RSA NETWITNESS® SUITE

Upgradehandbuch für physische Hosts

für Version 10.6.5.x auf 11.1

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

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

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

Juli 2018

Inhalt

Einführung

Die Anweisungen in diesem Handbuch gelten nur für das Upgrade von physischen Hosts auf RSA NetWitness® Suite

11.1. Anweisungen zum Durchführen eines Upgrades Ihrer virtuellen Hosts auf 11.1 finden Sie unter *RSA NetWitness® Suite 10.6.5 auf 11.1 Upgradehandbuch für virtuelle Hosts*.

NetWitness Suite 11.1 ist eine Hauptversion, die alle Produkte von NetWitness Suite betrifft. Die Komponenten der Suite sind NetWitness-Server (Admin-Server, Konfigurationsserver, Integration-Server, Investigate-Server, Orchestrierungsserver, Respond-Server und Security-Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA Primary, ESA Secondary, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector und Workbench.

Machen Sie sich anhand des *Leitfaden für die ersten Schritte mit RSA NetWitness Suite* mit den wichtigsten Änderungen der 11.x-Benutzeroberfläche vertraut. Machen Sie sich anhand des *RSA NetWitness Suite-Bereitstellungshandbuch* mit den wichtigsten Plattformänderungen von 11.x vertraut.

Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Hinweis: Die Reporting Engine ist auf dem NW-Serverhost installiert, Workbench auf dem Archiver-Host installiert, Warehouse Connector kann auf dem Decoder-Host oder dem Log Decoder-Host installiert werden.

Upgrade von CentOS6 auf CentOS7

NetWitness Suite 11.1 ist eine Hauptversion, bei der ein Upgrade auf eine neuere Version des Betriebssystems (CentOS6 auf CentOS7) durchgeführt wird. Die Plattformumgebung der Version 11.1 wurde außerdem erheblich verbessert, um den derzeitigen und künftigen physischen und virtuellen Bereitstellungsarten gerecht zu werden. Diese Änderungen erfordern ein Upgrade auf die neue Umgebung sowie ein Upgrade der Funktionen.

Upgrade-Pfad für RSA NetWitness® Suite 11.1

Der früheste unterstützte Upgradepfad für RSA NetWitness® Suite 11.1 ist Security Analytics 10.6.5.x. Wenn NetWitness Suite in einer Version vor 10.6.5.x ausgeführt wird, müssen Sie zunächst eine Aktualisierung auf Version 10.6.5.x durchführen, bevor Sie ein Upgrade auf Version 11.1 durchführen können. Siehe *RSA Security Analytics 10.6.5 – Aktualisierungsanweisungen* in RSA Link (https://community.rsa.com/docs/DOC-85119).

Unterstützte Host-Upgradepfade

Sie müssen einen Host auf denselben Hosttyp aktualisieren:

- Eine physische RSA-Appliance auf eine physische RSA-Appliance derselben Serie (d. h. Serie 4 auf Serie 4, Serie 5 auf Serie 5 usw.).
  RSA bietet in 11.1 keine Unterstützung für physische Hosts von Drittanbietern.
- Virtuell lokal auf virtuell lokal

Achtung: Das 11.1-Upgrade bietet keine Unterstützung für gemischte Plattformupgrades (z. B. wird physisch zu virtuell nicht unterstützt).

In 11.1 nicht unterstützte Hardware, Bereitstellungen, Services und Funktionen

RSA unterstützt für die folgende Hardware bzw. die folgenden Bereitstellungen, Services und Funktionen kein Upgrade auf 11.1.

- RSA All-in-One (AIO) Appliance
- Mehrere NetWitness-Server-Bereitstellungen
- IPDB-Service
- Malware Analysis-Service, der sich ebenfalls auf dem SA-Server befindet (Upgrade von Malware Analysis Enterprise wird in 11.1 unterstützt.)
- Eigenständiger Warehouse Connector-Service (Upgrade eines ebenfalls vorhandenen Warehouse Connector wird in 11.1 unterstützt.)
- Benutzerdefinierte Policy hinsichtlich Integrität und Zustand in 10.6.x für Context-Hub-Service
  Nach einem Upgrade auf NetWitness 11.1 ist Ihre benutzerdefinierte Policy nicht mehr

vorhanden. Stattdessen ist die sofort verwendbare Context Hub Server Monitoring Policy auf der Benutzeroberfläche vorhanden, die speziell für Version 11.1 gilt.

- Durch DISA-STIG (Defense Information Strategic Agency-Security Technical Information Guide) gesicherte Bereitstellungen
- Warehouse Analytics (Data Science)

Zu berücksichtigende Aspekte beim Upgrade von Event Stream Analysis (ESA)

In RSA NetWitness® Suite 11.1 hat RSA die Art und Weise geändert, wie ESA-Korrelationsregeln die vom System generierten Warnmeldungen speichern und übertragen. In 11.1 sendet ESA alle Warnmeldungen an ein zentrales Warnmeldungssystem. Der lokale Mongo-Speicher in ESA 10.6.5.x wurde entfernt.

Achtung: Wenn Sie in 10.6.5.x kein Incident-Management verwenden, überlegen Sie sehr gut, ob Sie auf Version 11.1 aktualisieren oder nicht.

Die folgenden Richtlinien sollten Sie Ihnen dabei helfen, herauszufinden, ob Sie Ihre ESA-Hosts auf 11.1 aktualisieren sollten.

Wenn Sie in Ihrer 10.6.5.x-Bereitstellung ...

- über einen ESA-Host mit oder ohne konfiguriertem Incident-Management verfügen, führen Sie ein Upgrade auf 11.1 durch.
- mehrere ESA-Hosts für die Verwendung von Incident-Management konfiguriert haben, aggregiert das System Warnmeldungen weiterhin zentral. Wenn das System korrekt dimensioniert ist und in 10.6.5.x wie erwartet arbeitet, können Sie ein Upgrade auf Version 11.1 durchführen.
- mehrere ESA-Hosts nicht für die Verwendung von Incident-Management konfiguriert haben und Sie eine Verbindung mit einzelnen ESA-Hosts herstellen, um Warnmeldungen anzuzeigen, führen Sie kein Upgrade auf Version 11.1 durch.

Hinweis: Wenn Sie in 10.6.5.x kein Incident-Management verwendet haben, können Sie die ESA-Warnmeldungen von 10.6.5.x nicht in der 11.1-Respond-Komponente anzeigen, ohne ein Migrationsskript auszuführen. Verwenden Sie das Skript ESA Alert Migration, um diese Warnmeldungen zu dem Ort in 11.1 zu migrieren, wo sie von der Respond-Komponente angezeigt werden können. Anweisungen zur Ausführung dieses Skripts finden Sie im Artikel *Anweisungen zur Migration von ESA-Warnmeldungen* der Wissensdatenbank (https://community.rsa.com/docs/DOC-81680) in RSA Link.

Phasen des Upgrades

RSA empfiehlt, die Hosts stufenweise zu aktualisieren, wie in diesem Abschnitt beschrieben. Das Update auf CentOS7 sowie die Notwendigkeit eines physischen oder iDRAC-Zugriffs führen dazu, dass das 11.1-Upgrade länger als die meisten Upgrades dauert.

Achtung: Bei Staffelung des Upgrades gilt Folgendes:
• Sie müssen zunächst die Hosts in Phase 1 aktualisieren, und zwar in der gezeigten Reihenfolge.
• Möglicherweise sind nicht alle Funktionen einsatzfähig, bis Sie das Update der gesamten Bereitstellung abgeschlossen haben.
• Es sind keine serviceadministrativen Funktionen verfügbar, bis Sie alle Hosts in Ihrer Bereitstellung aktualisiert haben.

Phase 1

Phase 1 wird zuerst durchgeführt. Sie müssen die Hosts in der folgenden Reihenfolge aktualisieren:

1. Security Analytics-Serverhost
2. Event Stream Analysis-Hosts
3. Malware Analysis-Hosts
4. Broker-Hosts (falls Sie keinen Broker haben, aktualisieren Sie Ihre Concentrator-Hosts)
   Der 11.1 NW-Server kann für die neue Investigate-Funktionalität nicht mit den 10.6.5.x-Core-Services kommunizieren. Deshalb müssen Sie die Broker- oder Concentrator-Hosts in Phase 1 aktualisieren.

Phase 2

Führen ein Upgrade der übrigen Hosts durch.

RSA empfiehlt jedoch, die Reihenfolge in Phase 2 einzuhalten, um folgende Risiken zu minimieren:

- Verlust von Funktionalität während der Untersuchung
- Ausfallzeiten mit der Folge von Verlusten bei Paket- und Protokollerfassung

Hinweis: Es besteht kein technischer Grund dafür, Ihre Hosts in der in Phase 2 gezeigten Reihenfolge zu aktualisieren (mit Ausnahme der Protokollsammlungs-Hosts mit Downstream-Ereigniszielen).

Dies ist die von RSA empfohlene Hostupgrade-Reihenfolge in Phase 2.

1. Decoder-Hosts
2. Concentrator-Hosts
3. Archiver-Hosts
4. Log Collection-Hosts – Log Collectors auf Log Decoder-Hosts (LDs), Virtual Log Collectors (VLCs) und Legacy Windows Collectors (LWCs)
   Bevor Sie einen Log Collection-Host aktualisieren, müssen Sie ihn für das Upgrade vorbereiten. Während dieser Vorbereitung wird sichergestellt, dass keine Ereignisdaten in Warteschlangen verbleiben. Dazu müssen Sie dafür sorgen, dass die Downstream-Ziele der Ereignisdaten (Log Collectors, Virtual Log Collectors und Log Decoders) funktionsfähig sind.

   Wenn Sie nachgelagert zum Log Decoder über Ereignisdatenziele verfügen, müssen Sie die Log Collectors vorbereiten und in der folgenden Reihenfolge aktualisieren.

   a. LDs (einer zur Zeit)

   b. VLCs und LWCs

   Wenn Sie nachgelagert zum Log Decoder über keine Ereignisdatenziele verfügen, können Sie mehrere LDs, VLCs und LWCs zusammen vorbereiten und aktualisieren.
5. Alle anderen Hosts

Im Abschnitt „Ausführen im gemischten Modus“ unter „Die Grundlagen“ im *RSA NetWitness Suite Leitfaden für die ersten Schritte mit Hosts und Services* finden Sie Informationen zu:

- Funktionslücken während der Ausführung in diesem Modus
- Beispiele für gestaffelte Upgrades

Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Investigate im gemischten Modus

Der gemischte Modus wird ausgeführt, wenn einige Services auf 11.1 aktualisiert werden und einige noch auf 10.6.5 basieren. Dies ist der Fall, wenn Sie ein phasenweises Upgrade auf 11.1 durchführen.

Hinweis: Sie müssen die unter Phasen des Upgrades beschriebene Reihenfolge für das Upgrade der Hosts einhalten, um den vollen Funktionsumfang von Investigate zu gewährleisten. Der 11.1-Investigate-Server wird installiert, wenn Sie den SA-Server aktualisieren, Broker-Hosts müssen aber auf 11.1 aktualisiert werden, um auf die Ansicht der Ereignisanalyse zuzugreifen. Wenn der Broker nicht aktualisiert wird, wird Analysten ein Warnsymbol neben dem Broker angezeigt und es können keine für diesen Broker aggregierten Daten angezeigt werden.

Nachdem Sie alle Services auf 11.1 aktualisiert haben und ein Analyst eine Untersuchung durchführt, funktioniert die rollenbasierte Zugriffskontrolle (RBAC) konsistent, um den Zugriff auf eingeschränkte Daten zu beschränken.

Wenn ein Analyst im gemischten Modus (das heißt, einige Services werden auf 11.1 aktualisiert, während andere noch auf 10.6.5 basieren) eine Untersuchung durchführt, wird RBAC nicht gleichmäßig auf Ansichten und Downloads angewendet.

Wenn die `sdk.packets`-Einstellung für die 10.6.x-Services nicht deaktiviert wurde, können Analysten mit Berechtigungen für SDK-Metadaten und -Rollen zur Beschränkung der Anzeige und der Rekonstruktion der Inhalte eines Ereignisses die PCAP eines Ereignisses herunterladen, das über Inhaltsbeschränkungen verfügt. Andere Arten von Downloads sind scheinbar erfolgreich, dann wird allerdings aufgrund unzureichender Berechtigungen ein Fehler erzeugt. Die Daten bleiben geschützt.

Bei einer stufenweisen Aktualisierung können Sie die `sdk.packets`-Einstellung der 10.6.x-Services deaktivieren, um das Herunterladen von PCAPs oder Protokollen im gemischten Modus durch Analysten einzuschränken. Nachdem Sie alle Services auf 11.1 aktualisiert und `sdk.packets` erneut aktiviert haben, funktioniert RBAC für alle Services gleich.

In dieser Tabelle ist angegeben, was Sie in Investigate anzeigen und herunterladen können, wenn Ihr NW-Server der Version 11.1 mit Services einer niedrigeren Version verbunden ist.

Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle mit eingeschränktem Inhalt	Anzeige	Kann eingeschränkten Inhalt erfolgreich herunterladen	Kann eingeschränkten Inhalt mit Fehlern herunterladen
11.1 Broker -> 10.6.5.x Concentrator -> 10.6.5.x Packet Decoder/Log Decoder	Ansicht „Ereignisse“	Analyst	Von RBAC erlaubte Elemente	PCAP	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich
	Ansicht der Ereignisrekonstruktion	Analyst	Von RBAC erlaubte Elemente	PCAP	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich
	Ansicht der Ereignisanalyse	Analyst	Von RBAC erlaubte Elemente	PCAP	Fehler beim Abrufen der Nutzlast vom Service für Payload, Request Payload, Response Payload

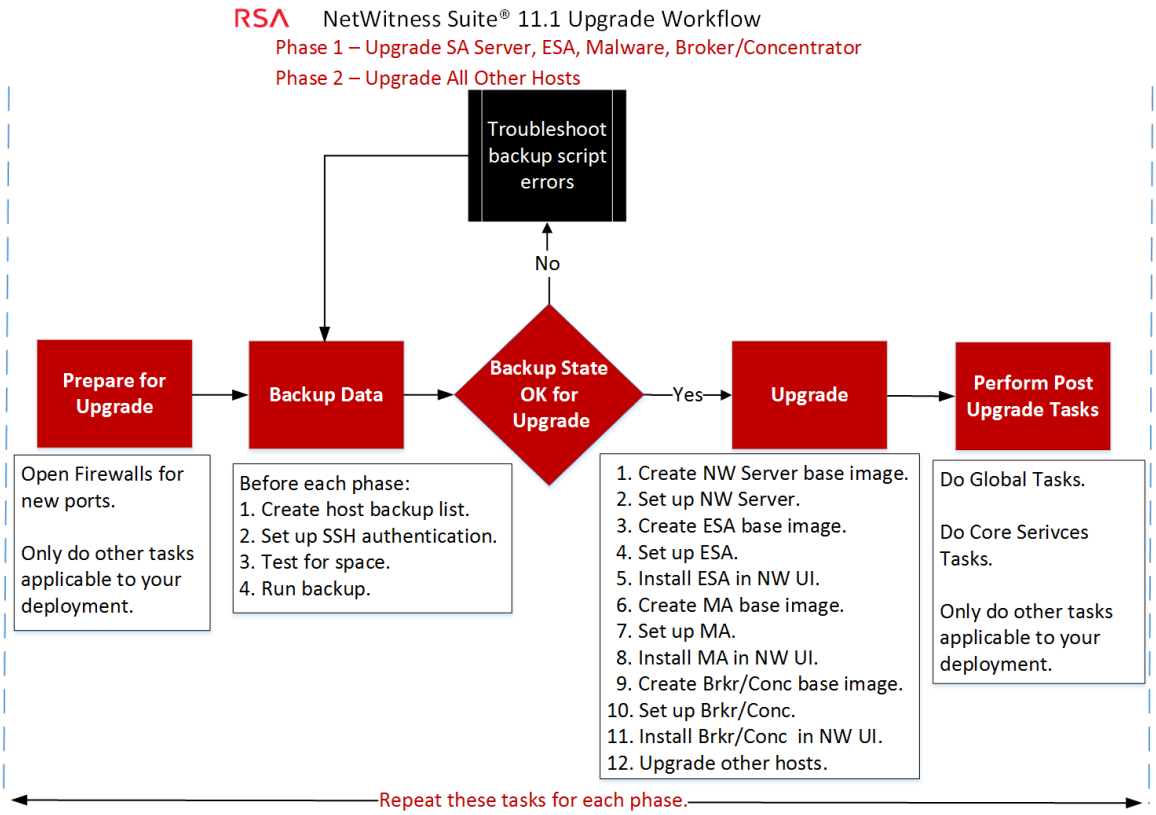
Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle mit eingeschränktem Inhalt	Anzeige	Kann eingeschränkten Inhalt erfolgreich herunterladen	Kann eingeschränkten Inhalt mit Fehlern herunterladen
11.1 Broker -> 11.1 Concentrator -> 11.1 Decoder/Log Decoder	Ansicht der Ereignisrekonstruktion	Analyst und Data Privacy Officer	Von RBAC erlaubte Elemente	PCAP	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich PCAPs und Protokolle werden als 0 Byte heruntergeladen

Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle mit eingeschränktem Inhalt	Anzeige	Kann eingeschränkten Inhalt erfolgreich herunterladen	Kann eingeschränkten Inhalt mit Fehlern herunterladen
11.1 Broker -> 11.0.0.x Concentrator -> 11.0.0.x Packet Decoder/Log Decoder	Ansicht „Ereignisse“	Analyst	Von RBAC erlaubte Elemente	Keine	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich PCAPs und Protokolle werden als 0 Byte heruntergeladen
	Ansicht der Ereignisrekonstruktion	Analyst	Von RBAC erlaubte Elemente	Keine	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich PCAPs und Protokolle werden als 0 Byte heruntergeladen

Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle mit eingeschränktem Inhalt	Anzeige	Kann eingeschränkten Inhalt erfolgreich herunterladen	Kann eingeschränkten Inhalt mit Fehlern herunterladen
	Ansicht der Ereignisanalyse	Analyst	Von RBAC erlaubte Elemente	Keine	Fehler beim Abrufen der Nutzlast vom Service für Payload, Request Payload, Response Payload PCAPs und Protokolle werden als 0 Byte heruntergeladen

Workflow für das Upgrade

Das folgende Diagramm stellt den Workflow für das RSA NetWitness® Suite 11.1-Upgrade dar.



Wenden Sie sich an den Kundensupport

Auf der Website „Contact RSA Customer Support“ (https://community.rsa.com/docs/DOC-1294) in RSA Link finden Sie Informationen darüber, wie Sie Hilfe zu RSA NetWitness Suite 11.1 erhalten.

Vorbereitung des Upgrades

Führen Sie die folgenden Aufgaben durch, um das Upgrade auf NetWitness Suite 11.1 vorzubereiten. Diese Aufgaben sind nach den folgenden Kategorien unterteilt.

Global

Sie müssen diese Aufgaben unabhängig davon ausführen, wie Sie NetWitness Suite bereitstellen und welche Komponenten Sie verwenden.

Aufgabe 1: Prüfen der Core-Ports und Öffnen von Firewallports

In den folgenden Tabellen sind die neuen Ports in 11.1 aufgeführt.

Achtung: Stellen Sie vor dem Upgrade sicher, dass die neuen Ports implementiert und getestet wurden, damit das Upgrade nicht aufgrund von fehlenden Ports fehlschlägt.

NW-Serverhost

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Hosts	NW-Server	TCP 4505, 4506	Salt Master-Ports
NW-Hosts	NW-Server	TCP 27017	MongoDB

ESA-Host

Quellhost	Zielhost	Zielports	Anmerkungen
NW-Server, NW-Endpunkt, ESA Secondary	ESA Primary	TCP 27017	MongoDB

Endpoint Hybrid oder Endpoint Log Hybrid

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint Hybrid oder Endpoint Log Hybrid	NW-Server	TCP 5672	Nachrichtenbus

Quellhost	Zielhost	Zielports	Anmerkungen
Endpoint-Server	NW-Server	TCP 27017	MongoDB

Alle NetWitness Suite-Core-Ports sind im Thema „Netzwerkarchitektur und Ports“ im *RSA NetWitness® Suite Bereitstellungshandbuch* aufgeführt, falls Sie die Services und Firewalls von NetWitness Suite neu konfigurieren müssen.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 2: Notieren des 10.6.5.x `admin user`-Passworts

Notieren Sie sich Ihr 10.6.5.x `admin user`-Passwort. Sie benötigen es, um das Upgrade abzuschließen.

Aufgabe 3: Erstellen eines Backups der `/etc/fstab` -Datei

Kopieren Sie die `/etc/fstab`-Datei aus allen physischen Hosts und auf Ihren lokalen Rechner (Backuphost oder Remoterechner).

Hinweis: Sie benötigen diese Datei zur Wiederherstellung eines physischen Hosts mit externen Speichermounts.

Respond

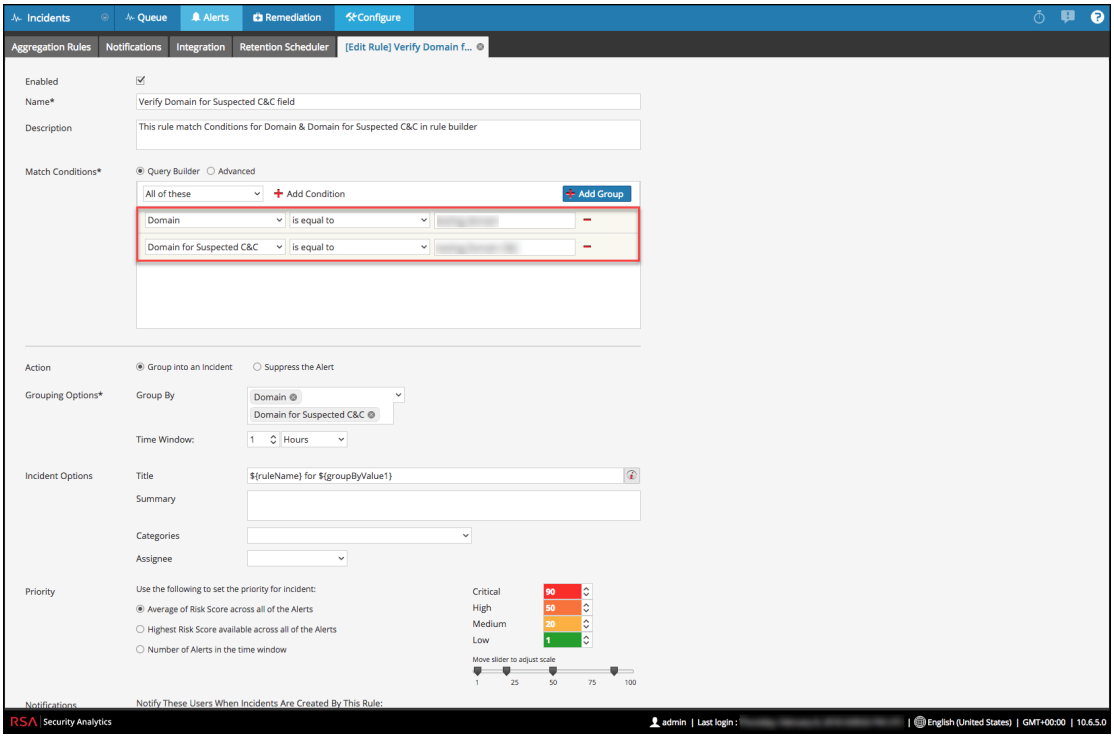
Aufgabe 4: Prüfen der Übereinstimmungsbedingungen von Aggregationsregeln für „Domain“ oder „Domain für verdächtige C&C“

Notieren Sie sich alle Incident-Management-Aggregationsregeln, die Übereinstimmungsbedingungen enthalten, die „Domain“ oder „Domain für verdächtige C&C“ in der Drop-down-Liste in der Regelerstellung verwenden. Sie müssen diese Regeln nach dem Upgrade auf 11.1 so ändern, dass sie „Domain“ verwenden, wie in den Aufgaben nach dem Upgrade für „Respond“ beschrieben.

Prüfen Sie bei jeder Aggregationsregel Folgendes:

1. Klicken Sie im Menü „Security Analytics 10.6.5.x“ auf **Incidents** > **Konfigurieren** > Registerkarte **Aggregationsregeln** und bearbeiten Sie die Regeln, um die passenden Bedingungen anzuzeigen.

2. Suchen Sie im Abschnitt **Bedingungen abstimmen** nach **Domain** oder **Domain für verdächtige C&C** in den Drop-Down-Listen für die Bedingungen.



3. Notieren Sie den Regelnamen und die gesamte Bedingung, die**Domain** oder **Domain für verdächtige C&C** verwendet, einschließlich Operatoren und Werten.

Reporting Engine

(Bedingungsabhängig) Aufgabe 5: Trennen des externen Speichers

Wenn die Reporting Engine über externen Speicher verfügt [z. B. ein Storage Area Network (SAN) oder Network Attached Storage (NAS) zum Speichern von Berichten], müssen Sie die folgenden Schritte ausführen, um die Verbindung des Speichers aufzuheben.

Für diese Schritte gilt Folgendes:

- `/home/rsasoc/rsa/soc/reporting-engine/` ist das Root-Verzeichnis der Reporting Engine.
- `/externalStorage/` ist der Ort, an dem der externe Speicher gemountet ist.

1. Stellen Sie über SSH eine Verbindung mit dem Reporting Engine-Host her und melden Sie sich mit Ihren `root` -Anmeldedaten an.
2. Beenden Sie den Reporting Engine-Service.
   ```
   stop rsasoc_re
   ```

3. Wechseln Sie zum `rsasoc`-Benutzer.
   ```
   su rsasoc
   ```
4. Wechseln Sie zum Root-Verzeichnis der Reporting Engine.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. Heben Sie die Verknüpfung des `resultstore`-Verzeichnisses auf, das zum externen Speicher gemountet ist.
   ```
   unlink /externalStorage/resultstore
   ```
6. Heben Sie die Verknüpfung des `formattedReports`-Verzeichnisses auf, das zum externen Speicher gemountet ist.
   ```
   unlink /externalStorage/formattedReports
   ```

Warehouse Connector

(Bedingungsabhängig) Aufgabe 6: Kopieren der `keytab`-Dateien im `root`- oder `etc`-Verzeichnis, das in einem anderen Verzeichnis gespeichert ist

Kopieren Sie die `keytab`-Dateien im `root`- oder `etc`-Verzeichnis, wenn es in einem anderen Verzeichnis gespeichert ist.

