen, während alle anderen Benutzer diese Quelle nicht verwenden können.

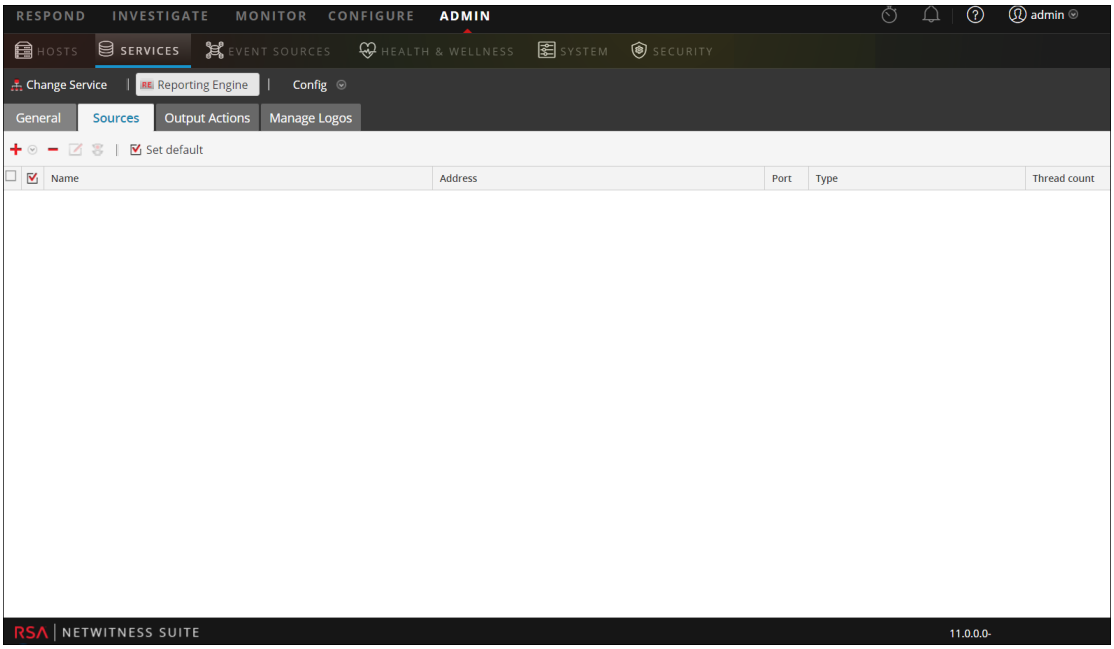
Hinweis: In 11.0 werden die Berechtigungen für NWDB- und Warehouse-Datenquellen automatisch anhand der Berechtigungen der Berichtobjekte festgelegt. Wenn z. B. die Berechtigungen der Rolle für ein Berichtobjekt in 10.5 auf **Schreibgeschützt/Lesen und Schreiben** festgelegt waren, wird dieser Rolle für alle Datenquellen, die in 10.5 vorhanden waren, automatisch die Berechtigung „Schreibgeschützt“ zugewiesen. Wenn für die Rolle keine Berechtigung festgelegt war, wird als Datenquellenberechtigung automatisch „Kein Zugriff“ festgelegt.

So konfigurieren Berechtigungen für Datenquellen:

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Klicken Sie auf  > **Ansicht** > **Konfiguration**.

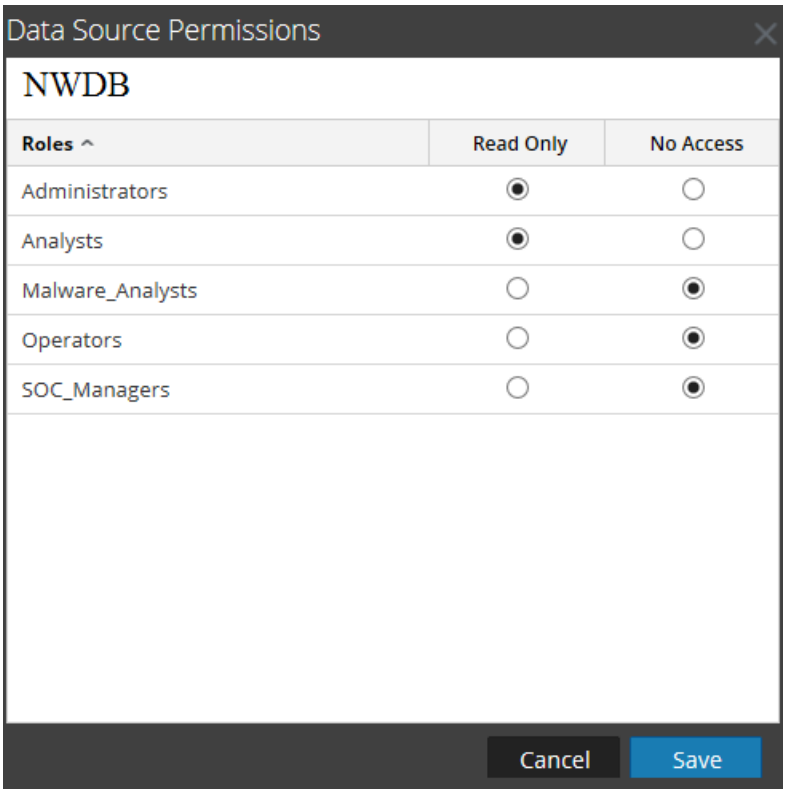
   Die Ansicht „Services > Konfiguration“ der Reporting Engine wird angezeigt.
4. Wählen Sie die Registerkarte **Quellen** aus.

   In der Ansicht „Service > Konfiguration“ wird die Registerkarte „Quellen“ angezeigt.



5. Wählen Sie durch Aktivieren des Kontrollkästchens die Datenquelle aus, für die Sie Berechtigungen konfigurieren möchten.
6. Klicken Sie auf .

   Das Dialogfeld Datenquellenberechtigungen wird angezeigt.



7. Ändern Sie die Zugriffsberechtigungen für verschiedene Benutzer basierend auf dem Typ des Servicekontos der Datenquelle. Die möglichen Berechtigungen sind **Schreibgeschützt** oder **Kein Zugriff**.
8. Klicken Sie auf **Speichern**.

   Die erforderlichen Berechtigungen für die Datenquelle werden konfiguriert.

Weitere Informationen finden Sie im *Reporting-Benutzerhandbuch*.

Konfigurieren der Reporting Engine-Einstellungen

Nach der Konfiguration der Reporting Engine und der erforderlichen Datenquellen basierend auf Ihren Anforderungen, können Sie einige Konfigurationen zum Anpassen Ihrer Berichte, Diagramme und Warnmeldungen ändern.

So konfigurieren Sie die Einstellungen:

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Wählen Sie in der Liste **Services** einen **Reporting Engine**-Service aus.
3. Klicken Sie auf  **> Ansicht > Konfiguration**.

   Die Servicekonfigurationsansicht der Reporting Engine wird mit markierter Registerkarte „Allgemein“ angezeigt. Weitere Informationen zur Reporting Engine-Registerkarte „Allgemein“ finden Sie unter Registerkarte „Allgemein“.
4. Bearbeiten Sie die Einstellungen für den Reporting Engine-Service und klicken Sie auf **Anwenden**.

   Die Serviceeinstellungen werden auf der Reporting Engine konfiguriert.

Aktivieren der LDAP-Authentifizierung

Um den LDAP-Modus der Authentifizierung mithilfe von Active Directory für HiveServer2 für die Warehouse-Datenquelle zu aktivieren, führen Sie die folgenden Schritte aus.

1. Melden Sie sich bei der RSA Analytics Warehouse Appliance als Root-Benutzer an.
2. Navigieren Sie zum Verzeichnis `/opt/mapr/hive/hive-0.11/conf.new/` . Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

   ```
   cd /opt/mapr/hive/hive-0.11/conf.new/
   ```
3. Bearbeiten Sie die Datei `hive-site.xml`. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

   ```
   vi hive-site.xml
   ```
4. Fügen Sie folgende Eigenschaften unter dem Tag `<Configuration>` hinzu:

   ```
   <property>
       <name>hive.server2.authentication</name>
       <value>LDAP</value>
   </property>
   ```

```
<property>
    <name>hive.server2.authentication.ldap.url</name>
    <value>LDAP_URL</value>
</property>
```

Dabei ist `LDAP_URL` die URL des LDAP-Servers.

5. Führen Sie einen Neustart des HiveServer2 aus.

Hinzufügen von zusätzlichem Speicherplatz für große Berichte

Um zusätzlichen Festplattenspeicher zur Reporting Engine für große Berichte hinzuzufügen, führen Sie die unten angegebenen Schritte aus. Wenn große Complianceberichte für Warehouse erzeugt werden müssen, wird der Festplattenspeicher der Reporting Engine möglicherweise schneller als erwartet aufgebraucht. In solchen Fällen können Sie externen Speicher, wie z. B. SAN oder NAS, zum Speichern der Berichte mounten.

Die Verzeichnisse, die auf der Festplatte tendenziell am schnellsten gefüllt werden, sind `resultstore` und `formattedReports` im Stammverzeichnis der Reporting Engine. Es wird empfohlen, diese beiden Verzeichnisse auf SAN oder NAS auszulagern und die ursprünglichen Speicherorte durch Softlinks zu ersetzen, die auf die neuen Speicherorte verweisen. Außerdem wird empfohlen, die übrigen Verzeichnisse auf dem lokalen Datenträger selbst zu belassen, da dies zuverlässiger ist und eine höhere I/O-Performance bietet.

Hinweis: Bei den folgenden Schritten wird davon ausgegangen, dass sich das Stammverzeichnis der Reporting Engine unter `/var/netwitness/re-server/rsa/soc/reporting-engine/` befindet und der externe Speicher unter `/externalStorage/` gemountet ist. Darüber hinaus muss der Benutzer „rsasoc“ Lese- und Schreibzugriff auf den angegebenen externen Speicherpfad haben.

So verschieben Sie Festplattenspeicherplatz für die Reporting Engine in externen Speicher:

1. Beenden Sie den Reporting Engine-Service als Root-Benutzer.

   ```
   service rsasoc_re stop
   ```

2. Wechseln Sie zum `rsasoc`-Benutzer.

   ```
   su rsasoc
   ```

3. Wechseln Sie zum RE-Stammverzeichnis.

   ```
   cd /var/netwitness/re-server/rsa/soc/reporting-engine/
   ```

4. Verschieben Sie das Verzeichnis „resultstore“ zu einem gemounteten externen Speicher. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

   ```
   mv resultstore /externalStorage
   ```

5. Verschieben Sie das Verzeichnis „formattedReports“ zu einem gemounteten externen

Speicher. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

```
mv formattedReports /externalStorage
```

6. Erstellen Sie einen Softlink für „resultstore“. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

   ```
   ln -s /externalStorage/resultstore /var/netwitness/re-server/rsa/soc/reporting-engine/resultstore
   ```

7. Erstellen Sie einen Softlink für „formattedReports“. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE:

   ```
   ln -s /externalStorage/formattedReports /var/netwitness/re-server/rsa/soc/reporting-engine/formattedReports
   ```

8. Beenden Sie den `rsasoc`-Benutzer.

   ```
   exit
   ```

9. Starten Sie den Reporting Engine-Service als Root-Benutzer.

   ```
   service rsasoc_re start
   ```

   Hinweis: Wenn der externe Speicher offline ist, können Sie die folgenden Aufgaben nicht durchführen:
   1) Berichte oder Reporting-Warnmeldungen ausführen
   2) Berichte oder Reporting-Warnmeldungen anzeigen
   Sie können allerdings neue Reporting-Objekte wie etwa Berichte und Diagramme erstellen und auf Diagramme und auf das für Diagramme erstellte Live-Dashboard zugreifen. Daher müssen Sie dafür sorgen, dass der externe Speicher zuverlässig ist und über den erforderlichen Speicherplatz verfügt.

   Wenn Sie außerdem Berichte länger als 100 Tage speichern möchten, müssen Sie die Aufbewahrungskonfiguration entsprechend den Schritten unter Konfigurieren der Reporting Engine-Einstellungen ändern.

