

# NetWitness<sup>®</sup> Plattform

Version 12.5

## Upgradehandbuch

## Contact Information

NetWitness Community unter <https://community.netwitness.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Case Management bereitgestellt werden.

## Marken

RSA und andere Marken sind Marken von RSA Security LLC oder deren Tochtergesellschaften („RSA“). Eine Liste der RSA-Marken finden Sie unter <https://www.rsa.com/de-de/company/rsa-trademarks>. Alle anderen Marken sind Marken ihrer jeweiligen Inhaber.

## Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von RSA Security LLC oder deren Tochtergesellschaften und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Angabe des unten stehenden 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 ist nicht als Verpflichtung von RSA zu verstehen.

Es wird empfohlen, keine Repositories von Drittanbietern bereitzustellen oder Änderungen am zugrunde liegenden NetWitness-Betriebssystem vorzunehmen, die nicht Teil der unterstützten NetWitness-Version sind. Jede derartige Änderung außerhalb des von NetWitness genehmigten Images kann zu einem Service- oder Funktionskonflikt führen und ein Re-Imaging des NetWitness-Systems erfordern, um NetWitness wieder in einen optimierten Funktionszustand zu versetzen. Falls ein Repository eines Drittanbieters bereitgestellt oder eine andere nicht unterstützte Änderung vom Kunden ohne Genehmigung von NetWitness vorgenommen wird, übernimmt der Kunde die volle Verantwortung für jegliche Systemfehlfunktion, bis das Problem durch Troubleshooting oder ein Re-Imaging des Services behoben werden kann.

## 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 NetWitness Community 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 müssen beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

## Verteilung

Für die Nutzung, das Kopieren und die Verteilung der in dieser Veröffentlichung beschriebenen Software von RSA Security LLC oder deren Tochtergesellschaften („RSA“) ist eine entsprechende Softwarelizenz erforderlich.

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

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. RSA MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.

## Sonstiges

Dieses Produkt, diese Software, die zugehörigen Dokumentationen sowie die Inhalte unterliegen den allgemeinen Geschäftsbedingungen von NetWitness, die zum Zeitpunkt der Veröffentlichung dieser Dokumentation gültig sind und unter <https://www.netwitness.com/standard-form-agreements/> zu finden sind.

© 2024 RSA Security LLC oder deren Tochtergesellschaften. Alle Rechte vorbehalten.

September 2024

# Inhalt

---

<b>Upgrade von NetWitness Platform</b> .....	<b>7</b>
Unterstützte Upgrade-Pfade für 12.5 .....	8
NetWitness-Upgraderichtlinien für Azure .....	9
Ausführung in einer Umgebung mit gemischtem Modus .....	9
Überlegungen zum Upgrade von ESA-Hosts .....	9
Aktualisieren oder Installieren der Windows Legacy Collection .....	11
Terminologie .....	11
<b>Ausführen der Upgrade-Vorabprüfungen</b> .....	<b>12</b>
Checkliste für die Betriebssystemmigration .....	12
Upgrade-Checkliste .....	13
Netzwerk-Checkliste .....	15
Zertifikat-Checkliste .....	16
<b>Vorbereiten des Upgrades von NetWitness Platform</b> .....	<b>17</b>
Aufgabe 1. (Wichtig) Vorbereiten des Upgrades des AlmaLinux-Betriebssystems .....	17
Nicht unterstütztes Dateisystem .....	17
Unmounten und Entfernen von BTRFS .....	17
Unmounten von NFS .....	17
Überprüfung des AVX/VMX-CPU-Befehlssatzes .....	18
PF_RING zur DPDK-Migrationsunterstützung .....	18
Aufgabe 2. (Empfohlen, aber optional) Entfernen der veralteten Paket-Repositorys .....	18
Aufgabe 3. Vorbereiten der ESA-Bereitstellungen für die Migration zu 12.5 .....	19
Managen von ESA-Bereitstellungen und Datenquellen .....	19
Aufgabe 4. Entfernen von Drittanbieterpaketen .....	21
Aufgabe 5. Single Sign-On (SSO): Aktivieren der SAML-Antwortsignierung in Microsoft Azure ADFS .....	21
Aufgabe 6. (optional). Deaktivieren STIG-basierter FIPS-Kernel-Kontrollmaßnahmen .....	21
Aufgabe 7. (optional). Überprüfen der Verbindung zum Live-Server .....	22
Aufgabe 8. Synchronisieren der Uhrzeit auf den Komponentenhosts mit dem NW-Serverhost .....	22
<b>Durchführen der Upgrade-Aufgaben</b> .....	<b>24</b>
Auswählen von Upgrade-Optionen .....	25
Option 1: Upgrade von NetWitness Platform mithilfe von Live-Services .....	25
Option 2: Upgrade von NetWitness Platform offline .....	26
Aufgabe 1: Füllen des Staging-Ordners (/var/netwitness/common/update-stage/) mit Versionsaktualisierungsdateien. Gehen Sie wie folgt vor. ....	27
Aufgabe 2: Anwenden von Upgrades aus dem Staging-Bereich auf jeden Host. Gehen Sie wie folgt vor. ....	27
Option 3: Upgrade von NetWitness Platform mit der CLI (offline) .....	28