1. Notieren Sie sich den absoluten Pfad des NFS-Mount-Verzeichnisses und der `keytab`-Datei.
   Sie benötigen diese Informationen zur Wiederherstellung von Warehouse Connector nach dem Upgrade.
2. Unmounten Sie das NFS-Verzeichnis.
   a. Stellen Sie über SSH eine Verbindung mit Warehouse Connector her und melden Sie sich mit den `root`-Anmeldedaten an.
   b. Senden Sie die folgenden Befehle zum Unmounten des NFS-Verzeichnisses.
      ```
      umount <NFS-absolute-path>
      ```

Anweisungen zum Backup

Eine Sicherung Ihrer Konfigurationsdaten für alle Hosts von 10.6.5.x ist der erste Schritt beim Upgrade von Security Analytics 10.6.5.x auf NetWitness Suite 11.1.

Hinweis: Es ist wichtig, dass Sie benutzerdefinierte Zertifikatdateien und alle Dateien einer anderen Zertifizierungsstelle (CA) im Ordner `/root/customcerts` speichern, um sicherzustellen, dass diese Zertifikatdateien gesichert werden. Ihre benutzerdefinierten Zertifikatdateien, die in diesem Verzeichnis abgelegt werden, werden während des Upgrades automatisch wiederhergestellt. Nach dem Upgrade auf 11.1 befinden sich Ihre benutzerdefinierten Zertifikatdateien in `/etc/pki/nw/trust/import`. Weitere Informationen zum Sichern dieser Arten von Dateien finden Sie unter Schritt 1 in Für alle Hosttypen.

Achtung: Diese Services werden beim Backup- und Upgrade-Prozess für 10.6.5.x nicht unterstützt.
- IPDB
- All-in-one-Server
- Malware Analysis parallel auf dem Security Analytics-Server
- Eigenständiger Warehouse Connector
- Warehouse Analytics (Datascience)

Die folgenden Typen von Hosts können gesichert werden. Sie werden während des Upgrades automatisch wiederhergestellt:

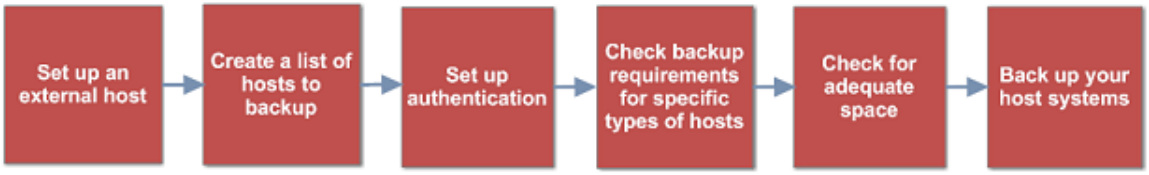
- **Security Analytics-Adminserver** (kann Malware Analysis, Incident-Management, Integrität und Zustand sowie Reporting Engine enthalten)
- **Malware Analysis** (eigenständig)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (einschließlich Context Hub und Incident-Management-Datenbank)
- **Concentrator**
- **Log Decoder** (einschließlich lokaler Log Collector und Warehouse Connector, falls installiert)
- **Log Hybrid**
- **Packet Decoder** (einschließlich Warehouse Connector, falls installiert)

- **Packet Hybrid**
- **Virtual Log Collector**

Die folgenden Arten von Dateien werden automatisch gesichert, müssen nach dem Upgrade aber manuell wiederhergestellt werden:

- PAM-Konfigurationsdateien: Informationen zum Wiederherstellen der PAM-Konfigurationsdateien finden Sie unter „Aufgabe 5: Neukonfigurieren des Pluggable Authentication Module (PAM) in 11.1.“ im Abschnitt „Global“ der **Aufgaben nach dem Upgrade**.
- `/etc/pfring/mtu.conf` und `/etc/init.d/pf_ring`: Um diese Dateien wiederherzustellen, müssen Sie sie manuell abrufen. Die `/etc/pfring/mtu.conf`-Dateien befinden sich unter `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf` und die `/etc/init.d/pf_ring`-Dateien unter `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. Informationen zum Wiederherstellen dieser Dateien finden Sie unter „(Bedingungsabhängig) Aufgabe 2: Wiederherstellen von Dateien für den 10G-Decoder“ im Abschnitt mit den hardwarebezogenen Aufgaben unter **Aufgaben nach dem Upgrade**.

Das folgende Diagramm zeigt den allgemeinen Ablauf der Schritte zum Sichern Ihrer Hosts.



In den folgenden Abschnitten werden die einzelnen Aufgaben beschrieben:

- Aufgabe 1: Einrichten eines externen Hosts für die Sicherung von Dateien
- Aufgabe 2: Erstellen einer Liste der zu sichernden Hosts
- Aufgabe 3: Einrichten der Authentifizierung zwischen Backup- und Zielhosts
- Aufgabe 4: Überprüfen der Backupanforderungen für bestimmte Hosttypen
- Aufgabe 5: Überprüfen auf ausreichend Speicherplatz für das Backup
- Aufgabe 6: Sichern der Hostsysteme
- Aufgaben nach dem Backup

Aufgabe 1: Einrichten eines externen Hosts für die Sicherung von Dateien

Sie müssen einen externen Host einrichten, der zum Sichern von Dateien verwendet werden soll. Auf dem Host muss CentOS 6 mit SSH-Konnektivität zum Security Analytics-Host-Stack ausgeführt werden.

Hinweis: Wenn Sie zur Sicherung von Dateien keinen externen Host verwenden können, wenden Sie sich an RSA Kundensupport (https://community.rsa.com/docs/DOC-1294), um Unterstützung zu erhalten.

Vergewissern Sie sich, dass die Hostnamen für die zu sichernden Systeme auf dem Backuphost aufgelöst werden können, entweder via DNS oder als Eintrag in der Datei `/etc/hosts`.

Hinweis: Diese Skripte können nur auf CentOS 6 ausgeführt werden. Sie müssen diese Skripte auf CentOS 6-Rechnern ausführen.

Es gibt verschiedene Skripte, die Sie während des Backups ausführen. Sie müssen die ZIP-Datei, die die Skripte (`nw-backup-v4.0.sh`) enthält, von RSA Link herunterladen unter: https://community.rsa.com/docs/DOC-81514. Kopieren Sie sie in Ihr CentOS 6-Backupsystem. Extrahieren Sie die Zip-Datei, um auf die Skripte zuzugreifen. Diese Skripte sind:

- `get-all-systems.sh`: Erstellt die Datei `all-systems`, die eine Liste all Ihrer Security Analytics-Server und zu sichernden Hostsysteme enthält.
- `ssh-propagate.sh`: Automatisiert die Freigabe von Schlüsseln zwischen den zu sichernden Systemen und dem Backup-Hostsystem, damit Sie nicht mehrmals zur Passworteingabe aufgefordert werden.
- `nw-backup.sh`: Führt das Backup Ihrer Hosts durch.
- `azure-mac-retention.ps1`: Gilt nur bei Verwendung von AZURE. Weitere Informationen finden Sie im *AZURE-Bereitstellungshandbuch*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

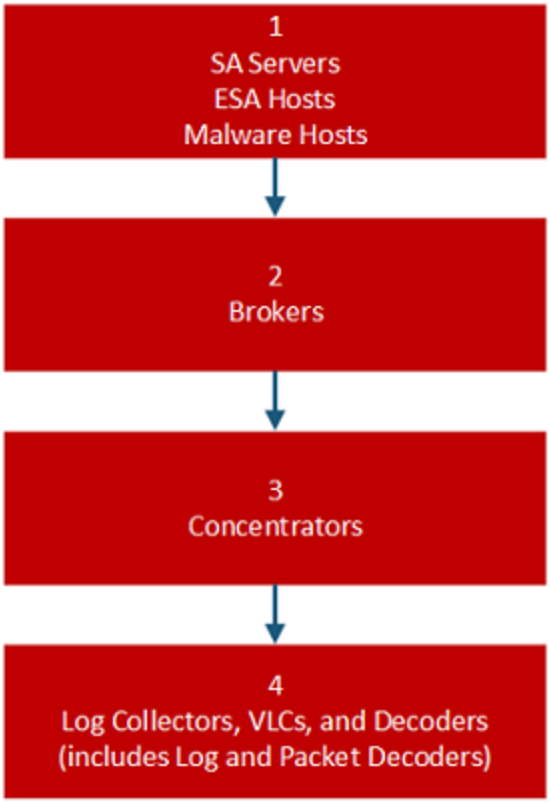
Hinweis: Wenn Sie die 10.6.x-Versionen der Backup- und Wiederherstellungsskripte auf Ihren 10.6.5-Hosts verwendet haben, müssen Sie trotzdem alle hier aufgelisteten Skripte ausführen.

Hinweis: Verwenden Sie NICHT die Skripte in der Datei `nw-backup-v4.0.zip` für regelmäßige Backups. Diese Skripte sind speziell für das Upgrade von 10.6.5.x auf 11.1 konzipiert.

Hinweis: Die Backupskripte unterstützen nicht das Sichern von Daten für STIG-gesicherte Hosts.

Aufgabe 2: Erstellen einer Liste der zu sichernden Hosts

Welches Skript Sie zum Sichern Ihrer Dateien verwenden, hängt von den Dateien `all-systems` und `all-systems-master-copy` ab, in denen die zu sichernden Hosts aufgelistet sind. Die Datei `all-systems-master-copy` enthält eine Liste aller Hosts. Die Datei `all-systems` wird für jede Backupsitzung verwendet und enthält nur die Hosts, die für eine bestimmte Sitzung gesichert werden. Sie führen das Skript `get-all-systems.sh` aus, um diese Dateien zu generieren. RSA empfiehlt, dass Sie Ihre Hosts in Gruppen und nicht gleichzeitig sichern. Im folgenden Diagramm ist die empfohlene Reihenfolge und Gruppierung der Hosts für die Backupsitzungen dargestellt:



Beschränken Sie jede Backupsitzung auf fünf Hosts, um sicherzustellen, dass der Speicherplatz für die Backupdateien weiterhin ausreicht. Sie erstellen `all-systems`-Dateien für Ihre Backupsitzungen mithilfe der Datei `all-systems-master-copy` als Referenz. Dann bearbeiten Sie manuell die Datei `all-systems`, um spezifische Hosts einzuschließen.

Erzeugen der Datei `all-systems` und `all-systems-master-copy`:

1. Machen Sie auf dem Host, auf dem der Sicherungsvorgang ausgeführt wird, das Skript `get-all-systems.sh` durch Ausführen des folgenden Befehls ausführbar:
   `chmod u+x get-all-systems.sh`
2. Führen Sie auf Stammebene das Skript `get-all-systems.sh` aus:
   `./get-all-systems.sh <IP-Address-of-SA-Admin-Server>`
   Sie werden einmal pro Host aufgefordert, das Passwort für jedes Hostsystem einzugeben.

Dieses Skript speichert die Dateien `all-systems` und `all-systems-master-copy` unter `/var/netwitness/database/nw-backup/`.

3. Überprüfen Sie, ob die Dateien `all-systems` und `all-systems-master-copy` generiert wurden und die richtigen Hosts enthalten.
4. Bearbeiten Sie die Datei `all-systems`, sodass sie nur die Systeme enthält, die Sie sichern möchten. Sie können dies mit der Datei `all-systems-master-copy` als Referenz erledigen. Sie öffnen dann die Datei `all-systems` in einem Editor (z. B. vi) und bearbeiten sie, sodass sie nur die zu sichernden Systeme enthält. RSA empfiehlt, dass Sie die Hosts auskommentieren, die Sie nicht sichern möchten (fügen Sie das Zeichen # an den Anfang der Zeile ein, die den Host enthält, die nicht gesichert werden soll).
   Die folgende Beispiele zeigen, wie der 10.6.5 Security Analytics-Server auskommentiert wird:
   ```
   loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-
   7ac5fa1d18d8,10.6.5.0
   #nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-
   7be4d8cf5e65,10.6.5.0
   ```

   Hinweis: Achten Sie bei Verwendung von vi darauf, den Pfad zum Speicherort der Datei `all-systems` anzugeben.

Hier ist ein Beispiel für eine `all-systems-master-copy`-Datei:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

Und hier ist ein Beispiel für eine `all-systems`-Datei, die in der ersten Backupsitzung verwendet werden könnte, in der nur der Security Analytics-Server, ESA-Host und Malware Analysis-Host gesichert werden:

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

Troubleshooting-Informationen

- Speichern Sie Kopien der Dateien `all-systems` und `all-systems-master-copy` an einem sicheren Ort. Befolgen Sie diese Empfehlungen:
  - Bearbeiten Sie nicht die Datei `all-systems-master-copy`.
  - Wenn Sie mehrere unterschiedliche Versionen der Datei `all-systems` erstellen (z. B. für mehrere Backupsitzungen), achten Sie darauf, dass jede Version der Datei nur diejenigen Hosts auflistet, die aktuell gesichert werden, und dass die anderen Hosts auskommentiert sind.
    Weitere Informationen finden Sie unter Aufgaben nach dem Backup.
- Wenn Hostsysteme ausgeschaltet sind, während Sie das Skript `get-all-systems.sh` ausführen, erstellt das Skript eine Liste der Hosts, für die es keine Informationen finden kann. Nachdem das Skript ausgeführt und die Datei `all-systems` erstellt wurde, müssen Sie die Datei `all-systems` manuell bearbeiten und die fehlenden Informationen für diese Hosts hinzufügen.
- Das Skript `get-all-systems.sh` erzeugt eine Liste der Hosts, die auf der Security Analytics-Benutzeroberfläche definiert wurden. Stellen Sie sicher, dass alle Hosts und Services ordnungsgemäß bereitgestellt werden. Wenn Hosts oder Services nicht ordnungsgemäß bereitgestellt werden, werden sie nicht gesichert. RSA empfiehlt, beim Hinzufügen von Hosts und Services zu Security Analytics die Security Analytics-Benutzeroberfläche zu verwenden, um sicherzustellen, dass sie ordnungsgemäß bereitgestellt

werden. Wenn Hosts oder Services auf der Benutzeroberfläche nicht definiert wurden, müssen Sie sie manuell zur Datei `all-systems` hinzufügen.

- Am Ende des Skripts `get-all-systems.sh` führt dieses eine Überprüfung auf eventuelle Unterschiede zwischen den Systemen durch, die der Security Analytics-Server aufgeführt hat, und den Systemen, für die das Skript alle erforderlichen Informationen gefunden hat. Wenn Node-IDs oder Systemnamen als fehlend aufgelistet werden, überprüfen Sie, ob diese Systeme vorhanden sind, alle zugehörigen Services ausgeführt werden und sie ordnungsgemäß mit dem Security Analytics-Server kommunizieren. (Windows-Legacy-Collectors oder AWS Cloud-Collectors werden nicht zur Datei `all-systems` hinzugefügt und können möglicherweise zu Diskrepanzen führen. **Fügen Sie diese Elemente NICHT manuell zur Datei `all-systems` hinzu**.)
- Wenn die Syntax in der Datei `all-systems` falsch ist, schlägt das Skript fehl. Wenn z. B. am Anfang oder Ende eines Hosteintrags ein zusätzliches Leerzeichen vorhanden ist, schlägt das Skript fehl.

Aufgabe 3: Einrichten der Authentifizierung zwischen Backup- und Zielhosts

RSA empfiehlt die Ausführung des Skripts `ssh-propagate.sh`, um die Freigabe der Schlüssel zwischen dem Backuphost und den Hostsystemen zu automatisieren.

Hinweis: Wenn Sie über SSH-Schlüssel verfügen, die mit Passphrase geschützt sind, können Sie `ssh-agent` verwenden, um Zeit zu sparen. Weitere Informationen finden Sie auf der `ssh-agent`-Manpage.

1. Machen Sie auf dem externen Backup-Hostsystem das Skript `ssh-propagate.sh` durch Ausführen des folgenden Befehls ausführbar:
   ```
   chmod u+x ssh-propagate.sh
   ```
2. Führen Sie im Stammverzeichnis den folgenden Befehl aus, wobei `<path-to-all-systems-file>` der Pfad zu dem Verzeichnis ist, in dem die Datei `all-systems` gespeichert ist:
   ```
   ssh-propagate.sh <path-to-all-systems-file>
   ```
3. Sie werden einmal pro Host aufgefordert, das Passwort einzugeben. Sie müssen es später während des Backupvorgangs aber nicht erneut eingeben.

Aufgabe 4: Überprüfen der Backupanforderungen für bestimmte Hosttypen

Nach der Erstellung der `all-systems`-Datei für das Backup müssen Sie überprüfen, ob für einen der in der Datei aufgelisteten Hosts Anforderungen bestehen, die erfüllt werden müssen, bevor das Backup ausgeführt werden kann.

Für alle Hosttypen

Führen Sie für alle Hosttypen die folgenden Schritte aus:

1. Speichern Sie auf dem Security Analytics-Server benutzerdefinierte Zertifikatdateien und alle Dateien einer anderen Zertifizierungsstelle (CA) im Ordner `/root/customcerts`, um sicherzustellen, dass diese Zertifikatdateien gesichert werden. Ihre benutzerdefinierten Zertifikatdateien, die in diesen Verzeichnissen abgelegt werden, werden während des Upgrades automatisch wiederhergestellt. Nach dem Upgrade auf 11.1 befinden sich Ihre benutzerdefinierten Zertifikatdateien in `/etc/pki/nw/trust/import`.
   Sie können mithilfe von OpenSSL CA-Zertifikate und Schlüssel in verschiedene Formate konvertieren, damit sie mit speziellen Arten von Servern oder Software kompatibel sind.

Beispielsweise können Sie eine normale PEM-Datei, die mit Apache kompatibel ist, in eine PFX (PKCS #12)-Datei konvertieren und sie mit Tomcat oder IIS verwenden. Um die Dateien zu konvertieren, stellen Sie über SSH eine Verbindung mit dem Security Analytics-Server her und führen Sie die folgenden Befehlszeichenfolgen aus, um die aufgeführten Umwandlungen vorzunehmen.

Konvertieren einer DER-Datei (.crt .cer .der) in PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Konvertieren einer PEM-Datei in DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Konvertieren einer PEM-Zertifikatdatei und eines privaten Schlüssels in PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -
in certificate.crt -certfile CACert.crt
```

Konvertieren einer PKCS#12-Datei (.pfx. p12) mit einem privaten Schlüssel und Zertifikaten in PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Hinweis:** Fügen Sie der Befehlszeichenfolge den folgenden Qualifizierer hinzu:
> mit `-nocerts` konvertieren Sie ausschließlich private Schlüssel.
> mit `-nokeys` konvertieren Sie ausschließlich Zertifikate.

2. Notieren Sie sich alle benutzerdefinierten Konfigurationen von CentOS 6 (z. B. Treiberanpassungen) für die Wiederherstellung nach der Aktualisierung auf CentOS 7. Benutzerdefinierte Konfigurationen von CentOS 6 werden nicht automatisch gesichert und wiederhergestellt.

Für ESA-Hosts mit Mongo-Datenbanken

Das Standardpasswort der 10.6.x Mongo-Datenbank lautet `netwitness`. Wenn Sie dieses Passwort angepasst haben, kann möglicherweise ein Fehler auftreten, während das Backupskript ausgeführt wird. Sie können entweder Ihr angepasstes Passwort für die Mongo-Datenbank während des Backups verwenden oder Sie können dieses Passwort wieder auf `netwitness` ändern, bevor Sie das `nw-backup.sh`-Skript ausführen.

1. Finden Sie heraus, ob das Passwort der Mongo-Datenbank `netwitness` ist oder ob es geändert wurde.
2. Wenn es geändert wurde, ändern Sie es entweder auf `netwitness` zurück oder stellen Sie sicher, dass Sie wissen, wie das angepasste Passwort lautet, damit Sie es während des Backups eingeben können.

Weitere Informationen finden Sie unter „ESA-Konfiguration: Ändern des MongoDB-Passworts für das Administratorkonto“ im *Konfigurationsleitfaden für NetWitness Suite Event Stream Analysis*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Für Decoder-, Concentrator- oder Broker-Hosts: Beenden der Datenerfassung und -aggregation

Zusätzlich zu den unter Für alle Hosttypen beschriebenen Aufgaben beenden Sie für Decoder-, Concentrator- oder Broker-Hosts die Datenerfassung und -aggregation auf allen Systemen, die gesichert werden sollen. Anweisungen dazu finden Sie unter Anhang B: Beenden der Datenerfassung und -aggregation.

Log Collectors (LC) und Virtual Log Collectors (VLCs): `prepare-for-migrate.sh` ausführen

Achtung: Diese Aufgabe beendet die Protokollsammlung, sodass Sie diesen Schritt unmittelbar vor dem Upgrade durchführen müssen, um Verluste bei der Ereignissammlung zu minimieren. Führen Sie diese Aufgabe in Übereinstimmung mit den Backup- und Upgrade-Aufgaben in diesem Handbuch aus.

Voraussetzungen

Sie benötigen die folgenden Informationen, bevor Sie LCs und VLCs für das Upgrade vorbereiten können.

- Wenn die Lockbox auf dem LC und VLC initialisiert wurde, müssen Sie das Lockbox-Passwort kennen. Dies ist erforderlich, um die Lockbox nach dem Upgrade neu zu konfigurieren.
- Wenn Sie das Passwort für den Benutzer `logcollector` für RabbitMQ festlegen, müssen Sie das Passwort kennen, damit Sie es nach dem Upgrade erneut einrichten können.

Vorbereiten des Upgrades für LCs und VLCs

1. Stellen Sie über SSH eine Verbindung mit dem Log Collector her.
2. Senden Sie die folgende Befehlszeichenfolge:
   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```
   Dieser Befehl bewirkt Folgendes:
   - Beendet den Puppet-Agent-Service.
   - Deaktiviert die Dateisammlungskonten („sftp“ und alle Benutzer in der Gruppe „upload“), die für das Hochladen von Protokolldateien zum Log Collector verwendet werden. Die Protokolldateien werden in den Ereignisquellen gesammelt, bis der Log Collector auf 11.1

aktualisiert wurde.

- Beendet alle Erfassungsprotokolle im Log Collector-Service.
- Speichert die Liste der Plug-in- und RabbitMQ-Konten.
- Konfiguriert den RabbitMQ-Server so, dass keine neuen Ereignisse mehr darauf veröffentlicht werden können. Verbraucher der Ereignisse in den Warteschlangen, z. B. Shovels und Log Decoder-Ereignisprozessoren, werden weiterhin ausgeführt.
- Wartet, bis die Log Collector-Warteschlangen leer sind.
- Beendet den Log Collector-Service.
- Erstellt eine Markerdatei, die angibt, dass der Log Collector erfolgreich für das Upgrade vorbereitet wurde.

Troubleshooting-Informationen

Das `prepare-for-migrate.sh` -Skript:

- Sendet Informations-, Warn- und Fehlermeldungen an die Konsole.
- Speichert ein Sitzungsprotokoll im Verzeichnis `/var/log/backup/`.

Sie müssen die folgenden Fehler beheben und die Vorbereitung fortsetzen. Wenden Sie sich an den RSA-Kundensupport (https://community.rsa.com/docs/DOC-1294), um Unterstützung zu erhalten.

- Es werden Log Collector-Warteschlangen mit Ereignissen, aber ohne Verbraucher gefunden.
- Der Puppet-Agent-Dienst kann nicht beendet werden.
- Ein Erfassungsprotokoll im Log Collector-Service kann nicht beendet werden.
- Ereignisherausgeber für den RabbitMQ-Server können nicht gesperrt werden.
- Verbrauch von Warteschlangenereignissen nicht möglich oder dauert zu lange. Das Skript unternimmt 30 Versuche und wartet, bis die Ereignisse verbraucht werden. Nach jedem Versuch ist es für 30 Sekunden inaktiv.
- Log Collector-Service kann nicht beendet werden.

Weitere Informationen zum Troubleshooting finden Sie unter Anhang A: Troubleshooting.

Für Integrationen mit Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpoint: Auflisten der RabbitMQ-Benutzernamen und -Passwörter

Auf dem 10.6.5.x-Host bzw. auf dem Security Analytics-Serverhost müssen Sie eine Liste aller RabbitMQ-Benutzernamen und -Passwörter abrufen, damit Sie nach dem Upgrade auf 11.1 die RabbitMQ-Benutzerkonten wiederherstellen können.

Führen Sie zum Abrufen der RabbitMQ-Benutzernamen und -Passwörter den folgenden Befehl aus:

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

Um RabbitMQ-Benutzerkonten wiederherzustellen, lesen Sie *Aufgabe 2: Für Integrationen mit Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpunkt – Konfigurieren von gegenseitig authentifizierten SSL-Verbindungen* in **Aufgaben nach dem Upgrade**.

Für Bluecoat-Ereignisquellen

Bluecoat ProxySG-Ereignisquellen verwenden das FTPS-Protokoll zum Hochladen von Protokolldateien zum Log Collector (LC) und Virtual Log Collector (VLC). Die Ereignisquellendokumentation enthält die Schritte zur Konfiguration des VSFTPD-Service auf dem LC und VLC.

- Wenn Schlüsselmaterial im Verzeichnis `/root/vsftpd/` in 10.6.5.x vorhanden ist, wird dieses Material gesichert und wiederhergestellt. **Wenn sich das Material an einem anderen Speicherort befindet, müssen Sie es manuell sichern und wiederherstellen.**
- Wenn die Datei `/etc/vsftpd/vsftpd.conf` in 10.6.5.x vorhanden ist, wird sie gesichert und wiederhergestellt.

Aufgabe 5: Überprüfen auf ausreichend Speicherplatz für das Backup

Sie können das Skript zum Testen des Backups ausführen, um zu prüfen, wie viel Speicherplatz für das Backup erforderlich ist. Verwenden Sie dazu die Option `-t`, die unter Testoptionen beschrieben wird. Sie können das Skript ausführen, ohne tatsächlich Dateien zu sichern oder Services zu beenden. RSA empfiehlt, diesen Schritt durchzuführen, um zu gewährleisten, dass Sie ausreichend Speicherplatz für das Backup bereitstellen, damit bei der Sicherung alle Ihre Daten erfasst werden.

So überprüfen Sie, ob ausreichend Speicherplatz vorhanden ist:

1. Mit dem folgenden Befehl sorgen Sie dafür, dass das Backupskript ausführbar ist:
   ```
   chmod u+x nw-backup.sh
   ```

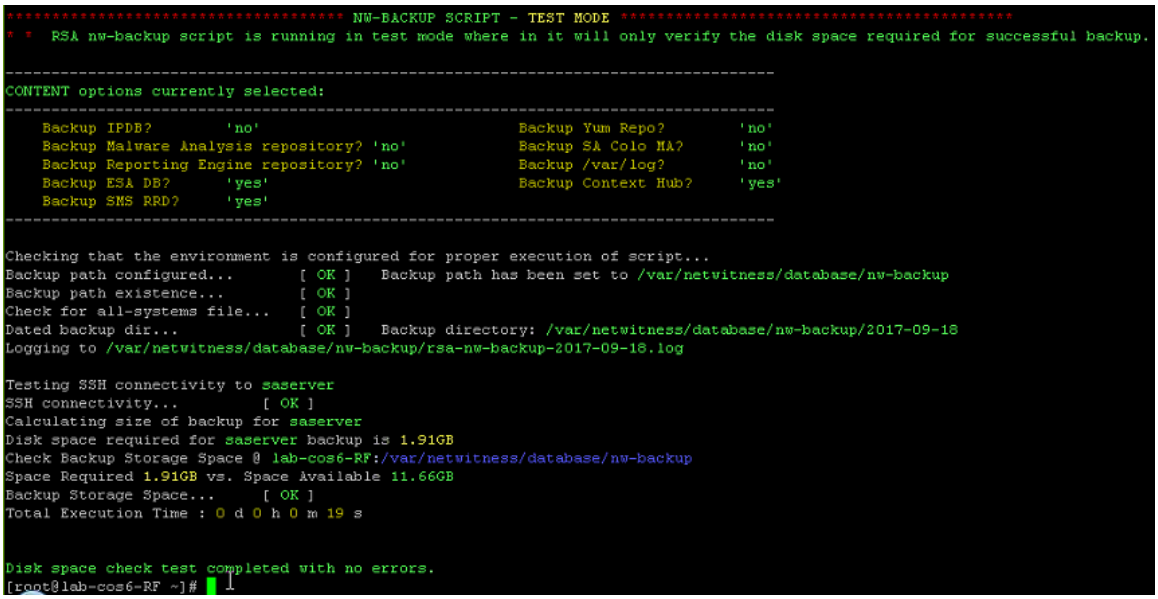
2. Führen Sie den folgenden Befehl auf Ebene des Stammverzeichnisses aus:

   `./nw-backup.sh -t`

   Die Ausgabe zeigt die Menge an Festplattenspeicher, die für das Backup erforderlich ist.

> **Hinweis:** Der Befehl `./nw-backup.sh -t` wird standardmäßig mit der Option `-d` ausgeführt. Wenn Sie präzisere Ergebnisse für den Festplattenspeicherplatz benötigen, können Sie die Option `-d` mithilfe von `-D` überschreiben. Über die Option `-D` wird angezeigt, wie viel Speicherplatz auf jedem Host für die zu sichernden Daten erforderlich ist. Es wird aber nicht angezeigt, wie viel Speicherplatz verfügbar ist. Wenn nicht genügend Speicherplatz verfügbar ist, löst die Option `-D` eine Fehlermeldung aus. Wenn Sie wissen möchten, wie viel Speicherplatz auf dem Zielhost vorhanden ist, müssen Sie den Befehl `df -h` auf dem Host ausführen.

Die folgende Abbildung zeigt ein Beispiel für die Ausgabe bei Verwendung der Option `-t`.



Aufgabe 6: Sichern der Hostsysteme

Bevor Sie das Backupskript ausführen, um das eigentliche Backup durchzuführen, achten Sie darauf, dass Sie über ausreichend Speicherplatz verfügen. Führen Sie zur Sicherung Ihrer Hosts das Skript `nw-backup.sh` mit der Option `-u` aus. Diese Option ist für ein Upgrade auf 11.1 erforderlich.

> **Hinweis:** Das Skript beendet bei seiner Ausführung Services. Sie können Services jedoch bei Bedarf auch vor Ausführung des Skripts manuell beenden.

Wenn Sie das Backupskript ausführen, können Sie aus mehreren Optionen auswählen. Diese werden in den folgenden Abschnitten beschrieben.

Nutzung:
`./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>`

Allgemeine Optionen

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) -COPY`

`-b <path to write backups> : path to the location for storing backup files on a backup server.` **`For upgrading to 11.1, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

Hinweis: Ändern Sie **nicht** den Backuppfad im Upgrade-Modus (-u).

Hinweis: Wenn Sie ein Backup mit der Option `-u` ausführen, werden alle Services beendet. Wenn Sie die 10.6.x-Maschine nach Ausführung des Backups weiterhin verwenden möchten, starten Sie das System 10.6.x neu, damit die Services neu gestartet werden.

Erweiterte Optionen zur Content-Auswahl

`-c : back up Colocated Malware Analysis on SA servers. Default: (no)`

`-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)`

`-m : back up Malware Analysis File Repository. Default: (no)`

`-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)`

`-v : back up system logs (/var/log). Default: (no)`

`-y : back up YUM Web Server & RPM Repository. Default: (no)`

`-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)`

`-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)`

`-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)`

Testoptionen

