



# Upgradehandbuch für virtuelle Hosts

für Version 11.0



## **Kontaktinformationen**

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

## **Marken**

Eine Liste der RSA-Marken finden Sie unter [germany.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://germany.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **Lizenzvereinbarung**

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

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

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

## **Drittanbieterlizenzen**

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

## **Hinweis zu Verschlüsselungstechnologien**

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

## **Verteilung**

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

Februar 2018

# Inhalt

---

<b>Einleitung</b> .....	<b>7</b>
Upgrade von CentOS6 auf CentOS7 .....	7
Upgrade-Pfad für RSA NetWitness® Suite 11.0 .....	8
Unterstützte Host-Upgradepfade .....	8
In 11.0 nicht unterstützte Hardware, Bereitstellungen, Services und Funktionen .....	8
Zu berücksichtigende Aspekte beim Upgrade von Event Stream Analysis (ESA) .....	9
Änderungen an Benutzerattributen und Rollen, die sich auf Investigate auswirken .....	10
Phasen des Upgrades .....	11
Investigate im gemischten Modus .....	12
Wenden Sie sich an den Kundensupport .....	17
<b>Vorbereitung des Upgrades</b> .....	<b>18</b>
Global .....	18
Aufgabe 1: Prüfen der Core-Ports und Öffnen von Firewallports .....	18
Aufgabe 2: Notieren des 10.6.4.x admin user-Passworts .....	19
Aufgabe 3: Erstellen eines Backups der /etc/fstab -Datei .....	19
Reporting Engine .....	19
(Bedingungsabhängig) Aufgabe 4: Trennen des externen Speichers .....	19
Respond und Incident-Management .....	20
(Bedingungsabhängig) Aufgabe 5: Deaktivieren der Datenaufbewahrung für Incident- Management .....	20
<b>Anweisungen zum Backup</b> .....	<b>21</b>
Aufgabe 1: Einrichten eines externen Hosts für die Sicherung von Dateien .....	23
Aufgabe 2: Erstellen einer Liste der zu sicherenden Hosts .....	24
Troubleshooting-Informationen .....	25
Aufgabe 3: Einrichten der Authentifizierung zwischen Backup- und Zielhosts .....	27
Aufgabe 4: Überprüfen der Backupanforderungen für bestimmte Hosttypen .....	27
Für alle Hosttypen .....	27
Für Decoder-, Concentrator- oder Broker-Hosts: Beenden der Datenerfassung und - aggregation .....	28
Log Collectors (LC) und Virtual Log Collectors (VLCs): prepare-for-migrate.sh ausführen	29

Für Integrationen mit Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpoint: Auflisten der RabbitMQ-Benutzernamen und -Passwörter .....	30
Für Bluecoat-Ereignisquellen .....	31
Aufgabe 5: Überprüfen auf ausreichend Speicherplatz für das Backup .....	31
Aufgabe 6: Sichern der Hostsysteme .....	32
Aufgaben nach dem Backup .....	35
Aufgabe 1: Speichern einer Kopie der Datei all-systems und der TAR-Backupdateien ...	35
Aufgabe 2: Sicherstellen, dass die erforderlichen Backupdateien generiert wurden .....	35
Aufgabe 3: (Bedingungsabhängig) Für mehrere ESA-Hosts – Kopieren der mongodb tar - Dateien zum primären ESA-Host .....	36
Aufgabe 4: Sicherstellen, dass alle erforderlichen Backupdateien auf jedem Host vorhanden sind .....	36
<b>Migrieren von Festplattenlaufwerken von 10.6.4.x zu 11.0 .....</b>	<b>39</b>
Aufgabe 1: Sichern der Daten auf den 10.6.4.x VMs .....	39
Aufgabe 2: Bereitstellen des gleichen 10.6.4.x VM-Stacks in 11.0 .....	40
Aufgabe 3: Kopieren und Hinzufügen der VMDK-Dateien zu den neuen virtuellen Maschinen als Festplatte .....	41
Aufgabe 4: Beibehalten der MAC-Adresse der aktualisierten SA-Server-VM .....	47
Aufgabe 5: Wiederherstellen der Backupdaten aus 10.6.4.x auf den 11.0 VMs .....	50
<b>Einrichten von virtuellen Hosts in Version 11.0 .....</b>	<b>56</b>
Phase 1: Einrichtung von SA-Server, Event Stream Analysis, Malware Analysis sowie Broker oder Concentrator-Hosts .....	56
Aufgabe 1: Einrichten von Version 11.0 NetWitness-Server .....	56
Aufgabe 2: Einrichten von 11.0 ESA .....	56
Aufgabe 3: Einrichten von 11.0 Malware Analysis .....	57
Aufgabe 4: Einrichten von 11.0 Broker oder Concentrator .....	57
Phase 2: Einrichtung der übrigen Komponentenhosts .....	57
Decoder und Concentrator-Hosts .....	57
Log Decoder-Host .....	57
Virtual Log Collector-Host .....	58
Einrichten des 11.0 NW-Serverhosts .....	59
Einrichten eines 11.0 Nicht-NW-Serverhosts .....	64

<b>Aktualisieren oder Installieren der Legacy Windows Collection .....</b>	<b>71</b>
<b>Aufgaben nach dem Upgrade .....</b>	<b>72</b>
Globale Aufgaben .....	72
Aufgabe 1: Entfernen von backupbezogenen Dateien aus den lokalen Hostverzeichnissen .....	72
Aufgabe 2: Wiederherstellen der NTP-Server .....	73
Aufgabe 3: Wiederherstellen von Lizenzen für Umgebungen ohne Zugriff auf FlexNet Operations-On Demand .....	73
Aufgabe 4: Erneutes Zuordnen der virtuellen NW-Serverlizenz zur MAC-Adresse 10.6.4.x .....	74
(Bedingungsabhängig) Aufgabe 5: Hinzufügen von benutzerdefinierten IPtables, sofern die Standardkonfiguration der Firewall deaktiviert wurde .....	74
(Bedingungsabhängig) Aufgabe 6: Angeben der SSL-Ports, sofern keine vertrauenswürdigen Verbindungen eingerichtet wurden .....	74
NetWitness Endpoint .....	76
Aufgabe 7: Erneutes Konfigurieren von Endpoint-Warmmeldungen über Nachrichtenbus	76
Aufgaben für Event Stream Analysis (ESA) .....	76
Aufgabe 8: Neukonfigurieren der automatisierten Bedrohungserkennung für ESA .....	76
Aufgabe 9: Konfigurieren von gegenseitig authentifiziertem SSL für Integrationen mit Web Threat Detection, NetWitness SecOps Manager oder NetWitness Endpoint .....	77
Aufgabe 10: Aktivieren des Dashboards „Bedrohung – Malwareindikatoren“ .....	78
Protokollsammlung .....	78
Aufgabe 11: Zurücksetzen der stabilen Systemwerte für Log Collector nach dem Upgrade .....	78
(Optional für Upgrades von 10.6.4.x mit für Log Collectors, Log Decoder und Packet Decoder aktiviertem FIPS) Aufgabe 12: Aktivieren des FIPS-Modus .....	79
Reporting Engine .....	79
Aufgabe 13: Wiederherstellen der CA-Zertifikate für externe Syslog-Server für die Reporting Engine .....	79
(Bedingungsabhängig) Aufgabe 14: Wiederherstellen von externem Speicher für die Reporting Engine .....	80
Reagieren .....	80
Aufgabe 15: Wiederherstellen der benutzerdefinierten Schlüssel für den Antwortservice	80
Aufgabe 16: Wiederherstellen der angepassten Skripte zur Normalisierung des Antwortservice .....	81

(Bedingungsabhängig) Aufgabe 17: Aktivieren der deaktivierten 10.6.4.x-Datenaufbewahrung für das Incident-Management .....	81
(Bedingungsabhängig) Aufgabe 18: Wiederherstellen von benutzerdefinierten Analystenrollen .....	82
NetWitness SecOps Manager .....	82
Aufgabe 19: Neukonfigurieren der NW SecOps Manager-Integration .....	82
Sicherheit .....	82
Aufgabe 20: Migrieren von Active Directory (AD) .....	82
Aufgabe 21: Ändern der migrierten AD-Konfiguration, um das Zertifikat hochzuladen ..	83
Aufgabe 22. Beheben von Fehler bei Authentifizierung in 11.0 .....	83
Aufgabe 23: Neukonfigurieren des Pluggable Authentication Module (PAM) in 11.0 ....	83
<b>Anhang A: Troubleshooting .....</b>	<b>84</b>
11.0 Setup-Programm (nwsetup-tui) .....	85
Backup (nw-backup-Skript) .....	86
Event Stream Analysis .....	86
Allgemein .....	87
Log Collector-Service (nwlogcollector) .....	88
NW Server .....	90
Reporting Engine-Service .....	90
<b>Anhang B: Beenden und Neustarten der Datenerfassung und -aggregation .....</b>	<b>91</b>
Beenden der Datenerfassung und -aggregation .....	91
Starten der Datenerfassung und -aggregation .....	93
<b>Revisionsverlauf .....</b>	<b>94</b>

## Einleitung

---

Die Anweisungen in diesem Handbuch gelten nur für das Upgrade von virtuellen Hosts auf RAS NetWitness Suite 11.0. Im *RSA NetWitness Suite Physical Host Upgrade Guide* finden Sie Anweisungen zum Upgrade Ihrer virtuellen Hosts von 10.6.4.x auf 11.0. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

NetWitness Suite 11.0 ist eine Hauptversion, die alle Produkte der NetWitness Suite betrifft. Die Suite umfasst die folgenden Komponenten: NetWitness-Server (NW Server), Archiver, Broker, Concentrator, Context Hub, Decoder, Entity Behavior Analytics, Event Stream Analysis, Hybrid, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response, Warehouse Connector und Workbench.

### Upgrade von CentOS6 auf CentOS7

NetWitness Suite 11.0 ist eine Hauptversion, bei der ein Upgrade auf eine neuere Version des Betriebssystems (CentOS6 auf CentOS7) durchgeführt wird. Die Plattformumgebung der Version 11.0 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 11.0

Der unterstützte Upgrade-Pfad für RSA NetWitness® Suite 11.0 ist Security Analytics 10.6.4.x. Wenn Sie eine Version von NetWitness Suite vor 10.6.4.x verwenden, müssen Sie ein Update auf 10.6.4.x durchführen, bevor Sie auf 11.0 aktualisieren können. Siehe *RSA Security Analytics 10.6.4 – Aktualisierungsanweisungen* in RSA Link (<https://community.rsa.com/docs/DOC-79055>).

**Achtung:** Es liegt ein bekanntes Problem vor, wenn Sie Active Directory-Benutzer in 10.6.4.x konfiguriert haben. Zur Behebung dieses Problems haben Sie zwei Möglichkeiten:

- Wenden Sie den Patch 10.6.4.2 an, bevor Sie Ihre Daten für das Upgrade auf 11.0 sichern.
- Wenn Sie den Patch 10.6.4.2 nicht anwenden konnten, können Sie unmittelbar nach dem Upgrade auf 11.0 den Patch 11.0.0.1 anwenden.

## 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 11.0 keine Unterstützung für physische Hosts von Drittanbietern.
- Virtuell lokal auf virtuell lokal

**Achtung:** Das 11.0-Upgrade bietet keine Unterstützung für gemischte Plattformupgrades (z. B. wird physisch zu virtuell nicht unterstützt).

## In 11.0 nicht unterstützte Hardware, Bereitstellungen, Services und Funktionen

RSA unterstützt für die folgende Hardware bzw. die folgenden Bereitstellungen, Services und Funktionen kein Upgrade auf 11.0.

- RSA All-in-One (AIO) Appliance
- Mehrere NetWitness-Server-Bereitstellungen
- Hosts, die in AWS bereitgestellt werden (Sie können AWS-Hosts in 11.0 bereitstellen, aber keine in 10.6.4.x bereitgestellten AWS-Hosts aktualisieren.)



- Hosts, die in Azure bereitgestellt werden (Sie können Azure-Hosts in 11.0 bereitstellen, aber keine in 10.6.4.x bereitgestellten Azure-Hosts aktualisieren.)
- IPDB-Service
- Malware Analysis-Service, der sich ebenfalls auf dem SA-Server befindet (Upgrade von Malware Analysis Enterprise wird in 11.0 unterstützt.)
- Eigenständiger Warehouse Connector-Service (Upgrade eines ebenfalls vorhandenen Warehouse Connector wird in 11.0 unterstützt.)
- Benutzerdefinierte Policy hinsichtlich Integrität und Zustand in 10.6.x für Context Hub Service  
Nach einem Upgrade auf NetWitness 11.0 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 11.0 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 11.0 hat RSA die Art und Weise geändert, wie ESA-Korrelationsregeln die vom System generierten Warnmeldungen speichern und übertragen. In 11.0 sendet ESA alle Warnmeldungen an ein zentrales Warnmeldungssystem. Der lokale Mongo-Speicher in ESA 10.6.4.x wurde entfernt.

**Achtung:** Wenn Sie in 10.6.4.x kein Incident-Management verwenden, überlegen Sie sehr gut, ob Sie auf Version 11.0 aktualisieren oder nicht.

Die folgenden Richtlinien sollten Sie Ihnen dabei helfen, herauszufinden, ob Sie Ihre ESA-Hosts auf 11.0 aktualisieren sollten.

Wenn Sie in Ihrer 10.6.4.x-Bereitstellung ...

- über einen ESA-Host mit oder ohne konfiguriertem Incident-Management verfügen, führen Sie ein Upgrade auf 11.0 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 10.6.4.x wie erwartet arbeitet, können Sie ein Upgrade auf Version 11.0 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 11.0 durch.

**Hinweis:** Wenn Sie in 10.6.4.x kein Incident-Management verwendet haben, können Sie die ESA-Warnmeldungen von 10.6.4.x nicht in der 11.0-Respond-Komponente anzeigen, ohne ein Migrationsskript auszuführen. Verwenden Sie das Skript *ESA Alert Migration*, um diese Warnmeldungen zu dem Ort in 11.0 zu migrieren, wo sie von der Respond-Komponente angezeigt werden können. Anweisungen zur Ausführung dieses Skripts finden Sie im Artikel *ESA Alert Migration Instructions for 10.6.4.x to 11.0* der Wissensdatenbank (<https://community.rsa.com/docs/DOC-81680>) in RSA Link.

## Änderungen an Benutzerattributen und Rollen, die sich auf Investigate auswirken

Die folgenden Änderungen haben Auswirkungen darauf, wie NetWitness Suite 11.0 Benutzer- und Rollenattribute in der Komponente Investigate verarbeitet.

- Benutzerattribute  
Wenn Sie ein Upgrade auf 11.0 durchführen, sind die in SA 10.6.4.x verfügbaren Benutzerattribute (Abfragepräfix, Sitzungs-Timeout und Abfrageschwellenwert) nicht mehr vorhanden. Diese Attribute sind auf Rollenebene verfügbar.  
Wenn Sie die Benutzerattribute zur Einschränkung des Benutzerzugriffs verwendet haben, führen Sie den Patch von RSA NetWitness® Suite 11.0.0.1 unmittelbar nach dem Upgrade auf 11.0.0.0 durch, um dieses Problem zu umgehen.
- Die Benutzer- und Rollenattribute (Abfragepräfix) gelten nicht für Ereignisanalysen von Investigate. Die Benutzer- und Rollenattribute, vor allem die Abfragepräfix, gelten nicht für die neuen Ereignisanalysen von Investigate. Jeder Benutzer kann die URL im Browser für den Zugriff auf Daten ändern, deren Anzeige eingeschränkt werden soll, selbst wenn der Abfragepräfix angewendet wird.  
Wenden Sie als Workaround Patch RSA NetWitness® Suite 11.0.0.1 sofort nach dem Upgrade auf 11.0.0.0 an.

**Achtung:** Wenn Sie Benutzer- oder Rollenattribute in 10.6.4.x konfiguriert haben, einschließlich Abfragepräfix, wenden Sie den Patch RSA NetWitness® Suite 11.0.0.1 sofort nach dem Upgrade auf 11.0.0.0 an. Nachdem Sie diesen Patch angewendet haben, führen Sie die Patch-Anweisungen aus, um zusätzliche Sicherheitskontrollen anzuwenden.

## 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 11.0-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 11.0 NW-Server kann für die neue Investigate-Funktionalität nicht mit den 10.6.4.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.

In Phase 2 besteht kein technischer Grund dafür, Ihre Hosts in der folgenden Reihenfolge zu aktualisieren (mit Ausnahme der Log Collection-Hosts mit Downstream-Ereigniszielen). 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

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 „Running in Mixed Mode“ unter „The Basics“ im RSA 11.0 *NetWitness Suite Hosts and Services Getting Started Guide* finden Sie Informationen zu:

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

Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Investigate im gemischten Modus

Der gemischte Modus wird ausgeführt, wenn einige Services auf 11.0 aktualisiert werden und einige noch auf 10.6.x basieren. Dies ist der Fall, wenn Sie ein phasenweises Upgrade auf 11.0 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 11.0-Investigate-Server wird installiert, wenn Sie den SA-Server aktualisieren, Broker-Hosts müssen aber auf 11.0 aktualisiert werden, um auf die Ansicht der Ereignisanalyse zuzugreifen.