Anweisungen für das Upgrade des externen Repository über die CLI .....	30
Option 4 (optional): Vorabbereitstellung des Upgrade-Repository durch Herunterladen von Paketen .....	32
<b>Durchführen von Aufgaben nach dem Upgrade .....</b>	<b>35</b>
Allgemein .....	35
Konfigurieren von Jetty .....	35
Sicherstellen, dass die Services neu gestartet wurden und Daten erfassen und aggregieren .....	35
Wiederherstellen der Inhalte der Core-Services .....	37
Event Stream Analysis (ESA) .....	37
Managen von ESA-Bereitstellungen und Datenquellen .....	38
Benutzerdefinierte Skripte für Benachrichtigungen migrieren .....	39
Reagieren .....	39
(Bedingt) Wiederherstellen aller benutzerdefinierten Schlüssel des Respond-Services in „custom_normalize_alerts.js“ und Unterstützen neuer Datenquellen .....	40
Analyse des Nutzer- und Entitätsverhaltens (UEBA) .....	40
Legacy-Windows-Log Collector .....	42
Aktualisieren Sie Legacy-Windows-Log-Collector-Zertifikate mit aktualisierten SA-Zertifikaten .....	42
Warehouse Connector .....	43
Festlegen des Wiederherstellungskennworts für die Lockbox .....	44
<b>Durchführen von Validierungsprüfungen nach dem Upgrade .....</b>	<b>45</b>
<b>Installation des 12.5-Relay-Servers .....</b>	<b>47</b>
Upgrade der Endpoint-Agents .....	47
<b>Beheben von Upgrade-Problemen .....</b>	<b>48</b>
Informationen zum Troubleshooting beim AlmaLinux-Betriebssystem .....	49
Migration von Lockbox zu SecureStore schlägt bei Admin-Server, Reporting Engine und SMS fehl .....	51
Fehler: deploy_admin-Benutzerkennwort abgelaufen .....	53
Downloadfehler .....	54
Fehler beim Bereitstellen der Version <Versionsnummer> Update-Pakete fehlen .....	55
Fehler beim Aktualisieren des externen Repository .....	55
Fehler: Hostaktualisierung fehlgeschlagen .....	56
Fehler: Update-Pakete fehlen .....	57
Fehler: Patch-Update für Nicht-NW-Server .....	57
Fehler: Host-Neustart nach Update über die Befehlszeile .....	58
Log Collector-Service (nwlogcollector) .....	58
NW-Server .....	60
Orchestrierung .....	61
Reporting Engine-Service .....	62
Event Stream Analysis .....	62
Legacy-Windows-Log Collector .....	63
ESA-Troubleshooting-Informationen .....	63
ESA-Regeln erstellen keine Warnmeldungen .....	63

Beispiel einer Warnmeldung des ESA-Korrelationservers für fehlende Metaschlüssel .....	65
<b>Nutzen Sie das NetWitness Community Portal zur Unterstützung .....</b>	<b>66</b>
Ressourcen zur Selbsthilfe .....	66
NetWitness Support kontaktieren .....	66
Feedback zur Produktdokumentation .....	67