Zugriff auf die Protokolldateien der Reporting Engine

Sie können auf die Protokolldateien der Reporting Engine, die in folgendem Protokollverzeichnis gespeichert werden, zugreifen: `/var/netwitness/re-server/rsa/soc/reporting-engine/logs/`

- Aktuelle Protokolle in der `reporting-engine.log` Datei.
- Sicherungskopien früherer Protokolle in der `reporting-engine.log.*` Datei.
- 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**.

Die Reporting Engine fügt die Protokollmeldungen, die vom systemd-Manager geschriebene Ausgabe und die Befehle, die zum Starten der Reporting Engine verwendet werden, an das Verzeichnis `/var/log/messages` an. Eine `/var/log/messages` Protokolldatei ist eine Systemprotokolldatei, die nur von einem Root-Benutzer gelesen werden kann.

Konfigurieren des Aufgabenplaners für eine Reporting Engine

Sie können Warteschlangen und Pools in der Reporting Engine zur Planung von NWDB- oder Warehouse-Berichten konfigurieren. Weitere Informationen zu Aufgabenplanern finden Sie unter „Aufgabenplaner für Warehouse Reporting“ im *Handbuch zu RSA Netwitness Suite Reporting*.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes ermittelt haben:

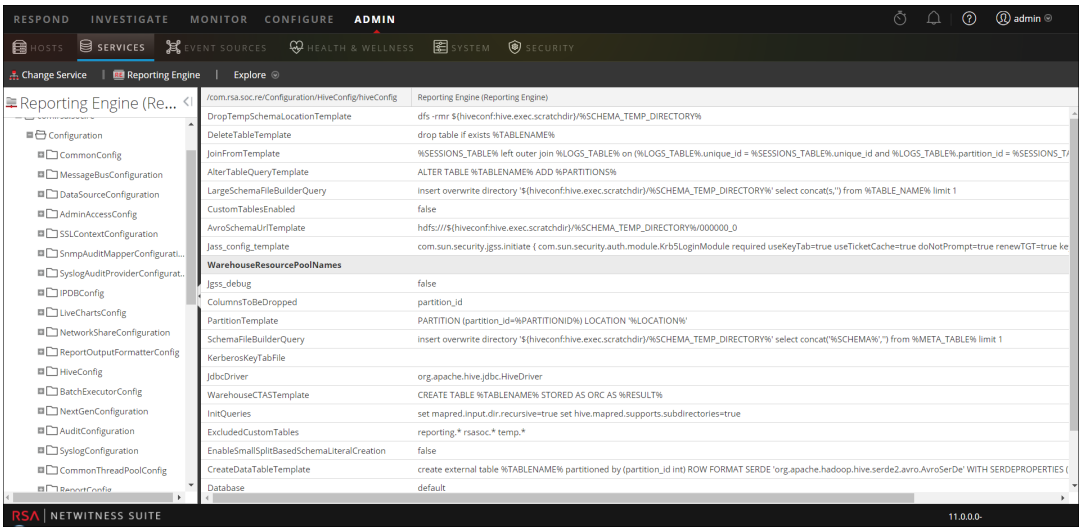
- Planungstyp und Pools oder Warteschlangen, die sie verwenden möchten. Sie können nur jeweils einen Planer für die Reporting Engine konfigurieren. Standardmäßig wird der Fair-Planer verwendet.
- Die Namen von Warteschlangen oder Pools und die Ressourcen, die jeder Warteschlange und jedem Pool zugeordnet sind.
- NetWitness Suite unterstützt nicht mehrere Warteschlangen oder Pools pro Cluster. RSA empfiehlt, den Warteschlangen oder Pools in allen Clustern eindeutige Namen zu geben oder dieselben Warteschlangen- oder Poolnamen in beiden Clustern verwenden. Ein großes Cluster kann mehr als 3 Pools oder Warteschlangen aufweisen.
- Bei Verwendung eines nicht unterstützten Planers wird von der Reporting Engine keine Eigenschaft für die von ihr gestarteten Jobs festgelegt.
- Wenn der Name des Pools oder der Warteschlange nicht im Cluster vorhanden ist, wird der Bericht vom Kapazitätenplaner in die Standardwarteschlange gestellt. Die Regel wird möglicherweise nicht vom Fair-Planer ausgeführt oder es wird ein neuer Pool mit der niedrigsten Share erstellt. Dies ist abhängig vom Wert, der für die Eigenschaft „Fair-Planer“ `mapred.fairscheduler.allow.undeclared.pools` festgelegt wurde.
- Wenn Sie keinen Pool oder keine Warteschlange angeben, befindet sich der durch die Testregel gestartete Job im `mapr`-Pool oder in der Standardwarteschlange. RSA empfiehlt, dass Sie einen mapr-Pool mit niedriger gemeinsamer Nutzung (rund 1/10 der

Gesamtkapazität) mit `maxRunningJobs = 2` konfigurieren, sodass das Ausführen von Berichten nicht durch diese Regeln unterbrochen wird. Achten Sie darauf, dass Sie diesen Poolnamen nicht für einen Bericht angeben.

Angeben der Speicherpools und Warteschlangen

So geben Sie Speicherpools und Warteschlangen an:

1. Navigieren Sie zu **ADMIN** > **Services**.
2. Wählen Sie **Reporting Engine** aus und klicken Sie auf  > **Ansicht** > **Durchsuchen**.
3. Wählen Sie **com.rsa.soc.re** > **Konfiguration** > **HiveConfig** > **hiveconfig** > **WarehouseResourcePoolNames** aus.
4. Geben Sie im Feld **WarehouseResourcePoolNames** die Pool- oder Warteschlangennamen ein (durch Leerzeichen getrennt). Wenn Sie beispielsweise vier Pools oder Warteschlangen mit den Namen pool1, pool2, wrong und default konfigurieren möchten, geben Sie die Namen durch ein Leerzeichen getrennt ein.



Definieren von Berichten, Diagrammen und Warnmeldungen

Nachdem Sie die Reporting Engine und die erforderliche Datenquelle entsprechend Ihren Anforderungen konfiguriert haben, können Sie Ihre Berichte, Diagramme und Warnmeldungen erzeugen.

Definieren von Berichten, Diagrammen und Warnmeldungen

Definieren von Berichte

Nach der Erstellung der Datenquellen und der Konfiguration der Benutzerberechtigungen für diese Datenquellen, können Sie diese Datenquellen jetzt verwenden, um die folgenden Aufgaben für das Reporting-Modul auszuführen:

- **Definieren einer Regel**
- **Testen einer Regel**
- **Planung von Berichten**
- **Hinzufügen einer Warnmeldung**
- **Hinzufügen eines Diagramms**
- **Testen eines Diagramms**

Weitere Informationen finden Sie in den oben genannten Themen im *Handbuch zu RSA Netwitness Reporting-Berichten*.

Definieren von Diagrammen

Nach der Erstellung der Datenquellen und der Konfiguration der Benutzerberechtigungen für diese Datenquellen, können Sie diese Datenquellen jetzt verwenden, um die folgenden Aufgaben für das Reporting-Modul auszuführen:

- **Definieren von Diagrammen und Diagrammgruppen**
- **Testen eines Diagramms**
- **Untersuchen von Diagrammen**
- **Managen von Diagrammen**

Weitere Informationen finden Sie in den oben genannten Themen im *Handbuch zu RSA Netwitness Reporting-Berichten*.

Definieren von Warnmeldungen

Nach der Erstellung der Datenquellen und der Konfiguration der Benutzerberechtigungen für diese Datenquellen können Sie diese Datenquellen jetzt verwenden, um die folgenden Aufgaben für das Alerting-Modul auszuführen:

- **Konfigurieren Sie Warnmeldungen**
- **Erzeugen von Warnmeldungen**
- **Hinzufügen einer Warnmeldung**
- **Anzeigen einer Warnmeldung**
- **Anzeigen von Warnmeldungsplänen**
- **Ermitteln einer Warnmeldung**

Weitere Informationen finden Sie in den oben genannten Themen im *Handbuch zu RSA Netwitness Reporting-Warnmeldungen*.

Konfigurieren der allgemeinen Reporting Engine-Einstellungen

Beim Hinzufügen und Konfigurieren des Reporting Engine-Services werden die Systemeinstellungen mit Standardwerten definiert, um optimale Ergebnisse zu erzielen. Sie können jedoch die Reporting Engine-Benachrichtigungen entsprechend Ihren Anforderungen ändern und anpassen, indem Sie zur Registerkarte „Allgemein“ in der Ansicht „Services > Konfiguration“ der Reporting Engine navigieren.

Zugriff auf die Registerkarte „Allgemein“

Sie müssen die Registerkarte „Allgemein“ öffnen, um die allgemeinen Parameter für die Reporting Engine zu konfigurieren.

So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **ADMINISTRATION** > **Services**.
2. Wählen Sie in der Liste der verfügbaren Services einen **Reporting Engine**-Service aus.
3. Klicken Sie auf **Ansicht** > **Konfiguration**.
4. Wählen Sie die Registerkarte **Allgemein** aus.
5. Klicken Sie nach dem Bearbeiten der Parameter auf **Anwenden**.

Nachdem Sie die Registerkarte „Allgemein“ geöffnet haben, können Sie die folgenden Parameter ändern.

- Systemkonfiguration
- Protokollierungskonfiguration
- Warehouse Analytics – Ausgabekonfiguration
- Warehouse Analytics – Modellkonfiguration
- Warehouse-Kerberos-Konfiguration

Weitere Informationen zu den Konfigurationsparametern finden Sie im Thema zur Registerkarte „Allgemein“.

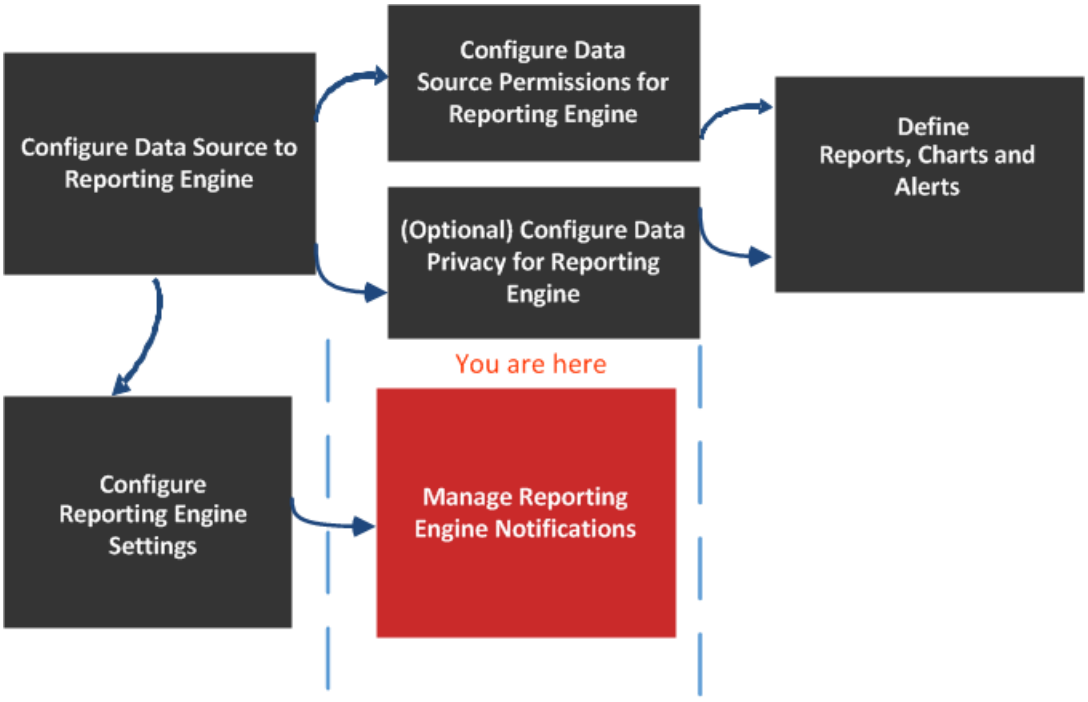
Referenzen

Damit Sie den Service anpassen und optimal nutzen können, können Sie die Reporting Engine-Einstellungen in der Ansicht „Services > Konfiguration“ ändern, die Parameter speziell für die Reporting Engine enthält.