Nachdem Sie alle Services auf 11.0 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 11.0 aktualisiert, während andere noch auf 10.6.x 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 scheinen zu funktionieren, dann wird aufgrund unzureichender Berechtigungen allerdings 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 11.0 aktualisiert haben, funktioniert RBAC für alle Services gleich.

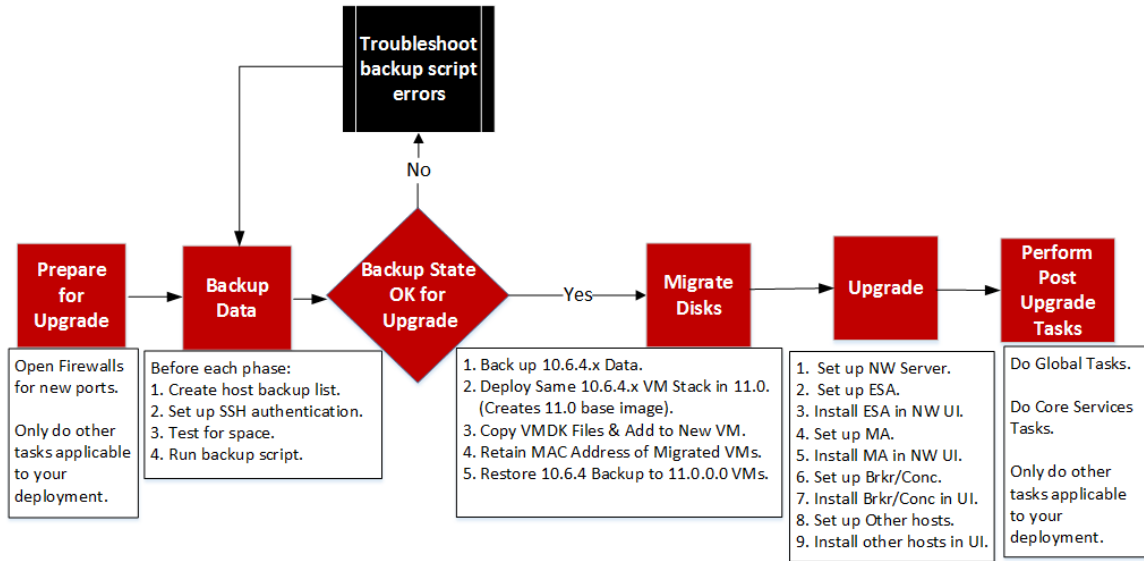
In dieser Tabelle ist angegeben, was Sie in Investigate anzeigen und herunterladen können, wenn Ihr NW-Server Version 11.0 aufweist und mit Services einer niedrigeren Version verbunden ist.

Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle	Anzeige	Download erfolgreich	Download abgeschlossen mit Fehlern
	Ansicht Ereignisse	Analyst		PCAP	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich
11.0 Broker -> 10.x Concentrator -> 10.x Packet Decoder/Log Decoder	Ansicht der Ereignisrekonstruktion	Analyst		PCAP	Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich
	Ansicht der Ereignisanalyse	Analyst		PCAP	Fehler beim Abrufen der Nutzlast vom Service für Payload, Request Payload, Response Payload

Version des verbundenen Service	Betroffene Anzeige	Benutzerrolle	Anzeige	Download erfolgreich	Download abgeschlossen mit Fehlern
	Ansicht der Ereignisrekonstruktion	Administrator			Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich
11.0 Broker -> 11.0 Concentrator -> 11.0 Decoder/Log Decoder	Ansicht der Ereignisrekonstruktion	Analyst und Data Privacy Officer	Von RBAC erlaubte Elemente		Dateiarchiv wird heruntergeladen, Entpacken aber nicht möglich PCAPs und Protokolle werden als 0 Byte heruntergeladen



**RSA NetWitness Suite® 11.0 VM Upgrade Workflow**  
 Phase 1 – Upgrade SA Server, ESA, and Malware  
 Phase 2 – Upgrade All Other Hosts



## 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 11.0 erhalten.

## Vorbereitung des Upgrades

Führen Sie die folgenden Aufgaben durch, um das Upgrade auf NetWitness Suite 11.0 vorzubereiten. Diese Aufgaben sind nach den folgenden Kategorien unterteilt:

- [Global](#)
- [Reporting Engine](#)
- [Respond und Incident-Management](#)

### 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 der folgende Tabelle sind die neuen Ports in 11.0 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

Alle NetWitness Suite-Core-Ports werden im Thema „Netzwerkarchitektur und Ports“ im *RSA NetWitness® Suite Leitfaden zur Bereitstellung* aufgeführt, falls Sie die Services und Firewalls von NetWitness Suite neu konfigurieren müssen. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Aufgabe 2: Notieren des 10.6.4.x admin user-Passworts

Notieren Sie sich Ihr 10.6.4.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 VMs auf Ihren lokalen Rechner (Backuphost oder Remoterechner).

**Hinweis:** Sie benötigen diese Datei zur Wiederherstellung einer VM mit externen Speichermounts.

## Reporting Engine

### (Bedingungsabhängig) Aufgabe 4: 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`

## Respond und Incident-Management

### **(Bedingungsabhängig) Aufgabe 5: Deaktivieren der Datenaufbewahrung für Incident-Management**

Gehen Sie wie folgt vor, um die Datenaufbewahrungsaufträge für das Incident-Management in 10.6.4.x zu deaktivieren

1. Melden Sie sich bei RSA Security Analytics 10.6.4.x an.
2. Navigieren Sie zu **Incident-Management > Konfigurieren > Aufbewahrungsplaner**.
3. Deaktivieren Sie das Kontrollkästchen **Datenaufbewahrungsplaner aktivieren** und klicken Sie auf **Anwenden**.

## Anweisungen zum Backup

---

Eine Sicherung Ihrer Konfigurationsdaten für alle Hosts von 10.6.4.x ist der erste Schritt beim Upgrade von 10.6.4.x auf 11.0.0.0.

**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 11.0.0.0 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:** 1) Diese Services werden beim Backup- und Upgrade-Prozess für 10.6.4.x nicht unterstützt.

- IPDB
- All-in-One-Server
- Malware Analysis, ebenfalls auf dem NetWitness-Server
- Eigenständiger Warehouse Connector

2) Es liegt ein bekanntes Problem vor, wenn Sie Active Directory-Benutzer in 10.6.4.x konfiguriert haben. Zur Behebung dieses Problems haben Sie zwei Möglichkeiten:

- Wenden Sie den Patch 10.6.4.2 an, bevor Sie Ihre Daten für das Upgrade auf 11.0 sichern.
- Wenn Sie den Patch 10.6.4.2 nicht anwenden konnten, können Sie unmittelbar nach dem Upgrade auf 11.0 den Patch 11.0.0.1 anwenden.

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

- **NetWitness-Server** (kann Malware Analysis, NetWitness Respond, Integrität und Zustand und Reporting Engine umfassen)
- **Malware Analysis** (eigenständig)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (einschließlich Context Hub und NetWitness Respond-Datenbank)
- **Concentrator**
- **Log Decoder** (einschließlich lokaler Log Collector und Warehouse Connector, falls installiert)
- **Log Hybrid**

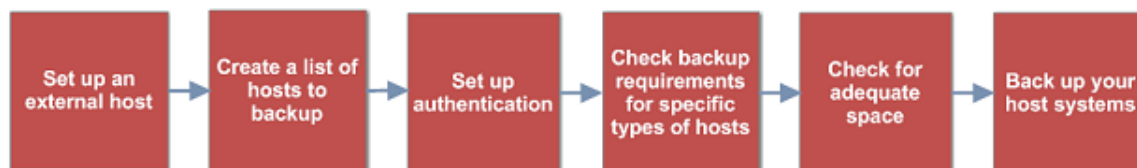
- **Packet Decoder** (einschließlich Warehouse Connector, falls installiert)
- **Packet Hybrid**
- **Virtual Log Collector**

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 11.0.0.0“ 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](#).

**Hinweis:** Wenn Sie beim Backup oder Upgrade auf Probleme stoßen und Daten verloren gehen, können Sie die Daten wiederherstellen und den Prozess erneut starten. Informationen zur Wiederherstellung von verloren gegangenen Daten finden Sie unter „Wiederherstellen von Daten nach Systemausfall“ im *Leitfaden Systemwartung*.

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 sicherenden 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 NetWitness Suite-Host-Stack ausgeführt werden.

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.

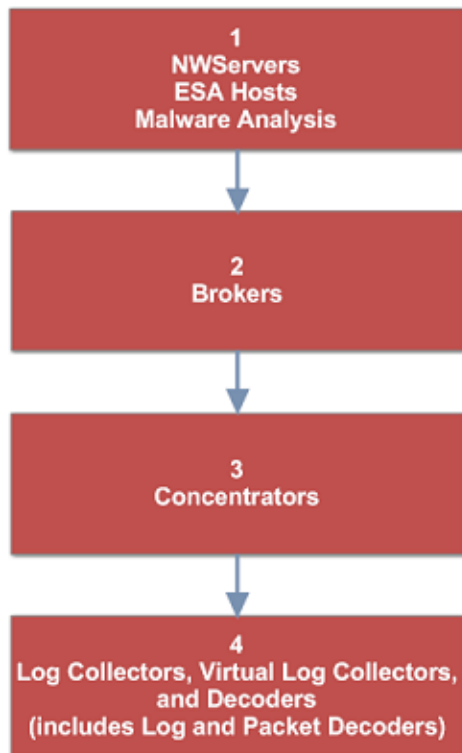
Es gibt verschiedene Skripte, die Sie während des Backups ausführen. Sie müssen die ZIP-Datei, die die Skripte (`nw-backup-v3.0.zip`) enthält, von RSA Link herunterladen unter: <https://community.rsa.com/docs/DOC-81514>. Kopieren Sie sie in Ihr CentOS 6-Backupsystem. Klicken Sie auf den Link **RSA NetWitness Logs & Packets 11.0 Backup Script (nw-backup-v3.0.sh)** und 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 NetWitness-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 Passwordeingabe aufgefordert werden.
- `nw-backup.sh`: Führt das Backup Ihrer Hosts durch.

**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-NetWitness-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/`.

- Überprüfen Sie, ob die Dateien `all-systems` und `all-systems-master-copy` generiert wurden und die richtigen Hosts enthalten.
- 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.

**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,10.6.4.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.4.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.4.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.4.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.4.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.4.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.4.0
```

Und hier ist ein Beispiel für eine `all-systems`-Datei basierend auf der `all-systems-master-copy`-Datei, die in der ersten Backupsitzung verwendet werden könnte:

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.4.0
```

## 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, bereits vorhandene Einträge aus der Datei zu entfernen, sodass die Datei nur die Hosts enthält, die aktuell gesichert werden. 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 NetWitness Suite-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 NetWitness Suite die NetWitness Suite-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 NetWitness-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 NetWitness-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 NetWitness-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 11.0.0.0 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 NetWitness-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-Zertifikatsdatei 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 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 und Neustarten 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 Upgradeaufgaben 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 11.0.0.0 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.
- Ereignisherenausgeber 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 10.6.4.x-Host bzw. auf dem NetWitness-Server-Host müssen Sie eine Liste aller RabbitMQ-Benutzernamen und -Passwörter abrufen, damit Sie nach dem Upgrade auf 11.0.0.0 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 Endpoint – 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 10.6.4.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 10.6.4.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`.

```

***** NW-BACKUP SCRIPT - TEST MODE *****
* * RSA nw-backup script is running in test mode where in it will only verify the disk space required for successful backup.
-----
CONTENT options currently selected:
-----
Backup IPDB?           'no'           Backup Yum Repo?      'no'
Backup Malware Analysis repository? 'no'          Backup SA Colo MA?   'no'
Backup Reporting Engine repository? 'no'          Backup /var/log?      'no'
Backup ESA DB?         'yes'          Backup Context Hub?   'yes'
Backup SMS RRD?        'yes'
-----
Checking that the environment is configured for proper execution of script...
Backup path configured... [ OK ] Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence... [ OK ]
Check for all-systems file... [ OK ]
Dated backup dir... [ OK ] Backup directory: /var/netwitness/database/nw-backup/2017-09-18
Logging to /var/netwitness/database/nw-backup/rsa-nw-backup-2017-09-18.log

Testing SSH connectivity to saserver
SSH connectivity... [ OK ]
Calculating size of backup for saserver
Disk space required for saserver backup is 1.91GB
Check Backup Storage Space @ lab-cos6-RF:/var/netwitness/database/nw-backup
Space Required 1.91GB vs. Space Available 11.66GB
Backup Storage Space... [ OK ]
Total Execution Time : 0 d 0 h 0 m 19 s

Disk space check test completed with no errors.
[root@lab-cos6-RF ~]#

```

## 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 11.0.0.0 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 -u -l -x -e <external-mnt> -b <backup file path>
```

### Allgemeine Optionen

**-u** : This option is required for upgrading to 11.0. Enables the upgrade flag to run backup for upgrading to 11.0. 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 11.0, please use the default location!** Default: (/var/netwitness/database/nw-backup)

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

### 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
```

das Backup mit den Optionen durchgeführt werden, 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 durchgeführt werden, der in dem Skript definiert ist, und zwar mit den folgenden Optionen:

-u : enables the upgrade flag to run backup for upgrading to 11.0. 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:  
10.6.3.x and 10.6.4.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 <additional options as needed>`

**Hinweis:** Sie müssen die Option `-u` verwenden, damit Ihre Dateien während des Upgrades auf 11.0.0.0 korrekt wiederhergestellt werden.

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 NetWitness-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 NetWitness-Server (insbesondere den Admin-Service) auf 11.0.0.0 durchgeführt haben.

### Aufgabe 2: Sicherstellen, dass die erforderlichen Backupdateien generiert wurden

Nach Ausführung der Backupskripte werden mehrere Dateien generiert. Diese Dateien sind für den 11.0.0.0-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 NetWitness-Server und ESA-Hosts erzeugt:

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

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

**Hinweis:** Das Backupsript kopiert die folgenden Dateien von allen ESA-Hosts in den Backuppfad des NetWitness-Server-Hosts.

- `<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 11.0.0.0 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.

**Hinweis:** Die Standardpfade für Backupdateien sind:

- NetWitness-Server-Hosts: /var/netwitness/database/nw-backup
- ESA-Hosts: /opt/rsa/database/nw-backup
- Malware-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)

## Migrieren von Festplattenlaufwerken von 10.6.4.x zu 11.0

---

In diesen Anweisungen erfahren Sie, wie Sie für virtuelle Hosts ein Upgrade von 10.6.4.x auf 11.0 durchführen.

**Achtung:** (1) Sie können die Migration nicht durchführen, wenn Sie über einen Snapshot für Ihre VM verfügen.  
2). Führen Sie das Backup für jede Phase unmittelbar vor dem Upgrade der Hosts durch, damit die Daten aktuell sind.  
3.) Dieser Leitfaden gilt ausschließlich für Upgrades von virtuellen Hosts. Wenn sich in Ihrer Bereitstellung sowohl physische als auch virtuelle Hosts befinden, finden Sie in den *RSA NetWitness® Suite Upgradeanweisungen für physische Hosts 11.0* eine Beschreibung der Schritte für Upgrades von physischen Hosts. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

**Hinweis:** Die Maschinen müssen über VMware ESX betrieben werden.

Es gibt fünf Aufgaben, die Sie ausführen müssen, um die Bereitstellungslaufwerke von virtuellen Maschinen (VMs) von Version 10.6.4.x nach 11.0 zu migrieren:

[Aufgabe 1: Sichern Sie die Daten der 10.6.4.x VMs.](#)

[Aufgabe 2: Stellen Sie den gleichen VM-Stack in 11.0 bereit wie in 10.6.4.x.](#)

[Aufgabe 3: Kopieren Sie die VMDK-Dateien und fügen Sie sie den neuen virtuellen Maschinen als Festplatte hinzu.](#)

[Aufgabe 4: Behalten Sie die MAC-Adresse der aktualisierten VMs bei.](#)

[Aufgabe 5: Stellen Sie die Backupdaten aus 10.6.4.x auf den 11.0 VMs wieder her.](#)

### Aufgabe 1: Sichern der Daten auf den 10.6.4.x VMs

1. Bereiten Sie Log Collector für die Migration vor:
  - a. Melden Sie sich bei Log Collector mit den Root-Anmeldedaten an.
  - b. Navigieren Sie zum Verzeichnis `/opt/rsa/nwlogcollector/nwtools/` und führen Sie den folgenden Befehl aus:

```
sh prepare-for-migrate.sh --prepare
```

Detaillierte Anweisungen zum Upgrade des VLC finden Sie unter [Virtual Log Collector-Host](#).

- Laden Sie die Datei `.zip`, die die 10.6.4.x Backupskripte enthält, von RSA Link (<https://community.rsa.com/docs/DOC-81514>) auf den externen Backuphost herunter.

**Hinweis:** Sie müssen einen externen Host einrichten, der zum Sichern von Dateien verwendet werden soll. Auf dem Host muss CentOS 6 mit SSH-Konnektivität zum NetWitness Suite-Host-Stack ausgeführt werden.