```
 -t : performs script test run for disk space check only. Services are
not stopped and excludes execution of backup. Can be combined with (-d)
or (-D) and other flags. Default: (-t)
```

Beispielsweise würde mit dem Befehl:
`./nw-backup.sh`
würde das Backup mit Optionen durchführen, wie sie in der Kopfzeile des Skripts selbst festgelegt sind.
ODER: Mit dem Befehl:
`./nw-backup.sh -ue /mnt/external_backup`
würde ein normales Backup über den Backuppfad durchführen, der in dem Skript definiert ist, und zwar mit den folgenden Optionen:

```
-u : enables the upgrade flag to run backup for upgrading to 11.1. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

Wenn Sie das Skript ausführen, wird oben im Skript der folgende Text angezeigt:

Achtung: `RSA nw-backup script backs up configuration files, data, and logs on the options provided in the script. It tars the content, with options to store the backup files on the backup server, move or copy them to external storage on a mount point (USB/NFS/SMB), or SCP them back to the target host.`
`This backup script has been qualified on the following versions of Security Analytics:`
`10.6.5.x`
`Use of this script on any other versions of the product may not give expected results and may not be supported by RSA Customer Service.Note: All non-RSA custom files, scripts, Cronjobs and other important files should be placed in /root, /home/'user', OR /etc to be included in the backup.`

Zum Ausführen des Skripts zum Sichern Ihrer Hosts müssen Sie:

1. Sicherstellen, dass die Datei `all-systems` nur die zu sichernden Hosts enthält.
   Informationen hierzu finden Sie unter Aufgabe 2: Erstellen einer Liste der zu sichernden Hosts.
2. Mit dem folgenden Befehl sorgen Sie dafür, dass das Backupskript ausführbar ist:
   `chmod u+x nw-backup.sh`
3. Beginnen Sie den Sicherungsprozess durch Ausführen des folgenden Befehls auf Stammverzeichnisebene:
   `./nw-backup.sh -u`

Hinweis: Sie müssen die Option `-u` verwenden, damit Ihre Dateien während des Upgrades auf 11.1 korrekt wiederhergestellt werden. Nehmen Sie KEINE Änderungen in der Kopfzeile des Backupskripts für den Backuppfad vor, da der Pfad upgradespezifisch ist und die Daten an einem spezifischen Ort liegen müssen.

Wenn der Text „`Backup completed with no errors`“ angezeigt wird, wurde das Backup erfolgreich abgeschlossen.

Im Backupverzeichnis wird eine Protokolldatei erstellt, mit einem Namen ähnlich dem folgenden Beispiel. Sie enthält Informationen zu den zu sichernden Dateien:
`rsa-nw-backup-2017-03-15.log`

4. Wenn das Backup abgeschlossen wurde, können Sie den folgenden Befehl ausführen, um eine Liste aller gesicherten Dateien anzuzeigen, damit sichergestellt ist, dass alle gewünschten Dateien gesichert wurden:
   `tar -tzvf hostname-ip-address-backup.tar.gz`
   Es werden folgende Archivdateien erstellt:
   Für alle Hosts:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `tar checksum`-Dateien
   `<hostname-IPaddress>-network.info.txt`
   Für Security Analytics-Server:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `<hostname-IPaddress>-mongodb.tar.gz`
   `tar checksum`-Dateien
   `<hostname-IPaddress>-network.info.txt`
   Für ESA-Hosts:
   `<hostname-IPaddress>-root.tar.gz`
   `<hostname-IPaddress>-backup.tar.gz`
   `<hostname-IPaddress>-mongodb.tar.gz`
   `<hostname-IPaddress>-controldata-mongodb.tar.gz`
   `tar checksum`-Dateien
   `<hostname-IPaddress>-network.info.txt`

Die archivierten Dateien befinden sich im Verzeichnis `/var/netwitness/database/nw-backup`. Wenn eine der TAR-Dateien kleiner als erwartet angezeigt wird, öffnen Sie sie, um sicherzustellen, dass die Dateien korrekt gesichert wurden.

Aufgaben nach dem Backup

Aufgabe 1: Speichern einer Kopie der Datei `all-systems` und der TAR-Backupdateien

Erstellen Sie Kopien der Datei `all-systems`, der Datei `all-systems-master-copy` und der TAR-Backupdateien und legen Sie die Kopien an einem sicheren Speicherort ab. Sie können diese Dateien nicht erneut generieren, nachdem Sie das Upgrade für Security Analytics-Server (insbesondere den Admin-Service) auf 11.1 durchgeführt haben.

Aufgabe 2: Sicherstellen, dass die erforderlichen Backupdateien generiert wurden

Nach Ausführung der Backupskripte werden mehrere Dateien generiert. Diese Dateien sind für den 11.1-Upgradeprozess erforderlich. Bevor Sie den Upgradeprozess starten, müssen Sie sicherstellen, dass die erforderlichen Backupdateien auf den Hosts vorhanden sind, die Sie aktualisieren möchten. Sie müssen die folgenden Aufgaben ausführen.

Die folgenden Dateien werden von den Backupskripten auf allen Hosts erzeugt:

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Zusätzlich zu den oben aufgeführten Dateien werden auch die folgenden Dateien auf dem Security Analytics-Server und ESA-Hosts erzeugt:

- `<hostname>-<host IP address>-mongodb.tar.gz`
- `<hostname>-<host IP address>-mongodb.tar.gz.sha256`

Das Backupskript erzeugt auch die folgenden `controldata-mongodb.tar.gz`-Dateien.

Hinweis: Das Backupskript kopiert die folgenden Dateien von allen ESA-Hosts in den Backuppfad des Security Analytics-Servers.

- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz
- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256

Aufgabe 3: (Bedingungsabhängig) Für mehrere ESA-Hosts – Kopieren der `mongodb tar` -Dateien zum primären ESA-Host

Wenn in Ihrem Unternehmen mehrere ESA-Hostsysteme vorhanden sind, kopieren Sie die folgenden zwei Dateien von jedem ESA-Host in das Verzeichnis `/opt/rsa/database/nw-backup/` auf dem primären ESA-Host-System (also dem Host, auf dem der Context Hub-Service ausgeführt wird):

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Aufgabe 4: Sicherstellen, dass alle erforderlichen Backupdateien auf jedem Host vorhanden sind

Bevor Sie ein Upgrade auf 11.1 durchführen, stellen Sie sicher, dass die entsprechenden Dateien auf den Hosts vorhanden sind, für die Sie das Upgrade durchführen, wie in den folgenden Listen beschrieben.

Sie sollten sich die standardmäßigen Speicherorte für das Backup notieren, damit der Benutzer weiß, wo diese abgelegt sind, und er sie überprüfen kann.

Hinweis: Die Standardpfade für Backupdateien lauten wie folgt:
- Security Analytics-Server:`/var/netwitness/database/nw-backup`
- ESA-Hosts:`/opt/rsa/database/nw-backup`
- Malware Analysis-Hosts: `/var/lib/rsamalware/nw-backup`

Erforderliche Dateien für NetWitness-Server

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256

Erforderliche Dateien für ESA-Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

Erforderliche Dateien für alle anderen Hosts

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

Hinweis: Die folgenden Dateien befinden sich in der TAR-Datei <hostname>-<host-IP-address>-backup.tar.gz auf allen Hosts:
appliance_info
service_info

Hinweis: Die Pfade zum Speicherort der Backup- und Wiederherstellungsdateien für iptables, NAT-Konfigurationen, Benutzerkonten und Crontab-Einträge sind in der folgenden Liste aufgeführt:
Backuppfade:
`BUPATH=/opt/rsa/database/nw-backup` für die ESA Correlation Engine
`BUPATH=/var/lib/rsamalware/nw-backup` für den Malware-Service
`BUPATH=/var/netwitness/database/nw-backup` für alle anderen Services
Wiederherstellungspfade:
`BUPATH/restore/etc/sysconfig` für iptable-Regeln
`BUPATH/restore/etc/sysconfig` für NAT-Konfigurationen
`BUPATH/restore/etc` für Crontab-Einträge
`BUPATH/restore/etc` für Benutzerkonten (Benutzer befinden sich der Datei `passwd` und Gruppen in der Datei `group`. Diese werden während des Upgrades nicht wiederhergestellt, können aber manuell wiederhergestellt werden.)
`BUPATH/restore/etc/ntp.conf` für NTP-Konfigurationen (sie müssen über die Benutzeroberfläche von NetWitness Suite wiederhergestellt werden)

Upgradeaufgaben

Dieses Thema enthält die Aufgaben, die Sie zur Aktualisierung von Security Analytics 10.6.5.x auf NetWitness Suite 11.1 ausführen müssen.

Achtung: 1.) Sichern Sie Ihre Security Analytics 10.6.5.x-Daten, bevor Sie ein Upgrade auf NetWitness Suite 11.1 durchführen.
2). Führen Sie das Backup für jede Phase unmittelbar vor dem Upgrade der Hosts so durch, dass das Wiederherstellen von veralteten Daten vermieden wird.
3.) Dieser Leitfaden gilt ausschließlich für Upgrades von physischen Hosts. Wenn sich in Ihrer Bereitstellung sowohl physische als auch virtuelle Hosts befinden, finden Sie im *RSA NetWitness® Suite 11.1 Upgradehandbuch für virtuelle Hosts* eine Beschreibung der Schritte für Upgrades von virtuellen Hosts. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Es gibt zwei Phasen, die in der angegebenen Reihenfolge beendet werden müssen.

- Phase 1: Upgrade von SA-Server, Event Stream Analysis (ESA) und Malware Analysis-Hosts

  Hinweis: Dies betrifft Event Stream Analysis. Wenn Sie C2-Module in 10.6.5.x aktiviert haben, gehen die Module nach dem Upgrade des Event Stream Analysis-Services auf Version 11.1 in eine Aufwärmphase über und sind erst verfügbar, wenn diese abgeschlossen ist.

- Phase 2: Upgrade für alle anderen Hosts durchführen

Phase 1: Upgrade von SA-Server, Event Stream Analysis, Malware Analysis-Hosts sowie Broker oder Concentrator durchführen

Aufgabe 1: Upgrade des 10.6.5.x SA-Servers auf 11.1 NW-Server durchführen

Befolgen Sie die Anweisungen unter Upgrade eines 10.6.5.x SA-Serverhosts auf 11.1 NW-Serverhost.

Aufgabe 2: Upgrade von 10.6.5.x ESA auf 11.1 durchführen

Achtung: Wenn Sie C2-Module in 10.6.5.x aktiviert haben, gehen die Module nach dem Upgrade des Event Stream Analysis-Service auf Version 11.1 in eine Aufwärmphase über und sind nicht verfügbar, bis diese abgeschlossen ist.

Befolgen Sie die Anweisungen unter Upgrade eines 10.6.5.x Nicht-SA-Serverhosts auf 11.1, um Ihre ESA-Hosts zu aktualisieren.

1. Erstellen Sie das Basis-Image auf Ihrem primären ESA-Host, richten Sie ihn über das Setup-Programm ein und installieren Sie **ESA Primary** auf dem Host in der Benutzeroberfläche der Ansicht **Admin Hosts**.

   Hinweis: Wenn Sie in Ihrem Unternehmen über mehrere ESA-Hosts verfügen, müssen Sie zunächst ein Upgrade für den primären ESA-Host durchführen, in dem sich alle `mongodb` (Mongo-Datenbank)-TAR-Backupdateien befinden, bevor Sie die sekundären ESA-Hosts aktualisieren.

2. (Bedingungsabhängig) Wenn Sie einen sekundären ESA-Host haben, erstellen Sie das Basis-Image auf dem sekundären ESA-Host, richten Sie ihn über das Setup-Programm ein und installieren Sie **ESA Secondary** auf dem Host in der Benutzeroberfläche der Ansicht **Admin Hosts**.

Aufgabe 3: Upgrade von Malware Analysis 10.6.5.x auf 11.1 durchführen

Befolgen Sie die Anweisungen unter Upgrade eines 10.6.5.x Nicht-SA-Serverhosts auf 11.1.

Aufgabe 4: Upgrade von Broker 10.6.5.x oder Concentrator 10.6.5.x auf 11.1

Befolgen Sie die Anweisungen unter Upgrade eines 10.6.5.x Nicht-SA-Serverhosts auf 11.1.

Hinweis: Wenn Sie keinen Broker haben, aktualisieren Sie Ihre Concentrator-Hosts. Der 11.1 NW-Server kann für die neuen Funktionen von Investigate nicht mit 10.6.5.x Core-Services kommunizieren. Deshalb müssen Sie die Broker- oder Concentrator-Hosts in Phase 1 aktualisieren.

Phase 2: Upgrade für alle anderen Hosts durchführen

In Anhang B: Beenden und Neustarten der Datenerfassung und -aggregation finden Sie Anweisungen zum Beenden und Neustarten der Datenerfassung und Aggregation beim Upgrade der Decoder-, Concentrator- und Protokollsammlungshosts.

Decoder und Concentrator-Hosts

1. Beenden Sie die Datenerfassung und -aggregation.
2. Befolgen Sie die Anweisungen unter Upgrade eines Nicht-NW-Serverhosts auf 11.1.
3. Starten Sie die Datenerfassung und -aggregation neu.

Log Decoder-Host

1. Stellen Sie sicher, dass Sie Log Collector vorbereitet haben, wie in „Log Collector (LC) und Virtual Log Collector (VLCs): prepare-for-migrate.sh ausführen“ in den Anweisungen zum Backup beschrieben.
2. Beenden Sie die Datenerfassung auf dem Log Decoder.
3. Befolgen Sie die Anweisungen unter Upgrade eines Nicht-NW-Serverhosts auf 11.1.
4. Starten Sie die Datenerfassung auf dem Log Decoder neu.

Hinweis: Starten Sie nach dem Upgrade die Protokollsammlung nach Abschluss von Aufgabe 27: Aktualisieren von Incident-Regeln, die in der Domain in der Upgrade-Vorbereitungsaufgabe für die Übereinstimmungsbedingungen identifiziert wurden in den **Aufgaben nach dem Upgrade** zurück.

Virtual Log Collector-Host

1. Stellen Sie sicher, dass Sie Virtual Log Collector vorbereitet haben, wie in „Log Collector (LC) und Virtual Log Collector (VLCs): prepare-for-migrate.sh ausführen“ in den Anweisungen zum Backup beschrieben.
2. Sichern Sie Ihren 10.6.5.x VLC durch Bearbeiten der `all-systems`-Datei auf dem Host, auf dem Sie das Backup durchgeführt haben.
   a. Vergewissern Sie sich, dass die Datei `all-systems` diese Informationen beinhaltet, bevor Sie diesen Schritt ausführen.
      `vlc,<host-name>,<IP-address>,<UUID>,10.6.5.x`
   b. Führen Sie den folgenden Befehl aus, um ein Backup zu erstellen:
      `./nw-backup.sh -u`
      Unter Anweisungen zum Backup finden Sie detaillierte Verfahren, um den Host zu sichern.
3. Stellen Sie sicher, dass der Backuphost das VLC-Backup im folgenden Format enthält.
   `<hostname>-<IPaddress>-root.tar.gz`
   `<hostname>-<IPaddress>-root.tar.gz.sha256`
   `<hostname>-<IPaddress>-backup.tar.gz`
   `<hostname>-<IPaddress>-backup.tar.gz.sha256`
   `<hostname-IPaddress>-network.info.txt`
   `all-systems-master-copy`
4. Schalten Sie den 10.6.5.x VLC aus, damit eine neue 11.1 VM mit derselben Netzwerkkonfiguration erstellt werden kann.

5. Stellen Sie einen neuen NetWitness 11.1 Nicht-NW-Serverhost mithilfe der 11.1 NetWitness Suite-OVA bereit.
6. Stellen Sie eine Verbindung zur VM-Konsole des neuen VLC her.
7. Aktualisieren Sie die Netzwerkkonfiguration, sodass sie dem 10.6.5.x VLC entspricht. Diese Informationen werden in der `<hostname-IPaddress>-network.info.txt` 10.6.5.x VLC-Backupdatei gespeichert.

   Hinweis: Stellen Sie sicher, dass IPv6 deaktiviert ist.

   a. Bearbeiten Sie die Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` und aktualisieren Sie die Einstellungen. Der Inhalt von `ifcfg-eth0` sollte wie folgt lauten:

   ```
   TYPE=Ethernet
   DEFROUTE=yes
   NAME=eth0
   UUID=<uuid>
   DEVICE=eth0
   DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
   DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
   BOOTPROTO=static
   IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
   NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
   GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
   NM_CONTROLLED=no
   ONBOOT=yes
   ```

   b. Senden Sie die folgende Befehlszeichenfolge:

   ```
   systemctl restart network.service
   ```

8. Erstellen Sie das Backupverzeichnis.

   ```
   # mkdir -p /var/netwitness/database/nw-backup/
   ```

9. Kopieren Sie das Backup aus dem Backuphost von `/var/netwitness/database/nw-backup` auf den neuen VLC in das Verzeichnis `/var/netwitness/database/nw-backup`.
10. Führen Sie die Schritte 2 bis einschließlich 12 in Upgrade eines 10.6.5.x Nicht-SA-Serverhosts auf 11.1 für den Rest der NetWitness Suite-Komponenten aus. Stellen Sie sicher, dass Sie **Log Collector** für den Service in Schritt 12 auswählen.

Alle anderen 10.6.5.x Hosts auf 11.1

Befolgen Sie die Anweisungen unter Upgrade eines 10.6.5.x Nicht-SA-Serverhosts auf 11.1.

Upgrade des 10.6.5.x SA-Serverhosts auf den 11.1 NW-Serverhost

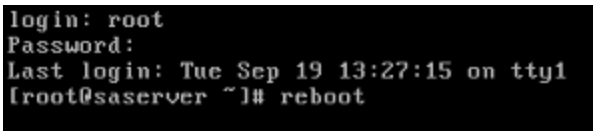
Stellen Sie sicher, dass Sie die 10.6.5.x-Daten für den SA-Serverhost gesichert haben. **Befolgen Sie die Anweisungen in Anweisungen zum Backup, um den Host zu sichern.**

Achtung: Führen Sie das Backup unmittelbar vor dem Upgrade der SA-Server auf 11.1 aus, damit die Daten so aktuell wie möglich sind. Sie müssen die **all-systems**-Datei vor dem Upgrade des SA-Servers erstellen, da dies nach dem Upgrade des SA-Servers auf 11.1 nicht mehr möglich ist.

Führen Sie die folgenden Schritte aus, um den 10.6.5.x SA-Serverhost auf den 11.1 NW-Serverhost zu aktualisieren.

1. Erstellen Sie ein Basis-Image auf dem Host.
   a. Verbinden Sie Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) mit dem Host. **Sie müssen den Build-Stick mit der Bezeichnung „OEMDRV“ verwenden.** Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Suite Build-Stick*.
      - Hypervisor-Installationen: Verwenden Sie das ISO-Image.
      - Physische Medien: Verwenden Sie die ISO-Datei, um startfähige Medien für Flash-Laufwerke mithilfe von Universal Netboot Installer (UNetbootin) oder einem anderen geeigneten Imaging-Tool zu erstellen. In den *Anweisungen zum RSA NetWitness® Suite Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks von der ISO-Datei. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.
      - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
        - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
        - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Datei.

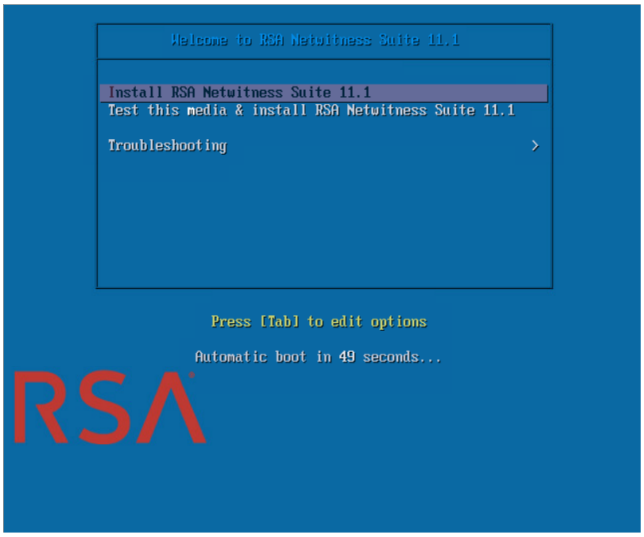
   b. Melden Sie sich beim Host an und starten Sie ihn neu.



   c. Wählen Sie während des Neustarts **F11** (Startmenü) aus, um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.
   Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü **Willkommen bei RSA NetWitness® Suite 11.1** angezeigt. Die

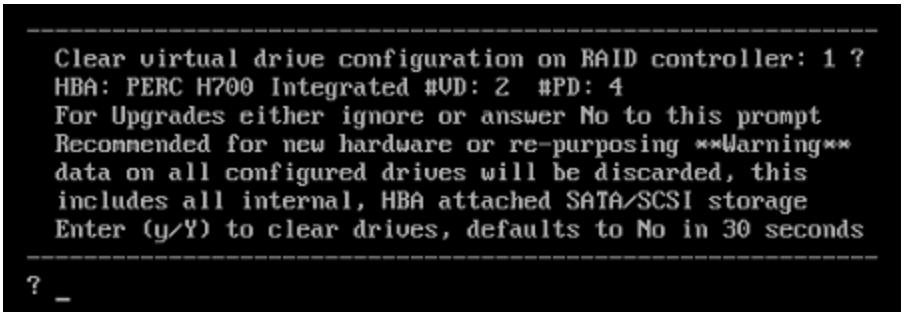
Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.

d. Wählen Sie **RSA NetWitness-Suite 11.1 installieren** (Standardauswahl) aus und drücken Sie die Eingabetaste.



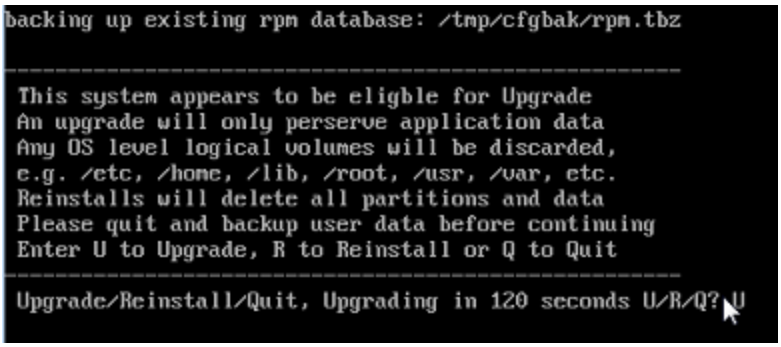
Das Installationsprogramm für das Betriebssystem wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten.

e. Geben Sie **n** (Nein) ein.
Die Standardaktion ist „Nein“. Wenn Sie also die Aufforderung ignorieren, wird innerhalb von 30 Sekunden „Nein“ ausgewählt und die Laufwerke werden nicht gelöscht.