Registerkarte „Allgemein“

Über die Registerkarte „Allgemein“ für den Reporting Engine-Service werden verschiedene Einstellungen gesteuert, mit denen die Performance eines Services abgestimmt und die Benutzeranmeldedaten für den Service angegeben werden. Navigieren Sie zu „Services > Ansicht > Konfiguration > Reporting Engine > Allgemein“. Diese Einstellungen werden ausschließlich für den Reporting Engine-Service verwendet.

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



Was möchten Sie tun?

Rolle	Aufgabe	Siehe
Administrator	Reporting Engine-Datenquellen konfigurieren	Konfigurieren der Datenquellen
Administrator	Datenquellenberechtigungen für Reporting Engine konfigurieren	Konfigurieren von Datenquellenberechtigungen

Rolle	Aufgabe	Siehe
Administrator	Datenschutz für Reporting Engine konfigurieren	Konfigurieren des Datenschutzes für die Reporting Engine
Administrator	Berichte, Diagramme und Warnmeldungen definieren	Definieren von Berichten, Diagrammen und Warnmeldungen
Administrator	Reporting Engine-Einstellungen konfigurieren	Konfigurieren der Reporting Engine-Einstellungen
Administrator/SOC-Manager	Systemeinstellungen konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Protokollierung konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Warehouse Analytics-Ausgabe konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Warehouse Analytics-Modelle konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Warehouse Kerberos konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen

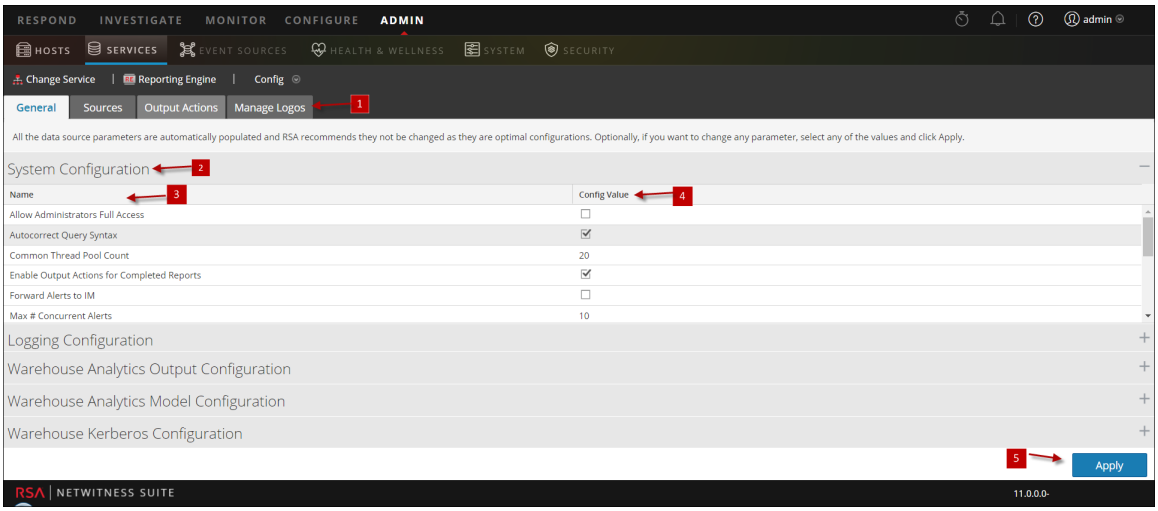
* Sie können diese Aufgaben hier durchführen.

Verwandte Themen

- Funktionsweise der Reporting Engine

Überblick

Im folgenden Beispiel der Registerkarte „Allgemein“ sind Servicekonfigurationen angezeigt.



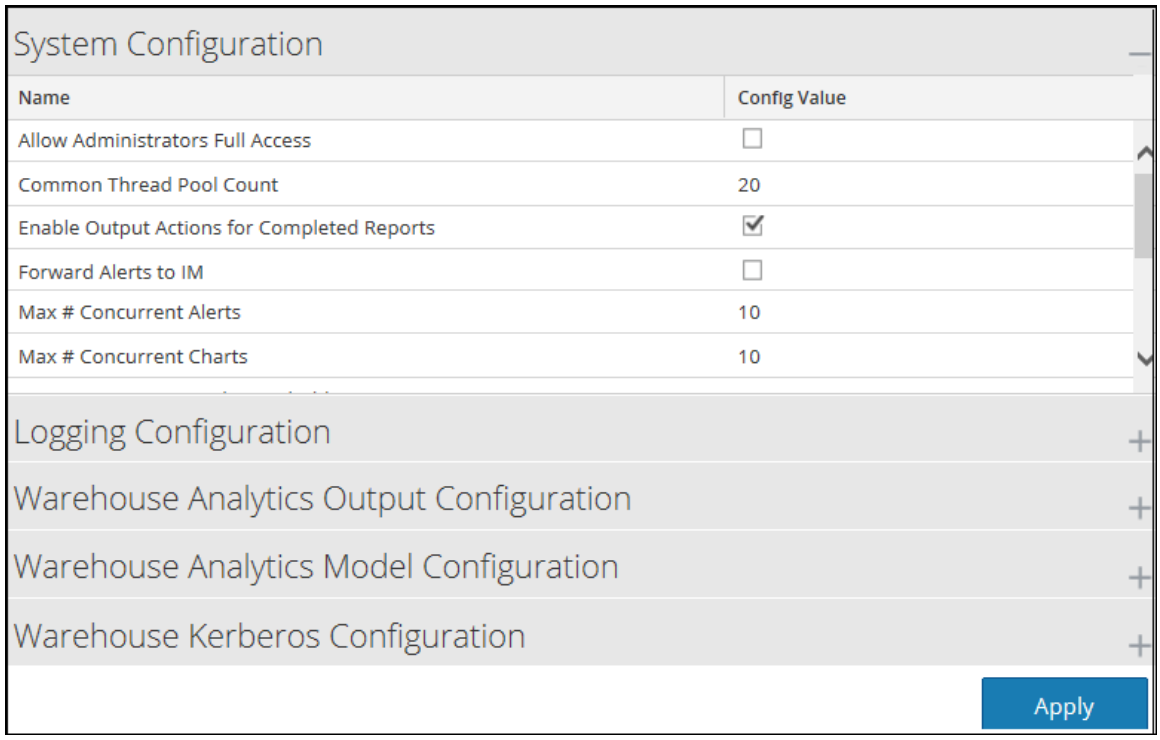
1. Zeigt alle verfügbaren konfigurierbaren Registerkarten an.
2. Zeigt die verfügbaren Konfigurationsparameter für das System an.
3. Zeigt den Namen des Parameters an.
4. Zeigt die für jeden Parameter festgelegten Werte an.
5. Wendet die Änderungen an.

Hinweis: Warehouse Analytics wird in Netwitness Suite Version 11.0 nicht unterstützt.

Systemkonfiguration

Anhand der Parameter des Bereichs „Systemkonfiguration“ für die Reporting Engine wird die Servicekonfiguration für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, sind Standardwerte wirksam. Die Standardwerte sind so ausgelegt, dass sie die meisten Umgebungen unterstützen. Es wird empfohlen, diese Werte nicht zu bearbeiten, da dies negative Auswirkungen auf die Performance haben kann.

In der folgenden Abbildung sind die Felder gezeigt, die im Bereich „Systemkonfiguration“ konfiguriert werden können:



In der folgenden Tabelle sind die Funktionen des Bereichs „Systemkonfiguration“ beschrieben.

Name	Konfigurationswert
Administratoren Vollzugriff ermöglichen	Aktivieren Sie das Kontrollkästchen, wenn Sie auf alle Reporting Engine-Objekte (Berichte, Regeln, Diagramme, Pläne und Listen) zugreifen möchten, die von anderen Benutzern (nicht Administratoren) erstellt wurden. Dabei handelt es sich um keine Standardeinstellung. **Hinweis:** Wenn Sie das Kontrollkästchen aktivieren und anschließend deaktivieren, ist kein Zugriff auf die Reporting Engine-Objekte mehr möglich, die durch Auswahl des Kontrollkästchens aktiviert wurden. Wenn Sie den Zugriff auf bestimmte Objekte jedoch über das Fenster „Berechtigungen“ (**Berichte > Verwalten > RE-Objekt >** **> Berechtigungen**) definiert haben, hat das Aktivieren/Deaktivieren dieses Kontrollkästchens keine Auswirkungen auf diese Objekte.

Name	Konfigurationswert
Allgemeine Threadpoolanzahl	Die Anzahl der Threadpools, die für die Ausführung allgemeiner Aufgaben in der Reporting Engine zugeordnet wurden. Ein gültiger Wert ist eine Ganzzahl (**20** ist der Standardwert).
Ausgabeaktionen für abgeschlossene Berichte aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Ausgabeaktionen nur für Berichte mit ausschließlich erfolgreichen Regelausführungen zu verarbeiten. Dies ist standardmäßig aktiviert. Wenn die Option deaktiviert ist, werden die Ausgabeaktionen für alle Szenarien verarbeitet (abgeschlossen, teilweise abgeschlossen, fehlgeschlagen).
Warnmeldungen weiterleiten an Antwort	Aktivieren Sie das Kontrollkästchen, um alle Warnmeldungen an „Antwort“ weiterzuleiten. Dabei handelt es sich um keine Standardeinstellung.
Maximale Anzahl gleichzeitiger Warnmeldungen	Die maximale Anzahl von Warnmeldungen, die gleichzeitig ausgeführt werden können. Dies hat direkte Auswirkungen auf den RSA-Service, für den die Warnmeldungen ausgeführt werden, da jede Warnmeldung einen Abfragethread auf dem RSA-Service verbraucht. Ein gültiger Wert ist eine Ganzzahl (**10** ist der Standardwert).
Maximale Anzahl gleichzeitiger Diagramme	Die maximale Anzahl von Diagrammen, die gleichzeitig ausgeführt werden können. Ein gültiger Wert ist eine Ganzzahl (**10** ist der Standardwert).
Maximale Anzahl gleichzeitiger LookupAndAdd-Abfragen	Die maximale Anzahl von parallelen LookupAndAdd-Abfragen, die pro NWDB-Regel ausgeführt werden können. Ein gültiger Wert ist eine Ganzzahl (**2** ist der Standardwert). Wenn Sie diesen Wert für eine bessere Performance erhöhen, müssen Sie sicherstellen, dass die NWDB-Datenquelle konfiguriert ist, um die parallelen Abfragen verarbeiten zu können.

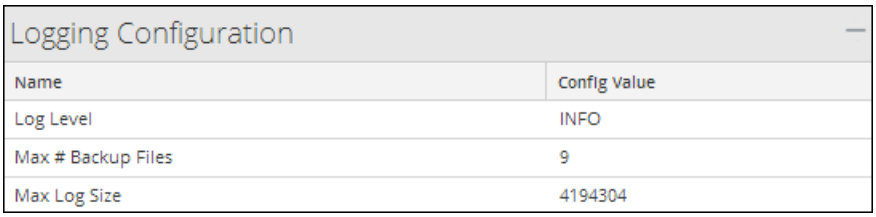
Name	Konfigurationswert
Maximale Anzahl gleichzeitiger Listenwertberichte	Die maximale Anzahl von Listenwertberichten pro Planung, die parallel erzeugt werden können. Ein gültiger Wert ist eine Ganzzahl (**1** ist der Standardwert).
Maximale Anzahl Listenwertberichte	Die maximale Anzahl an Listenwertberichten, die unabhängig von der Anzahl der Werte in der Liste erzeugt werden. Ein gültiger Wert ist eine Ganzzahl (**10000** ist der Standardwert).
Max. pro Regel gespeicherte Zeilen (Milliarden)	Die maximale Anzahl der Zeilen, die eine Regel bei einer Abfrage abrufen kann. Ein gültiger Wert ist eine Ganzzahl (**100** ist der Standardwert).
Maximaler Schwellenwert für Festplattenspeicherplatz	Der maximale Schwellenwert für den Speicherplatz (in GB) auf der Festplatte, der für die Ausführung von Berichten, Warnmeldungen und Diagrammen zugewiesen ist. Der erste Wert wird basierend auf dem verfügbaren Systemspeicherplatz konfiguriert.
Minimaler Schwellenwert für Festplattenspeicherplatz	Der minimale Schwellenwert für den Speicherplatz (in Prozent) auf der Festplatte, der für die Ausführung von Berichten, Diagrammen und Warnmeldungen zugewiesen ist. Dieser Wert ist standardmäßig auf 5 festgelegt. **Hinweis:** Hinweis: Wenn der minimale Schwellenwert erreicht ist, wird die Ausführung von Berichten, Diagrammen und Warnmeldungen beendet, selbst wenn der Service ausgeführt wird.
NWDB-Informationsabfragen-Timeout	Der Informationsabfragen-Timeout in Sekunden für NWDB-Server. Ein gültiger Wert ist eine Ganzzahl (**0** ist der Standardwert).
NWDB - max. Aggregationszeilen	Die maximale Anzahl der Zeilen, die zurückgegeben wird, wenn eine Aggregation in der NWDB-Regel verwendet wird. Ein gültiger Wert ist eine Ganzzahl (**1000** ist der Standardwert).