- Führen Sie die folgenden Befehle aus dem Verzeichnis `nw-backup/scripts` aus:

```
./get-all-systems.sh <SA-IP>
./ssh-propagate.sh <path-to-backup-directory/all-systems>
./nw-backup.sh -u
```

(Wenn Sie eine Malware-VM haben, ersetzen Sie `-m -u` für `-u` in dieser Befehlszeichenfolge (z. B. `./nw-backup.sh -m -u`).

## Aufgabe 2: Bereitstellen des gleichen 10.6.4.x VM-Stacks in 11.0

Sie müssen in 11.0 den gleichen virtuellen Host-Stack einrichten, der in 10.6.4.x verwendet wurde. Anweisungen hierzu finden Sie im *RSA NetWitness® Suite 11.0 Leitfaden zur Einrichtung von virtuellen Hosts*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

Es folgen die allgemeinen Schritte zur Bereitstellung eines OVA-Hosts in einer ESXi-Umgebung.

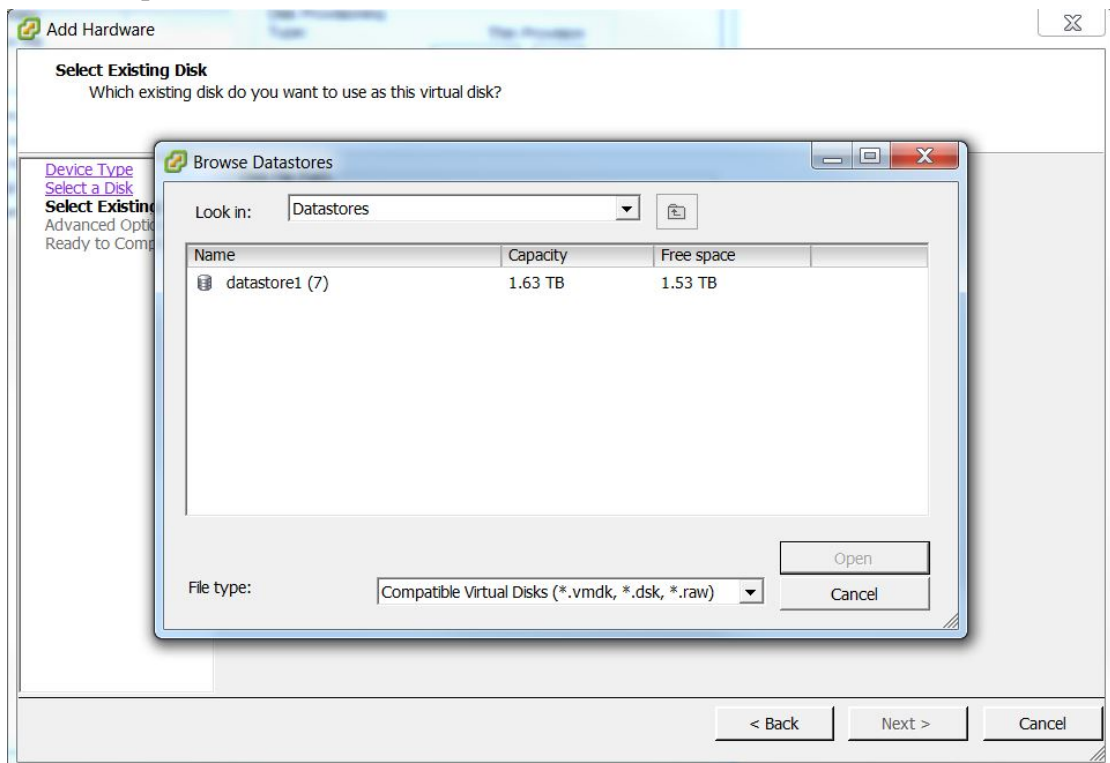
Laden Sie die 11.0 OVA (**Rsanw-11.0.0.0.1245.e17-x86\_64.ova**) von RSA Link Download Central in ein lokales Verzeichnis herunter.

- Melden Sie sich bei der ESXi-Umgebung an.
- Wählen Sie im Drop-down-Menü **Datei** die Option **OVF-Vorlage bereitstellen**. Das Dialogfeld „OVF-Vorlage bereitstellen“ wird angezeigt.
- Suchen Sie im lokalen Verzeichnis nach den 11.0 OVAs, die Sie in Schritt 1 heruntergeladen haben.
- Wählen Sie die Datei **rsanw-11.0.0.0.1245.e17-x86\_64.ova** aus, um die virtuelle Umgebung bereitzustellen, und klicken Sie auf **Weiter**.
- Wählen Sie die entsprechende Konfiguration für die virtuelle Maschine aus und klicken Sie auf **Weiter**.
- Schalten Sie die virtuelle Maschine ein, wechseln Sie zur Konsole und melden Sie sich bei der Maschine an.  
Die virtuelle Maschine verfügt jetzt über das 11.0 Basis-Image, das erforderlich ist, um das Setup-Programm auszuführen (d. h. `nwsetup-tui`).



### Aufgabe 3: Kopieren und Hinzufügen der VMDK-Dateien zu den neuen virtuellen Maschinen als Festplatte

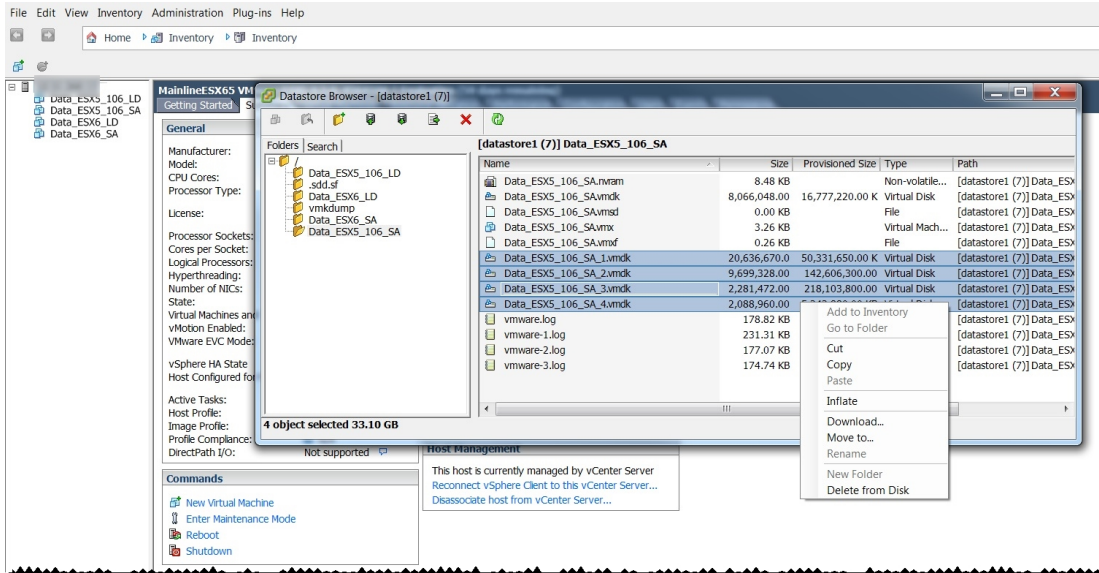
1. Schalten Sie die 10.6.4.x und 11.0 VMs aus.
2. Begeben Sie sich zu dem gewünschten ESX-Server und klicken Sie auf die Registerkarte **Konfiguration > Speicher**.
3. Klicken Sie mit der rechten Maustaste auf den obligatorischen Datenspeicher und wählen Sie **Datenspeicher durchsuchen** aus.



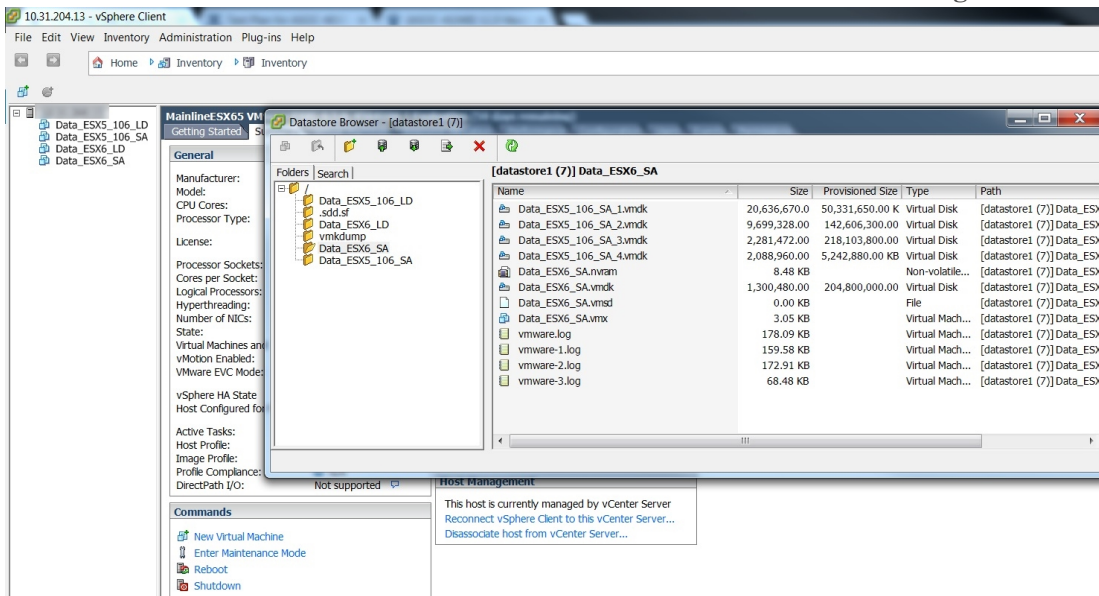
4. Navigieren Sie zu der vorhandenen 10.6.4.x VM im Datenspeicher.
5. Wählen Sie alle VMDK-Dateien im Datenspeicher aus, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Kopieren**.

**Achtung:** Kopieren Sie nicht die VMDK-Basisdatei (z. B. Data\_106\_SA), da sie CentOS 6 enthält.

Sie müssen alle nummerierten VMDK-Dateien kopieren. Beispiel: Wenn der Name der 10.6.4.x VM Data\_106\_SA lautet, kopieren Sie alle Dateien Data\_106\_SA\_1, Data\_106\_SA\_2, Data\_106\_SA\_3 usw.



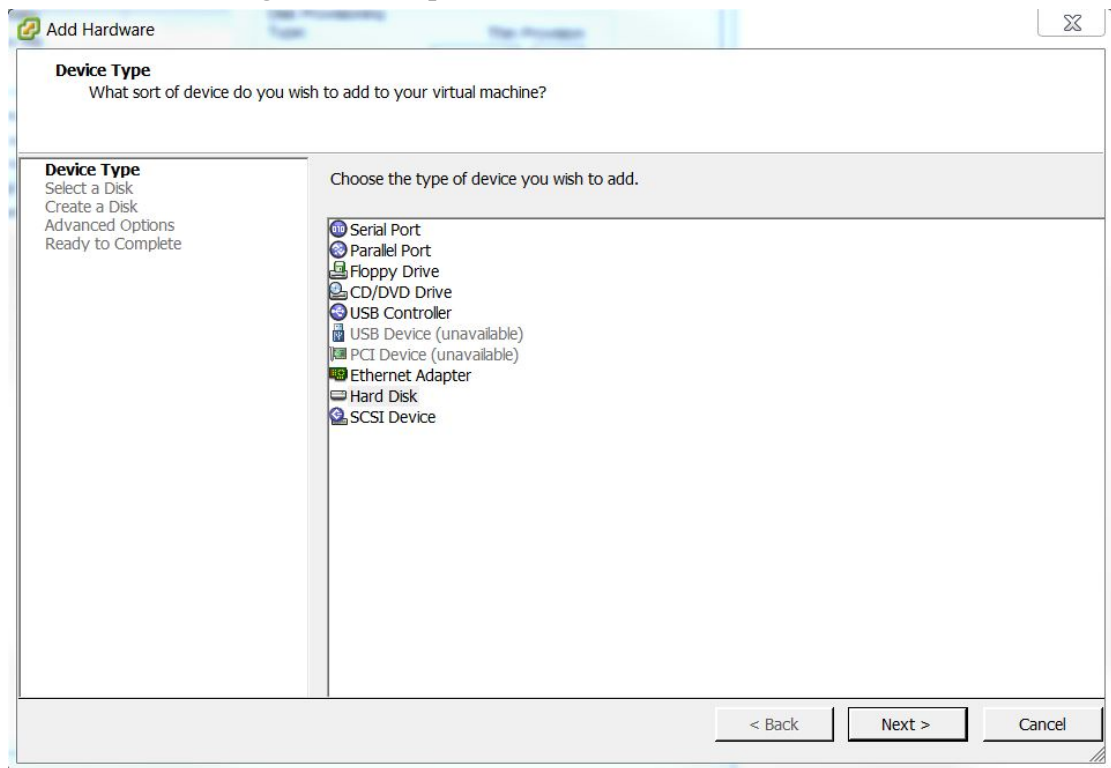
6. Navigieren Sie zu der neuen 11.0 VM im Datenspeicher.
7. Klicken Sie mit der rechten Maustaste darauf und wählen Sie den Befehl **Einfügen** aus.



**Hinweis:** Sie müssen warten, bis alle VMDK-Dateien vollständig von der vorherigen virtuellen Maschine in den Datenspeicher der neuen VM kopiert worden sind.

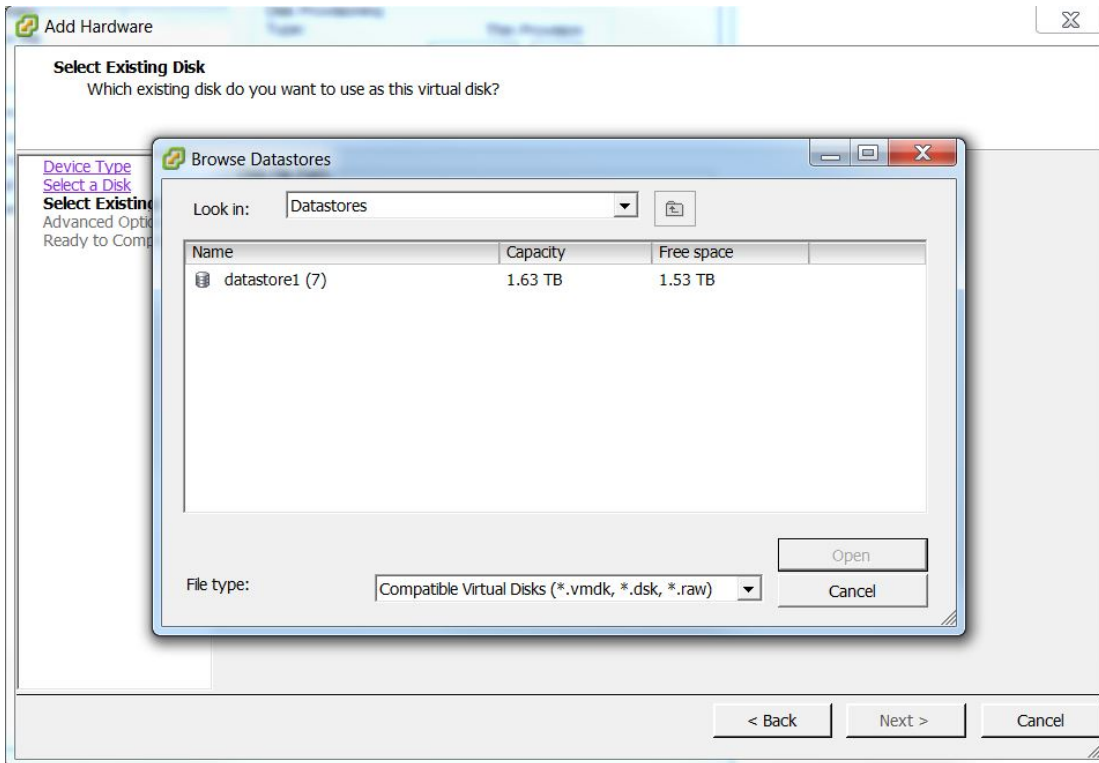
8. Wählen Sie die 11.0 VM aus und klicken Sie auf **Einstellungen bearbeiten** > **Hinzufügen**.