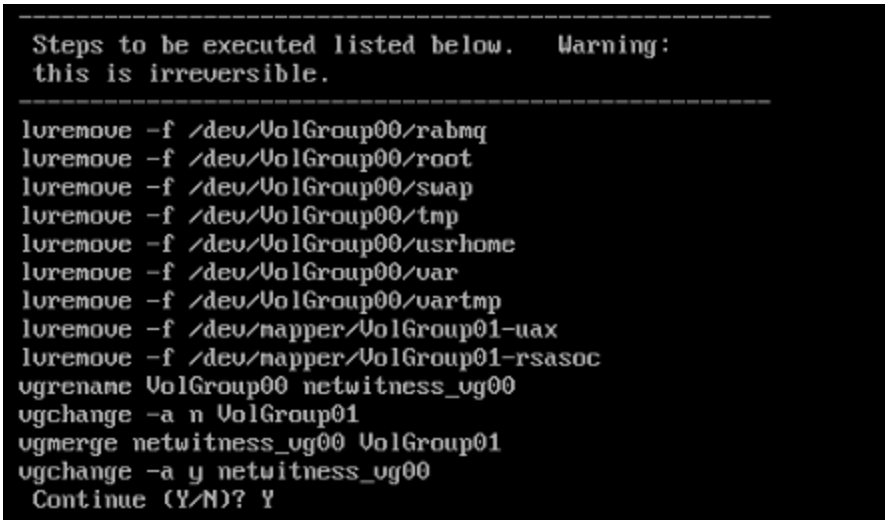
Die Eingabeaufforderung **Upgrade/Neuinstallation/Verlassen (U/R/Q)?** wird angezeigt.

f. Geben Sie **U** ein, um den Host zu aktualisieren.
Wenn Sie die Aufforderung ignorieren, wird nach 120 Sekunden U ausgewählt.



Es dauert einige Minuten, bis die CentOS7-Komponenten installiert sind. Das Installationsprogramm zeigt die Komponenten an, während sie installiert werden. Dies variiert je nach Appliance. Wenn die Installation von CentOS7 abgeschlossen ist, wird die Eingabeaufforderung **Fortfahren (J/N)?** angezeigt.

g. Geben Sie **J** ein und drücken Sie die **EINGABETASTE**, um zu bestätigen, dass Sie für diesen Host ein Upgrade durchführen möchten.



Das alte Betriebssystem wird entfernt. Die Warnung Fortfahren (J/N)? wird angezeigt.

h. Geben Sie **J** ein und drücken Sie die **EINGABETASTE**, um zu bestätigen, dass Sie das Betriebssystem ersetzen möchten.

Wenn das Upgrade auf CentOS7 durchgeführt wird, wird der Host automatisch neu gestartet und fordert Sie zur Anmeldung auf.

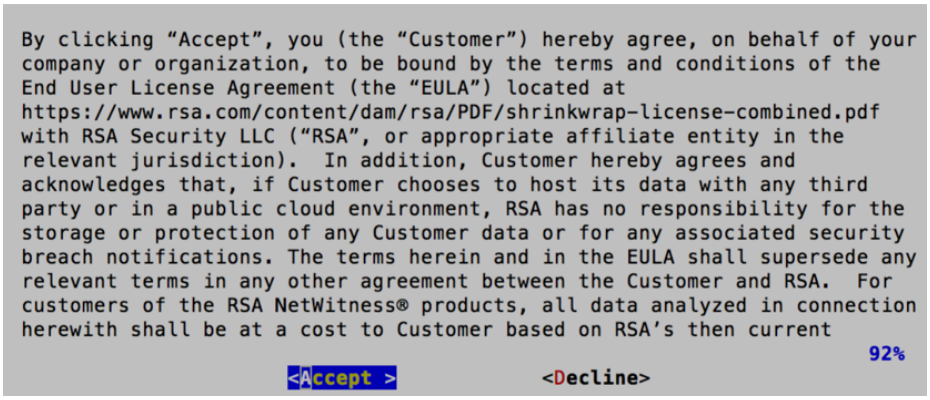
Achtung: Starten Sie die angeschlossenen Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) nicht neu.

i. Melden Sie sich mit den `root` -Anmeldedaten beim Host an.

2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.
   Dadurch wird das `nwsetup-tui` Setup-Programm gestartet und die EULA wird angezeigt.

   Hinweis: 1.) Wenn Sie durch die Eingabeaufforderungen des Setup-Programms navigieren, verwenden Sie die Pfeile nach unten und oben, um zwischen den Feldern zu wechseln, die Tabulatortaste, um zwischen den Befehlen zu wechseln (z. B. **<Ja>**, **<Nein>**, **<OK>** und **<Abbrechen>**. Drücken Sie die **EINGABETASTE**, um Ihre Befehlsantwort zu registrieren und mit der nächsten Eingabeaufforderung fortzufahren. 2.) Das Setup-Programm übernimmt das Farbschema des Desktops oder der Konsole, den bzw. die Sie für den Zugriff auf den Host verwenden.

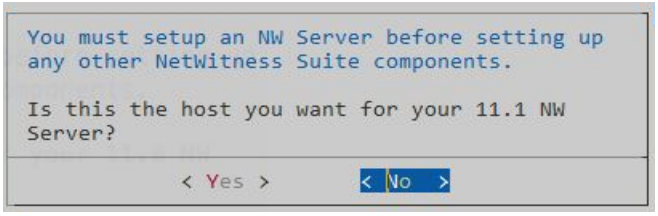
3. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.



   Es wird eine NW-Server-Aufforderung mit der Frage angezeigt, ob dies der Host ist, den Sie für Ihren 11.1 NW-Server verwenden möchten.

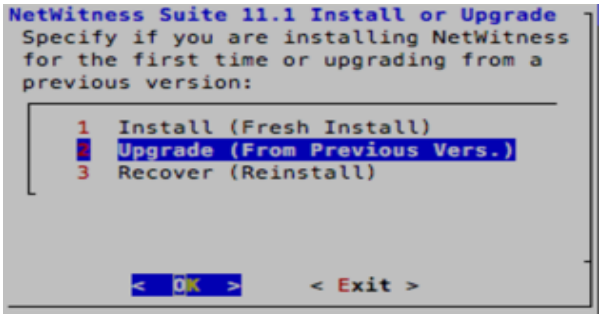
   Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm neu starten und alle nachfolgenden Schritte (2 bis 11) ausführen, um diesen Fehler zu korrigieren.

4. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.



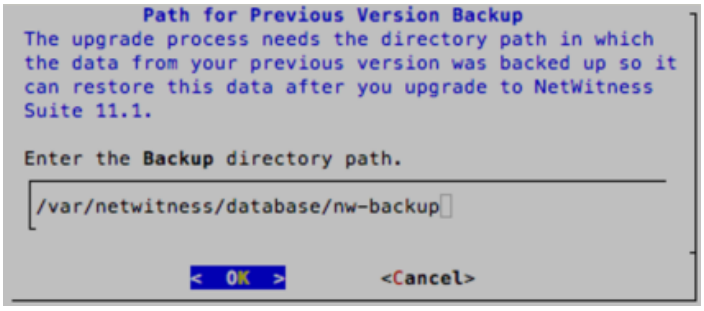
Wählen Sie **Nein** aus, wenn Sie den NW-Server bereits auf 11.1 aktualisiert haben.
Die Aufforderung **Installation** oder **Upgrade** wird angezeigt.

5. Wählen Sie mit dem Pfeil nach unten **2 Upgrade (von vorheriger Vers.)** aus, gehen Sie zu **OK** und drücken Sie die Eingabetaste.



Die Aufforderung zur Eingabe des Backuppfads wird angezeigt.

6. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, wenn Sie diesen Pfad behalten möchten. Wenn nicht, bearbeiten Sie den Pfad, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.



In dieser Tabelle werden die Backup- und Wiederherstellungspfade nach Host/Service aufgeführt.

Host	Backuppfad	Wiederherstellungspfad
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW-Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`

Host	Backuppfad	Wiederherstellungspfad
Alle anderen Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

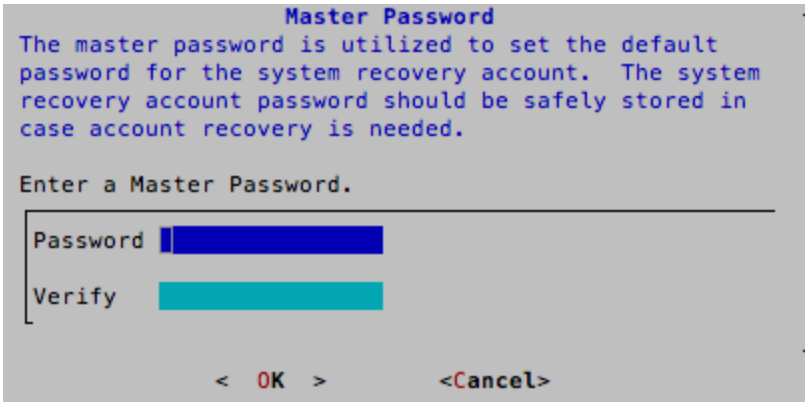
Die Aufforderung **Masterpasswort** wird angezeigt.

Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

- Symbole: ! @ # % ^ + ,
- Zahlen: 0-9
- Kleinbuchstaben: a-z
- Großbuchstaben: A-Z

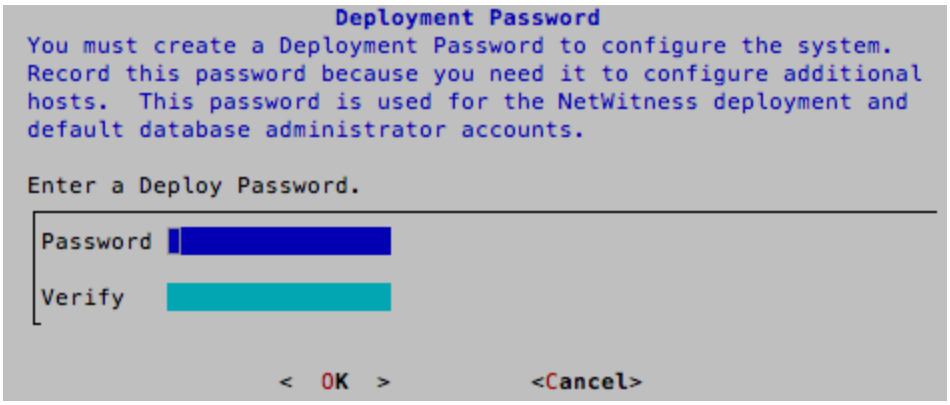
Beim Masterpasswort und Bereitstellungspasswort werden keine nicht eindeutigen Zeichen unterstützt. Beispiel:
Leerzeichen { } [ ] ( ) / \ ' " ` ~ ; : . < > -

7. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.



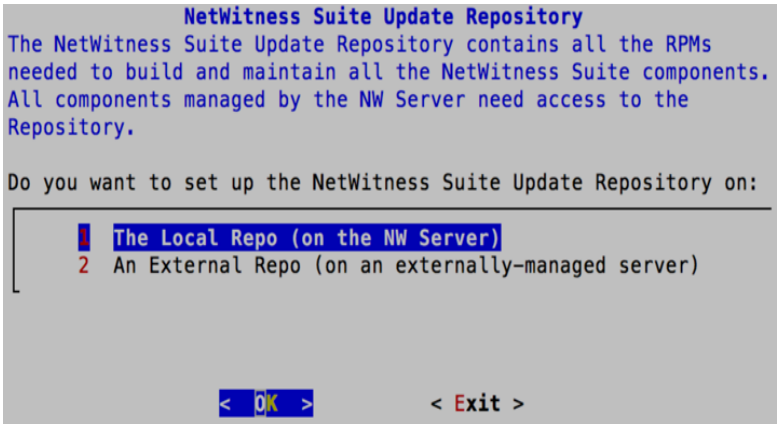
Die Aufforderung **Bereitstellungspasswort** wird angezeigt.

8. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.

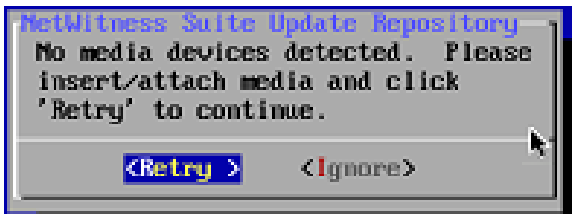


Die Eingabeaufforderung **Update-Repository** wird angezeigt.

9. Verwenden Sie die Pfeile nach oben und nach unten, um den Speicherort auszuwählen, von dem aus Sie Versionsaktualisierungen auf Ihre Hosts anwenden möchten, gehen Sie zu **OK** und drücken Sie die Eingabetaste.

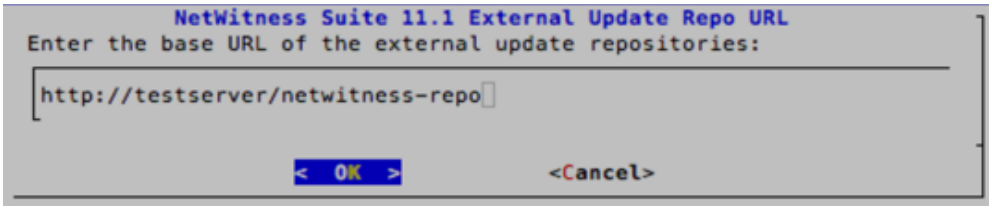


- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** stellt das Setup-Programm sicher, dass Sie die richtigen Medien mit dem Host verbunden haben (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen das Upgrade auf NetWitness Suite 11.1 abgerufen werden kann. Wenn das Programm die verbundenen Medien nicht finden kann, wird die folgende Aufforderung angezeigt.



- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositorys bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates. Anweisungen zum Erstellen dieses Repository und

der externen Repo-URL, damit Sie diese in die folgende Eingabeaufforderung eingeben können, finden Sie in Anhang D: Erstellen eines externen Repository.

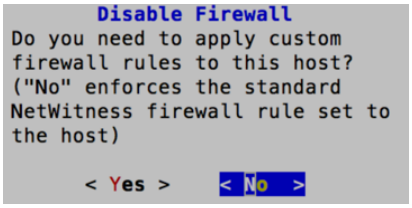


Geben Sie den Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**.

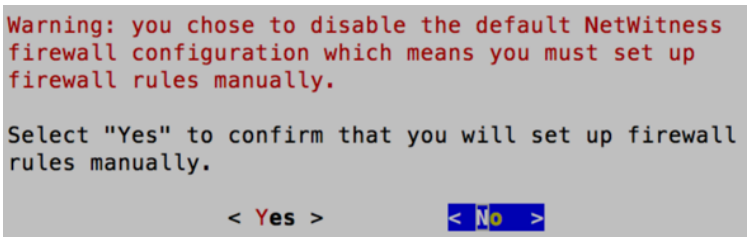
Anweisungen hierzu finden Sie unter „Einrichten eines externen Repository mit RSA und Betriebssystemupdates“ unter „Hosts und Services – Verfahren“ im *RSA NetWitness Suite – Leitfaden für die ersten Schritte mit Hosts und Services*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Die Aufforderung zur **Deaktivierung** oder Verwendung der Standardkonfiguration für **Firewalls** wird angezeigt.

10. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** und drücken die **EINGABETASTE**. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken die Eingabetaste.

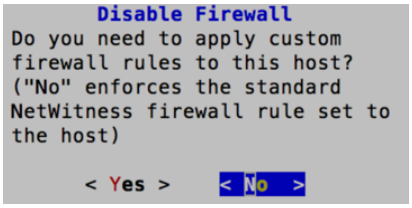


- Wenn Sie **Ja** ausgewählt haben, bestätigen Sie Ihre Auswahl.



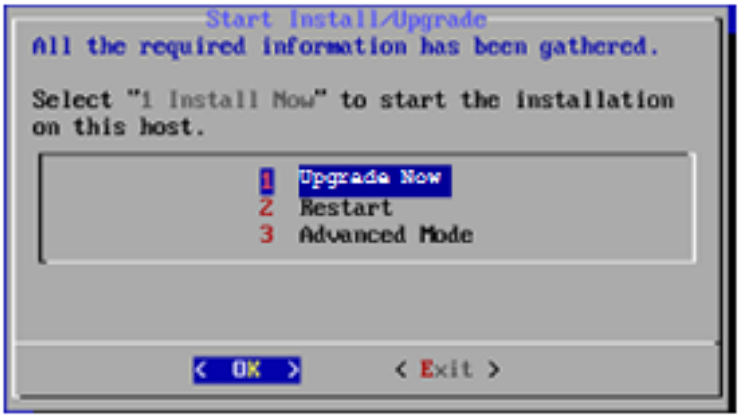
- Wenn Sie **Nein** ausgewählt haben, wird die Standardkonfiguration für Firewalls

angewendet.



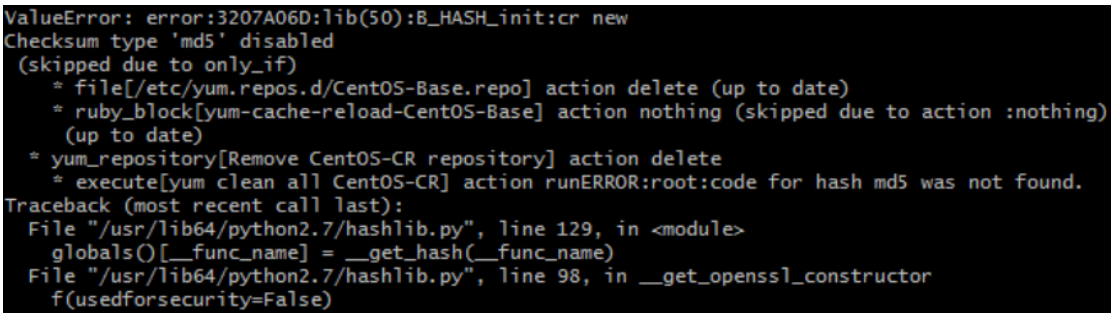
Die Aufforderung **Installieren** oder **Upgrade durchführen** wird angezeigt (**Wiederherstellen** gilt nicht für die Installation. Diese Option gilt für 11.1 Disaster Recovery).

11. Wählen Sie 1 **Upgrade jetzt durchführen** aus, gehen Sie zu **OK** und drücken Sie die Eingabetaste.



Wenn **Installation abgeschlossen** angezeigt wird, haben Sie den 10.6.5.x SA-Server auf den 11.1 NW-Server aktualisiert.

Hinweis: Ignorieren Sie Hashcodefehler wie die Fehler in der folgenden Abbildung, die angezeigt werden, wenn Sie den Befehl `nwsetup-tui` initiieren. Yum verwendet kein MD5 für Sicherheitsabläufe, sodass sie sich nicht auf die Sicherheit des Systems auswirken.



12. Schließen Sie die NW-Server ab, bevor Sie einen der Nicht-SA-Serverhosts auf 11.1 aktualisieren.

Upgrade eines 10.6.5.x Nicht-SA-Serverhost auf 11.1.

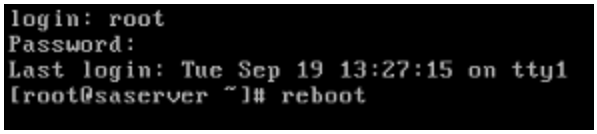
Stellen Sie sicher, dass Sie die 10.6.5.x-Daten für den Host gesichert haben. **Befolgen Sie die Anweisungen in** Anweisungen zum Backup**, um den Host zu sichern.**

Achtung: Führen Sie das Backup unmittelbar vor dem Upgrade des Hosts auf 11.1 aus, damit die Daten so aktuell wie möglich sind.

Führen Sie die folgenden Schritte aus, um einen 10.6.5.x Nicht-SA-Serverhost auf 11.1 zu aktualisieren.

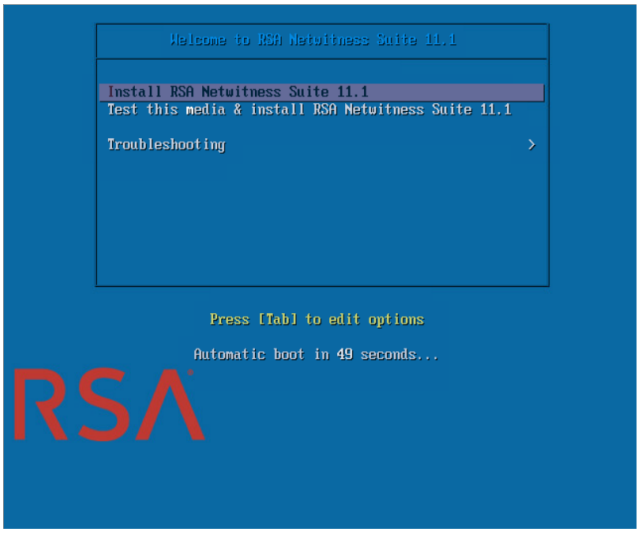
1. Erstellen Sie ein Basis-Image auf dem Host.
   a. Verbinden Sie Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) mit dem Host. Weitere Informationen finden Sie in den *Anweisungen zum RSA NetWitness Suite Build-Stick*.
      - Hypervisor-Installationen: Verwenden Sie das ISO-Image.
      - Physische Medien: Verwenden Sie die ISO-Datei, um startfähige Medien für Flash-Laufwerke mithilfe von Universal Netboot Installer (UNetbootin) oder einem anderen geeigneten Imaging-Tool zu erstellen. In den *Anweisungen zum RSA NetWitness® Suite Build-Stick* finden Sie Informationen zum Erstellen eines Build-Sticks aus dem ISO-Image. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.
      - iDRAC-Installationen – der Typ der virtuellen Medien lautet:
        - **Virtuelles Diskettenlaufwerk** für zugeordnete Flash-Laufwerke
        - **Virtuelle CD** für zugeordnete optische Mediengeräte oder ISO-Datei.

   b. Melden Sie sich beim Host an und starten Sie ihn neu.



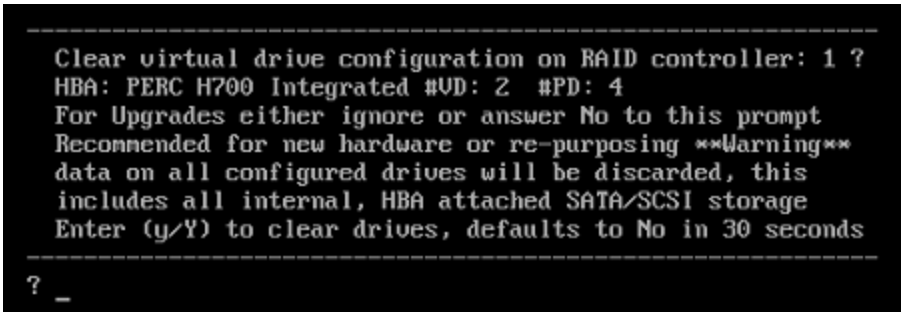
   c. Wählen Sie während des Neustarts **F11** (Startmenü) aus, um ein Startgerät auszuwählen und von den verbundenen Medien zu starten.
   Nach einigen Systemprüfungen während des Startvorgangs wird das folgende Installationsmenü **Willkommen bei RSA NetWitness® Suite 11.1** angezeigt. Die Grafiken im Menü werden anders dargestellt, wenn Sie ein physisches USB-Flash-Medium verwenden.

d. Wählen Sie **RSA NetWitness-Suite 11.1 installieren** (Standardauswahl) aus und drücken Sie die Eingabetaste.



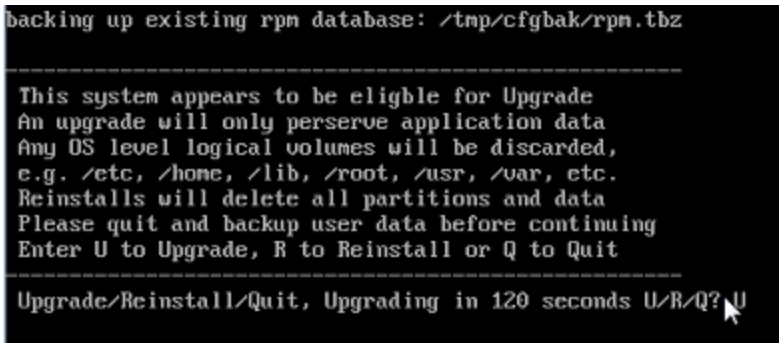
Das Installationsprogramm für das Betriebssystem wird ausgeführt. Es wird bei der Eingabeaufforderung **j/J eingeben, um Laufwerke zu löschen** angehalten.

e. Geben Sie **n** (Nein) ein.
Die Standardaktion ist **Nein**. Wenn Sie also die Aufforderung ignorieren, wird innerhalb von 30 Sekunden **Nein** ausgewählt und die Laufwerke werden nicht gelöscht.



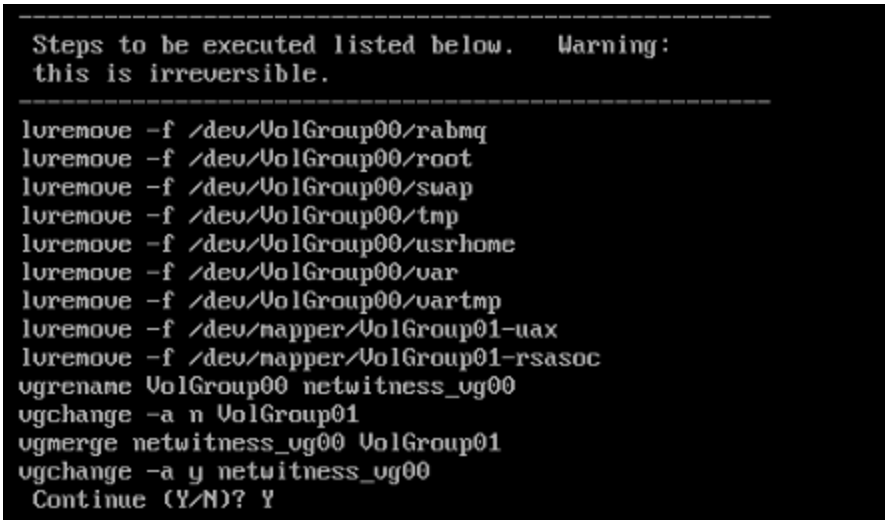
Die Eingabeaufforderung **Upgrade/Neuinstallation/Quit (U/N/Q?)** wird angezeigt.

f. Geben Sie **U** ein, um den Host zu aktualisieren.
Wenn Sie die Aufforderung ignorieren, wird nach 120 Sekunden **U** ausgewählt.