Name	Konfigurationswert
NWDB-Abfrage-Timeout	Das Timeout in Sekunden für den NWDB -Server zur Überschreitung der Regelausführung, wenn die Ergebnisse nicht innerhalb der konfigurierten Zeit verarbeitet werden können. Der Standardwert ist auf 0 eingestellt, was bedeutet, dass es kein Timeout gibt. Ein gültiger Wert ist eine Ganzzahl.
Verarbeiten von Ausgabeaktionen nur für erfolgreiche Berichte	Aktivieren Sie dieses Kontrollkästchen, um nur für Berichte mit ausschließlich erfolgreichen Regelausführungen Ausgabeaktionen zu verarbeiten. Wenn Sie die Auswahl dieses Kontrollkästchen wieder aufheben, werden Ausgabeaktionen für teilweise abgeschlossene, abgeschlossene und fehlgeschlagene Berichte ausgelöst. **Hinweis:** Dies kann auf alle Ausgabeaktionen mit Ausnahme der dynamischen Listenausgabeaktionen angewendet werden.
Warnmeldungsverlauf aufbewahren - Anzahl Tage	Die maximale Anzahl an Tagen, wie lange ein Warnmeldungsverlauf und -status aufbewahrt werden. Ein gültiger Wert ist eine Ganzzahl (**100** ist der Standardwert).
Diagrammverlauf aufbewahren - Anzahl Tage	Die maximale Anzahl der Tage, wie lange ein Diagrammverlauf und -status aufbewahrt wird. Ein gültiger Wert ist eine Ganzzahl (**30** ist der Standardwert).
Berichtsverlauf aufbewahren - Anzahl Tage	Die maximale Anzahl der Tage, wie lange das System einen Berichtsverlauf sowie -status aufbewahrt. Ein gültiger Wert ist eine Ganzzahl (**100** ist der Standardwert).
Anzahl der Planungsthreadpools	Die Anzahl der Threadpools, die geplanten Aufgaben (zum Beispiel Löschen des Verlaufs) in der Reporting Engine zugewiesen wurden. Ein gültiger Wert ist eine Ganzzahl (**5** ist der Standardwert).

Protokollierungskonfiguration

Mit den Parametern des Bereichs „Protokollierungskonfiguration“ der Reporting Engine wird die Protokollierungskonfiguration für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, sind Standardwerte wirksam. RSA hat die Standardwerte so ausgelegt, dass sie die meisten Umgebungen unterstützen, und empfiehlt, diese Werte nicht zu bearbeiten, da dies negative Auswirkungen auf die Performance der Reporting Engine haben kann.

In der folgenden Abbildung sind die Felder dargestellt, die im Bereich „Protokollierungskonfiguration“ konfiguriert werden können.



In der folgenden Tabelle sind die Funktionen des Bereichs „Protokollierungskonfiguration“ beschrieben.

Name	Konfigurationswert
Protokollebene	Protokollebene, die den Informationsumfang, der in den Protokolldateien enthalten ist, festlegt. Die möglichen Werte sind: • `ERROR` • `WARN` • `INFO (Standard)` • `DEBUG` • `ALL`
Maximale Anzahl an Backup-Dateien	Die maximale Anzahl an Backup-Protokolldatein, die das System aufbewahren kann. Ein gültiger Wert ist eine Ganzzahl (**9** ist der Standardwert).
Max. Protokollgröße	Die maximale Größe (in Bytes) der primären Protokolldatei. Ein gültiger Wert ist eine Ganzzahl (**4194304** ist der Standardwert).

Weitere Informationen zur Reporting Engine-Protokollierung finden Sie unter Zugriff auf die Protokolldateien der Reporting Engine.

Warehouse Analytics – Ausgabekonfiguration

Hinweis: Warehouse Analytics wird in Netwitness Suite Version 11.0 nicht unterstützt.

Anhand des Bereichs „Warehouse Analytics – Ausgabekonfiguration“ kann die Ausgabekonfiguration für Warehouse Analytics auf dieser Reporting Engine angegeben werden.

In der folgenden Abbildung sind die Felder gezeigt, die im Bereich „Warehouse Analytics – Ausgabekonfiguration“ konfiguriert werden können:

Stellen Sie nach einem Upgrade sicher, dass Sie die zentralisierten **Mongo-Datenbankdetails** aktualisieren, damit Sie Warehouse Analytics verwenden können.

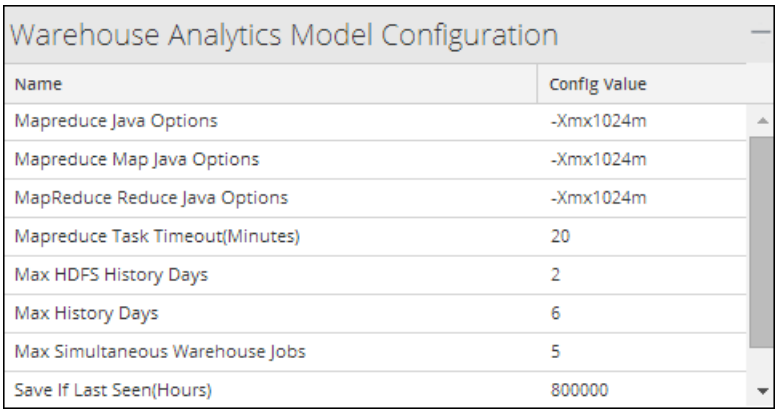
In der folgenden Tabelle sind die Funktionen des Bereichs „Warehouse Analytics – Ausgabekonfiguration“ beschrieben:

Name	Konfigurationswert
Name	**Konfigurationswert**
Benutzername	Benutzername für den Warehouse Analytics-Benutzer
Port	Der von Warehouse Analytics verwendete Port der Mongo-Datenbank
Host	Der von Warehouse Analytics verwendete Host der Mongo-Datenbank
Passwort	Passwort für den Warehouse Analytics Benutzer

Warehouse Analytics – Modellkonfiguration

Im Bereich „Warehouse Analytics – Modellkonfiguration“ kann die Warehouse Analytics-Modellkonfiguration in dieser Reporting Engine angegeben werden.

Die folgende Abbildung zeigt die Felder, die im Bereich Warehouse Analytics – Modellkonfiguration konfiguriert werden können.



In der folgenden Tabelle sind die Funktionen des Bereichs Warehouse Analytics – Modellkonfiguration beschrieben:

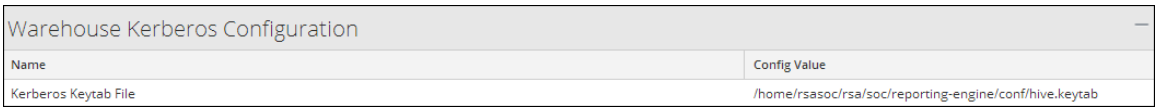
Name	Konfigurationswert
MapReduce Java-Optionen	JVM-Parameter für den Hadoop-Mapreduce-TaskTracker eines untergeordneten JVM Der Wert ist standardmäßig auf **-Xmx1024m** gesetzt.
MapReduce Map Java-Optionen	Parameter, der die JVM-Parameter für Zuordnungsjobs innerhalb des Hadoop-Clusters kontrolliert. Standardmäßig lautet der Wert **-Xmx1024m**.
MapReduce Reduce Java-Optionen	Parameter, der die JVM-Parameter für Reduzierungsjobs innerhalb des Hadoop-Clusters kontrolliert. Standardmäßig lautet der Wert **-Xmx1024m**.
Timeout der Mapreduce-Aufgabe (Minuten)	Anzahl der Minuten, innerhalb derer eine Aufgabe abgeschlossen sein muss, damit ein MapReduce-Framework diese nicht mit „reagiert nicht“ oder „im Leerlauf“ kennzeichnet. Ein gültiger Wert ist eine Ganzzahl (**20** ist der Standardwert).
Max. HDFS-Verlaufstage	Die maximale Anzahl der Tage, die temporäre Dateien sowie Ausgabedateien eines Jobs in HDFS erhalten bleiben. Ein gültiger Wert ist eine Ganzzahl (**2** ist der Standardwert).

Name	Konfigurationswert
Max. Verlaufstage	Die maximale Anzahl der Tage, die die Jobausgabe in der Mongo-Datenbank erhalten bleiben soll. Ein gültiger Wert ist eine Ganzzahl (**6** ist der Standardwert).
Max. gleichzeitige Warehouse-Jobs	Parameter, der die maximale Anzahl gleichzeitiger Jobs kontrolliert, die durch das Warehouse Analytics-Framework ausgeführt werden. Ein gültiger Wert ist eine Ganzzahl (**1** ist der Standardwert).
Speichern, wenn zuletzt gesehen (Stunden)	Parameter zum Speichern der Schlüssel aus der Jobausgabe, wenn sie in den letzten „n“ Stunden nicht gesehen wurden. Ein gültiger Wert ist eine Ganzzahl (**800000**ist der Standardwert).
Schwellenwertbewertung	Parameter zum Speichern der Schlüssel aus der Jobausgabe auf Watchlisten zur Verwendung durch ESA, wenn die Wertung höher als „n“ ist. Ein gültiger Wert ist eine Ganzzahl (**55** ist der Standardwert).

Warehouse-Kerberos-Konfiguration

Im Bereich „Warehouse-Kerberos-Konfiguration“ kann die Kerberos-Keytab-Datei in dieser Reporting Engine angegeben werden.

In der folgenden Abbildung sind die Felder gezeigt, die im Bereich „Warehouse-Kerberos-Konfiguration“ konfiguriert werden können.



In der folgenden Tabelle sind die Funktionen des Bereichs „Kerberos-Konfiguration“ beschrieben.

Name	Konfigurationswert
Kerberos-Keytab-Datei	Speicherort der Kerberos-Keytab-Datei. Beispiel: `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/hive.keytab`.