## Upgrade von NetWitness Platform

Dieses Dokument bietet Informationen über die Vorteile und den Prozess des Upgrades von NetWitness Platform auf 12.5. Stellen Sie sicher, dass Sie die Voraussetzungen und Aufgaben vor dem Upgrade durchgehen, bevor Sie NetWitness Platform aktualisieren. Abhängig von Ihrer Internetverbindung können Sie NetWitness Platform mit vier verschiedenen Optionen aktualisieren. Nach dem Upgrade sollten Sie auch bestimmte in diesem Handbuch aufgeführte Aufgaben und Validierungsprüfungen durchführen, um das Upgrade abzuschließen. Falls nicht anders angegeben, gelten die Anweisungen in diesem Dokument sowohl für physische als auch für virtuelle Hosts (einschließlich AWS, Azure Public Cloud und Google Cloud Platform).

**WICHTIG:** NetWitness rät Nutzern, ihre Softwareversionen zu überprüfen und weist darauf hin, dass die Versionen bis 12.2 am 31. März 2024 das Ende der Nutzungsdauer erreicht haben. Weitere Informationen finden Sie unter <https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875>. NetWitness empfiehlt, ein Upgrade auf Version 12.5 durchzuführen, um die neuesten Funktionen und Sicherheitsupdates nutzen zu können.

**WICHTIG:** NetWitness empfiehlt Ihnen dringend, vor dem Upgrade des UEBA-Servers auf Version 12.5 eine Sicherungskopie der Datei `schemas.json` zu erstellen. Sie finden diese Datei am folgenden Speicherort: `/var/netwitness/presidio/asl/adapter-config/schema-query/schemas.json`

**WICHTIG:** UEBA ist ab Version 12.5 standardmäßig mit App-Regeln aktiviert. Dies bedeutet, dass Decoder, die mit Neuinstallationen von 12.5 bereitgestellt werden, automatisch über die erforderlichen UEBA-bezogenen App-Regeln verfügen. Wenn Sie bereits App-Regeln mit einer älteren Version verwendet und dann auf 12.5 aktualisiert haben, funktionieren diese Regeln ohne Änderungen weiterhin. NetWitness empfiehlt Ihnen jedoch dringend, die neuen UEBA-Bundles von NetWitness Live auf Ihren Decodern bereitzustellen, um App-Regeln zu verwenden. Dadurch wird sichergestellt, dass Sie über alle aktuellen App-Regeln verfügen, die für die ordnungsgemäße Funktion von UEBA erforderlich sind. Weitere Informationen zur Bereitstellung der UEBA-Bundles auf Decodern finden Sie unter dem Thema [Suchen und Bereitstellen von Live-Ressourcen](#) im *Benutzerhandbuch zu NetWitness Live-Services für 12.5*.

**Bundle-Namen für die Bereitstellung von UEBA-bezogenen App-Regeln:**

- NetWitness UEBA-Authentifizierungsvorgänge
- NetWitness UEBA-Registrierungsvorgänge
- NetWitness UEBA-Active Directory-Vorgänge
- NetWitness UEBA-Prozessvorgänge
- NetWitness UEBA-Dateivorgänge
- NetWitness UEBA – Windows-Kerberos-Service-Request
- NetWitness UEBA – Netzwerk-TLS-Ausgangsverbindungen

**WICHTIG:** NetWitness 12.4 und spätere Versionen (AlmaLinux) unterstützen keine numerischen Benutzernamen. Das bedeutet, dass Kunden, die PAM SecurID nur mit Zahlen als Benutzernamen verwenden, nach dem Upgrade auf Version 12.5 nicht zu den Gruppen hinzugefügt werden können. Weitere Informationen zu dieser Einschränkung finden Sie unter <https://www.webconn.tech/kb/are-all-numeric-username-allowed-in-almalinux-8>.

**WICHTIG:** Die benutzerdefinierten Suchmuster, die Sie mit der Datei **search.ini** in Version 12.3.1 oder früher erstellt haben, werden nicht in das neue Dateiformat **search.xml** migriert, das in Version 12.5 und höher verwendet wird. Daher sind diese benutzerdefinierten Suchmuster nach dem Upgrade auf Version 12.5 oder höher nicht mehr verfügbar.