Es dauert einige Minuten, bis die CentOS7-Komponenten installiert sind. Das Installationsprogramm zeigt die Komponenten an, während sie installiert werden. Dies variiert je nach Appliance. Wenn die Installation von CentOS7 abgeschlossen ist, wird die Eingabeaufforderung **Fortfahren (J/N)?** angezeigt.

g. Geben Sie **J** ein und drücken Sie die Eingabetaste, um zu bestätigen, dass Sie diesen Host aktualisieren möchten.



Das alte Betriebssystem wird entfernt. Die Warnung Fortfahren (J/N)? wird angezeigt.

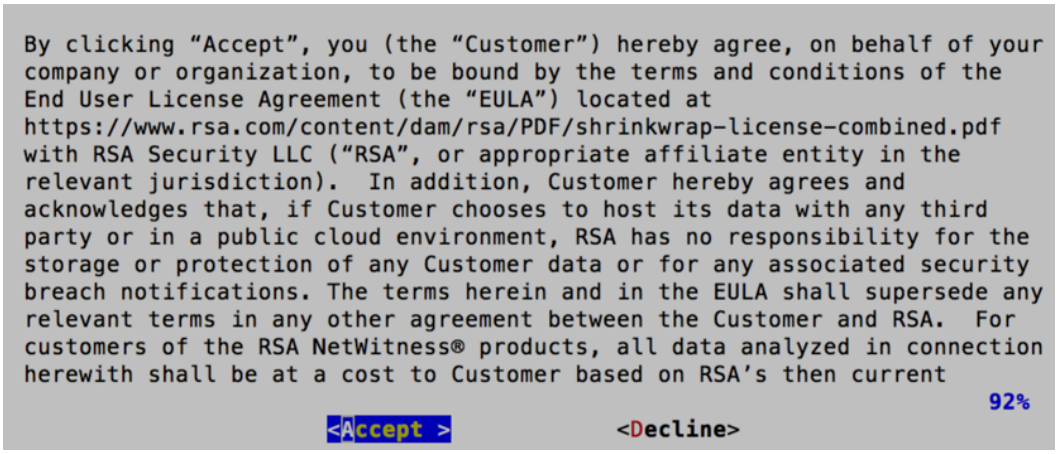
h. Geben Sie **J** ein und drücken Sie die **EINGABETASTE**, um zu bestätigen, dass Sie das Betriebssystem ersetzen möchten.

Wenn das Upgrade auf CentOS7 durchgeführt wird, wird der Host automatisch neu gestartet und fordert Sie zur Anmeldung auf.

Achtung: Starten Sie die angeschlossenen Medien (Medien mit der ISO-Datei, z. B. ein Build-Stick) nicht neu.

i. Melden Sie sich mit den `root`-Anmeldedaten beim Host an.

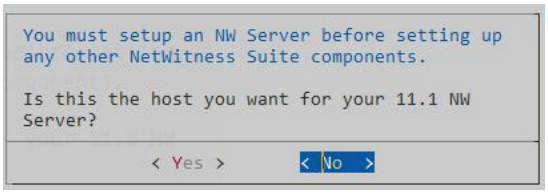
2. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.
   Dadurch wird das `nwsetup-tui` Setup-Programm gestartet und die EULA wird angezeigt.
3. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.



   Es wird eine Aufforderung mit der Frage angezeigt, ob dies der Host ist, den Sie für Ihren 11.1 NW-Server verwenden möchten.

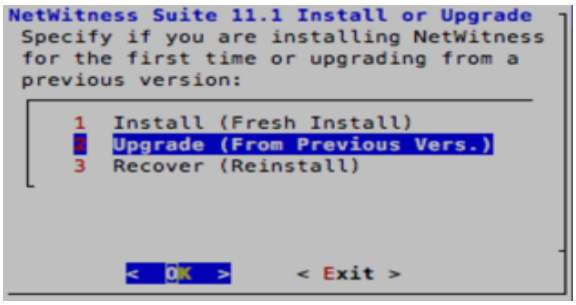
   Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Upgrade abschließen, müssen Sie das Setup-Programm neu starten und alle Schritte (2 bis 11) unter Upgrade des 10.6.5.x SA-Serverhosts auf den 11.1 NW-Serverhost ausführen, um diesen Fehler zu korrigieren.

4. Gehen Sie zu **Nein** und drücken Sie die **EINGABETASTE**.



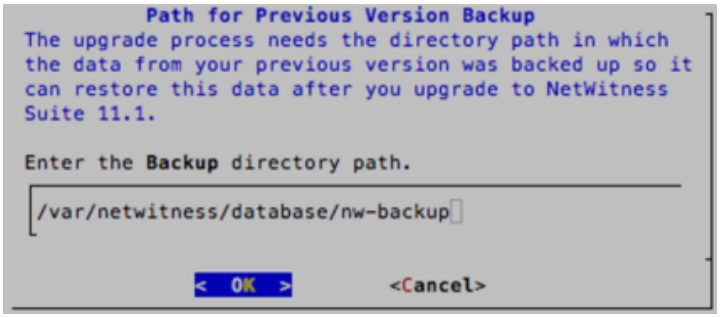
   Die Aufforderung **Installation** oder **Upgrade** wird angezeigt.

5. Wählen Sie mit dem Pfeil nach unten **2 Upgrade (von vorheriger Vers.)** aus, gehen Sie zu **OK** und drücken Sie die Eingabetaste.



Die Aufforderung zur Eingabe des Backuppfads wird angezeigt.

6. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, wenn Sie diesen Pfad behalten möchten. Wenn nicht, bearbeiten Sie den Pfad, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.



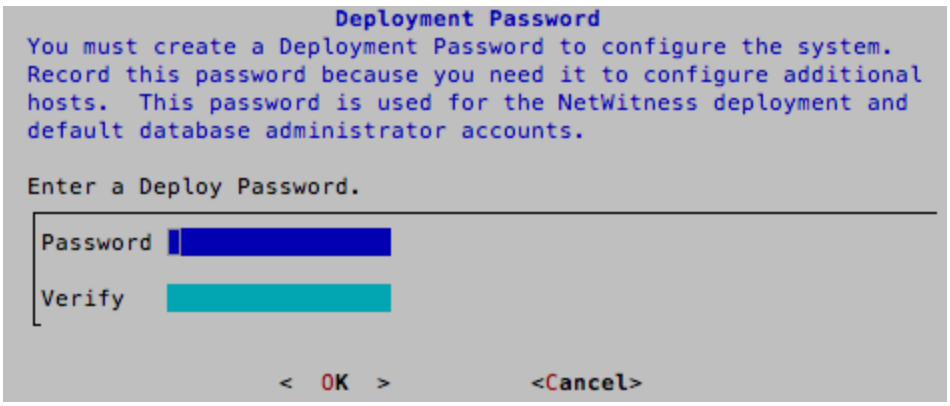
In dieser Tabelle werden die Backup- und Wiederherstellungspfade nach Host/Service aufgeführt.

Host	Backuppfad	Wiederherstellungspfad
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW-Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
Alle anderen Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Die Aufforderung **Bereitstellungspasswort** wird angezeigt.

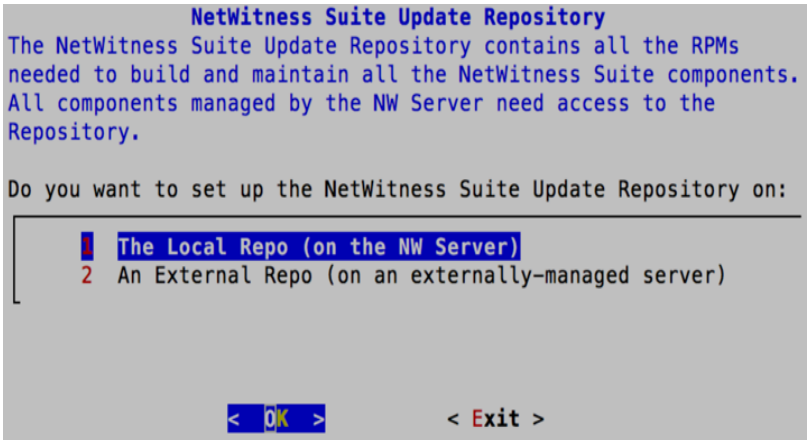
Hinweis: Sie müssen das gleiche Bereitstellungspasswort verwenden, das Sie beim Upgrade des NW-Servers verwendet haben.

7. Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.



Die Eingabeaufforderung **Update-Repository** wird angezeigt.
Wählen Sie für alle Hosts das gleiche Repository aus, das Sie beim Upgrade des NW-Serverhosts ausgewählt haben.

8. Verwenden Sie die Pfeile nach oben und nach unten, um den Speicherort auszuwählen, von dem aus Sie Versionsaktualisierungen auf Ihre Hosts anwenden möchten (z. B. **1 Das lokale Repository (auf dem NW-Host)**, gehen Sie zu **OK** und drücken Sie die Eingabetaste .

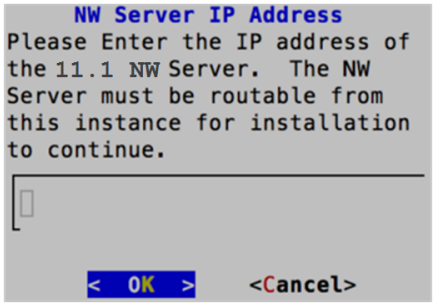


- Bei Auswahl von **1 Das lokale Repository (auf dem NW-Server)** stellt das Setup-Programm sicher, dass Sie die richtigen Medien mit dem Host verbunden haben (Medien mit der ISO-Datei, z. B. ein Build-Stick), von denen das Upgrade auf NetWitness Suite 11.1 abgerufen werden kann.
- Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe einer URL aufgefordert. Die Repositorys bieten Ihnen Zugriff auf

RSA-Updates und CentOS-Updates. Geben Sie den Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**. Die Repositorys bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates. Anweisungen zum Erstellen dieses Repository und der externen Repo-URL, damit Sie diese in die folgende Eingabeaufforderung eingeben können, finden Sie in Anhang D: Erstellen eines externen Repository.

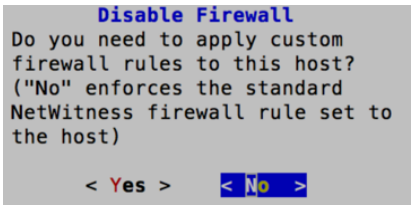
Die Aufforderung zur Eingabe der **IP-Adresse des NW-Servers** wird angezeigt.

9. Geben Sie die IP-Adresse des NW-Servers ein, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

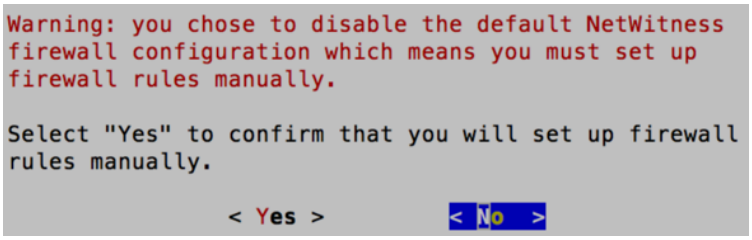


Die Aufforderung zur Deaktivierung oder Verwendung der Standardkonfiguration für Firewalls wird angezeigt.

10. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** und drücken die **EINGABETASTE**. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken die **EINGABETASTE**. Das folgende Beispiel zeigt **Nein** - Standardkonfiguration für Firewalls ausgewählt.



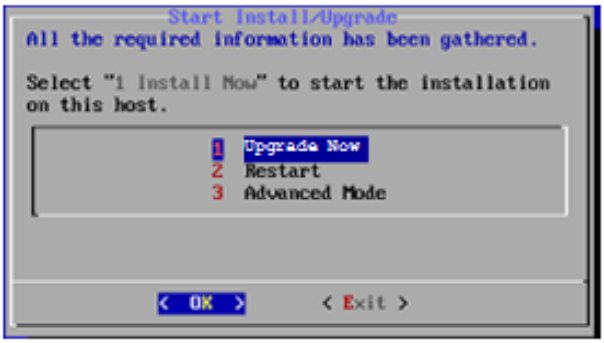
- Wenn Sie **Ja** ausgewählt haben, bestätigen Sie Ihre Auswahl.



- Wenn Sie **Nein** ausgewählt haben, wird die Standardkonfiguration für Firewalls angewendet.

Die Aufforderung **Installieren** oder **Upgrade durchführen** wird angezeigt (**Wiederherstellen** gilt nicht für die Installation. Diese Option gilt für 11.1 Disaster Recovery.).

11. Wählen Sie 1 **Upgrade jetzt durchführen** aus, gehen Sie zu **OK** und drücken Sie die Eingabetaste.



Wenn **Installation abgeschlossen** angezeigt wird, haben Sie den Host auf Version 11.1 aktualisiert.

12. Installieren Sie den Service auf diesem Host:

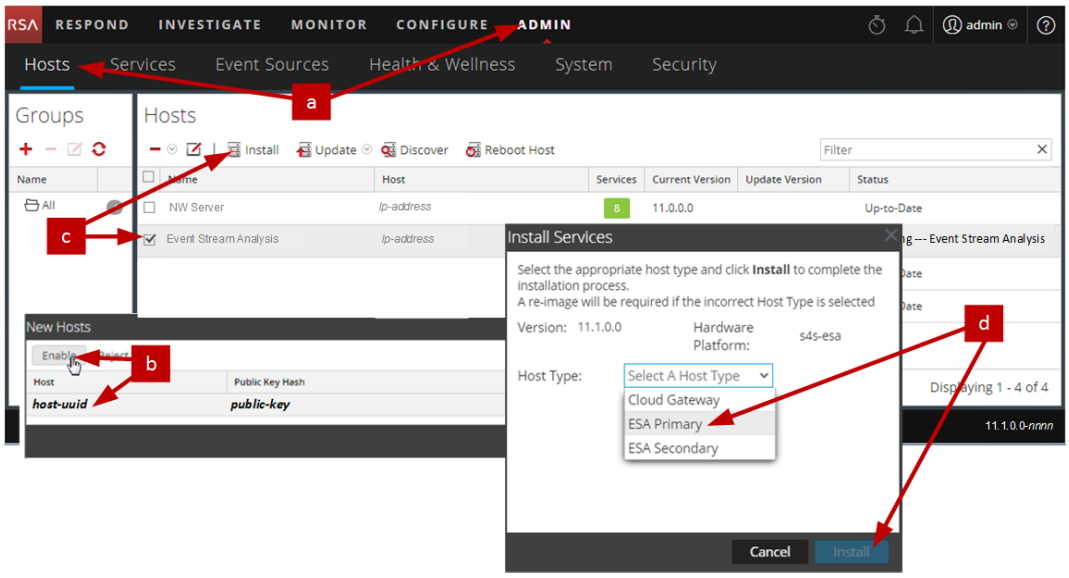
    a. Melden Sie sich bei NetWitness Suite an und klicken Sie auf **ADMIN** > **Hosts**.
    Das Dialogfeld **Neue Hosts** wird angezeigt; die Ansicht **Hosts** ist im Hintergrund abgeblendet.

    Hinweis: Wenn das Dialogfeld **Neue Hosts** nicht angezeigt wird, klicken Sie in der Symbolleiste der Ansicht „Hosts“ auf **Erkennen**.

    b. Klicken Sie im Dialogfeld **Neue Hosts** auf den Host und anschließend auf **Aktivieren**.
    Das Dialogfeld **Neue Hosts** wird geschlossen und der Host wird in der Ansicht **Hosts** angezeigt.

    c. Wählen Sie diesen Host (z. B. **Event Stream Analysis**) in der Ansicht **Hosts** aus und klicken Sie auf Install
    Das Dialogfeld **Services installieren** wird angezeigt.

    d. Wählen Sie den entsprechenden Service (z. B. **ESA Primary**) aus und klicken Sie auf **Installieren**.



Sie haben das Upgrade des Nicht-NW-Serverhosts in NetWitness Suite abgeschlossen

Hinweis: Wenn Sie einen Host für Respond von 10.6.5.x auf 11.1 aktualisieren, dauert es eine Weile, bis Respond wieder online verfügbar ist. Dies liegt daran, dass Respond während der Wiederherstellung Daten indexiert. Die Dauer hängt von der Größe der Daten in der Mongo-Datenbank ab.

Aktualisieren oder Installieren der Legacy-Windows-Sammlung

Siehe *Leitfaden RSA NetWitness Legacy Windows Collection*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Hinweis: Starten Sie nach dem Aktualisieren oder Installieren der Legacy Windows Collection das System neu, um sicherzustellen, dass Log Collection korrekt funktioniert.

Aufgaben nach dem Upgrade

Dieses Thema enthält die Aufgaben, die Sie nach der Aktualisierung Ihrer Hosts von 10.6.5.x auf 11.1 durchführen müssen. Diese Aufgaben sind nach den folgenden Kategorien unterteilt.

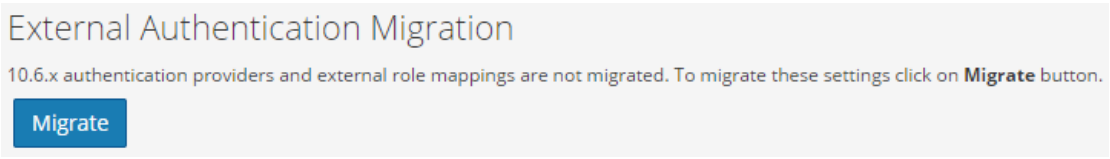
- NW-Server
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Untersuchen
- Protokollsammlung
- Reporting Engine
- Respond
- SecOps Manager (RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management und RSA Archer Issues Management)
- Warehouse Connector
- Backup

NW-Server

Aufgabe 1: Migrieren von Active Directory (AD)

Wenn Sie sich das erste Mal bei der NetWitness Suite 11.1-Benutzeroberfläche anmelden, müssen Sie auf die Schaltfläche „Migrieren“ klicken, um die Migration von AD abzuschließen.

1. Melden Sie sich bei NetWitness Suite 11.1 mit Ihren `admin user`-Anmeldedaten an.
2. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **SICHERHEIT** aus und klicken Sie auf die Registerkarte **Einstellungen**.
   Das folgende Dialogfeld wird angezeigt:

3. Klicken Sie auf **Migrieren**.
   Die Migration ist abgeschlossen und das Dialogfeld wird geschlossen.

Aufgabe 2: Ändern der migrierten AD-Konfiguration, um das Zertifikat hochzuladen

Wenn Sie die Authentifizierung über einen Active Directory-Server durchführen und in 10.6.5.x für die AD-Verbindung SSL aktiviert haben, müssen Sie die migrierte AD-Konfiguration ändern, um das Active Directory-Serverzertifikat hochzuladen.

Gehen Sie wie folgt vor, um die migrierte Active Directory-Konfiguration zum Hochladen des Zertifikats zu ändern.

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **Sicherheit** aus und klicken Sie auf die Registerkarte **Einstellungen**.
2. Wählen Sie unter **Active Directory-Einstellungen** eine AD-Konfiguration aus und klicken Sie auf .

   Das Dialogfeld „Konfiguration bearbeiten“ wird angezeigt.
3. Navigieren Sie zum Feld **Zertifikatdatei**, klicken Sie auf **Durchsuchen** und wählen Sie ein Zertifikat aus Ihrem Netzwerk aus.
4. Klicken Sie auf **Speichern**.

Aufgabe 3: Neukonfigurieren des Pluggable Authentication Module (PAM) in 11.1

Nach der Aktualisierung auf Version 11.1 müssen Sie das PAM neu konfigurieren. Anweisungen hierzu finden Sie unter „Konfigurieren der PAM-Anmeldefunktion“ im Handbuch *RSA NetWitness® Suite Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Beziehen Sie sich auf Ihre 10.6.5.x PAM-Konfigurationsdateien im Verzeichnis **/etc** Ihrer 10.6.5.x-Backupdaten.

Aufgabe 4: Wiederherstellen der NTP-Server

Sie müssen die Benutzeroberfläche von NetWitness Suite 11.1 verwenden, um NTP-Serverkonfigurationen wiederherzustellen. Informationen zu den NTP-Serverkonfigurationen finden Sie unter `$BUPATH/restore/etc/ntp.conf`. Verwenden Sie den Namen des NTP-Servers und den Hostnamen aus der Datei `/var/netwitness/restore/etc/ntp.conf`. Im *RSA NetWitness® Suite Systemkonfigurationsleitfaden* finden Sie unter „Konfigurieren von NTP-Servern“ detaillierte Anweisungen zum Hinzufügen von NTP-Servern. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 5: Wiederherstellen von Lizenzen für Umgebungen ohne Zugriff auf FlexNet Operations-On Demand

Wenn Ihre Umgebung keinen Zugriff auf FlexNet Operations-On Demand hat, müssen Sie Ihre NetWitness Suite-Lizenzen erneut herunterladen. Unter „Schritt 1. Registrieren von NetWitness Server“ im *Leitfaden zum Lizenzierungsmanagement für die RSA NetWitness Suite* finden Sie Anweisungen zum erneuten Herunterladen von Lizenzen. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

(Bedingungsabhängig) Aufgabe 6: Hinzufügen von benutzerdefinierten iptables, sofern die Standardkonfiguration der Firewall deaktiviert wurde

Während des Upgrades haben Sie die Möglichkeit, diese Regeln zu verwenden oder sie zu deaktivieren. Wenn Sie sie deaktivieren, befolgen Sie diese Anweisungen, um vom Benutzer verwaltete Firewallregelsätze auf allen Hosts zu erstellen, für welche die Firewall-Standardkonfiguration deaktiviert wurde.

Hinweis: `$BUPATH/restore/etc/sysconfig/iptables` und `$BUPATH/restore/etc/sysconfig/ip6tables` im Wiederherstellungsordner des Backups bieten Hinweise zum Update der `ip6tables`- und `iptables`-Dateien. Die `/etc/netwitness/firewall.cfg`-Datei enthält die `iptables`-Standardregeln für Firewalls.

1. Stellen Sie über SSH eine Verbindung mit jedem Host her und melden Sie sich mit Ihren Root-Anmeldedaten an.
2. Aktualisieren Sie die folgenden `ip6tables`- und `iptables`-Dateien mit den benutzerdefinierten Firewallregeln.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Laden Sie die `iptables`- und `ip6tables`-Services erneut.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Bedingungsabhängig) Aufgabe 7: Angeben der SSL-Ports, sofern keine vertrauenswürdigen Verbindungen eingerichtet wurden

Führen Sie diese Aufgabe nur dann durch, wenn keine vertrauenswürdigen Verbindungen eingerichtet wurden. Dies kann unter folgenden Bedingungen der Fall sein:

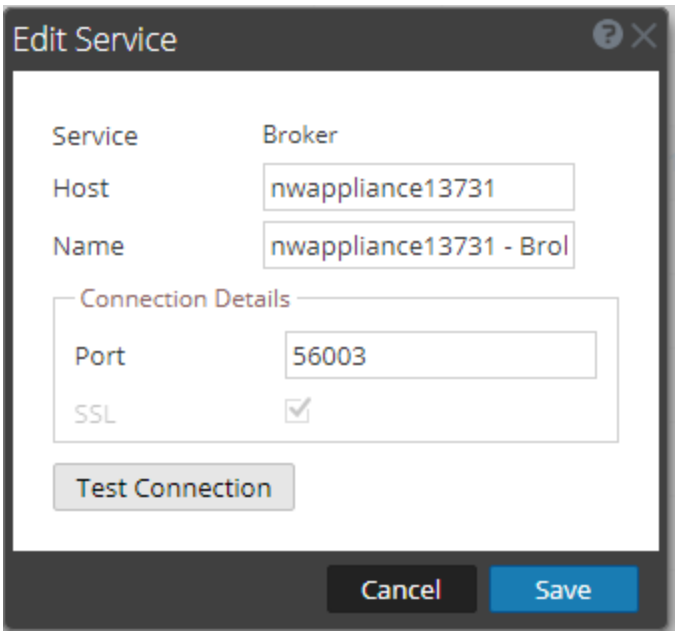
- Es wird ein Basis ISO-Image 10.3.2 oder früher verwendet.
- Das System wurde exklusiv mithilfe von RPMs aktualisiert, um Version 10.6.5.x zu erhalten.

NetWitness Suite 11.1 kann nicht mit den Core-Services für diese Kunden kommunizieren, da sie einen Nicht-SSL-Port 500XX verwenden. Sie müssen im Dialogfeld „Service bearbeiten“ die Core-Service-Ports auf einen SSL-Port aktualisieren.

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **Services** aus.
2. Wählen Sie jeden Core-Service aus und ändern Sie die Ports von Nicht-SSL- zu SSL-Ports.

Service	Nicht-SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

3. Klicken Sie in der Symbolleiste der Ansicht „Services“ auf (Bearbeiten).
   Das Dialogfeld „Service bearbeiten“ wird angezeigt.
4. Ändern Sie den Port von Nicht-SSL zu SSL, wie in der Tabelle dargestellt, und klicken Sie auf **Speichern**. (Ändern Sie z. B. den Broker-Port von 50003 zu 56003.)



Aufgabe 8: (Bedingungsabhängig) Korrigieren der Auditprotokollvorlagen, die in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert werden

Problem: Wenn ein Benutzer von 10.6.5 auf 11.1 und von 11.0.0.0 auf 11.1 aktualisiert, werden Auditprotokollvorlagen in der Logstash-Ausgabe-Konfigurationsdatei nicht aktualisiert, wenn globales Auditing eingerichtet ist.

Workaround: Wenn globales Auditing konfiguriert ist, müssen Sie einen der Syslog-Einträge auf den Servern für globale Benachrichtigungen bearbeiten und auf „Speichern“ klicken, um die aktuelle Auditprotokollkonfiguration anzuwenden.

Wenn Sie globales Auditing in 11.0.x konfiguriert hatten, müssen Sie das folgende Verfahren durchführen, um die aktuelle globale Auditingkonfiguration anzuwenden.

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **System** > **Globale Benachrichtigungen** aus.
   Die Ansicht **Globale Benachrichtigungen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server** und wählen Sie einen Syslog-Server aus.
3. Klicken Sie auf  (Symbol „Bearbeiten“) und anschließend auf **Speichern**.

RSA NetWitness® Endpoint

Aufgabe 9: Neukonfigurieren eines wiederkehrenden Feeds, der über Legacy Endpoint konfiguriert wurde, da sich die Java-Version geändert hat

Sie müssen den wiederkehrenden Legacy Endpoint-Feed aufgrund der Änderung der Java-Version neu konfigurieren. Führen Sie den folgenden Schritt zur Behebung des Problems aus.