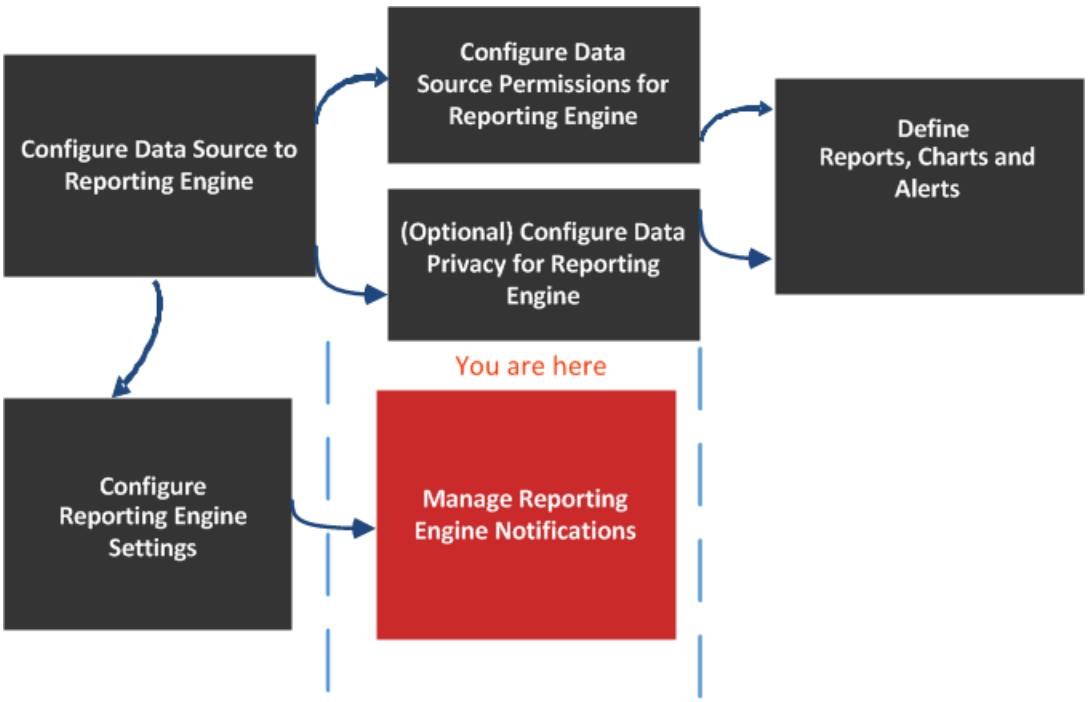
Die Standarddatei für die Kerberos-Konfiguration befindet sich unter `/etc/kbr5.conf` in der Reporting Engine. Sie können die Konfigurationsdatei ändern und Details für Kerberos-Bereiche und andere zu Kerberos gehörige Parameter angeben.

Der Hostname (oder vollständig qualifizierte Domainname) und die IP-Adressen der Horton Works-Nodes und des Warehouse Connector wurden dem DNS-Server hinzugefügt. Wenn kein DNS-Server konfiguriert ist, fügen Sie den Hostnamen (oder den vollständig qualifizierten Domainnamen) sowie die IP-Adressen der Horton Works-Nodes und des Warehouse Connector in die Datei `/etc/hosts` auf dem Host ein, auf dem der Warehouse Connector-Service installiert ist.

Registerkarte „Quellen“

In diesem Thema werden die Servicekonfigurationsparameter vorgestellt, die auf der Registerkarte „Quellen“ der Ansicht „Services“ > Konfiguration“ für die Reporting Engine verfügbar sind. Die Registerkarte „Quellen“ für den Reporting Engine-Service in der Ansicht „Service-Konfiguration“ steuert die mit einer Reporting Engine verbundenen Datenquellen. Die Registerkarte „Quellen“ besteht aus einem einzelnen Bereich mit einer Symbolleiste und einem Raster, in dem die mit der Reporting Engine verbundenen Datenquellen aufgeführt sind.

Workflow



Rolle	Ich möchte...	Siehe
Administrator	Konfigurieren der Datenquelle für Reporting Engine	Konfigurieren der Datenquellen
Administrator	Datenquellenberechtigungen für die Reporting Engine konfigurieren	Konfigurieren von Datenquellenberechtigungen

Rolle	Ich möchte...	Siehe
Administrator	Konfigurieren des Datenschutzes für Reporting Engine	Konfigurieren des Datenschutzes für die Reporting Engine
Administrator	Definieren von Berichten, Diagrammen und Warnmeldungen	Definieren von Berichten, Diagrammen und Warnmeldungen
Administrator	Konfigurieren der Reporting-Engine-Einstellungen	Konfigurieren der Reporting Engine-Einstellungen
Administrator	Einen neuen oder verfügbaren Service hinzufügen, löschen oder bearbeiten*	Konfigurieren der Datenquellen
Administrator	Einstellen einer Datenquelle als Standard*	Konfigurieren der Datenquellen
Administrator	Konfigurieren von Datenquellenberechtigungen*	Konfigurieren von Datenquellenberechtigungen

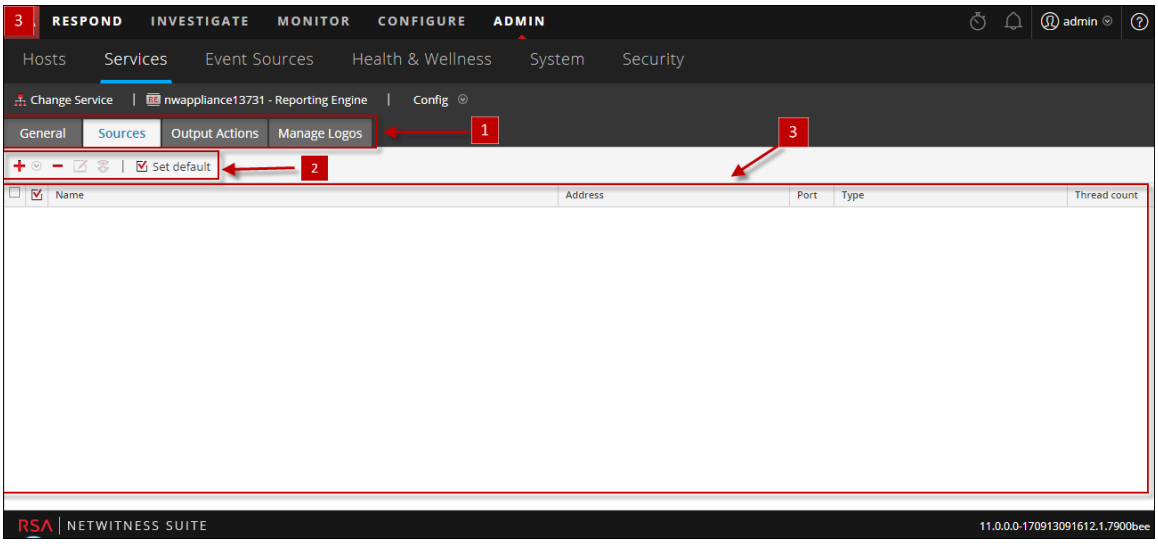
*Sie können diese Aufgaben hier durchführen.

Verwandte Themen

- Funktionsweise der Reporting Engine

Überblick

Hier ist Beispiel der Registerkarte „Quellen“, in der die verfügbaren Services angezeigt werden.



1 Zeigt alle verfügbaren konfigurierbaren Registerkarten an.

2 Zeigt die verfügbaren Konfigurationsparameter für den ausgewählten Service.

3 Zeigt die Feldparameter für den ausgewählten Service.

Die für die Reporting Engine verfügbaren Datenquellen, für die Sie Berichte, Diagramme und Warnmeldungen definieren, sind:

- **NWDB-Datenquellen**: Die NWDB-Datenquellen (NetWitness Database) sind Decoder, Log Decoder, Broker, Concentrators, Archiver und Collection.

  Hinweis: Wenn zur Beschränkung des Zugriffs auf sensible Daten auf einer Datenquelle ein Datenschutzplan implementiert wurde, müssen Sie in der Reporting Engine verschiedene Servicekonten für Benutzer mit den nötigen Berechtigungen und Benutzer ohne die nötigen Berechtigungen konfigurieren. Zum Konfigurieren verschiedener Servicekonten zu Datenschutzzwecken können Sie mehr als eine NWDB-Datenquelle hinzufügen. Dieses Verfahren ist verfügbar unter Konfigurieren der Reporting Engine-Einstellungen.

- **Warehouse-Datenquellen**: Die Warehouse-Datenquellen sind Horton Works und MapR.

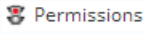
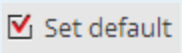
- **Respond-Datenquellen:** Respond wird zum Erzeugen von Berichten für Warnmeldungen und Incidents verwendet. Die Respond-Datenquellen sind Reporting Engine, ESA, Malware, Endpoint und Web Threat Detection. Respond wird zur Speicherung der Warnmeldungen und Incidents-Berichte verwendet.

Wenn Sie eine Quelle als Standarddatenquelle festlegen, nutzt NetWitness Suite diese Quelle beim Erstellen von Berichten und Warnmeldungen. Sie können die Standarddatenquelle jedoch mit einer der anderen auf dieser Registerkarte aufgeführten Quellen überschreiben.

Hinweis: Sie können die Zugriffssteuerung für NWDB- und Warehouse-Datenquellen managen. Weitere Informationen finden Sie unter Konfigurieren der Reporting Engine-Einstellungen.

Funktionen

Sie können auf der Registerkarte Quellen auch die folgenden Aktionen durchführen:

Symbol	Aktionen
	Fügt neue Services als Datenquellen für Reporting Engine hinzu. Bestehende Services (Archiver, Workbench, Collection) als Datenquellen für die Reporting Engine hinzufügen.
	Entfernt Datenquellen aus einer Reporting Engine.
	Diese Option konfiguriert die Datenquellenberechtigungen. Dies ist nur für NWDB- und Warehouse-Datenquellen aktiviert. Weitere Informationen erhalten Sie unter Konfigurieren von Datenquellenberechtigungen.
	Legt die Standarddatenquellen für eine Reporting Engine fest. Dies ist die Quelle, die im Feld **Datenquelle** der folgenden Ansichten standardmäßig von NetWitness Suite festgelegt wird: • Ansicht „Regeldefinition“ • Ansicht zum Erstellen oder Ändern von Warnmeldungen

Die NetWitness Suite Datenquellen sind wie folgt unter den unterschiedlichen Kategorien aufgeführt:

- Kategorie NWDB-Datenquellen zeigt die NetWitness-Datenquellen an.
- Kategorie Warehouse-Datenquellen zeigt die Warehouse-Datenquellen an.

Spalte	Beschreibung
	Durch Aktivieren des Kontrollkästchens wird die Datenquelle ausgewählt. Nach der Auswahl können Sie die Quelle mithilfe der Symbolleiste entfernen oder als Standard festlegen.
Name	Zeigt den Namen der Datenquelle an.
Adresse	Zeigt die IP-Adresse der Datenquelle an.
Port	Zeigt den Port der Datenquelle an.
Typ	Zeigt den Servicetyp der Datenquelle an.
Anzahl Threads	Zeigt die Größe des Threadpools zur Ausführung von Regeln für die Datenquelle an.

Registerkarte „Ausgabeaktionen“

Sie können Ausgabeaktionen für eine Reporting Engine konfigurieren, um das Format zu bestimmen, in dem Ihnen die Daten entsprechend Ihren Anforderungen angezeigt werden sollen. Die Servicekonfigurationsparameter sind auf der Registerkarte „Ausgabeaktionen“ der Ansicht „Services > Konfiguration“ verfügbar. Ausgabeaktionen werden für die Ausführung eines Berichts oder einer Warnmeldung konfiguriert. Diese Registerkarte enthält folgende Bereiche:

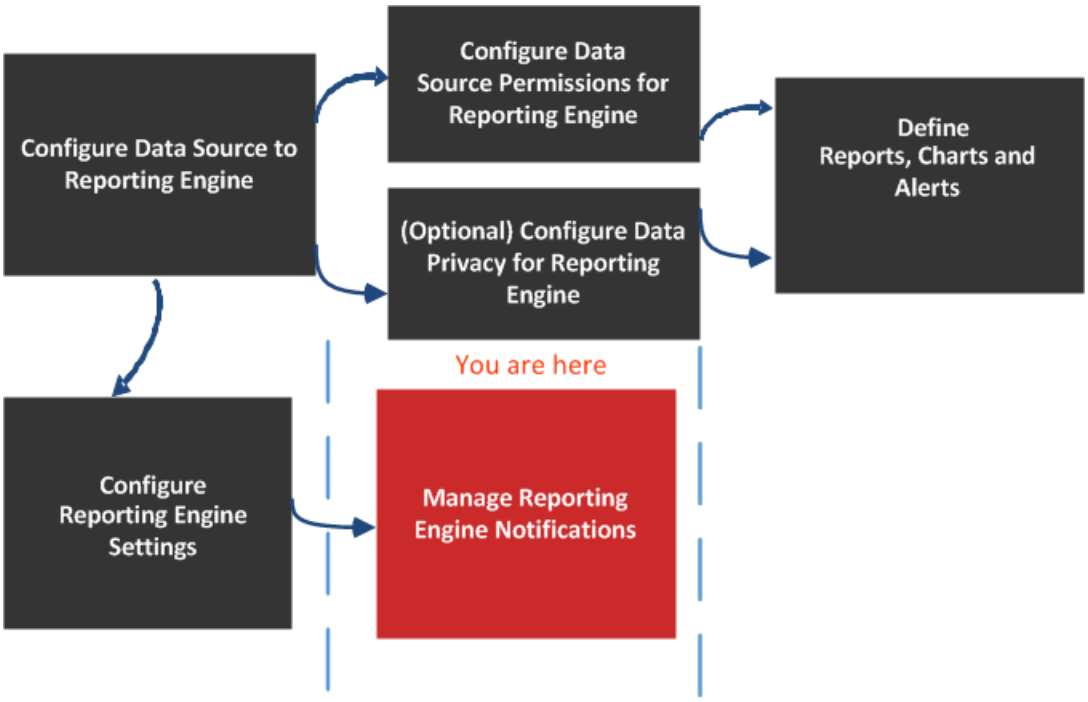
- NetWitness Suite-Konfiguration
- Simple Mail Transfer Protocol (SMTP)
- SNMP (Simple Network Management Protocol)
- Syslog
- Simple File Transfer Protocol (SFTP)
- Uniform Resource Locator (URL)
- Netzwerkfreigabe

Die Ausgabeaktion Syslog wird z. B. für Reporting Engine-Warnmeldungen verwendet, während die Ausgabeaktionen SFTP, URL und Netzwerkfreigabe für Reporting Engine-Berichte verwendet werden.