9. Klicken Sie im Dialogfeld auf **Festplatte** > **Weiter**.

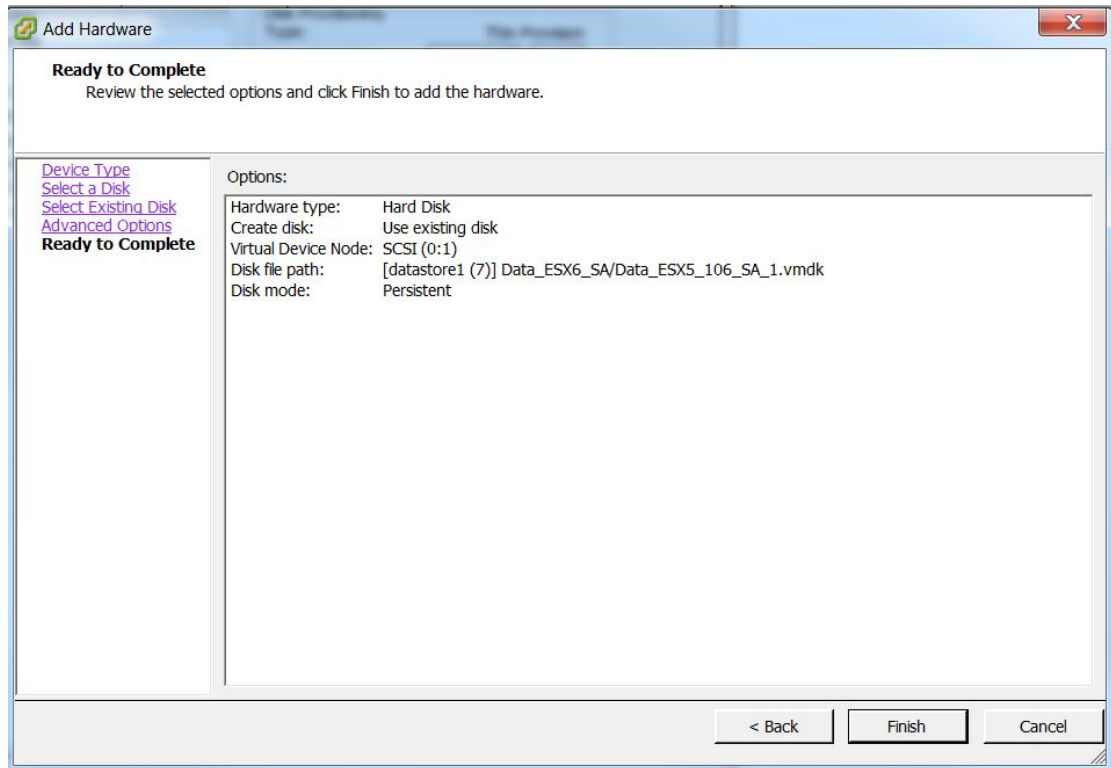


10. Klicken Sie auf **Bereits vorhandene Festplatte** > **Weiter**.

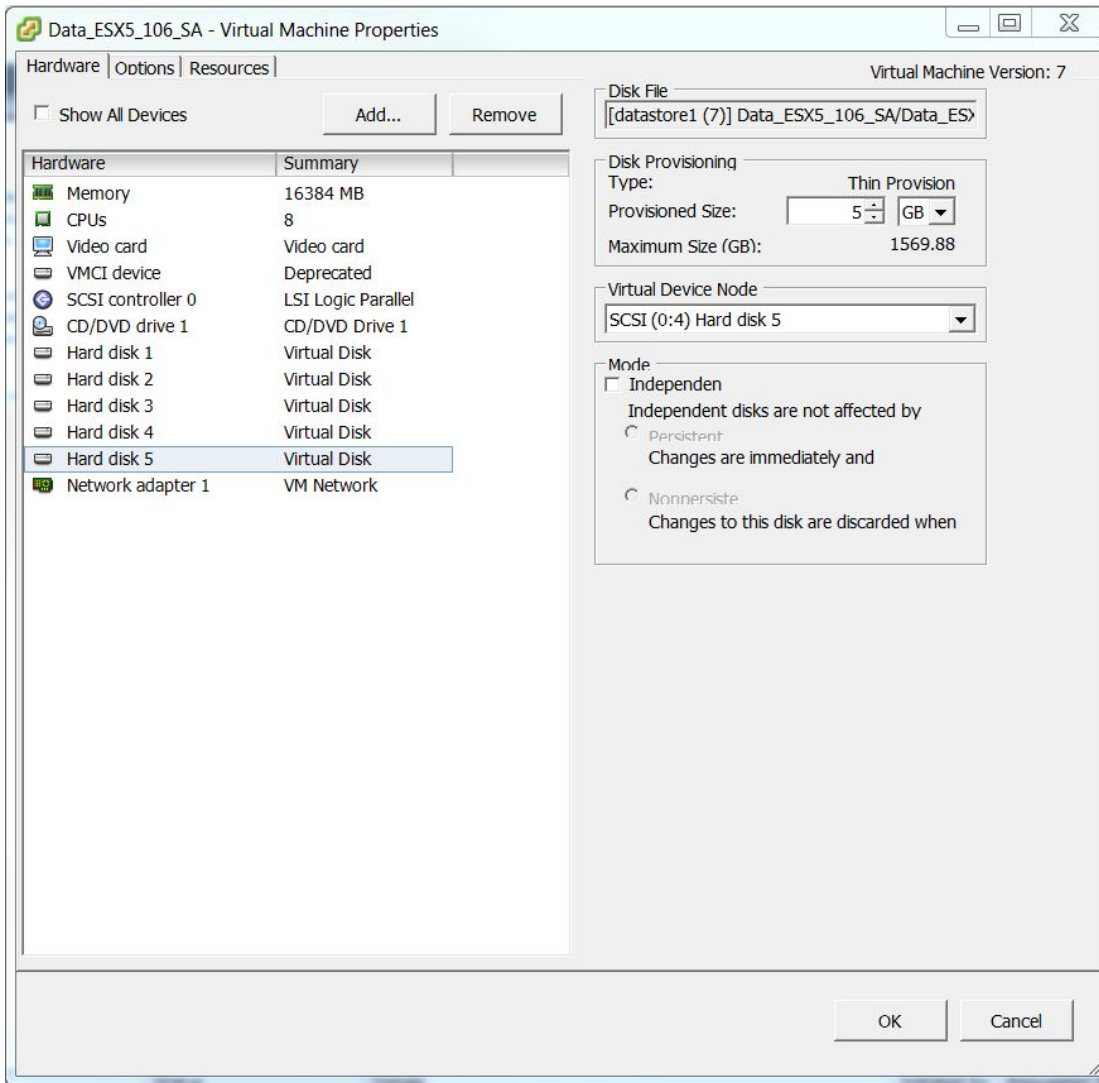
11. Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem Datenspeicherort, in den Sie die VMDK-Dateien kopiert haben.



12. Wählen Sie die VMDK-Datei aus der 11.0 VM aus, die Sie als Festplatte hinzufügen möchten.



13. Wiederholen Sie die Schritte 8 bis 12 für jede Festplatte, die Sie hinzufügen möchten.



## Aufgabe 4: Beibehalten der MAC-Adresse der aktualisierten SA-Server-VM

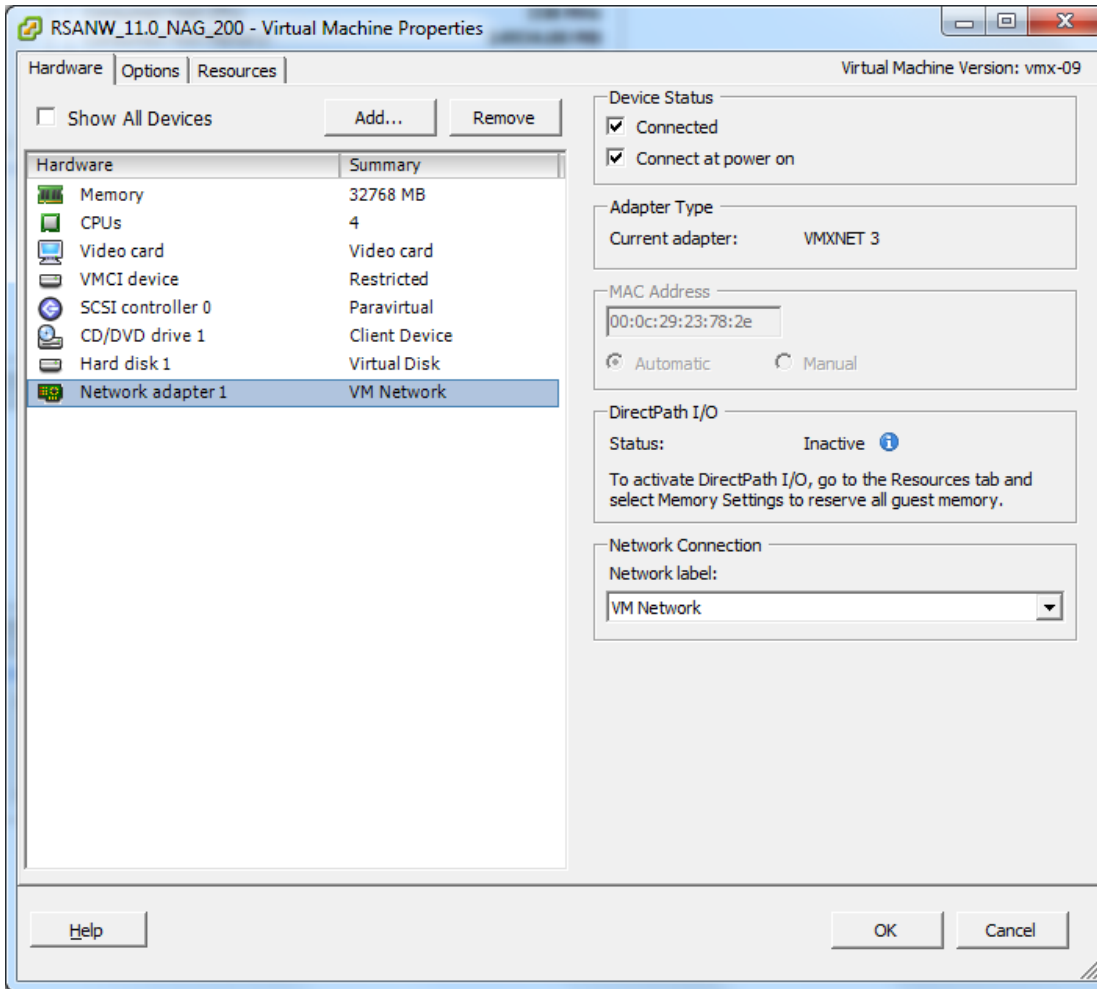
So behalten Sie die MAC-Adresse der virtuellen Maschine (VM) des migrierten SA-Servers (Security Analytics) bei:

**Hinweis:** Diese Schritte gelten für die Migration der SA-Server-VM (erstellt mit automatischer MAC-Adresszuweisung) zum 11.0 NetWitness-Server. Bei virtuellen Maschinen mit einer statischen MAC-Adresse können Sie die MAC-Adresse ändern, indem Sie „Edit Settings“ für eine virtuelle Maschine auswählen und die MAC-Adresse eingeben.

1. Melden Sie sich beim vCenter-Server an.

**Hinweis:** Es werden die vCenter-Versionen 5.5 bis einschließlich 6.5 unterstützt.

2. (Bedingungsabhängig) Wenn die beiden VMs (NetWitness 10.6.4.x und 11.0) eingeschaltet sind, **schalten Sie sie aus**.
3. Klicken Sie auf die Registerkarte **Zusammenfassung**. Klicken Sie dann mit der rechten Maustaste auf **Datenspeicher** und suchen Sie den Speicherort des Datenspeichers.
4. Navigieren Sie zu dem VM-Ordner und laden Sie die `.vmx`-Datei von Version 10.6.4.x und 11.0 in das lokale Repository herunter.  
Standardmäßig wird die mit der MAC-Adresse generierte virtuelle Maschine in dem Format erstellt (siehe Abbildung unten).



**Hinweis:** `00:0c:29:XX:YY:ZZ – 00:0c:29` ist die eindeutige Kennung für eine automatisch erzeugte MAC-Adresse. `00:50:56:XX:YY:ZZ – 00:50:56` ist die eindeutige Kennung für eine statische oder manuell erzeugte MAC-Adresse. Diese ist nur gültig, wenn vCenter nicht bereitgestellt wird. Wenn vCenter bereitgestellt wird, markiert diese MAC-Adresse die eindeutige Kennung für eine automatisch erzeugte MAC-Adresse.

5. Verwenden Sie einen Texteditor und kopieren Sie die Werte `uuid.location` und `ethernet0.generatedAddress` aus der `.vmx`-Datei von Version 10.6.4.x in die `.vmx`-Datei von Version 11.0.

**Hinweis:** Wenn Sie den 10.6.4.x-Stack direkt auf dem ESX-Server bereitgestellt haben (nicht über vCenter), müssen Sie auch den Wert für `uuid.bios` zusätzlich zu `uuid.location` und `ethernet0.generatedAddress` aus der `.vmx`-Datei von Version 10.6.4.x in die `.vmx`-Datei von Version 11.0 kopieren.

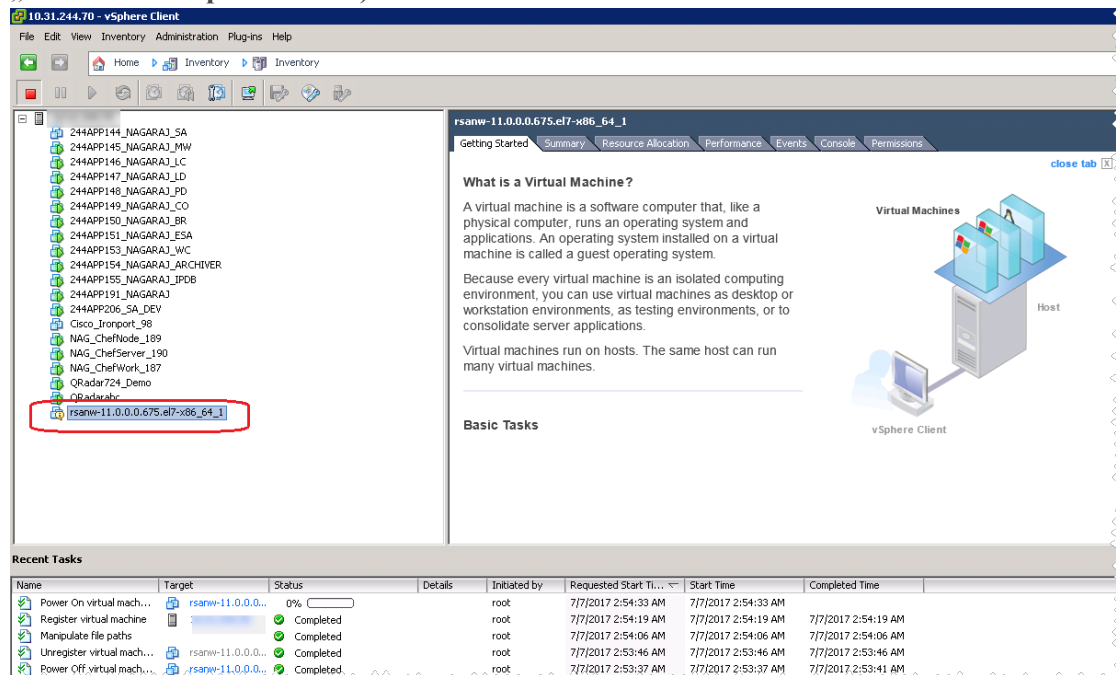


6. Entfernen Sie die 10.6.4.x und die 11.0 VMs aus dem Bestand.
  - a. Navigieren Sie zum vCenter-Server.
  - b. Klicken Sie mit der rechten Maustaste auf die 10.6.4.x und die 11.0 VMs.
  - c. Wählen Sie „Remove from Inventory“ aus.
7. Laden Sie die geänderte 11.0-.vmx-Datei in das Verzeichnis des Datenspeichers hoch, indem Sie sie gegen die vorhandene .vmx-Datei austauschen.
8. Klicken Sie im Datenspeicher mit der rechten Maustaste auf die 11.0-.vmx-Datei und wählen Sie „Add to Inventory“ aus.
9. Navigieren Sie zum vCenter-Server und **schalten Sie die VM ein**.