1. Importieren Sie das NetWitness Endpoint CA-Zertifikat in den vertrauenswürdigen NetWitness Suite-Speicher, wie in „Exportieren des SSL-Zertifikats von NetWitness Endpoint“ unter dem Thema „Konfigurieren kontextbezogener Daten von Endpoint über wiederkehrenden Feed“ im *RSA NetWitness Endpoint-Integrationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

RSA NetWitness® Endpoint Insights

(Optional) Aufgabe 10: Installieren von Endpoint Hybrid oder Endpoint Log Hybrid

Siehe:

RSA NetWitness Suite 11.1 Installationshandbuch für physische Hosts für Anweisungen für die Installation auf einem physischen Host

RSA NetWitness Suite 11.1 Installationshandbuch für virtuelle Hosts für Anweisungen für die Installation auf einem virtuellen Host

Aufgabe 11: Erneutes Konfigurieren von Endpoint-Warnmeldungen über den Nachrichtenbus

1. Ändern Sie auf dem NetWitness Endpoint-Server die Konfiguration des virtuellen Hosts in der `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe`-Datei, um die folgende Konfiguration widerzuspiegeln.
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Hinweis: In NetWitness Suite 11.1 ist der virtuelle Host `/rsa/system`. Für 10.6.5.x und frühere Versionen ist der virtuelle Host `/rsa/sa`.
2. Starten Sie den API-Server und Konsolenserver neu.
3. Stellen Sie über SSH eine Verbindung mit dem NW-Server her und melden Sie sich mit den `root`-Anmeldedaten an.
4. Senden Sie den folgenden Befehl, um dem Truststore alle Zertifikate hinzuzufügen:
   `orchestration-cli-client --update-admin-node`
5. Führen Sie den folgenden Befehl aus, um den RabbitMQ-Server neu zu starten:
   `systemctl restart rabbitmq-server`
   Das NetWitness Endpoint-Konto sollte auf RabbitMQ automatisch verfügbar sein.
6. Importieren Sie die `/etc/pki/nw/ca/nwca-cert.pem`- und `/etc/pki/nw/ca/ssca-cert.pem`-Dateien vom NW-Server und fügen Sie sie den Trusted Root Certification-Speichern auf dem Endpoint-Server hinzu.

Aufgaben für Event Stream Analysis

Aufgabe 12: Neukonfigurieren der automatisierten Bedrohungserkennung für ESA

Wenn Sie in 10.6.5.x die automatisierte Bedrohungserkennung verwendet haben, müssen Sie die folgenden Schritte ausführen, um sie über den ESA Analytics-Service in Version 11.1 neu zu konfigurieren.

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **System** > **ESA Analytics** aus.
   Für die Suspicious Domains-Module Command and Control (C2) für Pakete und C2 für

Protokolle ist eine Whitelist mit der Bezeichnung „**domains_whitelist**“ erforderlich.

2. Bedingungsabhängig: Wenn Ihre vorherige Whitelist zur automatisierten Bedrohungserkennung auf der Registerkarte **Listen** des Context-Hub-Services angezeigt wird:
   a. Klicken Sie auf **ADMIN** > **Services**, wählen Sie den Context-Hub-Service im Drop-down-Menü der Aktionsbefehle () aus und klicken Sie dann auf **Ansicht** > **Konfigurieren** > Registerkarte **Listen**.
   b. Benennen Sie Ihre alte Whitelist zur automatisierten Bedrohungserkennung für das Suspicious Domains-Modul in „`domains_whitelist`“ um.

Weitere Informationen finden Sie im Handbuch *NetWitness Suite – Automatisierte Bedrohungserkennung* und im Abschnitt „Konfigurieren von ESA Analytics“ im *NetWitness Suite ESA-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 13: Konfigurieren von gegenseitig authentifiziertem SSL für Integrationen mit Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpoint

Wenn Sie Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpoint integrieren, müssen Sie gegenseitig authentifiziertes SSL auf jedem integrierten System konfigurieren, sodass die Anwendung sich beim Verbinden mit dem RabbitMQ-Nachrichtenbus selbst authentifizieren kann.

Hinweis: Verwenden Sie die RabbitMQ-Benutzernamen und -Passwörter, die Sie bei der Sicherung Ihrer 10.6.5.x-Daten erhalten haben (siehe Anweisungen zum Backup).

1. Erstellen Sie einen Benutzer auf dem Hostsystem, das in NetWitness Suite integriert wird, durch Anmelden am Host und Ausführen des folgenden `rabbitmqctl`-Befehls:
   ```
   > rabbitmqctl add_user <username> <password>
   ```
   Beispiel:
   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```
2. Legen Sie Berechtigungen für Benutzer mit dem folgenden Befehl fest (verwenden Sie den Benutzernamen aus Schritt 1):
   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*",
   ".*"
   ```
   Beispiel:
   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*",
   ".*", ".*"
   ```

Aufgabe 14: Aktivieren des Dashboards „Bedrohung – Malwareindikatoren“

In Version 11.1 wurde das 10.6.5.x-Dashboard **Bedrohung – Indikatoren** umbenannt in **Bedrohung – Malwareindikatoren**. Wenn Sie dieses Dashboard in 10.6.5.x verwendet haben, müssen Sie folgende Schritte ausführen:

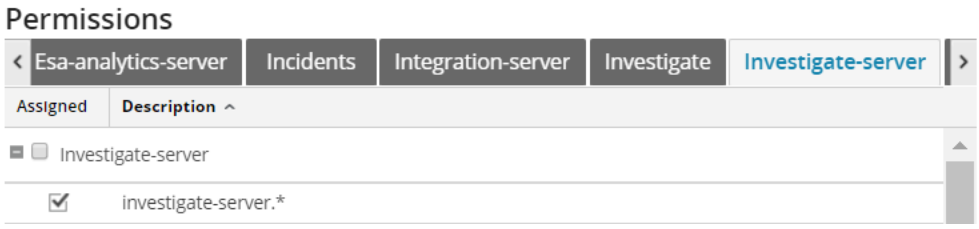
1. Aktivieren Sie das Dashboard **Bedrohung – Malwareindikatoren** in Version 11.1.
2. Legen Sie eine Datenquelle für neue Dashlets fest.
   Eine Beschreibung von Dashlets im Zusammenhang mit NetWitness Suite finden Sie unter „Dashlets“ auf RSA Link (https://community.rsa.com/docs/DOC-81463).

Ermittlung

Aufgabe 15: Sicherstellen, dass benutzerdefinierte Rollen für den Zugriff auf Ereignisanalysen über `Investigate-server`-Berechtigungen verfügen

Nach einem Upgrade auf Version 11.1.0.0 ist für benutzerdefinierte Rollen die `investigate-server.*` -Berechtigung nicht standardmäßig aktiviert. Gehen Sie folgendermaßen vor, um sicherzustellen, dass die entsprechenden Benutzerrollen berechtigt sind, auf die Ereignisanalyse zuzugreifen.

1. Melden Sie sich bei NetWitness Suite 11.1.0.0 mit Ihren `Admin user`-Anmeldedaten an.
2. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **Sicherheit** aus.
3. Klicken Sie auf die Registerkarte **Rollen**.
4. Wählen Sie die Rollen aus, die `investigate-server.*` -Berechtigungen benötigen, und klicken Sie auf (Symbol „Bearbeiten“).
5. Wählen Sie die Registerkarte **Investigate-Server** unter **Berechtigungen** aus.
6. Wenn das Kontrollkästchen „Investigate-Server“ nicht aktiviert ist, aktivieren Sie es für die Benutzer, die Zugriff auf die Ereignisanalyse benötigen.



7. Klicken Sie auf **Speichern**.

Protokollsammlung

Aufgabe 16: Zurücksetzen der stabilen Systemwerte für Log Collector nach dem Upgrade

Führen Sie die folgenden Aufgaben durch, um stabile Systemwerte für den Log Collector zurückzusetzen, nachdem Sie ihn auf Version 11.1 aktualisiert haben, um sicherzustellen, dass alle Sammlungsprotokolle den normalen Betrieb fortsetzen.

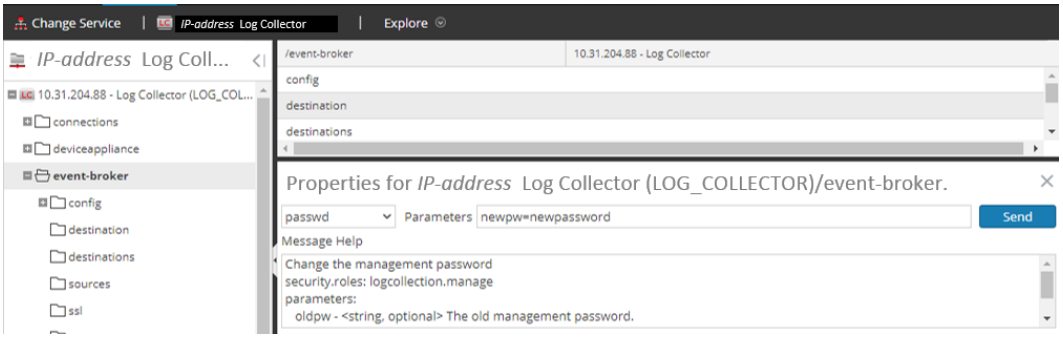
Zurücksetzen der stabilen Systemwerte für die Lockbox

Die Lockbox speichert den Schlüssel zum Verschlüsseln der Ereignisquelle und anderer Passwörter für den Log Collector. Der Log Collector-Service kann die Lockbox aufgrund der Änderungen an den stabilen Werten nicht öffnen. Daher müssen Sie die stabilen Systemwerte für die Lockbox zurücksetzen. Anweisungen hierzu finden Sie unter „Protokollsammlung: Schritt 3. Einrichten einer Lockbox“ im *RSA NetWitness® Suite Protokollsammlung-Konfigurationsleitfaden*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aktualisieren des RabbitMQ-Benutzerkontopassworts für den Log Collector-Service

Wenn das RabbitMQ-Benutzerkontopasswort für den Log Collector-Service geändert wurde, müssen Sie es nach dem Upgrade auf Version 11.1 erneut eingeben.

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **Services** aus.
2. Wählen Sie den Log Collector-Service aus.
3. Klicken Sie auf  (Aktionen) > **Ansicht** > **Erkunden**.
4. Klicken Sie mit der rechten Maustaste auf `event-broker` > **Eigenschaften**.
5. Wählen Sie `passwd` aus der Drop-Down-Liste aus, geben Sie bei den Parametern `newpw=><newpassword>` ein (wobei `<newpassword>` das RabbitMQ-Benutzerkontopasswort ist) und klicken Sie anschließend auf **Senden**.



(Optional für Upgrades von 10.6.5.x mit für Log Collectors, Log Decoder und Packet Decoder aktiviertem FIPS)

Aufgabe 17: Aktivieren des FIPS-Modus

FIPS ist für alle Services aktiviert, mit Ausnahme von Log Collector, Log Decoder und Decoder. FIPS kann für keinen Service deaktiviert werden, mit Ausnahme von Log Collector, Log Decoder und Decoder. Informationen zur Aktivierung von FIPS für diese Services finden Sie im Kapitel „Systemwartung: Aktivieren oder Deaktivieren von FIPS“ im *RSA NetWitness® SuiteLeitfaden Systemwartung*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Reporting Engine

(Bedingungsabhängig) Aufgabe 18: Wiederherstellen der CA-Zertifikate für externe Syslog-Server für die Reporting Engine

Nach dem Upgrade müssen Sie die CA-Zertifikate aus dem vor dem Upgrade angelegten Backup wiederherstellen. Das Backupskript sichert die 10.6.5.x-CA-Zertifikate im Verzeichnis `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts`.

Gehen Sie wie folgt vor, um die CA-Zertifikate in Version 11.1 wiederherzustellen.

1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
2. Exportieren Sie die CA-Zertifikate.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Kopieren Sie das CA-PEM in das Verzeichnis `/etc/pki/nw/trust/import`.

(Bedingungsabhängig) Aufgabe 19: Wiederherstellen von externem Speicher für die Reporting Engine

Wenn Sie externen Speicher für die Reporting Engine verwenden (z. B. SAN oder NAS zum Speichern von Berichten), müssen Sie den Mount wiederherstellen, den Sie vor dem Upgrade aufgehoben haben. Anweisungen hierzu finden Sie unter „Reporting Engine: Hinzufügen von zusätzlichem Speicherplatz für große Berichte“ im *RSA NetWitness® SuiteKonfigurationsleitfaden Reporting Engine*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Respond

(Bedingungsabhängig) Aufgabe 20: Wiederherstellen von benutzerdefinierte Analystenrollen

Wenn Sie in Version 10.6.5.x benutzerdefinierte Analystenrollen verwendet haben, müssen Sie diese in Version 11.1 reaktivieren. Siehe „Hinzufügen einer Rolle und Zuweisen von Berechtigungen“ im Handbuch *RSA NetWitness Suite Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 21: Wiederherstellen der benutzerdefinierten Schlüssel für den Respond-Service

Wenn Sie in Version 10.6.5.x benutzerdefinierte Schlüssel zur Verwendung in der **groupBy**-Klausel hinzugefügt haben, wurde die `alert_rules.json`-Datei geändert. Die Datei `alert_rules.json` enthält das Schema für Aggregationsregeln. RSA hat die `alert_rules.json`-Datei an den folgenden neuen Speicherort verschoben:
`/var/lib/netwitness/respond-server/scripts`

1. Kopieren Sie die benutzerdefinierten Schlüssel aus der `/opt/rsa/im/fields/alert_rules.json`-Datei im Backupverzeichnis.
   Dieses Verzeichnis befindet sich dort, wo die `alert_rules.json`-Datei aus dem 10.6.5.x-Backup wiederhergestellt wird.
2. Navigieren Sie zum `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.1.
   Dies ist die neue Datei für 11.1.
3. Bearbeiten Sie den `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` so, dass er die benutzerdefinierten Schlüssel enthält, die Sie im ersten Schritt kopiert haben.

Aufgabe 22: Wiederherstellen der angepassten Skripte zur Normalisierung des Respond-Services

RSA hat die Skripte zur Normalisierung des Respond-Services in Version 11.1 umstrukturiert und an den folgenden neuen Speicherort verschoben:
`/var/lib/netwitness/respond-server/scripts`
Wenn Sie diese Skripte in 10.6.5.x angepasst haben, gehen Sie wie folgt vor:

1. Navigieren Sie zum Verzeichnis `/opt/rsa/im/scripts`.
   Dieses Verzeichnis befindet sich dort, wo die folgenden Skripte zur Normalisierung des Antwortservice aus dem 10.6.5.x-Backup wiederhergestellt werden:
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Kopieren Sie die gesamte benutzerdefinierte Logik der 10.6.5.x-Skripte.
3. Navigieren Sie zum Verzeichnis `/var/lib/netwitness/respond-server/scripts`.
   Dieses Verzeichnis befindet sich dort, wo NetWitness Suite 11.1 die erneut angepassten Skripte speichert.
4. Bearbeiten Sie die neuen Skripte so, dass sie die angepasste Logik enthalten, die Sie in Schritt 2 aus den 10.6.5.x-Skripten kopiert haben.
5. Kopieren Sie die gesamte benutzerdefinierte Logik aus der Datei `/opt/rsa/im/fields/alert_rules.json`.
   Die Datei `alert_rules.json` enthält das Schema für Aggregationsregeln.

Aufgabe 23: Hinzufügen von Einstellungen für Antwort auf Benachrichtigungen für benutzerdefinierte Rollen

Berechtigungen für Einstellungen für Antwort auf Benachrichtigungen erlauben Respond-Administratoren, Datenschutzbeauftragten und SoC-Managern, auf die Reagieren-Benachrichtigungseinstellungen zuzugreifen (**Konfigurieren** > **Auf Benachrichtigungen antworten**). So können sie E-Mail-Benachrichtigungen senden, wenn Incidents erstellt oder aktualisiert werden.

Um diese Einstellungen aufzurufen, müssen Sie Ihren vorhandenen integrierten NetWitness Suite-Benutzerrollen weitere Berechtigungen hinzufügen. Sie müssen auch Ihren benutzerdefinierten Rollen Berechtigungen hinzufügen. Weitere Informationen finden Sie im Thema „Berechtigungen für Einstellungen für Antwort auf Benachrichtigungen“ im *Konfigurationsleitfaden für NetWitness Respond*. Ausführliche Informationen zu Benutzerberechtigungen finden Sie im Handbuch *Systemsicherheit und Benutzerverwaltung*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 24: Manuelles Konfigurieren von Einstellungen für Antwort auf Benachrichtigungen

Die Benachrichtigungseinstellungen für das Incident-Management in NetWitness Suite 10.6.5.x unterscheiden sich von den Einstellungen für Antwort auf Benachrichtigungen in Version 11.1. Ihre bestehenden Einstellungen für Version 10.6.5.x werden daher nicht auf Version 11.1 migriert.

NetWitness Einstellungen für Antwort auf Benachrichtigungen ermöglichen das Senden von E-Mail-Benachrichtigungen an SoC-Manager und den einem Incident zugewiesenen Analysten, wenn ein Incident erstellt oder aktualisiert wird.

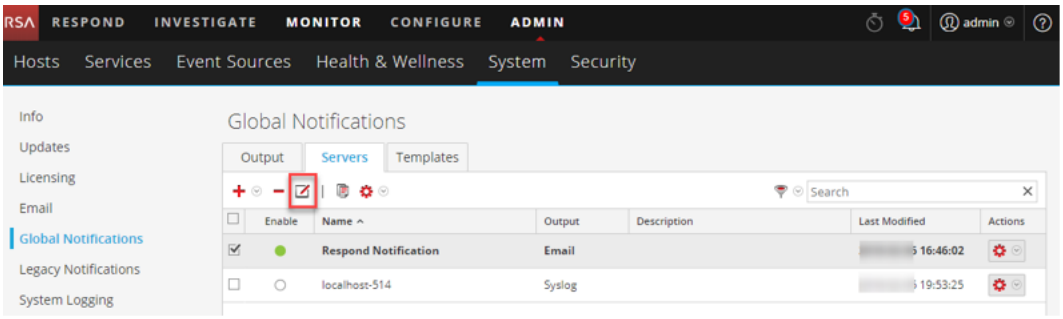
Um die Einstellungen für Antwort auf Benachrichtigungen manuell zu konfigurieren, navigieren Sie zu **Konfigurieren** > **Auf Benachrichtigungen antworten.** Beachten Sie hierzu das Verfahren „Konfigurieren von Respond-Benachrichtigungseinstellungen“ im *Konfigurationsleitfaden für NetWitness Respond*.

Benachrichtigungsserver von Version 10.6.5.x werden in der Drop-down-Liste des E-Mail-Servers nicht angezeigt. Die E-Mail-Server müssen im Bereich „Globale Benachrichtigungsserver“ (**ADMIN** > **System** > **Globale Benachrichtigungen** > Registerkarte **Server**) bearbeitet und gespeichert werden.

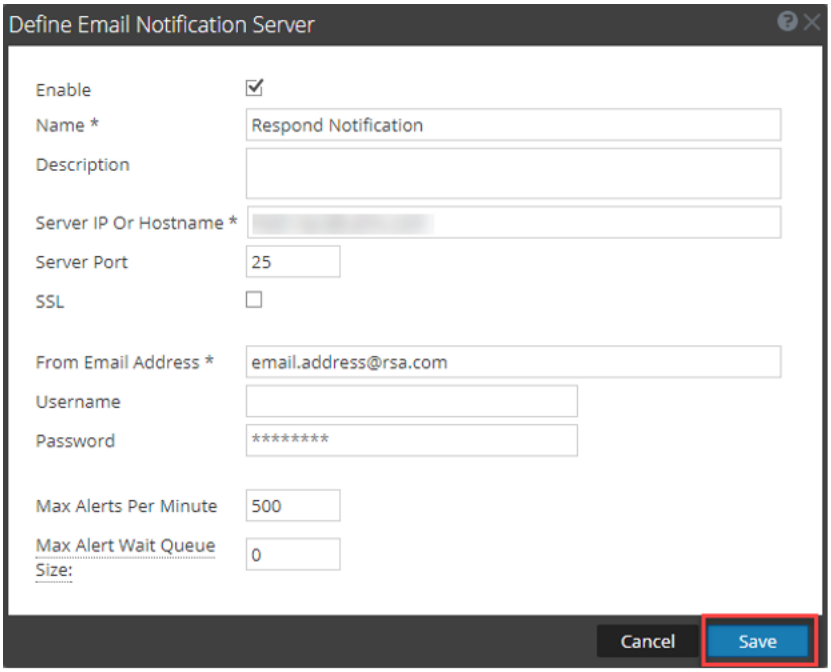
1. Wählen Sie im **NetWitness Suite** 11.1-Menü **ADMIN** > **System** > **Globale Benachrichtigungen** > Registerkarte **Server** aus.
2. Navigieren Sie zu **Konfigurieren** > **Auf Benachrichtigungen antworten**. Die Ansicht „Einstellungen für Antwort auf Benachrichtigung“ wird angezeigt.
   Beachten Sie, dass die E-Mail-Benachrichtigungsserver in der Drop-down-Liste E-MAIL-SERVER nicht angezeigt werden.
3. Klicken Sie auf den Link **E-Mail-Server-Einstellungen**.
   Der Bereich „Globale Benachrichtigungen“ wird angezeigt.
4. Klicken Sie auf die Registerkarte **Server**.

5. Gehen Sie für jeden E-Mail-Benachrichtigungsserver wie folgt vor:

   a. Wählen Sie den E-Mail-Benachrichtigungsserver aus und klicken Sie auf .



   b. Klicken Sie im Dialogfeld **E-Mail-Benachrichtigungsserver definieren** auf Speichern.



6. Navigieren Sie zurück zu **Konfigurieren** > **Auf Benachrichtigungen antworten**. Ihre Server werden in der Drop-down-Liste **E-MAIL-SERVER** angezeigt. Benutzerdefinierte Benachrichtigungsvorlagen für das Incident-Management können nicht auf Version 11.1 migriert werden. In Version 11.1 werden keine benutzerdefinierten Vorlagen unterstützt.

Aufgabe 25: Aktualisieren der „Gruppieren nach“-Werte der Incident-Standardregel

Vier der Incident-Standardregeln verwenden als „Gruppieren nach“-Wert jetzt „Quell-IP-Adresse“. Um die Standardregeln zu aktualisieren, ändern Sie den „Gruppieren nach“-Wert der folgenden Standardregeln in „Quell-IP-Adresse“:

- Warnmeldungen mit hohem Risiko: Reporting Engine
- Warnmeldungen mit hohem Risiko: Malware Analysis
- Warnmeldungen mit hohem Risiko: NetWitness Endpoint
- Warnmeldungen mit hohem Risiko: ESA

1. Navigieren Sie zu **Konfigurieren** > **Incident-Regeln** und klicken Sie bei der Regel, die Sie aktualisieren möchten, auf den Link in der Spalte **Name**. Die Detailansicht der Incident-Regel wird angezeigt.
2. Wählen Sie im Feld **Gruppieren nach** den neuen „Gruppieren nach"-Wert aus.
3. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.

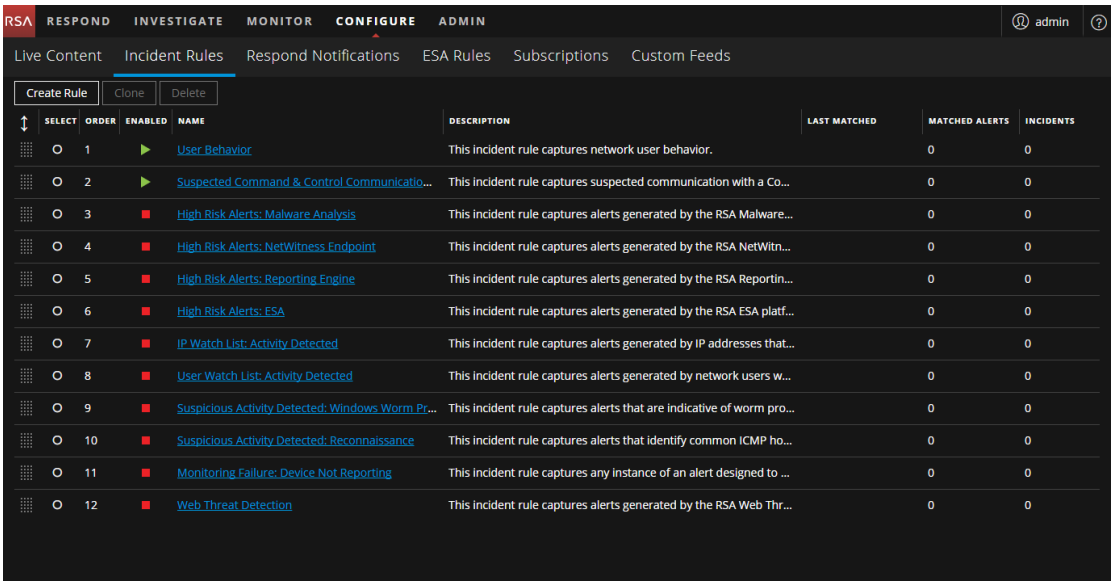
Aufgabe 26: Hinzufügen des Felds „Gruppieren nach" zu Incident-Regeln

Das Feld **Gruppieren nach** ist in Version 10.6.5 nicht erforderlich, in Version 11.1 hingegen schon. Nach dem Upgrade auf Version

11.1 werden einige Incident-Regeln kein Feld **Gruppieren nach** enthalten. Diesen Regeln müssen Sie das Feld hinzufügen, oder die Regeln funktionieren nicht und erstellen keine Incidents.