Sie können die erforderliche Berechtigung für den Zugriff auf diese Ansicht im Bereich „Services managen“ konfigurieren.

Sie müssen sich vergewissern, dass die Reporting Engine betriebsbereit ist und die Datenquelle, aus der Sie einen Bericht erzeugen möchten, in der NetWitness Suite konfiguriert ist.

Workflow



Was möchten Sie tun?

Rolle	Ich möchte...	Siehe
Administrator	Datenquelle für Reporting Engine konfigurieren	Konfigurieren der Datenquellen
Administrator	Datenquellenberechtigungen für die Reporting Engine konfigurieren	Konfigurieren von Datenquellenberechtigungen
Administrator	Datenschutz für die Reporting Engine konfigurieren	Konfigurieren des Datenschutzes für die Reporting Engine
Administrator	Berichte, Diagramme und Warnmeldungen definieren	Definieren von Berichten, Diagrammen und Warnmeldungen

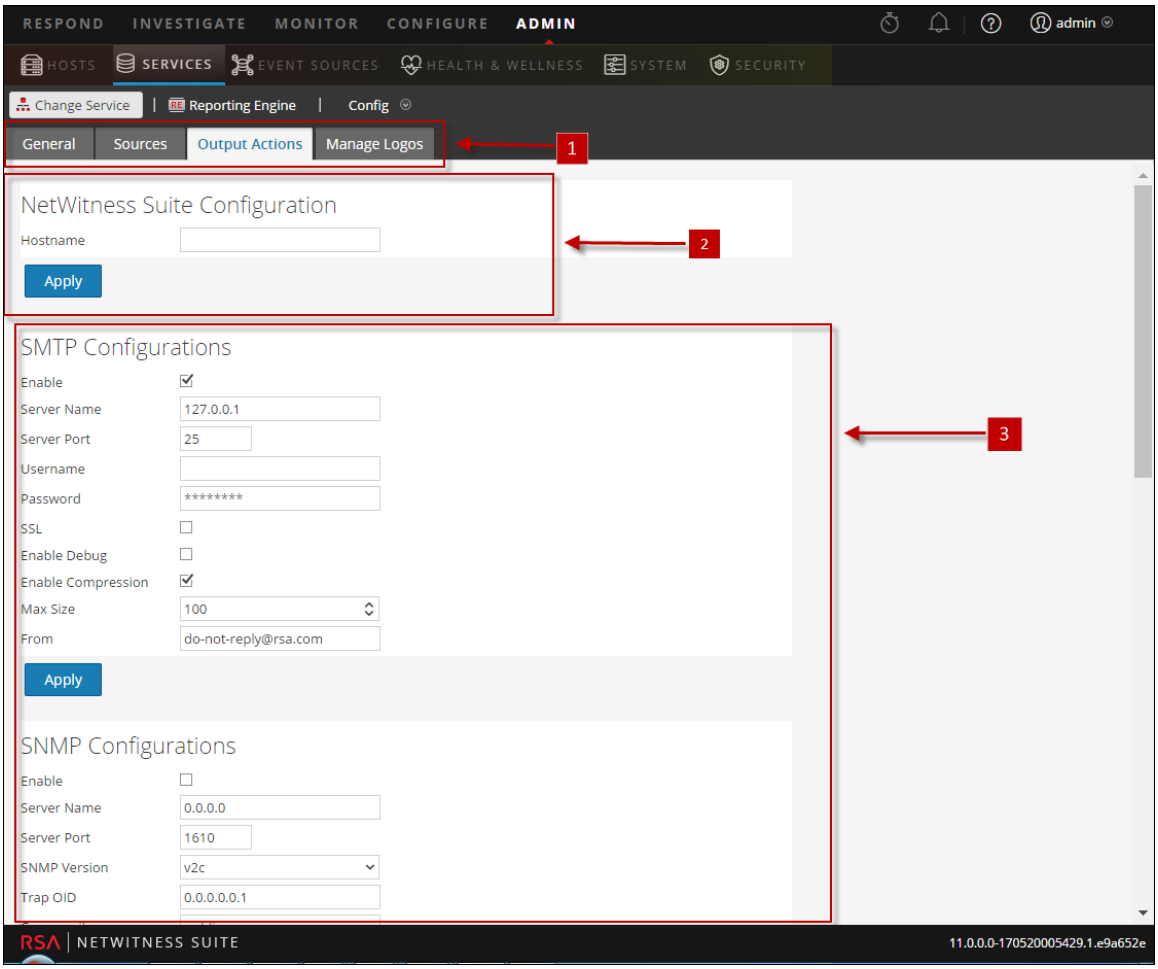
Rolle	Ich möchte...	Siehe
Administrator	Einstellungen der Reporting Engine konfigurieren	Konfigurieren der Reporting Engine-Einstellungen
Administrator	NetWitness Suite-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	SMTP-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	SNMP-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	Syslog-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	SFTP-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	URL-Konfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator	Netzwerkfreigabenkonfiguration konfigurieren*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen

*Sie können diese Aufgaben hier durchführen.

Verwandte Themen

- Funktionsweise der Reporting Engine

Überblick



1	Zeigt alle verfügbaren konfigurierbaren Registerkarten an.
2	Zeigt den Host für die NetWitness Suite-Konfiguration an.
3	Zeigt alle Arten der Ausgabeaktionen an, die konfiguriert werden können.

NetWitness Suite-Konfiguration

In der folgenden Abbildung ist die NetWitness Suite-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.

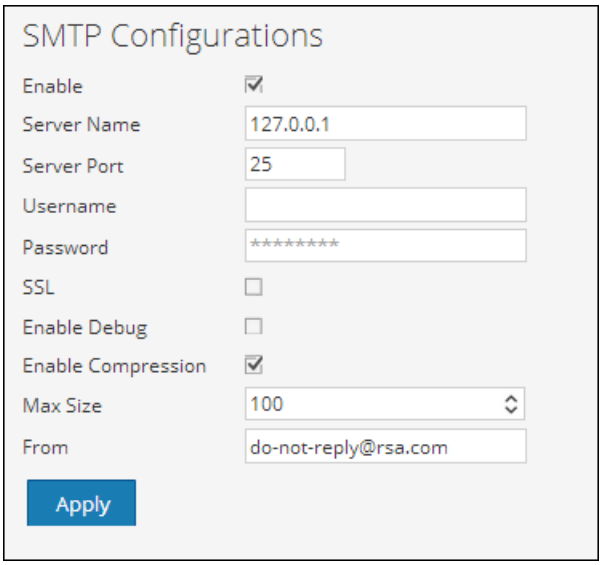
Die folgenden Parameter kennzeichnen den NetWitness Suite-Host, der der Reporting Engine zugeordnet ist.

Name	Konfigurationswert
Hostname	IP-Adresse oder Hostname des NetWitness Suite-Servers. Sie müssen diesen Parameter für alle Bereitstellungsarten angeben, damit Sie sich auf diese Adresse beziehen können, wenn Sie Ermittlungslinks zu NetWitness Suite aus Berichten, Warnmeldungen usw. erstellen. In NetWitness Suite werden mit diesen Parametern folgende Aktionen richtig erzeugt: • Ausgabeaktion SMTP • Ausgabeaktion SNMP • Ausgabeaktion Syslog • Ausgabeaktion SFTP • Ausgabeaktion URL • Ausgabeaktion Netzwerkfreigabe • Hyperlinks für Metawerte in Berichts-PDFs
Anwenden	Aktualisieren Sie die Konfiguration.

SMTP

Nachdem eine Ausführung abgeschlossen ist, wird basierend auf der SMTP-Konfiguration eine E-Mail-Benachrichtigung an den Benutzer gesendet.

In der folgenden Abbildung ist die SMTP-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.



Die folgenden Parameter verwalten die Konfiguration der SMTP-Ausgabeaktion (E-Mail) für einen Reporting Engine-Service. Wenn Sie einen Reporting Engine-Service hinzufügen, gelten die Standardwerte. Sie müssen die **Konfigurationswerte** dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

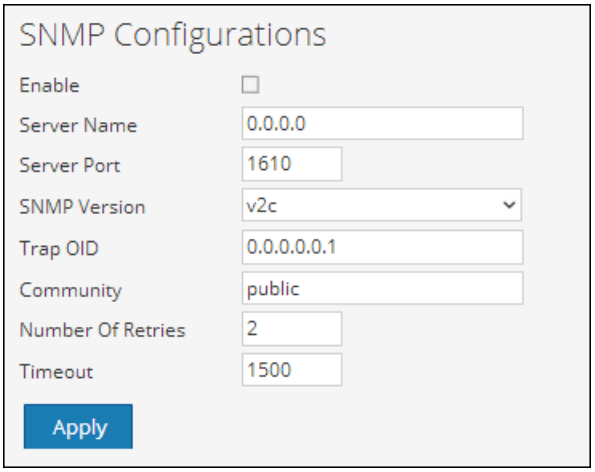
Name	Konfigurationswert
Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um SMTP als Ausgabeaktion für Warnmeldungen und Berichte aus dieser Reporting Engine zu aktivieren. Dieser Wert ist standardmäßig aktiviert.
Servername	Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem der SMTP-Server ausgeführt wird. Der Standardwert ist 0.0.0.0.
Serverport	Geben Sie die Portnummer des SMTP-Servers an. Der Standardwert ist 25.
Benutzername	Geben Sie den Benutzernamen Ihres SMTP-Kontos an. Der Standardwert ist leer. Geben Sie ein Passwort an.
Passwort	Geben Sie das Passwort Ihres SMTP-Kontos an.
SSL	Aktivieren Sie dieses Kontrollkästchen, um Secure Socket Layer (SSL) für die Kommunikation mit dem SMTP-Server zu verwenden. Laut Standardwert wird SSL nicht verwendet.

Name	Konfigurationswert
Debuggen aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Debuggen zu aktivieren. Laut Standardwert ist Debuggen nicht aktiviert.
Komprimierung einschalten	Aktivieren Sie dieses Kontrollkästchen, um Komprimierung einzuschalten. Der Standardwert ist Komprimierung einschalten. Wenn dieser Wert aktiviert ist, haben die Ausgabedateien die Erweiterung `.zip`.
Max. Größe	Legen Sie die maximale Größe für Anhänge fest, die gesendet werden können. Der Standardwert beträgt 100.
Von	Geben Sie die E-Mail-Adresse an, von der Security Analytics alle Nachrichten versenden soll. Der Standardwert beträgt `do-not-reply@rsa.com`.
Anwenden	Aktualisieren Sie die Konfiguration.

SNMP

Nachdem eine Ausführung abgeschlossen ist, wird basierend auf der SNMP-Konfiguration eine Trap-Benachrichtigung an den Benutzer gesendet.

In der folgenden Abbildung ist die SNMP-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.