Die folgende Meldung wird angezeigt:

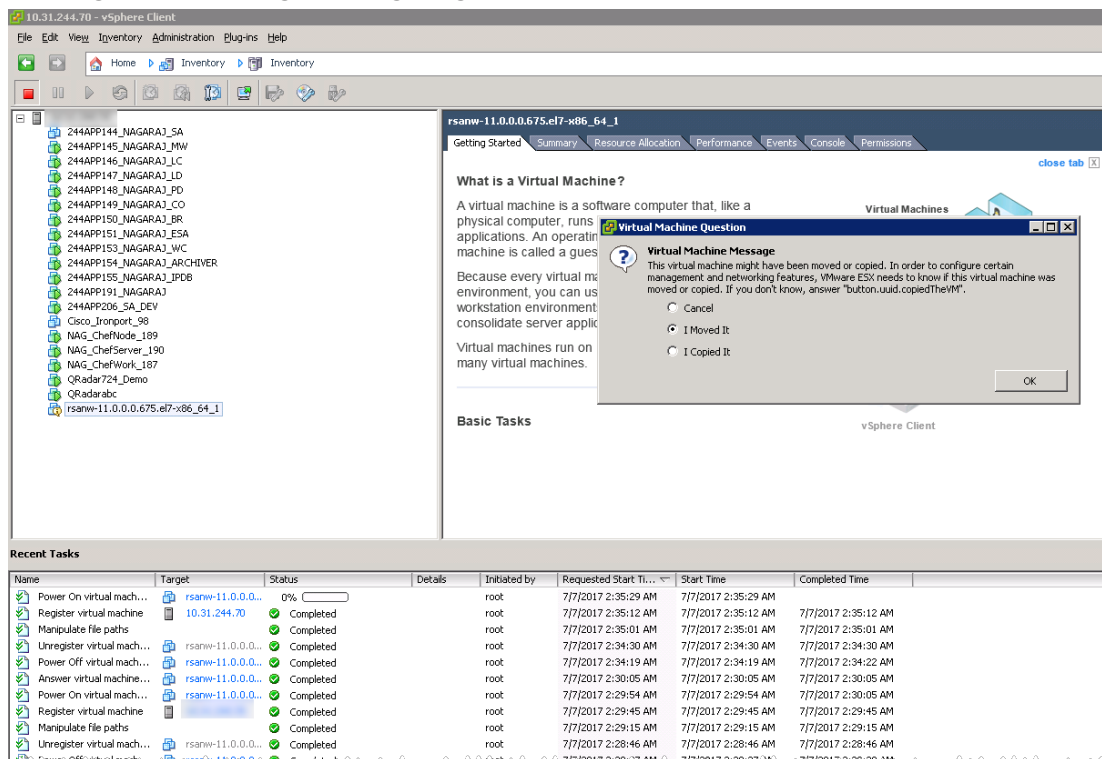
**Möglicherweise wurde die virtuelle Maschine verschoben oder kopiert. Um bestimmte Management- und Netzwerkfunktionen zu konfigurieren, muss VMware ESX wissen, ob diese virtuelle Maschine verschoben oder kopiert wurde. Wenn Sie die Antwort nicht kennen, reagieren Sie mit**

**„button.uuid.copiedTheVM).“**



10. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Guest > Answer Question** aus.

Die folgende Abbildung wird angezeigt:



11. Wählen Sie **I Moved It** aus.

12. Klicken Sie auf **OK**.

Die MAC-Adresse aus 10.6.4.x wird als MAC-Adresse für 11.0 beibehalten.

## Aufgabe 5: Wiederherstellen der Backupdaten aus 10.6.4.x auf den 11.0 VMs

Schalten Sie die 10.6.4.x und 11.0 VMs **aus**.

1. Melden Sie sich beim vCenter-Server an.
2. Kopieren Sie die VMDK-Dateien aus Version 10.6.4.x auf die 11.0 VMs im Datenspeicher. Detaillierte Anweisungen hierzu finden Sie unter [Aufgabe 3: Kopieren und Hinzufügen der VMDK-Dateien zu den neuen virtuellen Maschinen als Festplatte](#).
3. Fügen Sie alle kopierten VMDKs als neue Festplatten auf den 11.0 Maschinen mit den vorhandenen VMDKs hinzu.
4. Ändern Sie die MAC-Adresse der 11.0 VM zu jener der 10.6.4.x VM. Detaillierte Anweisungen hierzu finden Sie unter [Aufgabe 4: Beibehalten der MAC-Adresse von migrierten VMs](#).

5. Schalten Sie die 11.0 VMs ein.
6. Kopieren Sie die gesicherten Daten aus dem Verzeichnis `nw-backup` auf die 11.0 VMs.
  - Für den NW-Server (SA-Server in 10.6.4.x):

**Hinweis:** Detaillierte Anweisungen zum Upgrade des VLC finden Sie unter [Virtual Log Collector-Host](#) .

- a. Erstellen Sie das Verzeichnis `nwhome` unter `/tmp`.
- b. Mounten Sie `VolGroup00-nwhome` auf `/tmp/nwhome/`.  
`mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/`
- c. Kopieren Sie den Inhalt des Verzeichnisses `/tmp/nwhome/` nach `/var/netwitness/`.  
`cp -r /tmp/nwhome/* /var/netwitness/`
- d. Mounten Sie `VolGroup02-redb` auf `/var/netwitness/database`.  
`mount /dev/mapper/VolGroup02-redb /var/netwitness/database/`

**Hinweis:** Stellen Sie sicher, dass `/var/netwitness/database/nw-backupdirectory` mit Backup-Tarballs der Appliance vorhanden ist.

- e. Unmounten Sie `VolGroup00-nwhome` von `/tmp/nwhome/`.  
`umount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/`
- Für Archiver, Broker, Concentrator, Log Decoder/Log Collector und Packet Decoder:

**Hinweis:** Wenn Ihr 10.6.4.x Decoder oder Log Decoder mehrere Netzwerkschnittstellen hatte:

1. Schalten Sie die 11.0 VM, den 11.0 Decoder bzw. die Log Decoder-VM **aus**.
2. Navigieren Sie für die virtuelle Maschine zu **Einstellungen bearbeiten** und fügen Sie die erforderliche Anzahl von Ethernet-Adaptern hinzu.
3. Schalten Sie die VM ein.
4. Fügen Sie die Ethernet-Adapter hinzu, bevor Sie die Backupdaten wiederherstellen.

- a. Erstellen Sie das Verzeichnis `nwhome` unter `/tmp`.
- b. Erstellen Sie einen temporären Mount `VolGroup00-nwhome` auf `/tmp/nwhome/`.  
`mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/`
- c. Kopieren Sie den Inhalt des Verzeichnisses `/tmp/nwhome/` nach `/var/netwitness/`.  
`cp -r /tmp/nwhome/* /var/netwitness/`
- d. Unmounten Sie `VolGroup00-nwhome` von `/tmp/nwhome/`.  
`umount /tmp/nwhome`

- Für Malware Enterprise (gemeinsame Malware wird im 11.0-Upgrade nicht unterstützt):
  - a. Erstellen Sie das Verzeichnis `apps` unter `/tmp/`.
  - b. Erstellen Sie einen temporären Mount `VolGroup01-apps` auf `/tmp/apps/`.  
`mount /dev/mapper/VolGroup01-apps /tmp/apps/`
  - c. Kopieren Sie das Verzeichnis `nw-backup` nach `/var/netwitness/`.  
`cp -r /tmp/apps/nw-backup /var/netwitness`
  - d. Unmounten Sie `VolGroup01-apps` von `/tmp/apps/`.  
`umount /tmp/apps`
- Für Event Stream Analysis:
  - a. Erstellen Sie das Verzeichnis `apps` unter `/tmp/`.
  - b. Erstellen Sie einen temporären Mount `VolGroup01-apps` auf `/tmp/apps/`.  
`mount /dev/mapper/VolGroup01-apps /tmp/apps/`
  - c. Kopieren Sie das Verzeichnis `nw-backup` nach `/var/netwitness/`.  
`cp -r /tmp/apps/database/nw-backup /var/netwitness`
  - d. Unmounten Sie `VolGroup01-apps` von `/tmp/apps/`.  
`umount /tmp/apps`

## 7. Mounten Sie die Festplatten.

**Hinweis:** Wenn Sie externe Mount-Punkte auf den VMs im Stack für eines der folgenden Verzeichnisse konfiguriert haben, mounten Sie die externen Mount-Punkte anstelle der folgenden Mounts erneut:

- Für den NW-Server:

```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/  
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

**Hinweis:** Stellen Sie sicher, dass das Verzeichnis `/var/netwitness/database/nw-backup` mit Backup-Tarballs der Appliance vorhanden ist.

- Für den Log Collector und Log Decoder:

**Hinweis:** Die folgenden Mounts sind für Virtual Log Collector nicht erforderlich.

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/logdecoder/sessiondb
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/logdecoder/packetdb
```

- Für den Packet Decoder:

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/decoder/packetdb
```

- Für den Concentrator:

```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
mount /dev/mapper/VolGroup01-metadb
/var/netwitness/concentrator/metadb
```

- Für den Archiver:

```
mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
```

- Für den Broker:

```
mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
```

8. Fügen Sie die folgenden Mount-Einträge zu `/etc/fstab` hinzu.

- Für den NW-Server:

```
/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
defaults,noatime,nosuid 1 2
```

- Für den Log Collector und Log Decoder:

**Hinweis:** Die folgenden Mounts sind für Virtual Log Collector nicht erforderlich.

```

/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb
/var/netwitness/logdecoder/sessiondb xfs defaults,noatime,nosuid 1
2
/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
xfs defaults,noatime,nosuid 1 2

```

- **Für den Packet Decoder:**

```

/dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
xfs defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb
xfs defaults,noatime,nosuid 1 2

```

- **Für den Concentrator:**

```

/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime
1 2
/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
xfs defaults,noatime,nosuid 1 2

```

- **Für den Archiver:**

```

/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
defaults,nosuid,noatime 1 2
/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
defaults,nosuid,noatime 1 2

```

- Für den Broker:

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs  
defaults,nosuid,noatime 1 2
```

## Einrichten von virtuellen Hosts in Version 11.0

Es gibt zwei Phasen zur Einrichtung des virtuellen Stacks 11.0, die in der angegebenen Reihenfolge beendet werden müssen.

- [Phase 1: Einrichtung von SA-Server, Event Stream Analysis, Malware Analysis sowie Broker oder Concentrator-Hosts](#)

**Hinweis:** Dies betrifft Event Stream Analysis. Wenn Sie C2-Module in 10.6.4.x aktiviert haben, gehen die Module nach dem Upgrade des Event Stream Analysis-Service auf Version 11.0 in eine Aufwärmphase über und sind nicht verfügbar, bis diese abgeschlossen ist.

- [Phase 2: Einrichtung der übrigen Komponentenhosts](#)

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

#### Aufgabe 1: Einrichten von Version 11.0 NetWitness-Server

Befolgen Sie die Anweisungen unter [Einrichten des 11.0 NW-Serverhosts](#).

#### Aufgabe 2: Einrichten von 11.0 ESA

**Achtung:** Wenn Sie C2-Module in 10.6.4.x aktiviert haben, gehen die Module nach dem Upgrade des Event Stream Analysis-Service auf Version 11.0 in eine Aufwärmphase über und sind nicht verfügbar, bis diese abgeschlossen ist.

Befolgen Sie die Anweisungen unter [Einrichten eines 11.0 Nicht-NW-Serverhosts](#), um die ESA-Hosts einzurichten.

1. Richten Sie den primären ESA-Host 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, 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: Einrichten von 11.0 Malware Analysis**

Befolgen Sie die Anweisungen unter [Einrichten eines 11.0 Nicht-NW-Serverhosts](#).

### **Aufgabe 4: Einrichten von 11.0 Broker oder Concentrator**

Befolgen Sie die Anweisungen unter [Einrichten eines 11.0 Nicht-NW-Serverhosts](#).

**Hinweis:** Wenn Sie keinen Broker haben, aktualisieren Sie Ihre Concentrator-Hosts. Der 11.0 NW-Server kann für die neuen Funktionen von Investigate nicht mit 10.6.4.x Core-Services kommunizieren. Deshalb müssen Sie die Broker- oder Concentrator-Hosts in Phase 1 aktualisieren.

## **Phase 2: Einrichtung der übrigen Komponentenhosts**

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. Führen Sie die Schritte unter [Einrichten eines 11.0 Nicht-NW-Serverhosts](#) aus.
3. Starten Sie die Datenerfassung und -aggregation neu.

### **Log Decoder-Host**

1. Stellen Sie sicher, dass Sie Log Collector vorbereitet haben, wie beschrieben in [Log Collector \(LC\) und Virtual Log Collectors \(VLCs\): Führen Sie prepare-for-migrate.sh](#) in den **Anweisungen zum Backup** aus.
2. Beenden Sie die Erfassung auf dem Log Decoder.
3. Führen Sie die Schritte unter [Einrichten eines 11.0 Nicht-NW-Serverhosts](#) aus.
4. Starten Sie die Datenerfassung auf dem Log Decoder neu.

**Hinweis:** Nach dem Upgrade starten Sie die Protokollsammlung nach Abschluss von [Aufgabe 11: Zurücksetzen der stabilen Systemwerte für Log Collector nach dem Upgrade](#) in den **Aufgaben nach dem Upgrade** neu.

## Virtual Log Collector-Host

1. Stellen Sie sicher, dass Sie Virtual Log Collector vorbereitet haben, wie beschrieben in [Log Collector \(LC\) und Virtual Log Collector \(VLCs\): Führen Sie `prepare-for-migrate.sh` aus.](#)
2. Sichern Sie Ihren 10.6.4.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>,10.6.4.0`
  - 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 10.6.4.x VLC aus, damit eine neue 11.0 VM mit derselben Netzwerkkonfiguration erstellt werden kann.
5. Stellen Sie einen neuen Nicht-NW-Serverhost mithilfe der 11.0 NetWitness Suite-OVA bereit.
6. Stellen Sie eine Verbindung zur VM-Konsole des neuen VLC her.
7. Aktualisieren Sie die Netzwerkkonfiguration, sodass sie dem 10.6.4.x VLC entspricht. Diese Informationen werden in der `<hostname-IPaddress>-network.info.txt` 10.6.4.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 [Einrichten des 11.0 Nicht-SA-Serverhosts](#) für den Rest der NetWitness Suite-Komponenten aus. Stellen Sie sicher, dass Sie **Log Collector** für den Service in Schritt 12 auswählen.

## Einrichten des 11.0 NW-Serverhosts

Stellen Sie sicher, dass Sie die 10.6.4.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 11.0 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 11.0 nicht mehr möglich ist.

Führen Sie die folgenden Schritte aus, um den 11.0 NW-Serverhost einzurichten:

1. Schalten Sie die VM des NW-Servers ein und führen Sie den Befehl `nwsetup-tui` aus. Dadurch wird das 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.

By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at <https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf> with RSA Security LLC ("RSA", or appropriate affiliate entity in the relevant jurisdiction). In addition, Customer hereby agrees and acknowledges that, if Customer chooses to host its data with any third party or in a public cloud environment, RSA has no responsibility for the storage or protection of any Customer data or for any associated security breach notifications. The terms herein and in the EULA shall supersede any relevant terms in any other agreement between the Customer and RSA. For customers of the RSA NetWitness® products, all data analyzed in connection herewith shall be at a cost to Customer based on RSA's then current

92%

&lt;Accept &gt;

&lt;Decline&gt;

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

Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.

You must setup an NW Server before setting up any other NetWitness Suite components.

Is this the host you want for your 11.0 NW Server?

&lt; Yes &gt;

&lt; No &gt;

**Achtung:** Wenn Sie den falschen Host für den NW-Server auswählen und das Upgrade abschließen, müssen Sie die Schritte 1 bis 11 von [Einrichten des 11.0 NW-Serverhosts](#) wiederholen, um diesen Fehler zu korrigieren.

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

Wählen Sie „Nein“, wenn Sie den NW-Server bereits auf 11.0 aktualisiert haben.

Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.

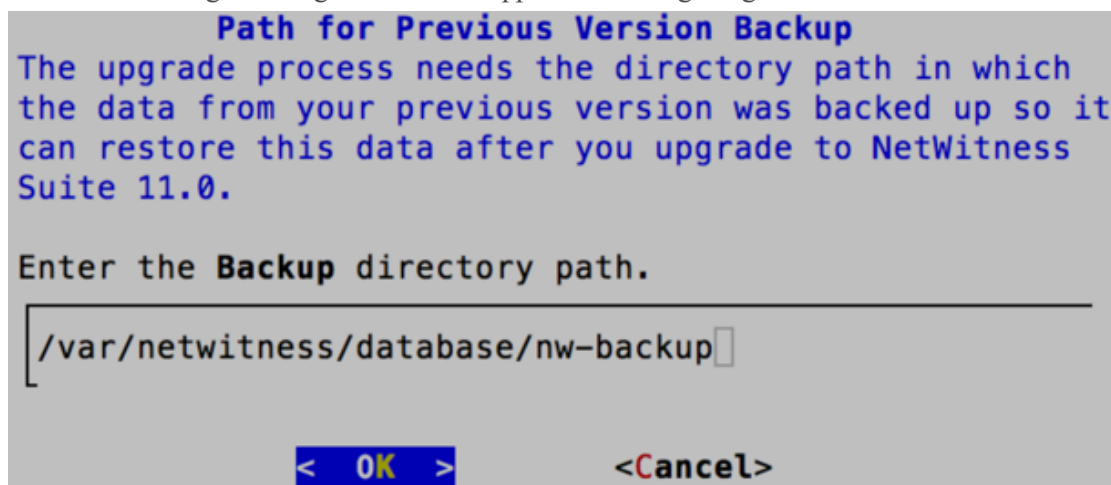
```
NetWitness Suite 11.0 Install or Upgrade
Specify if you are installing NetWitness
for the first time or upgrading from a
previous version:

  1 Install (Fresh Install)
  2 Upgrade (From Previous Vers.)

< OK >      < Exit >
```

4. 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.