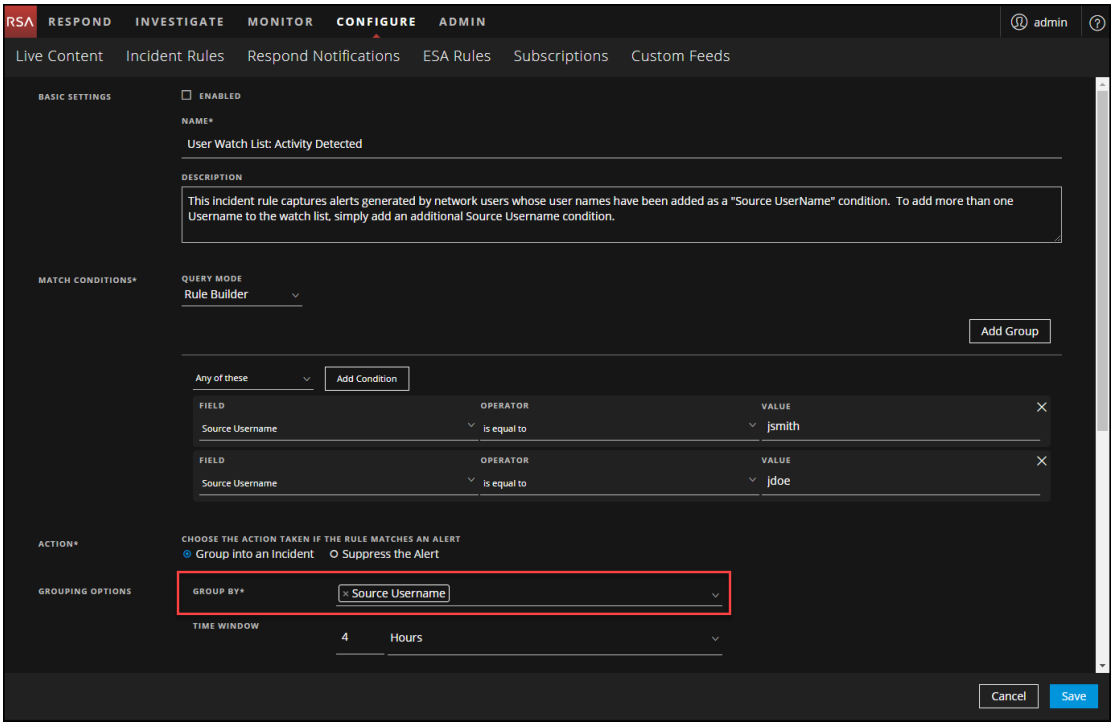
Führen Sie für jede Incident-Regel die folgenden Schritte aus:

1. Melden Sie sich bei RSA NetWitness® Suite an.
2. Navigieren Sie zu **Konfigurieren** > **Incident-Regeln** und klicken Sie bei der Regel, die Sie aktualisieren möchten, auf den Link in der Spalte „Name".



.

3. Überprüfen Sie im Feld „Gruppieren nach“, ob ein „Gruppieren nach“-Wert ausgewählt ist. Falls dies nicht der Fall ist, wählen Sie einen „Gruppieren nach“-Wert aus.



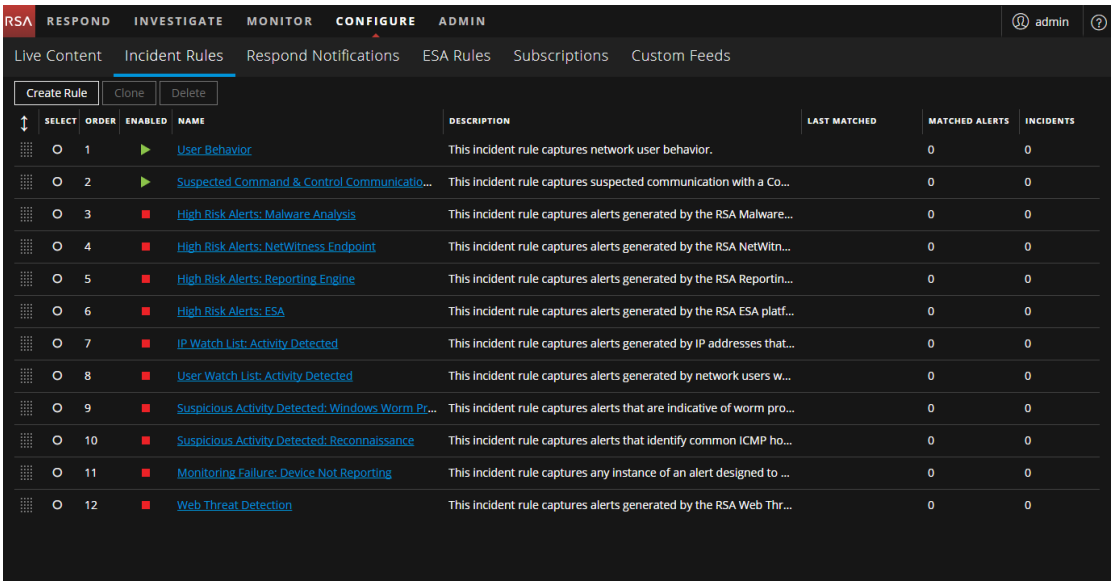
4. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.
   Informationen zu Incident-Regeln finden Sie im *Konfigurationsleitfaden für NetWitness Respond*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 27: Aktualisieren von Incident-Regeln, die in der Domain in der Upgrade-Vorbereitungsaufgabe für die Übereinstimmungsbedingungen identifiziert wurden

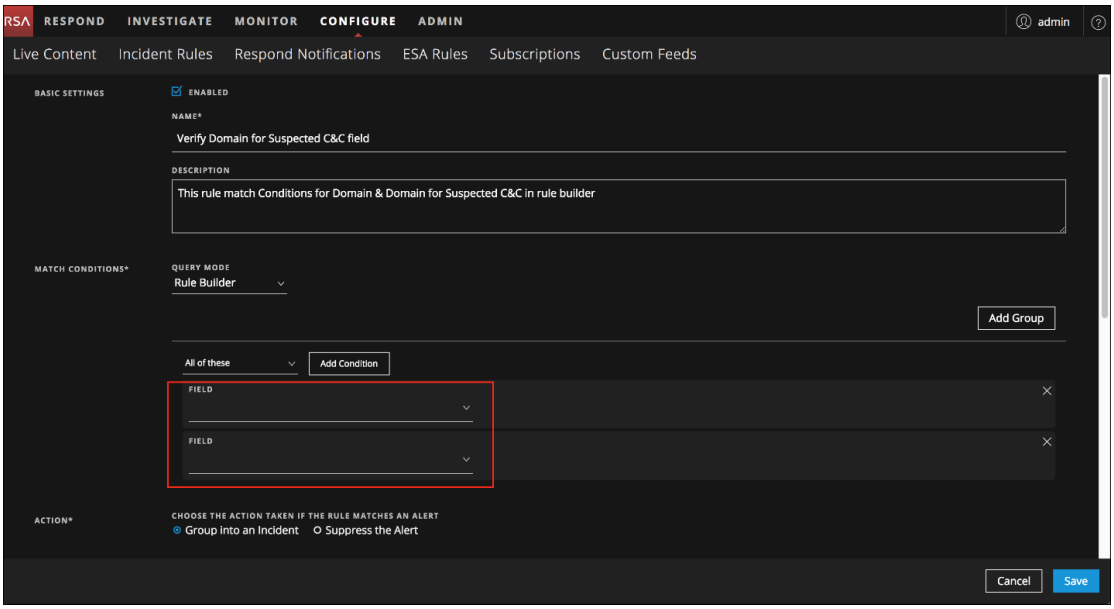
Ändern Sie die Incident-Regeln, für die Sie in der Upgrade-Vorbereitungsaufgabe Aufgabe 4: Prüfen der Übereinstimmungsbedingungen von Aggregationsregeln für „Domain“ oder „Domain für verdächtige C&C“ festgestellt hatten, dass sie in den Übereinstimmungsbedingungen in der Regelerstellung „Domain“ oder „Domain für verdächtige C&C“ enthielten, dahingehend, dass sie nur „Domain“ verwenden.

Gehen Sie für jede zuvor identifizierte Regel wie folgt vor:

1. Wählen Sie im **NetWitness Suite** 11.1-Menü **Konfigurieren** > **Incident-Regeln** aus und klicken Sie bei der Regel, die Sie aktualisieren möchten, auf den Link in der Spalte „Name“.



2. Wählen Sie im Bereich **Bedingungen abstimmen** für die leeren Felder in der Drop-down-Liste **Domain** aus. Wählen Sie anschließend die Bedingungen aus, die Sie zuvor in den Aufgaben vor dem Upgrade identifiziert hatten.



3. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.
Informationen zu Incident-Regeln finden Sie im *Konfigurationsleitfaden für NetWitness Respond*.Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

SecOps Manager

(RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management und RSA Archer Issues Management)

Aufgabe 28: Neukonfigurieren der NW SecOps Manager-Integration

Informationen zum Neukonfigurieren von NW SecOps für Event Stream Analysis, Reporting Engine und Respond finden Sie im *RSA Archer-Integrationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Warehouse Connector

Aufgabe 29: Wiederherstellen der `keytab` -Dateien, Mounten von NFS und Installieren des Service

1. Stellen Sie die `keytab`-Dateien aus dem Verzeichnis `<backup-path>/restore` wieder her.
2. Stellen Sie die Kerberos-Bereichsnamenkonfiguration aus `<backup-path>/restore/etc/krb5.conf` in `/etc/krb5.conf` wieder her.
3. (Bedingungsabhängig) Wenn Sie das Upgrade aus einer Nicht-FIPS-Umgebung durchführen und der Parameter `isCheckValidationRequired` im Ziel nicht aktiviert ist, konfigurieren Sie das SFTP-Ziel wie folgt:
   a. Stellen Sie über SSH eine Verbindung mit dem Warehouse Connector-Host her und übermitteln Sie die folgenden Befehle:
   ```
   cd /root/.ssh/
    mv id_dsa id_dsa.old
   OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_
   dsa.old -out id_dsa
   ```
   Sie werden aufgefordert, die Passphrase einzugeben.
   b. Geben Sie das Passwort für die Verschlüsselung ein.
   c. Führen Sie den folgenden Befehl aus:
   ```
   chmod 600 id_dsa
   ```
4. Installieren Sie den Warehouse Connector-Service.
   Anweisungen finden Sie im *NetWitness Suite Warehouse Connector-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Aufgabe 30: Aktualisieren der Warehouse Connector Lockbox und Starten des Streams

Hinweis: Wenn für die Streams in 10.6.5.x automatische Starts aktiviert sind, gibt es eine kleine Verzögerung, bevor Sie den Warehouse Connector-Service in der NetWitness Suite-Benutzeroberfläche erkennen können.

1. Aktualisieren Sie die Lockbox von Warehouse Connector.
2. Stellen Sie über SSH eine Verbindung mit Warehouse Connector her und melden Sie sich mit den Root-Anmeldedaten an.
3. Starten Sie den Service neu.
   ```
   service nwwarehouseconnector restart
   ```
4. (Bedingungsabhängig) Wenn der automatische Start in 10.6.5.x nicht aktiviert wurde, müssen Sie den Stream nach dem Neustart des Services manuell starten.

Backup

Aufgabe 31: Entfernen von backupbezogenen Dateien aus den lokalen Hostverzeichnissen

Achtung: 1) Sie müssen eine Kopie aller Backupdateien auf einem externen Host hinterlegen. 2) Überprüfen Sie, ob alle Daten aus dem Backup in Version 11.1 wiederhergestellt wurden, bevor Sie die backupbezogenen Dateien aus den lokalen Verzeichnissen auf den 11.1-Hosts entfernen.

`.tar`-Backupdateien

Nachdem alle Hosts auf Version 11.1 aktualisiert wurden, müssen Sie folgende Dateien entfernen:

- Die Backupdateien aus den lokalen Verzeichnissen auf den Hosts.
- Alle Dateien aus den Verzeichnissen `nw-backup` und `restore` auf den Hosts.

Host	Backuppfad	Wiederherstellungspfad
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`

Host	Backuppfad	Wiederherstellungspfad
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
NW-Server	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
Alle anderen Hosts	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Anhang A: Troubleshooting

Es gibt zwei Abschnitte in diesem Anhang.

Abschnitt 1: Allgemeine Troubleshooting-Informationen

Dieser Abschnitt beschreibt Lösungen für Probleme, die während Installationen oder Upgrades auftreten können. In den meisten Fällen erstellt NetWitness Suite Protokollmeldungen, wenn Probleme auftreten.

Hinweis: Wenn Sie Probleme beim Upgrade mithilfe der folgenden Troubleshooting-Lösungen nicht beheben können, wenden Sie sich an den Kundensupport (https://community.rsa.com/docs/DOC-1294).

Dieser Abschnitt enthält Troubleshooting-Dokumentation für die folgenden Services, Funktionen und Prozesse:

- CLI (Command Line Interface)
- Backupskript
- Event Stream Analysis
- Log Collector-Service (`nwlogcollector`)
- NW-Server
- Reporting Engine

CLI (Command Line Interface)

Fehlermeldung	CLI (Command Line Interface) wird angezeigt: „Orchestrierung ist fehlgeschlagen.“ `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Ursache	Es wurde das falsche Passwort für `deploy_admin` in `nwsetup-tui` eingegeben.
Lösung	Rufen Sie Ihr Passwort für `deploy_admin` ab.

	1. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` Stellen Sie über SSH eine Verbindung mit dem fehlgeschlagenen Host her. 2. Führen Sie `nwsetup-tui` erneut mit dem korrekten Passwort für `deploy_admin` aus.

Fehlermeldung	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health.AlarmsController - Cannot connect to System Management Service`
Ursache	NetWitness Suite erkennt den Servicemanagement-Service (SMS) nach einem erfolgreichen Upgrade als „down“, obwohl der Service ausgeführt wird.
Lösung	Starten Sie den SMS-Service neu. `systemctl restart rsa-sms`

Backup (`nw-backup`-Skript)

Fehlermeldung	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Ursache	Das ESA Mongo-Admin-Passwort enthält Sonderzeichen (z. B. "! @# $% ^ qwertz').
Lösung	Ändern Sie das ESA Mongo-Admin-Passwort zurück auf den ursprünglichen Standard „NetWitness“, bevor Sie das Backup ausführen. Weitere Informationen finden Sie unter „ESA-Konfiguration: Ändern des MongoDB-Passworts für das Administratorkonto“ im *Konfigurationsleitfaden für Event Stream Analysis. Navigieren Sie zu* Masterinhaltsverzeichnis *für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.*

Fehler	Backupfehler aufgrund der Einstellung des Attributs `immutable`. Hier ist ein Beispiel für einen Fehler, der angezeigt werden kann:
	`Backing up NetWitness Config (/etc/netwitness) files from: saserver1`
	`WARNING: Errors occurred while backing up NetWitness Configuration files.`
	`Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz`
	`Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz`
	`Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1`

Ursache	Wenn Sie Dateien haben, bei denen das Flag „unveränderlich“ eingestellt ist (um zu verhindern, dass der Puppet-Prozess eine angepasste Datei überschreibt), wird die Datei nicht in den Backupprozess einbezogen und es wird ein Fehler generiert.
Lösung	Führen Sie auf dem Host, der die Dateien mit gesetztem Flag „unveränderlich“ enthält, folgenden Befehl aus, um die Einstellung „unveränderlich“ aus den Dateien zu entfernen: `chattr -i <filename>`

Fehler	Fehler beim Erstellen der Datei mit Netzwerkkonfigurationsinformationen aufgrund von doppelten oder ungültigen Einträgen in primärer Netzwerkkonfigurationsdatei: `/etc/sysconfig/network-scripts/ifcfg-em1` Überprüfen Sie den Inhalt von `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Ursache	Es gibt falsche oder doppelte Einträge für jedes der folgenden Felder: DEVICE, BOOTPROTO, IPADDR, NETMASK oder GATEWAY, die beim Lesen der primären Ethernet-Schnittstellenkonfigurationsdatei des zu sichernden Host gefunden wurden.

Lösung	Erstellen Sie manuell eine Datei am Backupspeicherort auf dem externen Backupserver sowie am lokalen Backupspeicherort des Rechners, auf dem andere Backups bereitgestellt wurden. Der Dateiname muss das Format `<hostname>-<hostip>-network.info.txt` haben und die folgenden Einträge enthalten:
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problem	Der ESA-Service stürzt nach dem Upgrade auf 11.1.0.0 aus einem Setup mit FIPS-Aktivierung ab.
Ursache	Der ESA-Service verweist auf einen ungültigen Keystore.

Lösung	1. Stellen Sie über SSH eine Verbindung mit dem ESA Primary-Host her und melden Sie sich an.
	2. Ersetzen Sie in Datei `/opt/rsa/esa/conf/wrapper.conf` die folgende Zeile:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	durch:
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Geben Sie den folgenden Befehl ein, um ESA neu zu starten:
	`systemctl restart rsa-nw-esa-server`
	Hinweis: Wenn Sie über mehrere ESA-Hosts verfügen, auf denen dasselbe Problem auftritt, wiederholen Sie die Schritte 1 bis 3 inklusive auf jedem sekundären ESA-Host.

Log Collector-Service (`nwlogcollector`)

Log Collector-Protokolle werden an `/var/log/install/nwlogcollector_install.log` auf dem Host, auf dem der `nwlogcollector` -Service ausgeführt wird, gesendet.

Fehlermeldung	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Ursache	Die Log Collector Lockbox konnte nach der Aktualisierung nicht geöffnet werden.
Lösung	Melden Sie sich bei NetWitness Suite an und setzen Sie den Systemfingerabdruck zurück, indem Sie das Passwort für den Systemstabilitätswert der Lockbox zurücksetzen, wie im Thema „Zurücksetzen des Systemstabilitätswerts“ unter „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Fehlermeldung	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Ursache	Die Log Collector Lockbox wird nach der Aktualisierung nicht konfiguriert.
Lösung	(Bedingungsabhängig) Wenn Sie eine Log Collector Lockbox verwenden, melden Sie sich bei NetWitness Suite an und konfigurieren die Lockbox wie im Thema „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschriebenNavigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Fehlermeldung	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Ursache	Sie müssen das Feld für den Schwellenwert des Stabilitätswerts für die Log Collector Lockbox zurücksetzen.
Lösung	Melden Sie sich bei NetWitness Suite an und setzen Sie das Passwort für den Systemstabilitätswert der Lockbox zurück, wie im Thema „Zurücksetzen des Systemstabilitätswerts“ unter „Konfigurieren von Lockbox-Sicherheitseinstellungen“ im *Protokollsammlung-Konfigurationsleitfaden* beschrieben. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Problem	Sie haben einen Log Collector für das Upgrade vorbereitet und möchten kein Upgrade mehr durchführen.
Ursache	Verzögerungen beim Upgrade.
Lösung	Verwenden Sie die folgende Befehlszeichenfolge, um einen Log Collector, der für ein Upgrade vorbereitet wurde, in den normalen Betrieb zurückzusetzen. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

NW-Server

Diese Protokolle werden an `/var/netwitness/uax/logs/sa.log` auf dem NW-Serverhost gesendet.

Problem	Nach dem Upgrade bemerken Sie, dass Auditprotokolle nicht zur konfigurierten globalen Audit-Einrichtung weitergeleitet werden oder Die folgende Meldung, angezeigt in `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Ursache	Die globale Audit-Einrichtung des NW-Servers konnte nicht von Version 10.6.5.x auf 11.1.0.0 migriert werden.
Lösung	1. Stellen Sie über SSH eine Verbindung mit dem NW-Server her. 2. Senden Sie den folgenden Befehl: `orchestration-cli-client --update-admin-node`

Reporting Engine-Service

Reporting Engine-Aktualisierungsprotokolle werden an die Datei `/var/log/re_install.log` auf dem Host übermittelt, auf dem der Reporting Engine-Service ausgeführt wird.

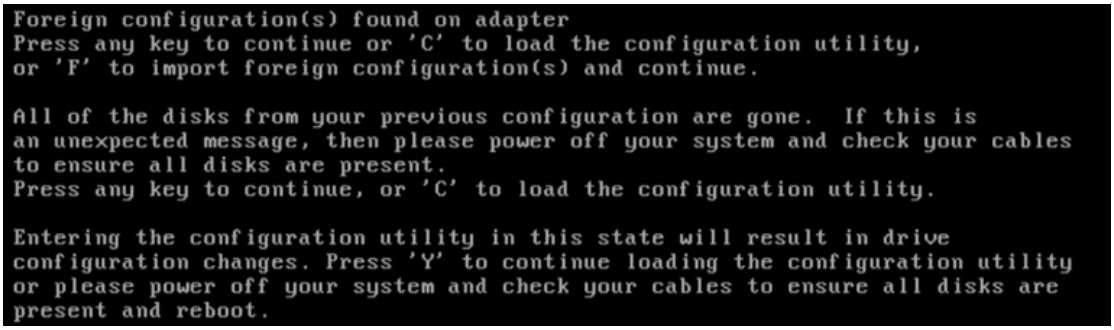
Fehlermeldung	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Ursache	Die Aktualisierung der Reporting Engine ist fehlgeschlagen, da Sie nicht über ausreichend Speicherplatzverfügen.
Lösung	Geben Sie Festplattenspeicherplatz frei, um den in der Protokollmeldung angezeigten erforderlichen Speicherplatz bereitzustellen. Anweisungen zum Freigeben von Festplattenspeicherplatz finden Sie unter „Hinzufügen von zusätzlichem Speicherplatz für große Berichte“ im *Reporting Engine-Konfigurationsleitfaden*. Navigieren Sie zu Masterinhaltsverzeichnis für RSA NetWitness Logs & Packets 11.x, um alle Dokumente zu NetWitness Suite 11.x zu suchen.

Abschnitt 2: Hardwarebezogene Troubleshooting-Informationen

Importieren einer fremden Konfiguration für die Appliance der Serie 4 mit externem Speicher

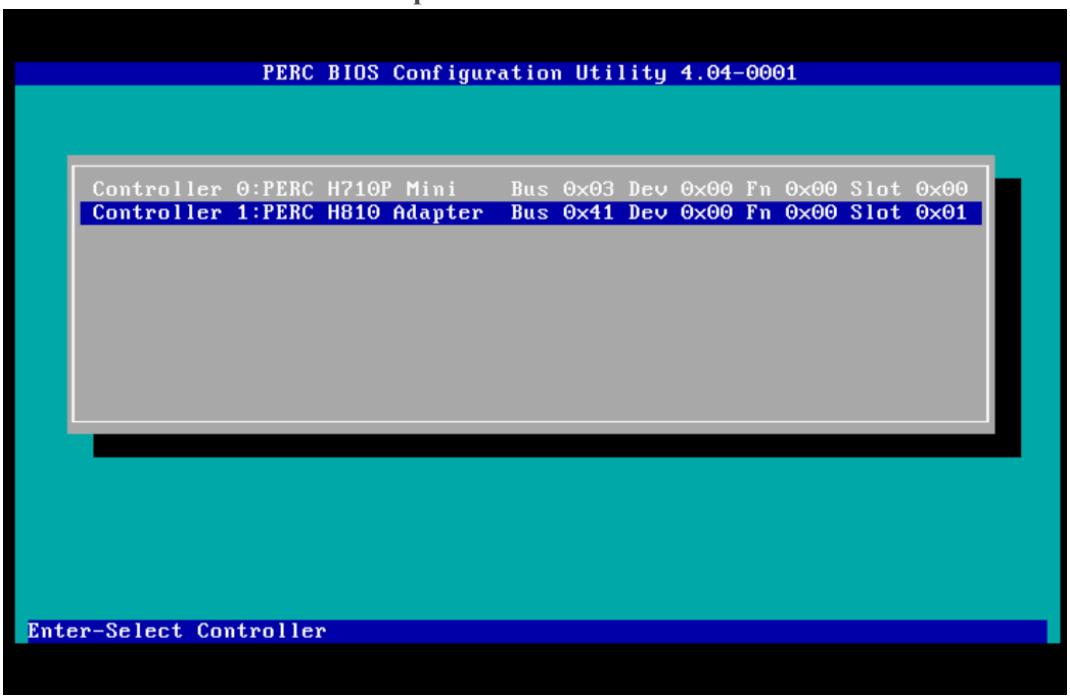
Wenn Sie einen Host mit externem Speicher (z. B. DAC) auf 11.1 aktualisieren und versuchen, die Appliance neu zu starten, erkennt das System möglicherweise, dass er über eine fremde Konfiguration verfügt. Führen Sie bei einer entsprechenden Fehlermeldung die folgenden Schritte durch:

1. Starten Sie die Appliance mit externem Speicher neu.
   Daraufhin werden die folgenden Meldungen angezeigt:



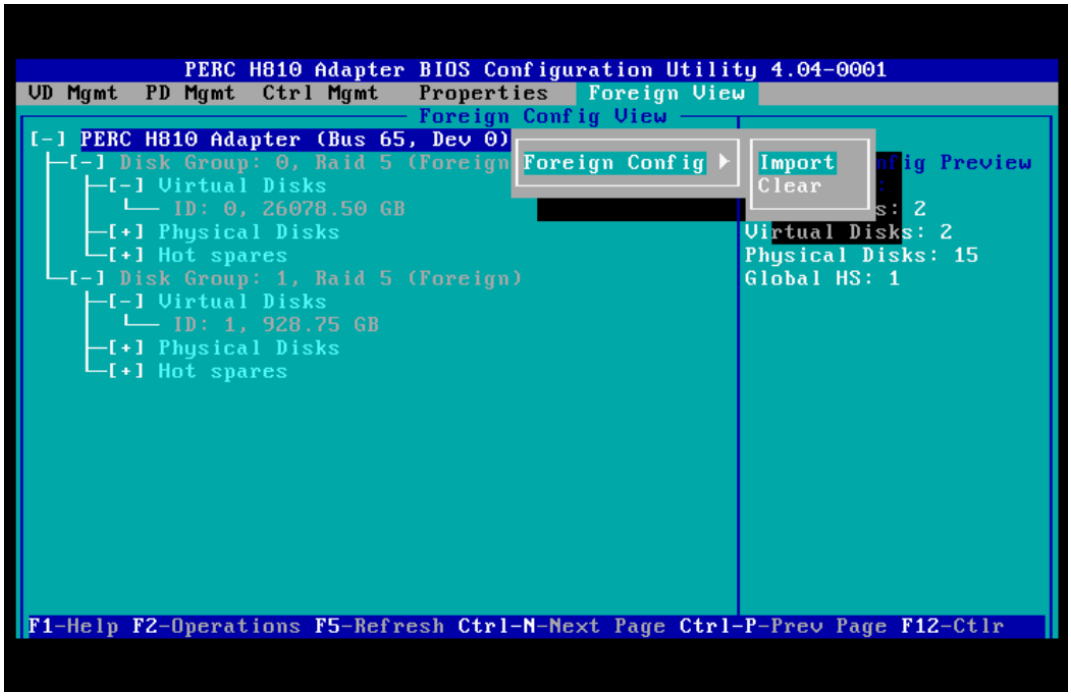
2. Drücken Sie die Taste **F** und starten Sie die Appliance neu.
   Wenn hierdurch die Konfiguration erfolgreich importiert und die Appliance neu gestartet wird, sind Sie fertig. Wenn es nicht funktioniert, fahren Sie mit Schritt 3 fort.