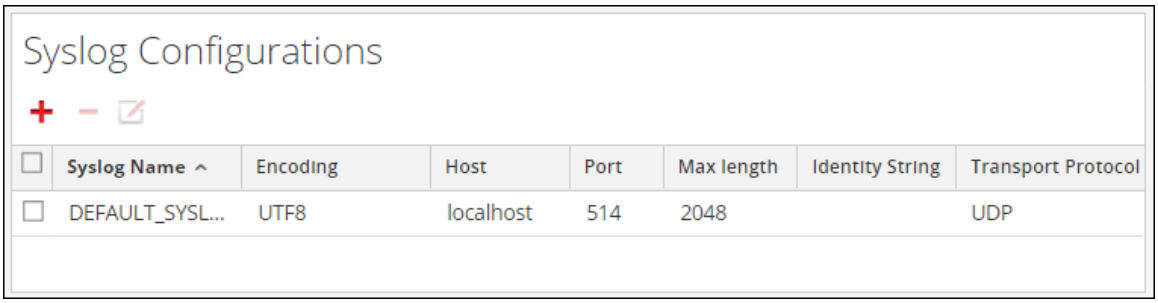
Mit den folgenden Parametern wird die Konfiguration der SNMP-Ausgabeaktion (Nachricht an Services im Netzwerk) für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, sind Standardwerte wirksam. Sie müssen die **Konfigurationswerte** dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

Name	Konfigurationswert
Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Ausgabeaktion „SNMP“ als Ausgabe für Warnmeldungen aus dieser Reporting Engine zu aktivieren. Der Standardwert ist Deaktivieren.
Servername	Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem der SNMP-Server ausgeführt wird. Der Standardwert ist **0.0.0.0**.
Serverport	Geben Sie die Portnummer des Servers an, auf dem der SNMP-Server für Fehler und Ausnahmen empfangsbereit ist. Der Standardwert ist **1610**.
SNMP-Version	Geben Sie die Versionsnummer des SNMP-Protokolls an, mit dem NetWitness Suite SNMP-Traps sendet.
Trap-OID	Geben Sie die Objektidentifikationsnummer an, die den zu sendenden Trap-Typ identifiziert. Der Standardwert ist **0.0.0.0.0.1**.
Community	Geben Sie die SNMP-Gruppe an, zu der NetWitness Suite gehört. Der Standardwert ist **öffentlich**.
Anzahl erneuter Versuche	Geben Sie die maximale Anzahl der Versuche an, die NetWitness Suite unternehmen soll, um eine Warnmeldung über SNMP zu senden. Der Standardwert ist **2**.
Timeout	Geben Sie die Anzahl an Sekunden an, nach deren Ablauf ein Timeout auftritt und NetWitness Suite keine weiteren SNMP-Warnmeldungen mehr sendet. Der Standardwert beträgt **1500**.
Anwenden	Aktualisieren Sie die Konfiguration.

Syslog

Nachdem eine Ausführung abgeschlossen ist, werden basierend auf der Syslog-Konfiguration alle Benachrichtigungen über Syslog-Meldungen an einen bestimmten Host gesendet. Im Bereich „Syslog-Konfiguration“ können mehrere Syslog-Server konfiguriert werden.

In der folgenden Abbildung ist die Syslog-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.



Mit den folgenden Parametern wird die Konfiguration der Syslog-Ausgabeaktion für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, können Sie Werte für diese Ausgabekonfiguration definieren, da keine Standardwerte für diese Konfiguration verfügbar sind. Sie müssen die **Konfigurationswerte** dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

Name	Konfigurationswert
Syslog-Name	Geben Sie den Namen der Syslog-Konfiguration ein. **Hinweis:** Sie können keine Syslog-Konfiguration mit einem Namen erstellen, der bereits in der Liste der Syslog-Konfigurationen in der Reporting Engine vorhanden ist.
Codierung	Geben Sie die Kodierung für die Internationalisierung von Syslog-Meldungen an. Der Standardwert ist **UTF8**.
Servername	Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem der Syslog-Prozess ausgeführt wird. Der Standardwert ist leer.
Serverport	Geben Sie die Portnummer des Servers an, auf dem der Syslog-Server für Fehler und Ausnahmen empfangsbereit ist. Der Standardwert ist **514**.
Max. Länge	Geben Sie die maximale Größe in Byte an, die eine Syslog-Warnmeldung haben kann. Der Standardwert ist **2048**. Wenn der Transporttyp **UDP** ist und die Größe der Syslog-Meldungen mehr als 1024 Byte beträgt, müssen Sie einen Syslog-Server konfigurieren, der Meldungen unterstützt, die größer als 1024 Byte sind.

Name	Konfigurationswert
Identitätszeichenfolge	Geben Sie die Zeichenfolge an, die NetWitness Suite als Präfix in allen Syslog-Warnmeldungen einfügt. Der Standardwert ist leer.
Lokalen Hostnamen hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um den Namen des lokalen Hosts in allen Syslog-Warnmeldungen hinzuzufügen. Der Standardwert ist Lokalen Hostnamen nicht angeben.
Nachricht abschneiden	Aktivieren Sie dieses Kontrollkästchen, um alle Syslog-Warnmeldungen abzuschneiden. Laut Standardwert werden Syslog-Meldungen nicht abgeschnitten.
Identität verwenden	Aktivieren Sie dieses Kontrollkästchen, um das IDENT-Protokoll zu verwenden. Laut Standardwert wird dieses Protokoll nicht verwendet.
Lokalen Zeitstempel hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um den lokalen Zeitstempel in allen Syslog-Warnmeldungen hinzuzufügen. Der Standardwert ist Lokalen Zeitstempel nicht angeben.
Transportprotokoll	Geben Sie den Transporttyp für die Bereitstellung von Syslog-Meldungen an. Es gibt drei Optionen für den Syslog-Transporttyp: UDP, TCP und SECURE_TCP. Der Standardwert ist **UDP**.
Syslog-Nachrichtentrennzeichen	Geben Sie das Trennzeichen für Syslog-Meldungen an. Es gibt drei Trennzeichen: CR, LF und CRLF. Der Standardwert ist **CR**. **Hinweis:** Dieses Feld wird ausgefüllt, wenn Sie TCP oder SECURE_TCP als Transportprotokoll auswählen.
Truststore-Passwort	Geben Sie das Passwort für den Truststore an. **Hinweis:** Dieses Feld wird ausgefüllt, wenn Sie SECURE_TCP als Transportprotokoll auswählen.

Name	Konfigurationswert
Keystore-Passwort	Geben Sie das Passwort für den Keystore an. **Hinweis:** Dieses Feld wird ausgefüllt, wenn Sie SECURE_TCP als Transportprotokoll auswählen.
Anwenden	Speichern Sie die Konfiguration.

SFTP

Nachdem eine Ausführung abgeschlossen ist, können Sie basierend auf der SFTP-Konfiguration Dateien an einen Remotestandort senden oder übertragen.

In der folgenden Abbildung ist die SFTP-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.

Mit den folgenden Parametern wird die Konfiguration der SFTP-Ausgabeaktion (Dateiübertragung an ein lokales Laufwerk) für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, können Sie Werte für diese Ausgabekonfiguration definieren, da keine Standardwerte für diese Konfiguration verfügbar sind. Sie müssen die **Konfigurationswerte** dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

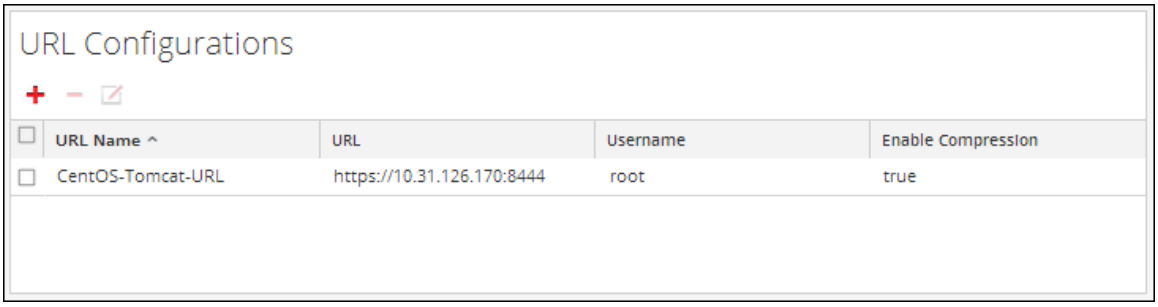
Name	Konfigurationswert
SFTP-Name	Gibt den Namen der SFTP-Konfiguration an. **Hinweis:** Sie können keine SFTP-Konfiguration mit einem Namen erstellen, der bereits in der Liste der Reporting Engine-SFTP-Konfigurationen vorhanden ist.
Host	Die IP-Adresse oder der Hostname des Reporting Engine-Servers, der mit dem Dateitransfer verknüpft ist.

Name	Konfigurationswert
Port	Wenn Sie einen anderen Port als den Standardport verwenden möchten, geben Sie eine Portnummer ein. Der Standardwert ist **22**.
Benutzername	Geben Sie den Benutzernamen für die SFTP-Konfiguration an.
Password	Geben Sie das Passwort für die SFTP-Konfiguration an.
Benutzerdefinierter Ordner	Wählen Sie einen SFTP-Speicherort, zu dem Sie die Datei übertragen möchten. Sie können die vordefinierte Windows- oder Linux-Verzeichnisstruktur im benutzerdefinierten Ordnerpfad verwenden. Beispiel: **/root/Downloaded_Files**. **Hinweis:** Wenn dieses Verzeichnis noch nicht vorhanden ist, erzeugt die RE es im benutzerdefinierten Ordnerpfad und kopiert die Dateien in dieses Verzeichnis.
Komprimierung einschalten	Aktivieren Sie dieses Kontrollkästchen, um die Komprimierung einzuschalten. Standardmäßig ist die Komprimierung aktiviert. Wenn dieser Wert aktiviert ist, haben die Ausgabedateien die Erweiterung „.zip“.

URL

Nachdem eine Ausführung abgeschlossen ist, werden die Ausgabedateien basierend auf der URL-Konfiguration in einer URL veröffentlicht.

In der folgenden Abbildung ist die URL-Konfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.



Mit den folgenden Parametern wird die Konfiguration der URL-Ausgabeaktion (Dateiübertragung an eine URL) für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, können Sie Werte für diese Ausgabekonfiguration definieren, da keine Standardwerte für diese Konfiguration verfügbar sind. Sie müssen die Konfigurationswerte dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

Name	Konfigurationswert
URL-Name	Zeigt den Namen der URL-Konfiguration an. **Hinweis:** Sie können keine URL-Konfiguration mit einem Namen erstellen, der bereits in der Liste der Reporting Engine-URL-Konfigurationen vorhanden ist.
URL	Die URL-Adresse, die mit dem Dateitransfer verknüpft ist
Benutzername	Geben Sie den Benutzernamen für die URL-Konfiguration an.
Password	Geben Sie das Passwort für die URL-Konfiguration an.
Komprimierung einschalten	Aktivieren Sie dieses Kontrollkästchen, um die Komprimierung einzuschalten. Standardmäßig ist die Komprimierung aktiviert. Wenn dieser Wert aktiviert ist, haben die Ausgabedateien die Erweiterung „.zip“.

Wenn die URL konfiguriert ist, werden die Dateien in das Verzeichnis „URL_OUTPUT_ACTION“ kopiert und folgende Parameter werden gemeinsam mit der komprimierten Datei an den Server gesendet.