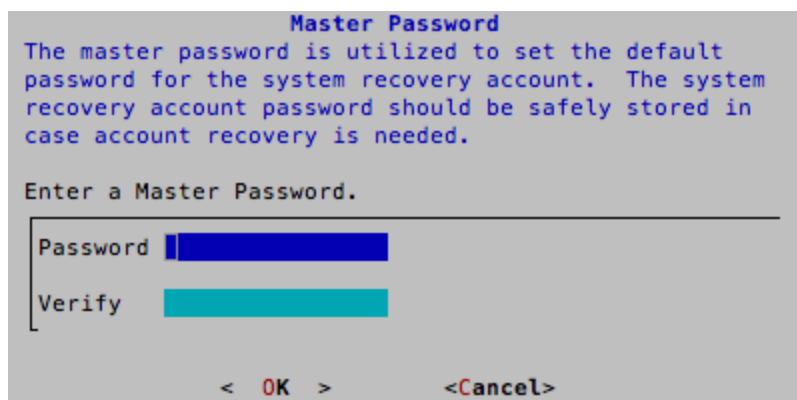
5. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, wenn Sie diesen Pfad behalten möchten. Wenn nicht, bearbeiten Sie den Pfad, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.

Die Aufforderung „Masterpasswort“ wird angezeigt.

Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

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

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



6. Geben Sie das **Password** 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.

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.

Sie müssen für alle Hosts das gleiche Repository verwenden, das Sie für die NW-Serverhosts verwendet haben.

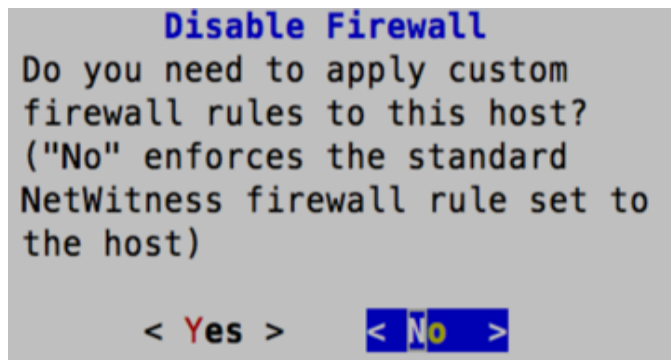
8. Verwenden Sie den Pfeil nach oben oder unten, um **2 Ein externes Repository (auf einem extern gemanagten Server)** auszuwählen. Sie werden zur Eingabe eines URL aufgefordert.

Anweisungen hierzu finden Sie unter „Einrichten eines externen Repository mit RSA und Betriebssystemupdates“ unter „Hosts und Services – Verfahren“ in der *RSA NetWitness Suite 11.0 – Leitfaden für die ersten Schritte mit Hosts und Services*. Navigieren Sie zu

[Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

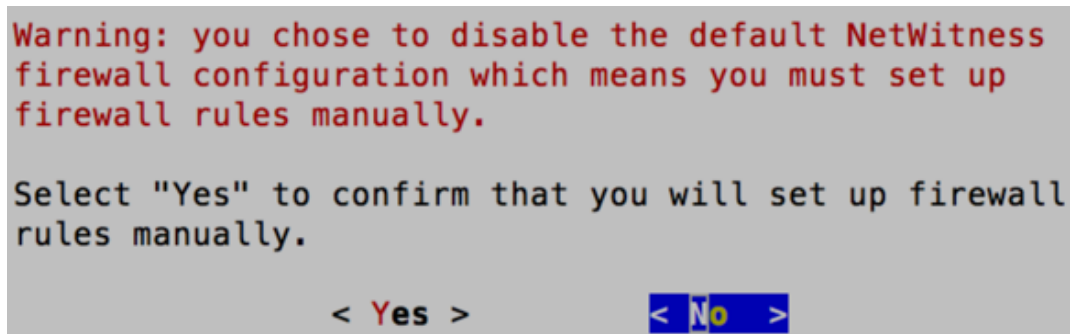
9. Geben Sie den Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**.

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



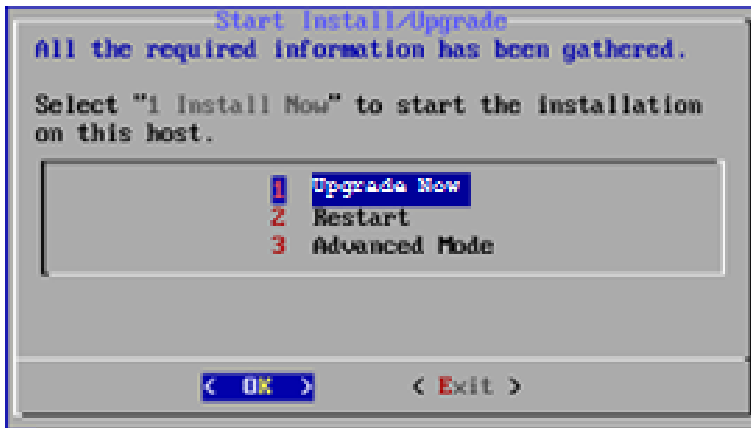
10. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** und drücken die **EINGABETASTE**. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken die **EINGABETASTE**.

- Wenn Sie „Ja“ ausgewählt haben, bestätigen Sie Ihre Auswahl.



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

Die Eingabeaufforderung „Upgrade starten“ wird angezeigt.



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

Wenn „Installation abgeschlossen“ angezeigt wird, haben Sie den 10.6.4.x SA-Server auf 11.0 NW-Server aktualisiert.

**Hinweis:** Ignorieren Sie die Hashcodefehler ähnlich 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.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

## Einrichten eines 11.0 Nicht-NW-Serverhosts

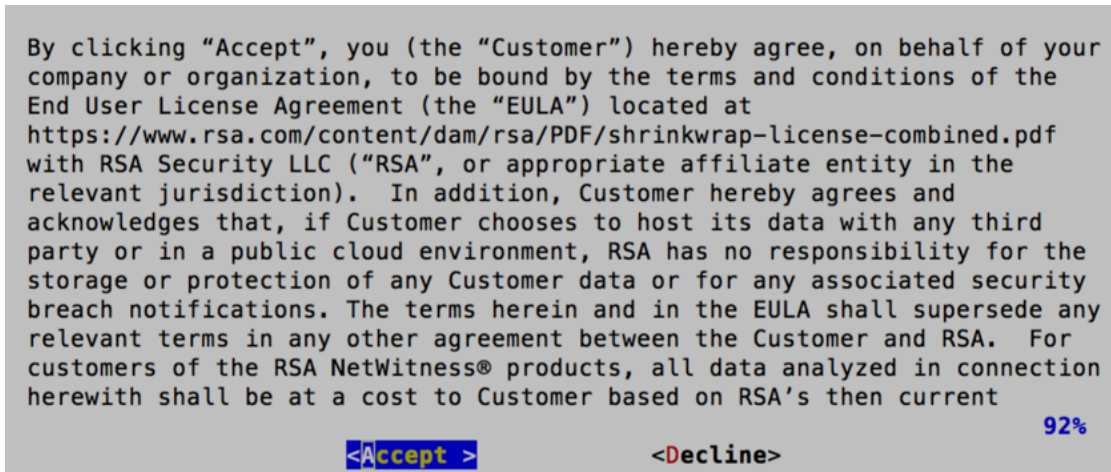
Stellen Sie sicher, dass Sie die 10.6.4.x-Daten für den Host gesichert haben. **Befolgen Sie die Anweisungen in [Anweisungen zum Backup](#), um den Host zu sichern.**

**Achtung:** Führen Sie das Backup unmittelbar vor dem Upgrade des Hosts auf 11.0 aus, damit die Daten so aktuell wie möglich sind.

Führen Sie die folgenden Schritte aus, um einen 11.0 Nicht-NW-Serverhost einzurichten:

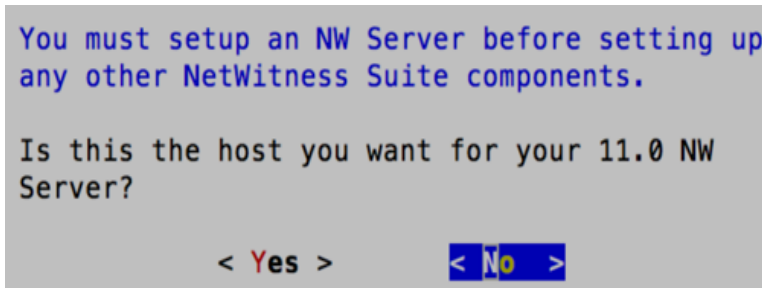
- Schalten** Sie die VM des NW-Servers ein und führen Sie den Befehl `nwsetup-tui` aus. Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.





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

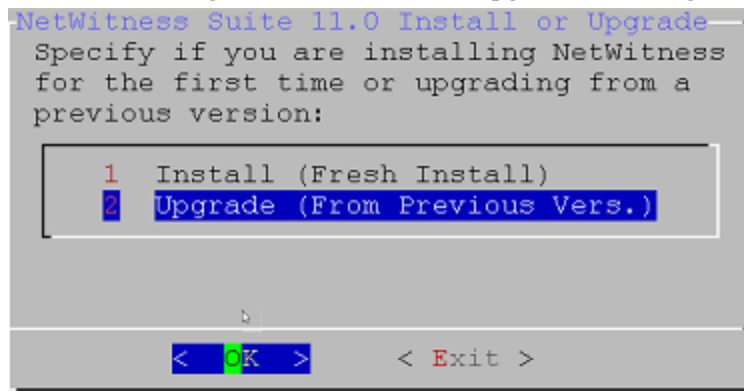
Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.



**Achtung:** Wenn Sie den falschen Host für den NW-Server auswählen und das Upgrade abschließen, müssen Sie die Schritte 1 bis 11 von [Einrichten des 11.0 NW-Serverhosts](#) wiederholen, um diesen Fehler zu korrigieren.

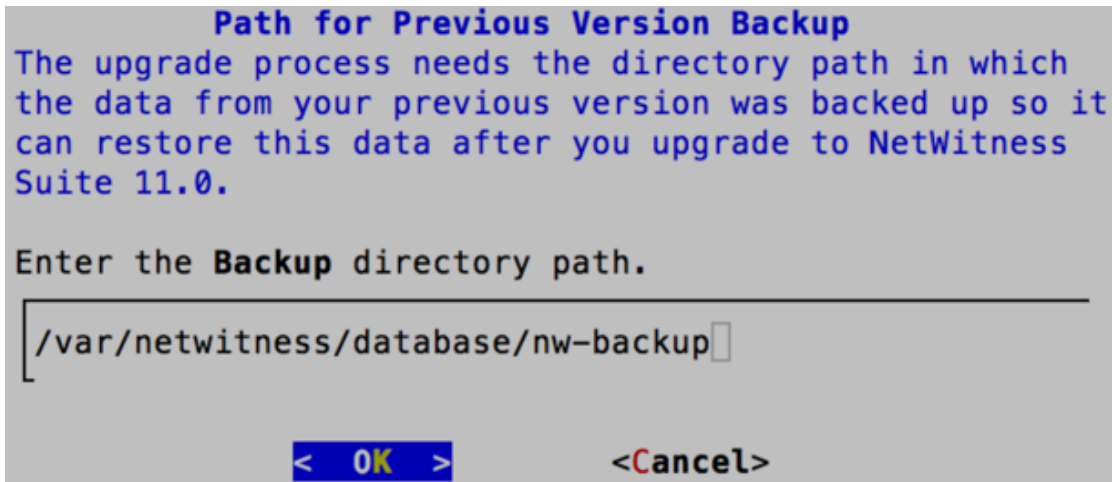
3. Gehen Sie zu **Nein** und drücken Sie die **EINGABETASTE**.

Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.



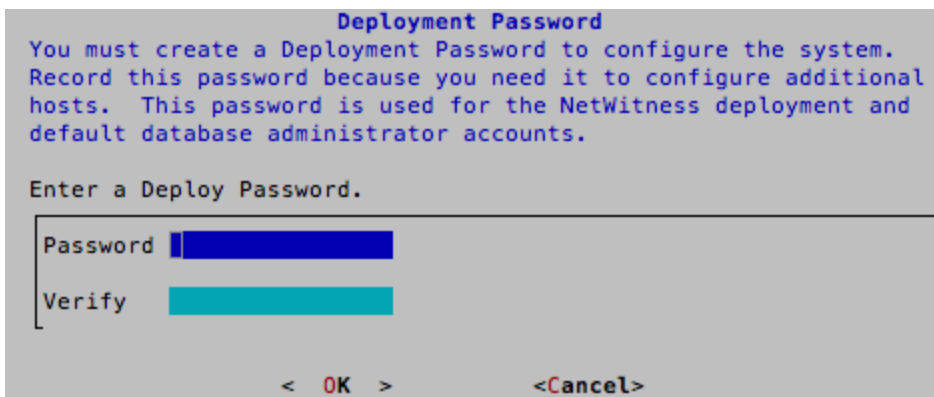
4. Wählen Sie mit dem Pfeil nach unten **2 Upgrade (von vorheriger Vers.)** aus, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Die Aufforderung zur Eingabe des Backuppfads wird angezeigt.



5. 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.

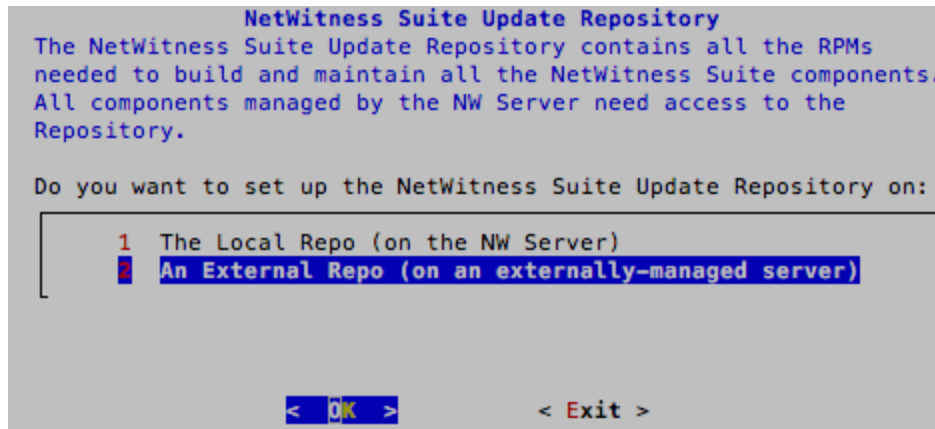
Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.



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

6. 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**.

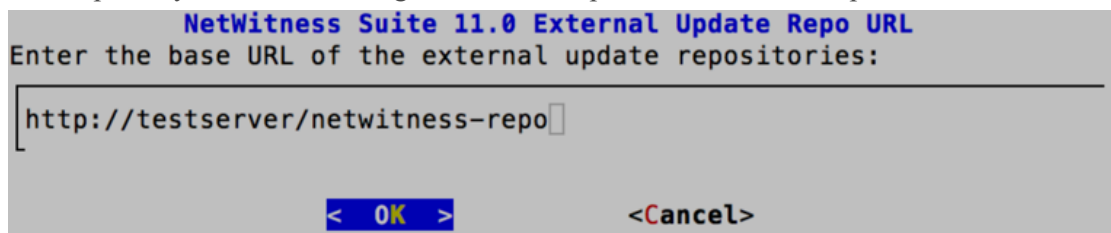
Die Eingabeaufforderung „Update-Repository“ wird angezeigt.



7. Verwenden Sie den Pfeil nach oben oder unten, um **2 Ein externes Repository (auf einem extern gemanagten Server)** auszuwählen, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

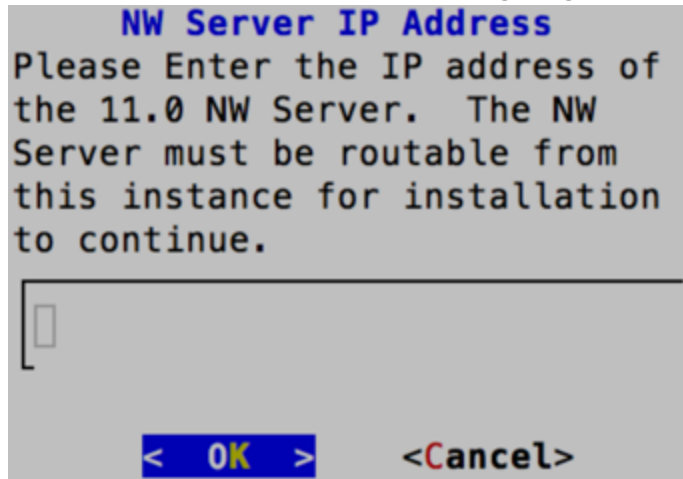
Sie werden aufgefordert, einen URL einzugeben.

Die Repositories bieten Ihnen Zugriff auf RSA-Updates und CentOS-Updates.



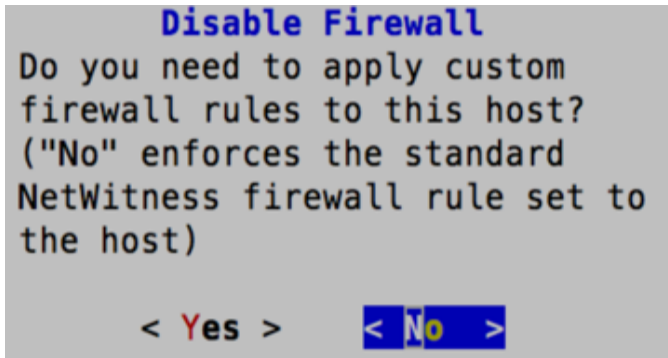
8. Geben Sie den Basis-URL für das externe NetWitness Suite-Repository ein und klicken Sie auf **OK**.