3. Drücken Sie **C**, um das Konfigurationsdienstprogramm zu starten.
   a. Wählen Sie den **PERC H8x0 Adapter** aus.

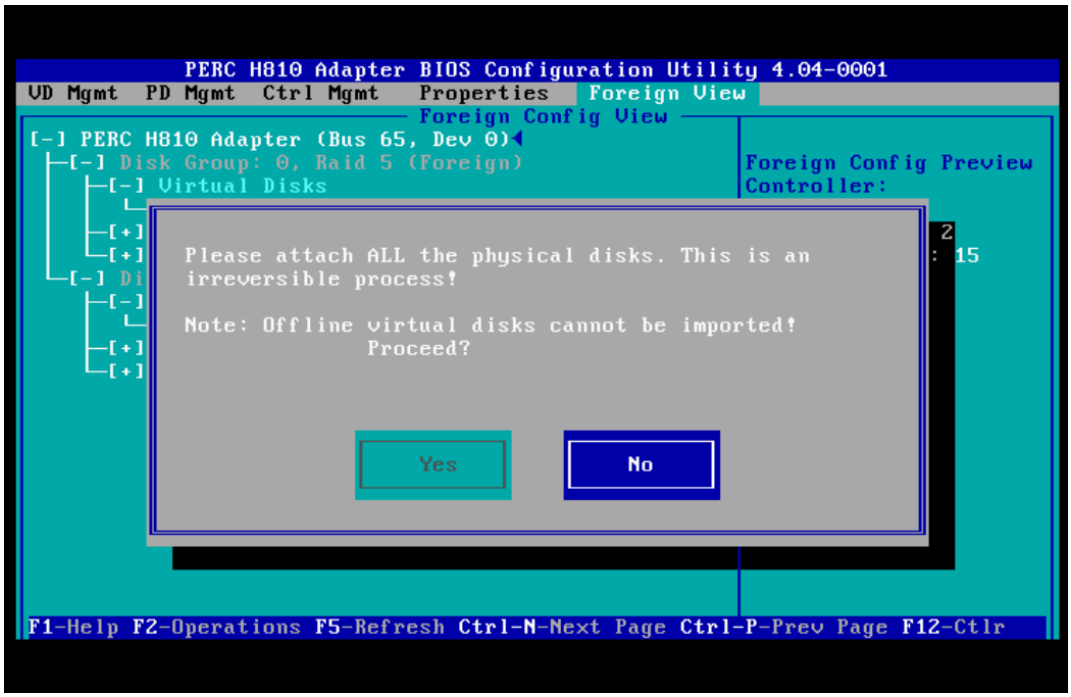


   b. Markieren Sie die erste Zeile [z. B. **PERC H810 Adapter (Bus 65, Dev 0)**].
   c. Wählen Sie **Foreign View** in der Menüleiste aus.

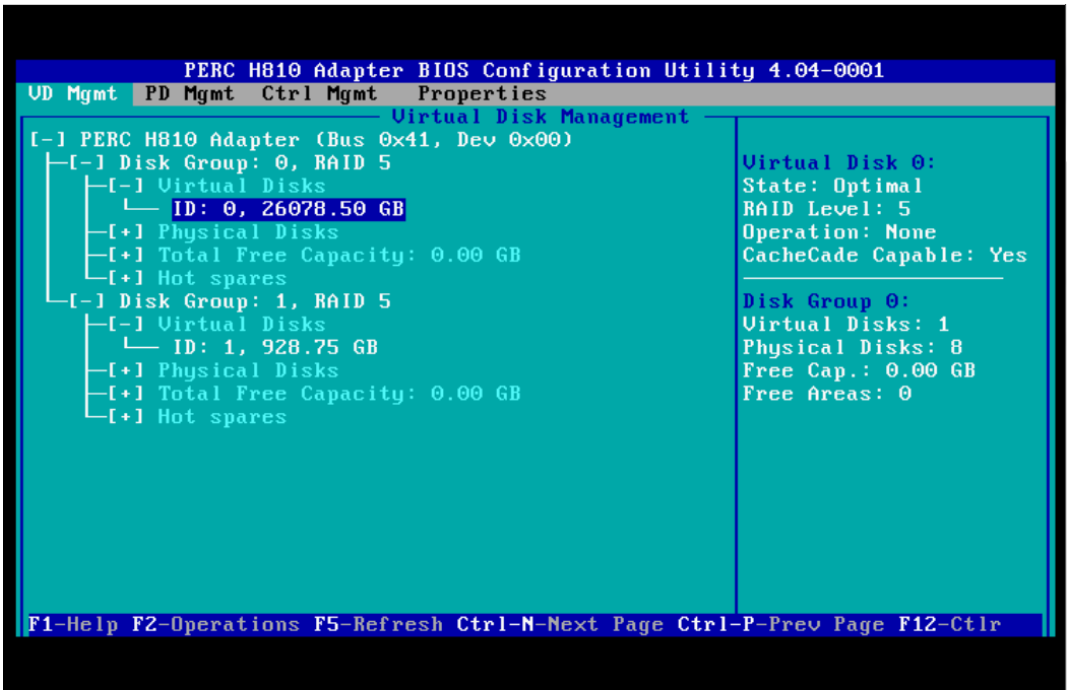
d. Drücken Sie **F2**, um das Drop-down-Menü **Fremde Konfiguration** aufzurufen und wählen Sie **Importieren** aus.



e. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie die fremde Konfiguration importieren möchten.

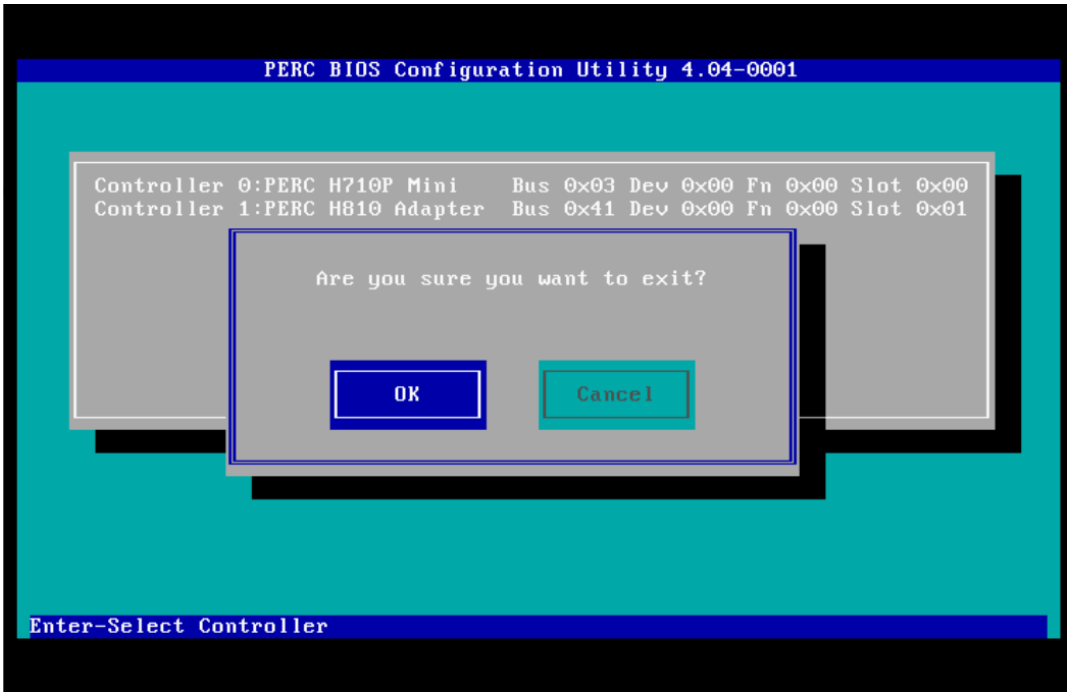


f. Stellen Sie sicher, dass keine weiteren fremden Konfigurationen auf dem System vorhanden sind.



g. Drücken Sie **Esc**, um den Vorgang zu beenden.

h. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie ihn beenden möchten.



4. Drücken Sie **STRG+ALT+ENTF**, um die Hardware-Appliance neu zu starten.

Achtung: Wenn die fremde Konfiguration fehlschlägt, wenden Sie sich an den Kundensupport (https://community.rsa.com/docs/DOC-1294).

Wiederherstellen der Dateien für den 10G-Decoder

Wenn Sie den 10G-Decoder-Hardwaretreiber verwenden und das `/etc/init.d/pf_ring`-Skript für die Verwendung von MTU aus der `/etc/pf_ring/mtu.conf`-Datei angepasst haben, müssen Sie die Dateien `mtu.conf` und `pf_ring` aus dem Verzeichnis `./etc/init/pfring_bkup` wiederherstellen.

1. Stellen Sie in Version 11.1 die Datei `pf_ring` im Verzeichnis /etc/init.d/ wieder her.
   `/etc/init.d/pf_ring`
2. Stellen Sie in 11.1 die Datei `mtu.conf` im Verzeichnis `/etc/pf_ring/` wieder her.
   `/etc/pf_ring/mtu.conf`

Anhang B: Beenden und Neustarten der Datenerfassung und -aggregation

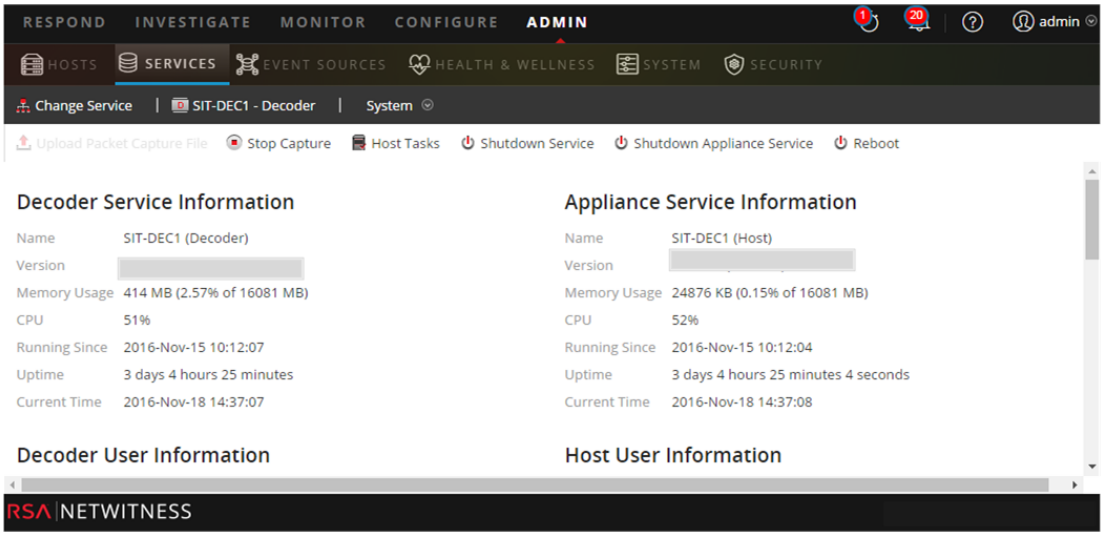
RSA empfiehlt, vor dem Upgrade eines Decoders, Concentrators oder Broker-Hosts auf 11.1.0.0 die Erfassung und Aggregation von Paketen und Protokollen zu beenden. Wenn Sie dies tun, müssen Sie nach der Aktualisierung der Hosts die Erfassung und Aggregation von Paketen und Protokollen neu starten.

Beenden der Datenerfassung und -aggregation

Beenden der Paketerfassung

So beenden Sie die Erfassung von Paketen:

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Decoder**-Services aus.



3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.
4. Klicken Sie in der Symbolleiste auf 

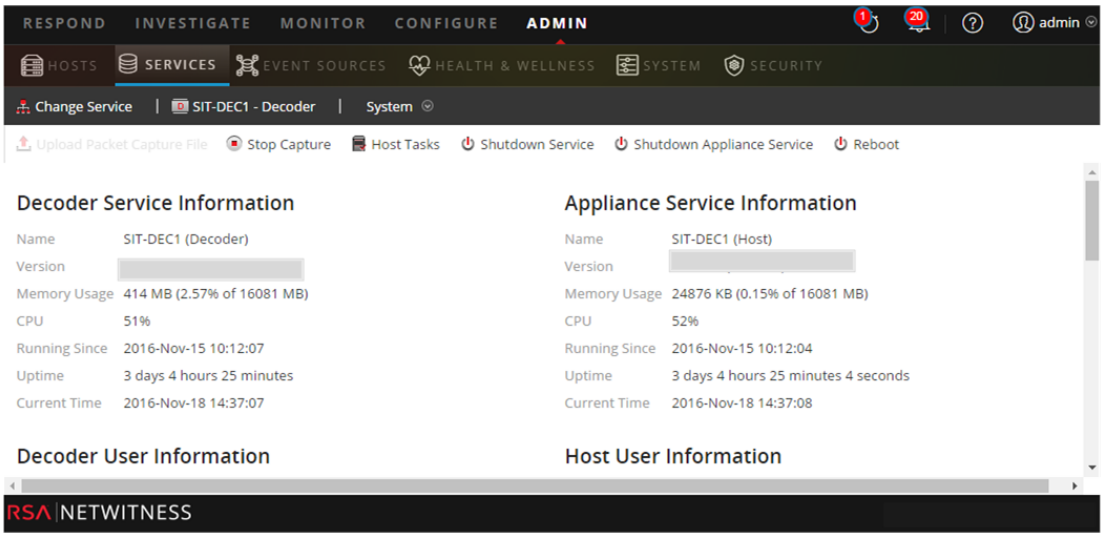
.

Beenden der Protokollerfassung

So beenden Sie die Protokollerfassung:

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN** > **Services**.
   Die Ansicht „Services“ wird angezeigt.

2. Wählen Sie die einzelnen **Log Decoder**-Services aus.



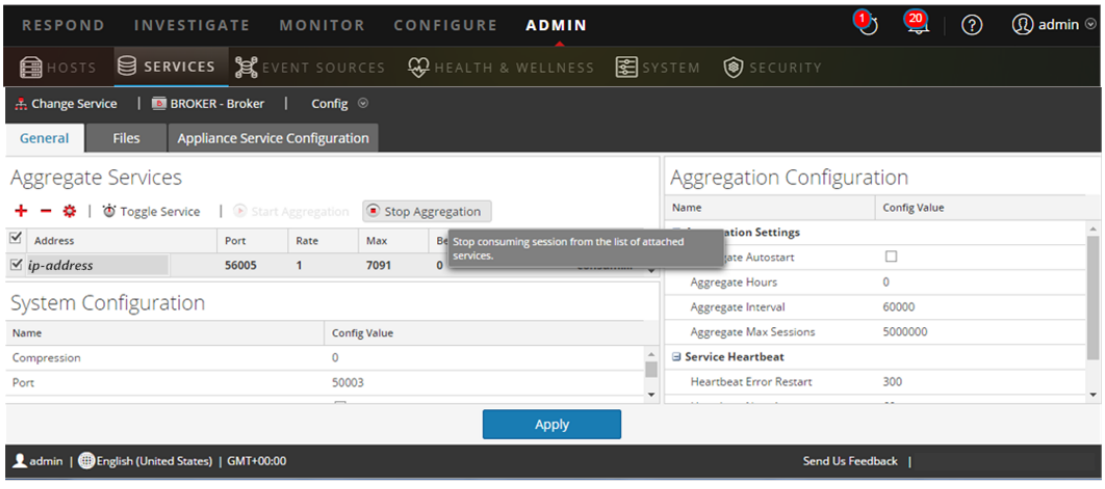
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.

4. Klicken Sie in der Symbolleiste auf 

.

Aggregation beenden

1. Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN** > **Services**.
2. Wählen Sie den **Broker**-Service aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **Konfiguration** aus.
4. Die Registerkarte **Allgemein** wird angezeigt.



5. Klicken Sie unter **Aggregierte Services** auf 

.

Starten der Datenerfassung und -aggregation

Starten Sie Paket- und Protokollerfassung sowie Paket- und Protokollaggregation nach der Aktualisierung auf 11.1.0.0 neu.

Starten der Paketerfassung

So starten Sie die Paketerfassung:

1. Wählen Sie im Menü **NetWitness Suite** die Optionen **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Decoder**-Services aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.
4. Klicken Sie in der Symbolleiste auf 

.

Starten der Protokollerfassung

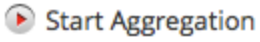
So starten Sie die Protokollerfassung:

1. Wählen Sie im Menü **NetWitness Suite** die Optionen **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie die einzelnen **Log Decoder**-Services aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **System** aus.
4. Klicken Sie in der Symbolleiste auf 

.

Aggregation starten

So starten Sie die Aggregation:

1. Wählen Sie im Menü **NetWitness Suite** die Optionen **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Für jeden Concentrator- und Broker-Service.
   a. Wählen Sie den
   -Service aus.
   b. Wählen Sie unter  (Aktionen) die Optionen **Ansicht** > **Konfiguration** aus.
   c. Klicken Sie in der Symbolleiste auf 

.

Anhang C: Verwenden von iDRAC

Viele Kunden verfügen über Remotestandorte mit eingeschränktem physischen Zugriff und begrenzter Bandbreite vom Desktop des Administrators. Wenn dies der Fall ist, können Sie iDRAC mit dem ISO-Image verwenden, das von einem NFS-Share freigegeben wird, der für die zu aktualisierenden oder zu installierenden Geräte lokal ist. Damit können Sie auch ein vorhandenes NetWitness-Gerät als Freigabehost verwenden.

Sie haben beispielsweise

- einen Concentrator und Decoder an einem geografisch entfernten Standort,
- die Bandbreite vom Standort des Administrators zu diesem Standort ist relativ gering,
- einen USB-Stick zu versenden und zu veranlassen, dass ihn jemand in die Geräte steckt, während Sie das Upgrade durchführen, ist keine praktikable Lösung.

In diesem Fall können Sie Folgendes tun:

1. Installieren Sie nfs-utils rpm.
2. Konfigurieren Sie die NFS-Freigabe.
3. Konfigurieren Sie iDRAC so, dass eine Verbindung zu diesem Share hergestellt wird. Stellen Sie sicher, dass Sie die von der iDRAC-Firmware unterstützten Windows- und Linux-Betriebssysteme aktualisieren. Zu diesem Zweck laden Sie die Dell Update-Pakete für unterstützte Windows- und Linux-Betriebssysteme über die Dell Support-Website unter http://www.support.dell.com herunter und führen diese aus. Weitere Informationen finden Sie im Benutzerhandbuch zum Dell Update-Paket auf der Dell Support-Website unter http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.

4. Starten Sie auf dem virtuellen Medium, das die ISO-Datei enthält, und fahren Sie mit dem Upgrade fort.

Konfigurieren von NFS-Server – NFS-Server-Config-Datei

1. Installieren Sie NFS und die allgemeinen Utilitys mithilfe von yum.
   ```
   yum install nfs-utils
   ```
2. Konfigurieren Sie den NFS-Service so, dass er beim Systemstart ausgeführt wird.
   ```
   chkconfig nfs on
   ```
3. Konfigurieren Sie den Service „rpcbind“ so, dass er beim Systemstart ausgeführt wird. Dieser Service ist für NFS erforderlich und muss ausgeführt werden, bevor NFS gestartet

werden kann.
`chkconfig rpcbind on`

4. Starten Sie den Service „rpcbind“.
   `service rpcbind start`
5. Starten Sie den NFS-Service:
   `service nfs start`
6. Erstellen Sie ein Verzeichnis für den ersten Export.
   `mkdir /exports/files`
7. Öffnen Sie die NFS-Exportdatei in einem Texteditor.
   `vi /etc/exports`
8. Um das Verzeichnis für alle Benutzer mit Lesezugriff zu exportieren, fügen Sie die folgende Zeile hinzu.
   `/exports/files *(ro)`
9. Speichern Sie die Änderungen und schließen Sie den Editor.
   `:wq!`
10. Exportieren Sie das oben definierte Verzeichnis.
    `exportfs -a`
11. Deaktivieren Sie während der Durchführung von Upgrades die Firewallregeln.
    `service iptables stop`
12. Kopieren Sie Installationsmedien mit der ISO-Datei in das Verzeichnis `/exports/files` .

Starten von iDRAC in der NFS-Konfiguration

Hinweis: Sie müssen sicherstellen, dass die idrac-Firmware mindestens 1.57.57 für Serie 4 (R620) ist.

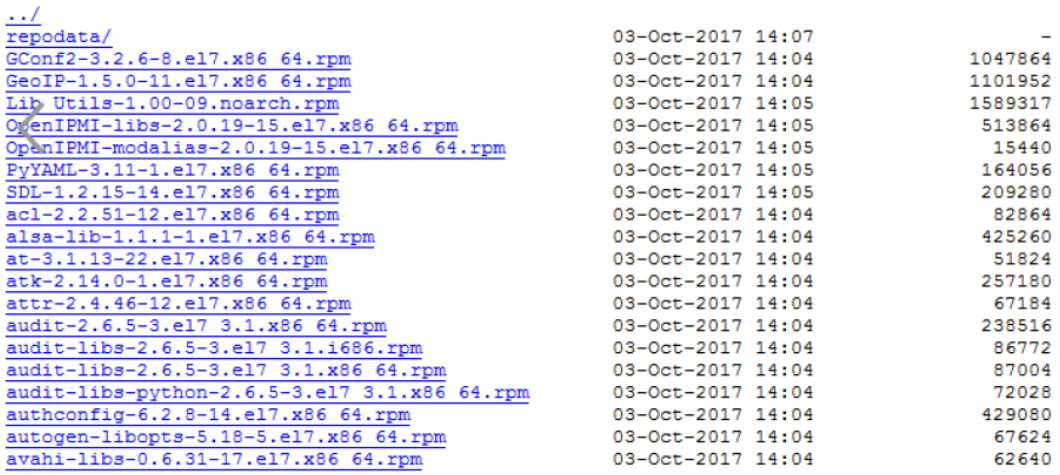
1. Melden Sie sich an der iDRAC-Benutzeroberfläche an.
2. Hängen Sie Medien über Remotedateifreigabe an.
   `<server ip>:/export/files/11.1.0.0.iso`
   Beispiel: `10.10.10.10:/exports/files/rsa-11.1.0.0.1948.el7-usb.iso`
3. Klicken Sie auf **Verbinden**.
4. Starten Sie die **Konsole**.
5. Wählen Sie aus dem Menü **Nächster Systemstart** die Option **Virtuelle DVD/CD** aus.
6. Starten Sie das Gerät neu.

Anhang D: Erstellen eines externen Repository

Führen Sie das folgende Verfahren aus, um ein externes Repository (Repo) einzurichten.

Hinweis: 1.) Auf dem Host muss ein Dienstprogramm zum Entpacken installiert sein, damit Sie dieses Verfahren abschließen können. 2.) Sie müssen wissen, wie Sie einen Webserver erstellen, bevor Sie das folgende Verfahren durchführen.

1. Melden Sie sich bei dem Webserverhost an.
2. Erstellen Sie ein Verzeichnis, um das NW-Repository (`netwitness-11.1.0.0.zip`) zu hosten, z. B. `ziprepo` unter `web-root` des Webservers. Beispiel: `/var/netwitness` ist der `web-root`, senden Sie die folgende Befehlszeichenfolge.
   `mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Erstellen Sie das Verzeichnis 11.1.0.0 unter `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Erstellen Sie die Verzeichnisse `OS` und `RSA` unter `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Entpacken Sie die Datei `netwitness-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   Durch das Entpacken von `netwitness-11.1.0.0.zip` entstehen zwei Zip-Dateien (`OS-11.1.0.0.zip` und `RSA-11.1.0.0.zip`) und einige andere Dateien.
6. Entpacken Sie die Datei:
   a. `OS-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
      Das folgende Beispiel zeigt, wie die Dateistruktur des Betriebssystems (OS) angezeigt wird, nachdem Sie die Datei entpackt haben.

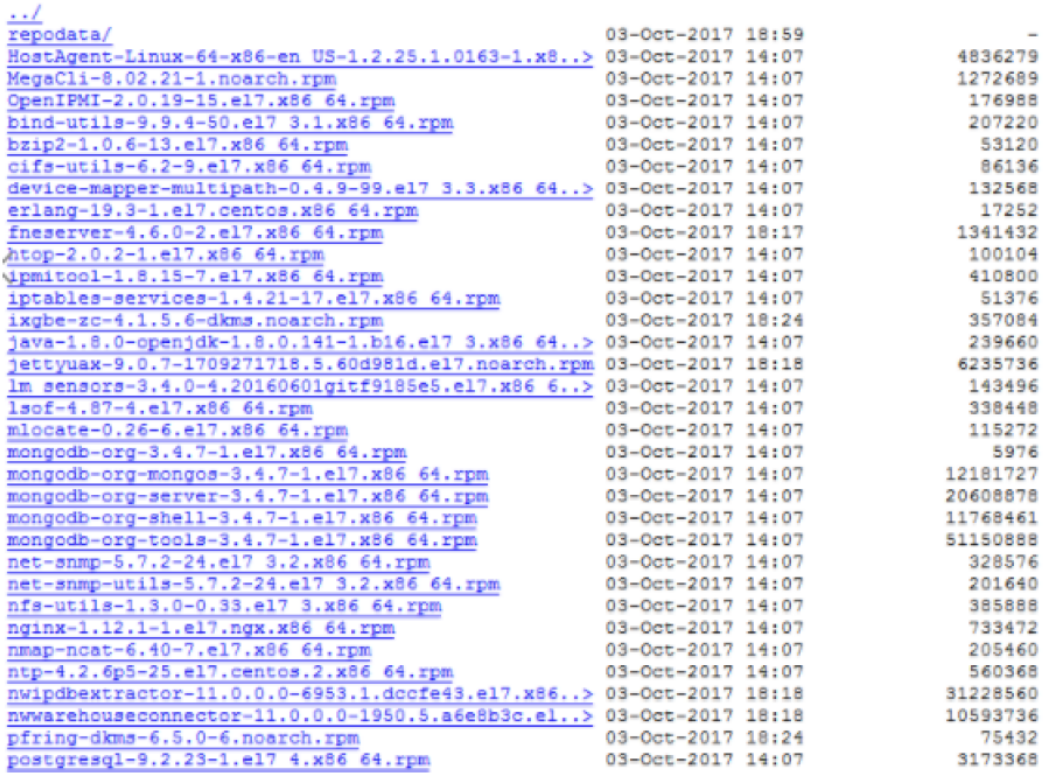


../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

b. `RSA-11.1.0.0.zip` in das Verzeichnis `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA
```

Das folgende Beispiel zeigt, wie die Dateistruktur der RSA Versionsaktualisierung angezeigt wird, nachdem Sie die Datei entpackt haben.



../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

Der externe URL für das Repository ist `http://<web server IP address>/<your-zip-file-repo>`.

7. Verwenden Sie die `http://<web server IP address>/<your-zip-file-repo>` als Antwort auf die Eingabeaufforderung **Geben Sie den Basis-URL des externen Update-Repository ein** des NW 11.1.0.0 Setup-Programms (`nwsetup-tui`).

Revision History

Revision	Date	Description	Author
1.0	8-Mar-18	Release to Operations (RTO)	IDD