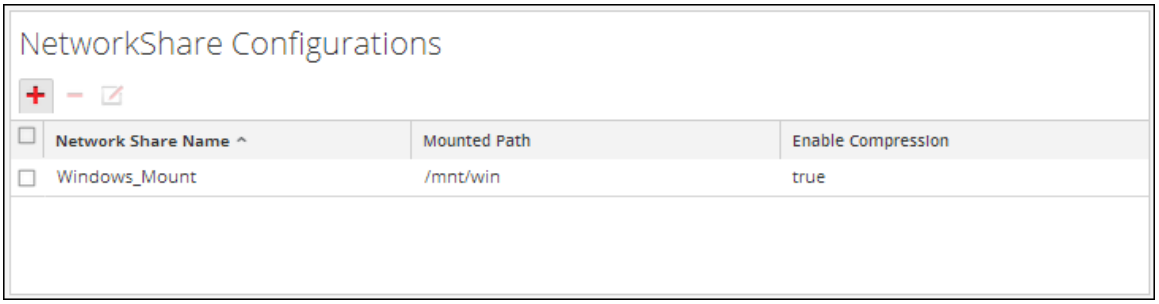
Name	Konfigurationswert
filename	Der Name der Datei.
Dateigröße	Die Dateigröße in Byte.
filetype	Der Dateityp der Datei.
Dateiprüfsumme	Die von einer Datei berechnete Zahl, mit der bestätigt wird, dass die erwartete Datei heruntergeladen und ordnungsgemäß gespeichert wurde.
Hashing-Algorithmus	Der Hashing-Algorithmus, mit dem die Prüfsumme der Datei berechnet wurde.

Name	Konfigurationswert
Berichtname	Der Name des heruntergeladenen Berichts.
Ausführungs-ID	Die Ausführungs-ID der Berichtsausführung.
Startzeit der Berichtausführung	Die Startzeit der Ausführung des Berichts.
status	Der Berichterstellungsstatus.
Statusbeschreibung	Die Statusbeschreibung.

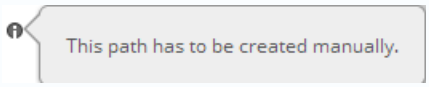
Netzwerkfreigabe

Nachdem eine Ausführung abgeschlossen ist, können Sie die Ausgabedateien basierend auf der Netzwerkfreigabenkonfiguration an einen gemounteten Pfad oder einen gemeinsamen Standort übertragen.

In der folgenden Abbildung ist die Netzwerkfreigabenkonfiguration auf der Registerkarte „Ausgabeaktionen“ dargestellt.



Mit den folgenden Parametern wird die Konfiguration der Netzwerkfreigabe-Ausgabeaktion (Dateiübertragung an einen gemeinsamen Standort im Netzwerk) für einen Reporting Engine-Service verwaltet. Wenn Sie einen Reporting Engine-Service hinzufügen, können Sie Werte für diese Ausgabekonfiguration definieren, da keine Standardwerte für diese Konfiguration verfügbar sind. Sie müssen die **Konfigurationswerte** dieser Parameter entsprechend den Anforderungen Ihres Unternehmens ändern.

Name	Konfigurationswert
Netzwerkfreigabename	Der Name des Netzwerk-Share. **Hinweis:** Sie können keine Netzwerkfreigabe-Konfiguration mit einem Namen erstellen, der bereits in der Liste der Netzwerkfreigabe-Konfigurationen in der Reporting Engine vorhanden ist.
Gemounteter Pfad	Der Pfad (der Standort), der der Dateiübertragung zugeordnet ist. Sie können die vordefinierte Linux-Verzeichnisstruktur als gemounteten Pfad verwenden. Beispiel: **/mnt/win**. **Hinweis:** Der Benutzer „rsasoc“ muss Lese- und Schreibzugriff auf den angegebenen gemounteten Pfad für die Netzwerkfreigabe haben.
	Klicken Sie hier, um anzuzeigen, wie der gemountete Pfad erstellt wird. In diesem Popup-Menü wird angezeigt, dass Sie den gemounteten Pfad manuell erstellen müssen.
Komprimierung einschalten	Aktivieren Sie dieses Kontrollkästchen, um die Komprimierung einzuschalten. Standardmäßig ist die Komprimierung aktiviert. Wenn dieser Wert aktiviert ist, haben die Ausgabedateien die Erweiterung „.zip“.

In der folgenden Tabelle werden die allgemeinen Vorgänge, die Sie in den Abschnitten „Syslog“, „SFTP“, „URL“ und „Netzwerkfreigabe“ durchführen können.

Vorgang	Beschreibung
	Erstellen Sie eine Syslog-, SFTP-, URL- und Netzwerkfreigabenkonfiguration.
	Löschen Sie eine Syslog-, SFTP-, URL- und Netzwerkfreigabenkonfiguration.
	Bearbeiten Sie eine Syslog-, SFTP-, URL- und Netzwerkfreigabenkonfiguration.

Registerkarte „Logos verwalten“

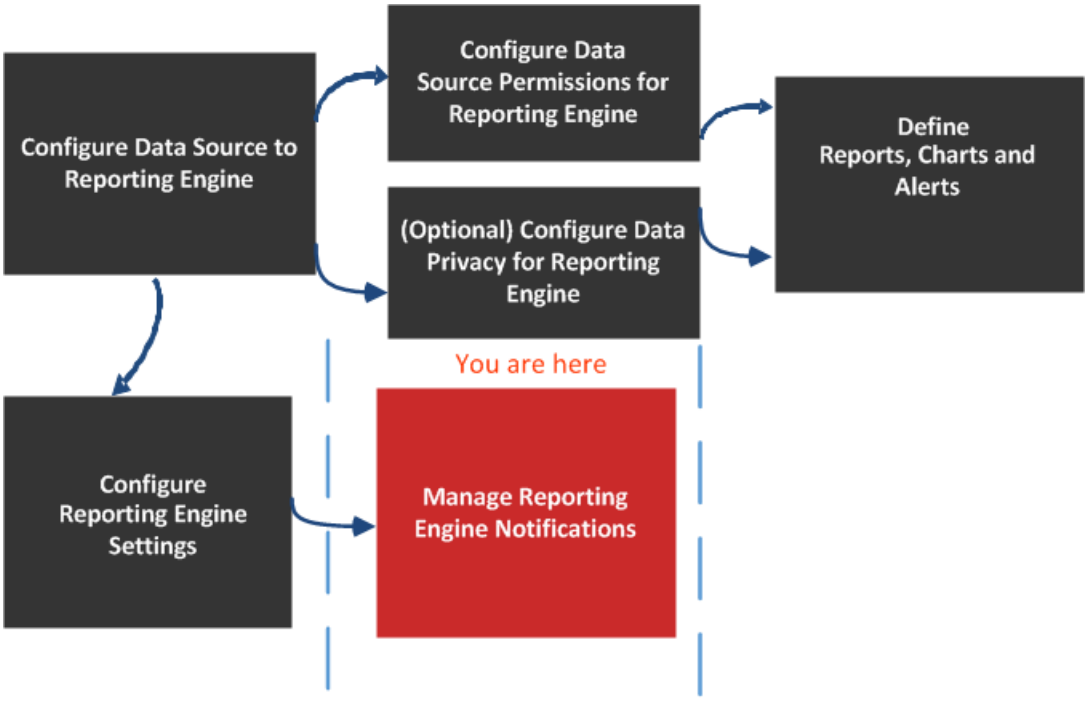
Die Option „Logos verwalten“ in der Ansicht **Services-Konfiguration** > Registerkarte **Logos verwalten** hilft Ihnen beim Managen der Logos zur Reporting Engine. Die Registerkarte „Logos verwalten“ besteht aus einem einzigen Bereich mit einer Symbolleiste und einem Raster, in dem die Logos aufgelistet sind.

Sie können die Logos hochladen, die Sie im Bericht verwenden möchten. Nachdem Sie das Logo hochgeladen haben, können Sie ein beliebiges Logo als Standardlogo festlegen, das automatisch in allen geplanten Berichten verwendet wird. Beim Planen eines Berichts können Sie das Standardlogo durch ein anderes Logo auf dieser Registerkarte überschreiben. Weitere Informationen finden Sie unter „Dialogfeld Logo auswählen“ im *Reporting-Benutzerhandbuch*.

Folgende Bildformate werden unterstützt:

- .jpg
- .png
- .gif

Workflow



Was möchten Sie tun?

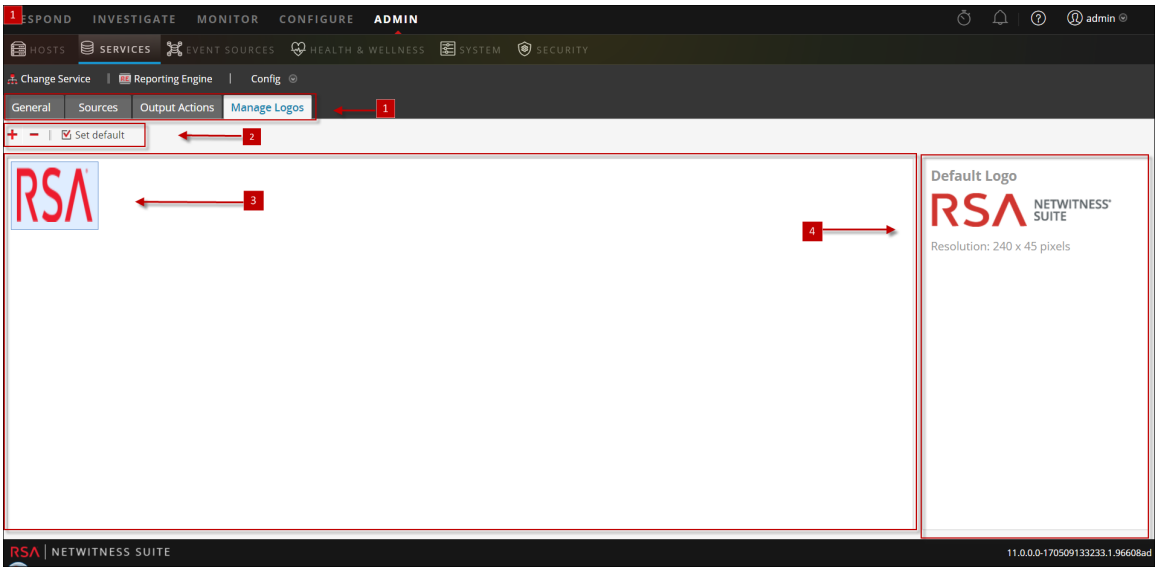
Rolle	Ich möchte...	Siehe
Administrator	Konfigurieren der Datenquelle für Reporting Engine	Konfigurieren der Datenquellen
Administrator	Datenquellenberechtigungen für die Reporting Engine konfigurieren	Konfigurieren von Datenquellenberechtigungen
Administrator	Konfigurieren des Datenschutzes für Reporting Engine	Konfigurieren des Datenschutzes für die Reporting Engine
Administrator	Definieren von Berichten, Diagrammen und Warnmeldungen	Definieren von Berichten, Diagrammen und Warnmeldungen
Administrator	Konfigurieren der Reporting-Engine-Einstellungen	Konfigurieren der Reporting Engine-Einstellungen
Administrator/SOC-Manager	Hinzufügen oder Löschen von Logos*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Anzeigen der Liste der Logos*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen
Administrator/SOC-Manager	Ein Logo als Standard festlegen*	Konfigurieren der allgemeinen Reporting Engine-Einstellungen

*Sie können diese Aufgaben hier durchführen.

Verwandte Themen

- Funktionsweise der Reporting Engine

Überblick



Hinweis: Das hochzuladende Logo darf 500 KB nicht überschreiten. Die erforderliche Berechtigung für den Zugriff auf diese Ansicht ist Services managen.

1	Zeigt alle verfügbaren konfigurierbaren Registerkarten an.
2	Zeigt Aktionen zum Bearbeiten an.
3	Zeigt die Logos, die verwendet wurden
4	Zeigt das verwendete Standardlogo.

Auf der Registerkarte Logos verwalten können Sie die folgenden Aktionen ausführen.

Symbol	Aktionen
	Fügen Sie neue Logos aus dem lokalen Verzeichnis des Systems zur Reporting Engine hinzu. **Hinweis:** Das Logo darf nicht größer als 500 KB sein. Die gewählten Logos müssen einen der folgenden Dateitypen haben: * .jpg * .gif * .png
	Entfernt Logos aus der Reporting Engine. **Hinweis:** Mit (Strg+Klicken) können Sie mehrere Logos zum Löschen auswählen.
	Legt das Standardlogo für eine Reporting Engine fest. Dieses Logo wird von NetWitness Suite standardmäßig im Bereich **Logo** der Ansicht „Einen Bericht planen“ verwendet. **Hinweis:** Wenn kein Standardlogo ausgewählt ist, wird das RSA-Logo angezeigt.