Die IP-Adresse des NW-Servers wird angezeigt.

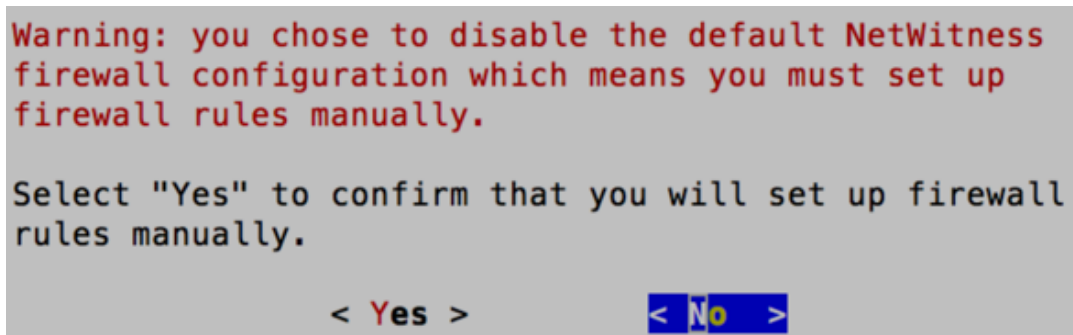


9. Geben Sie die IP-Adresse des NW-Servers ein, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

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

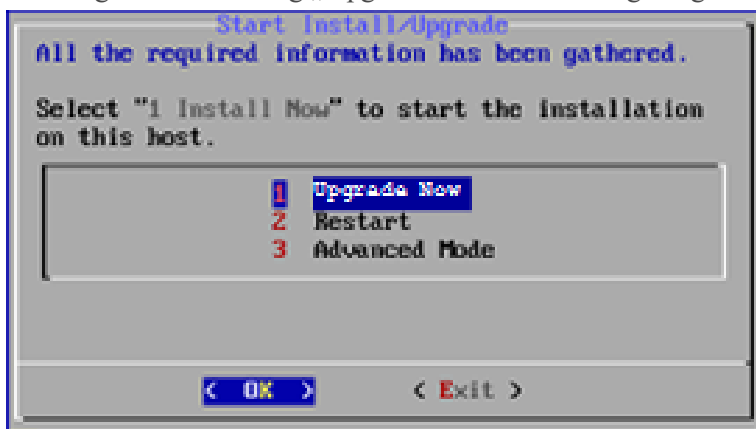


10. Um die Standardkonfiguration für Firewalls zu verwenden, gehen Sie zu **Nein** und drücken die **EINGABETASTE**. Um die Standardkonfiguration für Firewalls zu deaktivieren, gehen Sie zu **Ja** und drücken die **EINGABETASTE**.
  - Wenn Sie **Ja** ausgewählt haben, bestätigen Sie Ihre Auswahl.



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

Die Eingabeaufforderung „Upgrade starten“ wird angezeigt.



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 11.0 aktualisiert.

12. Installieren Sie den Service auf diesem Host:

- a. Melden Sie sich bei NetWitness Suite an.

Geben Sie `https://<NW-Server-IP-Address>/login` in Ihrem Browser ein, um zum NetWitness Suite-Anmeldebildschirm zu gelangen.

- b. Klicken Sie auf **ADMIN > Hosts**.

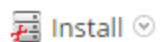
Das Dialogfeld **Neue Hosts** wird angezeigt; die Ansicht **Hosts** ist im Hintergrund abgeblendet.

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

- c. Klicken Sie im Dialogfeld **Neue Hosts** auf den Host und anschließend auf **Aktivieren**.

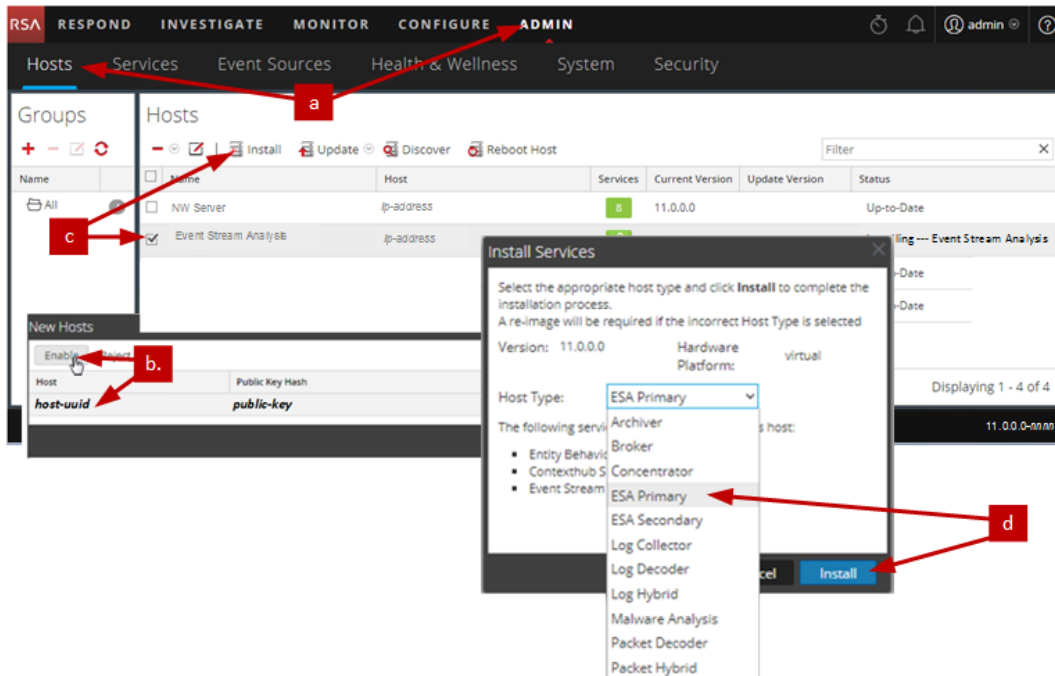
Das Dialogfeld **Neue Hosts** wird geschlossen und der Host wird in der Ansicht **Hosts** angezeigt.

- d. Wählen Sie diesen Host (z. B. **Event Stream Analysis**) aus und klicken Sie auf



Das Dialogfeld **Services installieren** wird angezeigt.

- e. 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.

## Aktualisieren oder Installieren der Legacy Windows Collection

---

Detaillierte Anweisungen zur Installation oder zum Update der Legacy Windows Collection finden Sie im *Leitfaden RSA NetWitness 11.0 Legacy Windows Collection* auf RSA Link (<https://community.rsa.com/docs/DOC-75593>).

**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 10.6.4.x auf 11.0 durchführen müssen. Diese Aufgaben sind nach den folgenden Kategorien unterteilt.

- [Global](#)
- [NetWitness Endpoint](#)  
RSA unterstützt NetWitness Endpoint in den Versionen 4.3.0.4, 4.3.0.5 und 4.4 nur für NetWitness Suite 11.0.
- [Event Stream Analysis](#)
- [Protokollsammlung](#)
- [Reporting Engine](#)
- [Reagieren](#)
- [NetWitness SecOps Manager](#)
- [Sicherheit](#)

### Globale Aufgaben

#### Aufgabe 1: 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 11.0 wiederhergestellt wurden, bevor Sie die backupbezogenen Dateien aus den lokalen Verzeichnissen auf den 11.0-Hosts entfernen.

##### **.tar-Backupdateien**

Nachdem alle Hosts auf Version 11.0 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
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

## Aufgabe 2: Wiederherstellen der NTP-Server

Sie müssen die Benutzeroberfläche von NetWitness Suite 11.0 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 11.0 Systemkonfigurationsleitfaden* finden Sie unter „Konfigurieren von NTP-Servern“ detaillierte Anweisungen zum Hinzufügen von NTP-Servern. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Aufgabe 3: 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 [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## **Aufgabe 4: Erneutes Zuordnen der virtuellen NW-Serverlizenz zur MAC-Adresse 10.6.4.x**

Wenn Sie ein Upgrade für einen Security Analytics-Server durchführen, der auf einer virtuellen Maschine ausgeführt wird, ändern Sie den virtuellen 11.0 NW-Serverhost auf die MAC-Adresse 10.6.4.x, um die Lizenzierung beizubehalten. Anweisungen zum erneuten Zuordnen einer Lizenz zu einer MAC-Adresse finden Sie unter „Lizenzierung: Schritt 1. Registrieren von NetWitness Server“ im *Leitfaden zum Lizenzierungsmanagement für die RSA NetWitness Suite*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## **(Bedingungsabhängig) Aufgabe 5: 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 6: 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:

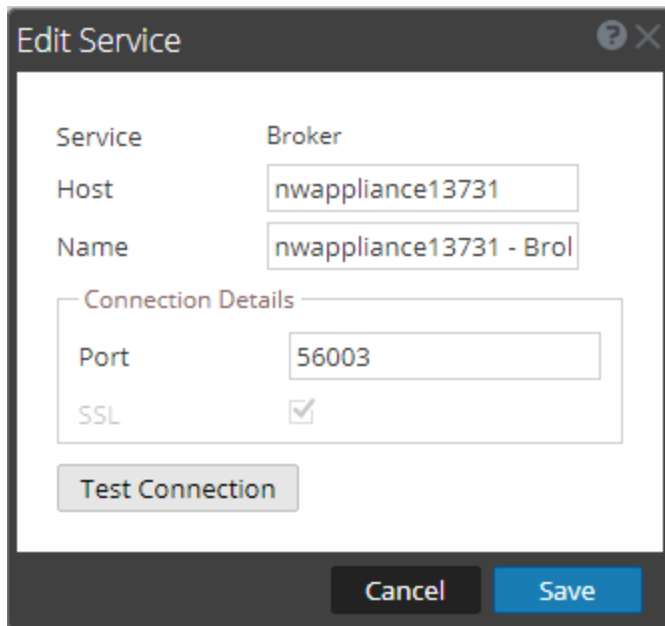
- Es wird ein Basis ISO-Image 10.3.2 oder früher verwendet.
- Das System wurde exklusiv mithilfe von RPMs aktualisiert, um Version 10.6.4 zu erhalten.

NetWitness Suite 11.0 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. Melden Sie sich bei NetWitness Suite an.
2. Navigieren Sie zu **ADMIN > Services**.
3. 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

4. Klicken Sie in der Symbolleiste in der Ansicht **Services** auf  (Bearbeiten). Das Dialogfeld „Service bearbeiten“ wird angezeigt.
5. 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 auf 56003).



**Edit Service**

Service: Broker

Host: nwappliance13731

Name: nwappliance13731 - Bro

Connection Details

Port: 56003

SSL:

Test Connection

Cancel Save

## NetWitness Endpoint

### Aufgabe 7: Erneutes Konfigurieren von Endpoint-Warmmeldungen über 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 11.0 ist der virtuelle Host `/rsa/system`. Für 10.6.4.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 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 (ESA)

### Aufgabe 8: Neukonfigurieren der automatisierten Bedrohungserkennung für ESA

Wenn Sie in 10.6.4.x die automatisierte Bedrohungserkennung verwendet haben, müssen Sie die folgenden Schritte ausführen, um sie über den ESA Analytics-Service in Version 11.0 neu zu konfigurieren.

1. Melden Sie sich bei NetWitness Suite 11.0 an.

2. Klicken Sie auf **ADMIN > System > ESA Analytics**.  
Für die Suspicious Domains-Module Command and Control (C2) für Pakete und C2 für Protokolle ist eine Whitelist mit der Bezeichnung „domains\_whitelist“ erforderlich.
3. Bedingungsabhängig: Wenn Ihre vorherige Whitelist zur automatisierten Bedrohungserkennung auf der Registerkarte **Listen** des Context Hub-Service 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 [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## **Aufgabe 9: 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 10.6.4.x-Daten erhalten haben (siehe [Anweisungen zum Backup](#)).

1. Erstellen Sie einen Benutzer auf dem Hostsystem, das in NetWitness Suite integriert wird, durch Anmeldung 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 10: Aktivieren des Dashboards „Bedrohung – Malwareindikatoren“

In Version 11.0.0 wurde das 10.6.4.x-Dashboard **Bedrohung – Indikatoren** umbenannt in **Bedrohung – Malwareindikatoren**. Wenn Sie dieses Dashboard in 10.6.4.x verwendet haben, müssen Sie folgende Schritte ausführen:

1. Aktivieren Sie das Dashboard **Bedrohung – Malwareindikatoren** in Version 11.0.
2. Legen Sie eine Datenquelle für neue Dashlets fest.  
Weitere Informationen finden Sie im RSA-Link (<https://community.rsa.com/docs/DOC-81463>) unter „Dashlets“.

## Protokollsammlung

### Aufgabe 11: 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 11.0 aktualisiert haben, um sicherzustellen, dass alle Sammlungsprotokolle den normalen Betrieb fortsetzen.

#### Zurücksetzen der stabilen Systemwerte für die Lockbox

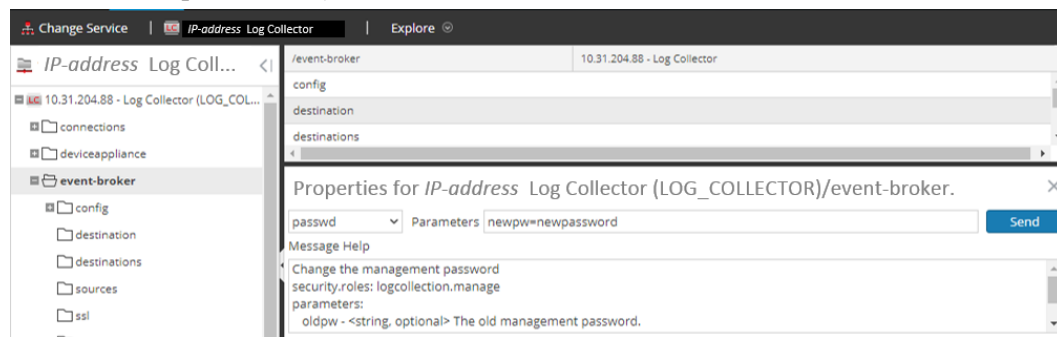
Die Lockbox speichert den Schlüssel zum Verschlüsseln der Ereignisquelle und anderer Passwörter für den Log Collector. Der Log Collector-Service kann die Lockbox aufgrund der Änderungen an den stabilen Werten nicht öffnen. Daher müssen Sie die stabilen Systemwerte für die Lockbox zurücksetzen. Anweisungen hierzu finden Sie unter „Protokollsammlung: Schritt 3. Einrichten einer Lockbox“ im *RSA NetWitness® Suite Protokollsammlung-Konfigurationsleitfaden*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 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 11.0 erneut eingeben.

1. Melden Sie sich bei NetWitness Suite an.
2. Klicken Sie auf **ADMIN > Services**.
3. Wählen Sie den Log Collector-Service aus.
4. Klicken Sie auf  (Aktionen) > **Ansicht > Erkunden**.
5. Klicken Sie mit der rechten Maustaste auf `event-broker` > **Eigenschaften**.
6. 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 10.6.4.x mit für Log Collectors, Log Decoder und Packet Decoder aktiviertem FIPS) Aufgabe 12: 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 [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Reporting Engine

### Aufgabe 13: Wiederherstellen der CA-Zertifikate für externe Syslog-Server für die Reporting Engine

Nach dem Upgrade müssen Sie die CA-Zertifikate des vor dem Upgrade angelegten Backups wiederherstellen. Das Backupskript sichert die 10.6.4.x-CA-Zertifikate im Verzeichnis `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.e16_8.x86_64/jre/lib/security/cacerts`.

Gehen Sie wie folgt vor, um die CA-Zertifikate in Version 11.0 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 Zertifikat (pem-Datei) in das Verzeichnis `/etc/pki/nw/trust/import`.

## **(Bedingungsabhängig) Aufgabe 14: 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® Suite Konfigurationsleitfaden Reporting Engine*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## **Reagieren**

### **Aufgabe 15: Wiederherstellen der benutzerdefinierten Schlüssel für den Antwortservice**

Wenn Sie in Version 10.6.4.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 10.6.4.x-Backup wiederhergestellt wird.
2. Navigieren Sie zum `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` in 11.0.  
Dies ist die neue Datei für 11.0.
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 16: Wiederherstellen der angepassten Skripte zur Normalisierung des Antwortservice

RSA hat die Skripte zur Normalisierung des Antwortservice in Version 11.0 umstrukturiert und an den folgenden neuen Speicherort verschoben:

```
/var/lib/netwitness/respond-server/scripts
```


Wenn Sie diese Skripte in 10.6.4.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 10.6.4.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 10.6.4.x-Skripte.
3. Navigieren Sie zum Verzeichnis `/var/lib/netwitness/respond-server/scripts`.  
Dieses Verzeichnis befindet sich dort, wo NetWitness Suite 11.0 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 10.6.4.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.

## (Bedingungsabhängig) Aufgabe 17: Aktivieren der deaktivierten 10.6.4.x-Datenaufbewahrung für das Incident-Management

Gehen Sie wie folgt vor, um die Datenaufbewahrungsaufträge für das Incident-Management, die Sie vor dem Upgrade deaktiviert haben, zu aktivieren:

1. Melden Sie sich bei RSA NetWitness® Suite an.
2. Wechseln Sie zu **ADMIN > Services** und wählen Sie den **Respond-Server** aus.
3. Klicken Sie auf  (Aktionen), **Ansicht > Erkunden**.

4. Navigieren Sie zum Node `respond/dataretention`.
5. Legen Sie den Parameter `enable` auf `true` fest.

## (Bedingungsabhängig) Aufgabe 18: Wiederherstellen von benutzerdefinierten Analystenrollen

Wenn Sie in Version in 10.6.4.x benutzerdefinierte Analystenrollen verwendet haben, müssen Sie diese in Version 11.0 reaktivieren. Informationen hierzu finden Sie unter *Hinzufügen von Rollen und Zuweisen von Berechtigungen für die Rollen* im *RSANetWitness Suite-Leitfaden Warehouse Analytics*. Navigieren Sie zu [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## NetWitness SecOps Manager

### Aufgabe 19: 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 [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Sicherheit

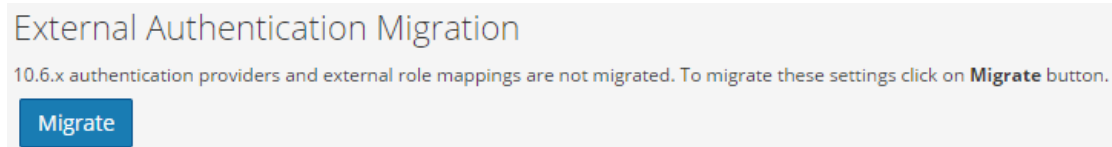
### Aufgabe 20: Migrieren von Active Directory (AD)

Wenn Sie sich das erste Mal bei der NetWitness Suite 11.0-Benutzeroberfläche anmelden, müssen Sie auf die Schaltfläche „Migrieren“ klicken, um die Migration von AD abzuschließen.

**Achtung:** Wenn Sie kein Upgrade von Version 10.6.4.2 durchgeführt haben, müssen Sie den 11.0.0.1-Patch anwenden, bevor Sie sich das erste Mal bei NetWitness Suite 11.0 anmelden und Active Directory migrieren. Sie brauchen den 11.0.0.1-Patch nicht anzuwenden, wenn Sie von 10.6.4.2 auf 11.0 aktualisiert haben.

1. Melden Sie sich bei NetWitness Suite mit Ihren `admin user`-Anmeldedaten an.
2. Klicken Sie auf **ADMIN > Sicherheit** und dann auf die Registerkarte **Einstellungen**.

Das folgende Dialogfeld wird angezeigt:




3. Klicken Sie auf **Migrieren**.

Die Migration ist abgeschlossen und das Dialogfeld wird geschlossen.

## **Aufgabe 21: Ändern der migrierten AD-Konfiguration, um das Zertifikat hochzuladen**

Wenn Sie in Active Directory (AD)-Server ein selbstsigniertes Zertifikat verwendet haben und in 10.6.4.x SSL für die Active Directory-Verbindung aktivieren, müssen Sie die migrierte Active Directory-Konfiguration zum Hochladen des Zertifikats ändern (entweder das selbstsignierte Zertifikat oder das CA-Zertifikat).

Gehen Sie wie folgt vor, um die migrierte Active Directory-Konfiguration zum Hochladen des Zertifikats zu ändern (entweder das selbstsignierte Zertifikat oder das CA-Zertifikat):

1. Melden Sie sich bei NetWitness Suite an.
2. Klicken Sie auf **ADMIN > Sicherheit** und dann auf die Registerkarte **Einstellungen**.
3. Wählen Sie unter **Active Directory-Einstellungen** eine AD-Konfiguration aus und klicken Sie auf .

Das Dialogfeld „Konfiguration bearbeiten“ wird angezeigt.

4. Navigieren Sie zum Feld **Zertifikatdatei**, klicken Sie auf **Durchsuchen** und wählen Sie ein Zertifikat aus Ihrem Netzwerk aus.
5. Klicken Sie auf **Speichern**.

## **Aufgabe 22. Beheben von Fehler bei Authentifizierung in 11.0**

Benutzer können sich nicht an der NetWitness Suite-Benutzeroberfläche anmelden, nachdem Sie ein Upgrade auf 11.0 durchgeführt haben, da die Benutzeroberfläche Benutzerkontoinformationen von MongoDB nicht abrufen kann.

- Wenden Sie sofort nach der Aktualisierung auf 11.0 den Patch 11.0.0.1 an, um dieses Problem zu beheben.

## **Aufgabe 23: Neukonfigurieren des Pluggable Authentication Module (PAM) in 11.0**

Nach der Aktualisierung auf Version 11.0 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 [Master Table of Contents](#) für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

Beziehen Sie sich auf Ihre 10.6.4.x PAM-Konfigurationsdateien im Verzeichnis `/etc` Ihrer 10.6.4.x-Backupdaten.

## Anhang A: Troubleshooting

---

Dieser Abschnitt beschreibt Probleme, die während eines Upgrades auftreten können, und die entsprechenden Lösungen. In den meisten Fällen erstellt NetWitness Suite Protokollmeldungen, wenn Probleme auftreten.

**Hinweis:** Wenn Sie Probleme bei der Aktualisierung 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:

- [11.0 Setup-Programm \(nwsetup-tui\)](#)
- [Backup](#)
- [Event Stream Analysis](#)
- [Allgemeines](#)
- [Log Collector-Service \(nwlogcollector\)](#)
- [NW-Server](#)
- [Reporting Engine](#)

## 11.0 Setup-Programm (nwsetup-tui)

<p><b>Problem</b></p>	<p>Host-Setup-Programm (nwsetup-tui) wird mit folgender Fehlermeldung in /var/log/netwitness/bootstrap/launch/security-server/security-server.log beendet:</p> <pre>&lt;yyyy-mm-dd hh:mm:ss,nnn&gt; [ main] ERROR SystemOperation Service startup failed. Running in safe mode org.h2.jdbc.JdbcSQLException: The database is read only [90097-193] at org.h2.message.DbException. getJdbcSQLException(DbException.java:345) ... at org.springframework.jdbc.datasource. AbstractDriverBasedDataSource.getConnection (AbstractDriverBasedDataSource.java:159) at com.rsa.asoc.security.upgrade.legacy. MigrationDatabase.&lt;init&gt;(MigrationDatabase.java:113)</pre>
<p><b>Ursache</b></p>	<p>Die H2-Datenbank benötigt Schreibberechtigung zum Abschließen der Hostinstallation.</p>
<p><b>Lösung</b></p>	<p>Stellen Sie über die Befehlszeile des NW-Servers Schreibberechtigung für H2.db her und starten Sie zunächst den NW-Server und dann das Setup-Programm „nwsetup-tui“ neu.</p> <pre>chmod o+w /var/lib/netwitness/uax/db/platform.h2.db systemctl restart rsa-nw-security-server.service nwsetup-tui</pre>

## Backup (`nw-backup`-Skript)

Meldung	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 <i>RSA NetWitness® Suite Konfigurationsleitfaden für Event Stream Analysis. Navigieren Sie zu <a href="#">Master Table of Contents</a> für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.</i>

## Event Stream Analysis

Problem	Der ESA-Service stürzt nach dem Upgrade auf 11.0 aus einem Setup mit FIPS- Aktivierung ab.
Ursache	Der ESA-Service verweist auf einen ungültigen Keystore.
Lösung	<ol style="list-style-type: none"> <li>1. Stellen Sie über SSH eine Verbindung mit dem ESAPrimary-Host her und melden Sie sich an.</li> <li>2. Ersetzen Sie in Datei <code>/opt/rsa/esa/conf/wrapper.conf</code> die Zeile „ <code>wrapper.java.additional.5=-</code> <code>Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore</code> “ durch: <code>wrapper.java.additional.5=-</code> <code>Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore</code></li> <li>3. Geben Sie den folgenden Befehl ein, um ESA neu zu starten: <code>systemctl restart rsa-nw-esa-server</code></li> </ol> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p><b>Hinweis:</b> 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.</p> </div>

## Allgemein

Die in diesem Abschnitt genannten Protokolle werden an `/var/log/install/install.log` auf dem NW-Serverhost gesendet.

Meldung	<code>ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service</code>
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 mit dem folgenden Befehl neu: <code>systemctl restart rsa-sms</code>

Meldung	<code>&lt;timestamp&gt; &lt;host&gt;: SMS_PostInstall: INFO: Free disk space on /opt is nGB &lt;timestamp&gt; &lt;host&gt;: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.</code>
Ursache	Für den SMS-Service wurde geringer oder nicht ausreichender Festplattenspeicherplatz zugewiesen.
Lösung	RSA empfiehlt, mindestens 10 GB Festplattenspeicherplatz für eine optimale Ausführung des SMS-Services bereitzustellen.

Problem	Nachdem Sie das Setup-Programm für einen Nicht-NW-Serverhost ausgeführt haben, müssen Sie die Benutzeroberfläche aufrufen, den Host aktivieren und den Service auf dem Host über die Ansicht „Hosts“ installieren. Wenn in der Spalte <b>Status</b> der Ansicht „Hosts“ die Meldung „Fehler bei der Installation <u>Details anzeigen</u> “ angezeigt wird, hat der Host die Verbindung aufgrund von Netzwerkproblemen verloren.
Lösung	Installieren Sie den Service auf dem Host über die Ansicht „Hosts“ neu.

## Log Collector-Service (`nwlogcollector`)

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

Meldung	<code>&lt;timestamp&gt;.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.</code>
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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Master Table of Contents</a> für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

Meldung	<code>timestamp NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Master Table of Contents</a> für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.



Meldung	<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 <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben. Navigieren Sie zu <a href="#">Master Table of Contents</a> für Version 11.0, um Dokumente zu NetWitness Suite 11.0 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 wird in sa.log angezeigt: Syslog Configuration migration failed. Restart jetty service to fix this issue
Ursache	Die globale Audit-Einrichtung des NW-Servers konnte nicht von Version 10.6.4 auf 11.0 migriert werden.
Lösung	<ol style="list-style-type: none"> <li>1. Stellen Sie über SSH eine Verbindung mit dem NW-Server her.</li> <li>2. Senden Sie den folgenden Befehl: <code>orchestration-cli-client --update-admin-node</code></li> </ol>

## 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.

Meldung	<code>&lt;timestamp&gt; : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]</code>
Ursache	Die Aktualisierung der Reporting Engine ist fehlgeschlagen, da Sie nicht über ausreichend Speicherplatz verfügen.
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 <i>Reporting Engine-Konfigurationsleitfaden</i> . Navigieren Sie zu <a href="#">Master Table of Contents</a> für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

## Anhang B: Beenden und Neustarten der Datenerfassung und -aggregation

RSA empfiehlt, vor dem Upgrade eines Decoders, Concentrators oder Broker-Hosts auf 11.0 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.

The screenshot shows the NetWitness Suite ADMIN interface. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main menu has HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The current view is SERVICES, with a sub-menu showing SIT-DEC1 - Decoder and System. Below the navigation, there are several action buttons: Upload Packet Capture File, Stop Capture, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into two columns: Decoder Service Information and Appliance Service Information. The Decoder Service Information table shows: Name: SIT-DEC1 (Decoder), Version: [redacted], Memory Usage: 414 MB (2.57% of 16081 MB), CPU: 51%, Running Since: 2016-Nov-15 10:12:07, Uptime: 3 days 4 hours 25 minutes, Current Time: 2016-Nov-18 14:37:07. The Appliance Service Information table shows: Name: SIT-DEC1 (Host), Version: [redacted], Memory Usage: 24876 KB (0.15% of 16081 MB), CPU: 52%, Running Since: 2016-Nov-15 10:12:04, Uptime: 3 days 4 hours 25 minutes 4 seconds, Current Time: 2016-Nov-18 14:37:08. Below these tables are sections for Decoder User Information and Host User Information. The bottom of the interface features the RSA NETWITNESS logo.

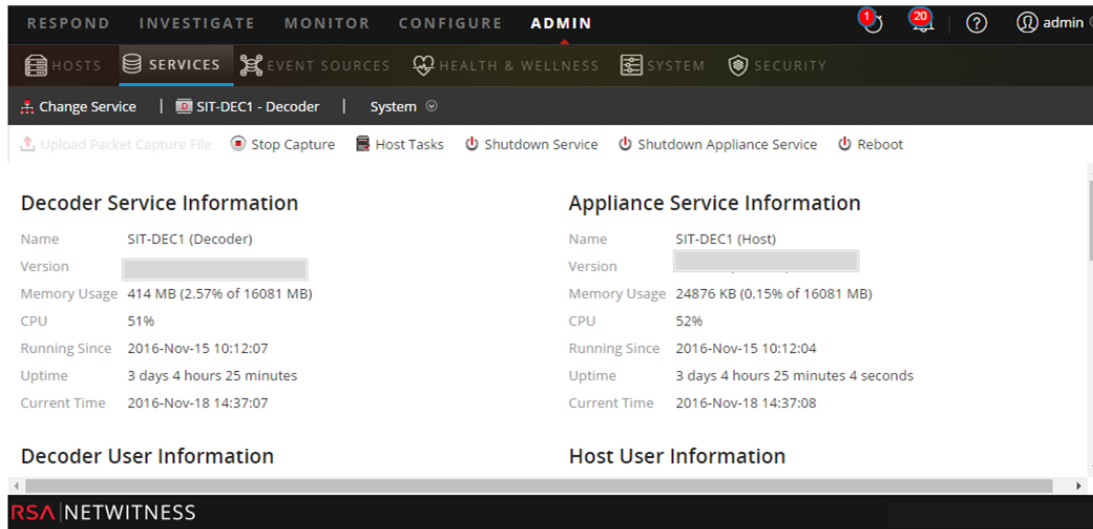
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.
4. Klicken Sie in der Symbolleiste auf  **Stop Capture**.


#### 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.

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




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

- Klicken Sie in der Symbolleiste auf  **Stop Capture**.

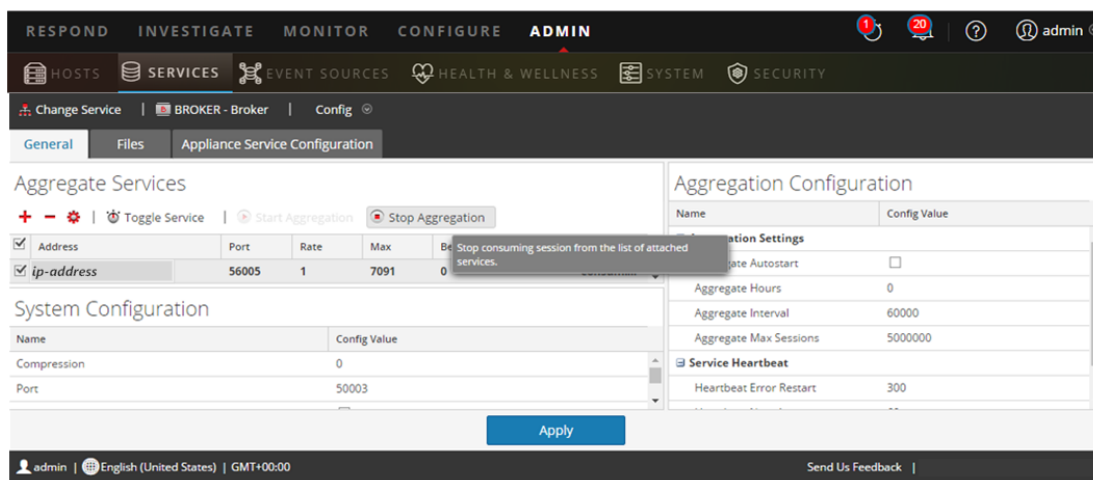
### Aggregation beenden

- Melden Sie sich bei NetWitness Suite an und wechseln Sie zu **ADMIN > Services**.

- Wählen Sie den **Broker**-Service aus.

- Wählen Sie unter  (Aktionen) die Optionen **Ansicht > Konfiguration** aus.

- Die Registerkarte **Allgemein** wird angezeigt.




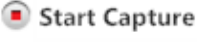
- Klicken Sie unter **Aggregierte Services** auf  **Stop Aggregation**.

## Starten der Datenerfassung und -aggregation

Starten Sie die Paket- und Protokollerfassung und -aggregation nach der Aktualisierung auf 11.0 neu.


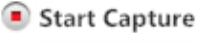
### Starten der Paketerfassung

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  **Start Capture**.

### 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  **Start Capture**.

### Aggregation starten

Während des Upgrades von 10.6.4.x auf 11.0 wird der Broker-Service neu gestartet und damit wird automatisch die Aggregation gestartet.

## Revisionsverlauf

Version	Datum	Beschreibung	Verfasser
1,0	16-Okt-17	Betriebsfreigabe	IDD
1.1	25-Okt-17	Änderungen: <ul style="list-style-type: none"><li>• Die Workarounds „Active Directory“ und „Änderungen an Benutzerattributen und Rollen, die sich auf Investigate auswirken“ wurden geändert, um den Patches 10.6.4.2 und 11.0.0.1 zu entsprechen.</li><li>• Fehler bei Authentifizierung in 11.0</li></ul>	IDD