Um diese benutzerdefinierten Suchmuster in der neuen Version neu zu erstellen, müssen Sie sie erneut manuell konfigurieren. Sie haben zwei Möglichkeiten:

– Gehen Sie zur Ansicht **Investigate > Ereignisse** und erstellen Sie die Suchmusterregeln und stellen Sie diese in einer Policy bereit, die Packet Decoder enthält.

– Gehen Sie zu **Inhaltsbibliothek > Mehr > Suchmusterregel** und erstellen Sie die Regeln.

Ausführliche Anweisungen zum Erstellen von Suchmusterregeln finden Sie im Abschnitt **Erstellen eines Suchmusters auf der Registerkarte Textim Thema Analysieren von Ereignissen in der Ansicht „Ereignis“** des [Investigate-Benutzerhandbuchs](#) oder im Thema **Verwalten von Suchmusterregeln** im [Handbuch zum zentralisierten Contentmanagement für NetWitness](#).

**Hinweis:** NetWitness Platform unterstützt jetzt die Installation mehrerer UEBA-Server in Ihrer Umgebung. Weitere Informationen finden Sie im Thema **Konfigurieren mehrerer UEBA-Server** im *NetWitness UEBA-Konfigurationshandbuch*.

**Hinweis:** Ab NetWitness 12.5 ist die Startseite die Standard-Zielseite für Benutzer, die die NetWitness Platform zum ersten Mal installieren. Bestandsbenutzer verwenden als Startseite weiterhin Springboard. Die Springboard-Funktion wird jedoch in zukünftigen Versionen nicht mehr unterstützt und die Startseite wird zur standardmäßigen Landingpage. Weitere Informationen finden Sie im *NetWitness-Handbuch „Erste Schritte“ für 12.5* unter **Springboard verwalten**.

Es gibt viele interessante neue Funktionen, die Sie nach dem Upgrade auf 12.5 aktivieren können. Eine detaillierte Beschreibung der neuen Funktionen in dieser Version finden Sie in den *Versionshinweisen zu NetWitness Platform 12.5*. Navigieren Sie zur Seite [NetWitness All Versions Documents](#) und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen. Weitere Informationen zu den neuen Funktionen, die in den vorherigen Versionen veröffentlicht wurden, finden Sie unter <https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-x-to-12-x/ta-p/695650>.

## Unterstützte Upgrade-Pfade für 12.5

Die folgenden Upgradepfade werden für NetWitness 12.5 unterstützt:

- NetWitness 12.4.2.0 auf 12.5
- NetWitness 12.4.1.0 auf 12.5
- NetWitness 12.4.0.0 auf 12.5
- NetWitness 12.3.1.0 auf 12.5
- NetWitness 12.3.0.0 auf 12.5
- NetWitness 12.2.0.1 auf 12.5
- NetWitness 12.2.0.0 auf 12.5

## NetWitness-Upgraderichtlinien für Azure

In-Place-Upgrades auf Azure-VMs werden unterstützt, wenn die im Azure-Installationshandbuch beschriebene Standardkonfiguration befolgt wird. Die Nutzer sind dafür verantwortlich, dass keine VM-Policies auf der Azure-Abonnementebene das Betriebssystem der VM beeinträchtigen, wie z. B. Konfigurationen im Zusammenhang mit der Azure-Steuerungsebene.

Wenn Sie die Azure-Installationsanleitung richtig befolgen, sollte der Upgradevorgang reibungslos und ohne Warnungen ablaufen. Ein Abweichen von diesen Richtlinien oder das Hinzufügen zusätzlicher Konfigurationen, wie z. B. solche, die die Azure-Steuerungsebene betreffen, kann jedoch zu Fehlern führen, wie unten dargestellt:

## Ausführung in einer Umgebung mit gemischtem Modus

NetWitness Platform unterstützt den gemischten Modus während des Upgrades. Der gemischte Modus tritt auf, wenn einige Services auf eine neue Version aktualisiert werden und andere Services noch mit der älteren Versionen arbeiten.


Weitere Informationen finden Sie im Thema **Ausführen im gemischten Modus** im *NetWitness – Leitfaden für die ersten Schritte mit Hosts und Services*.

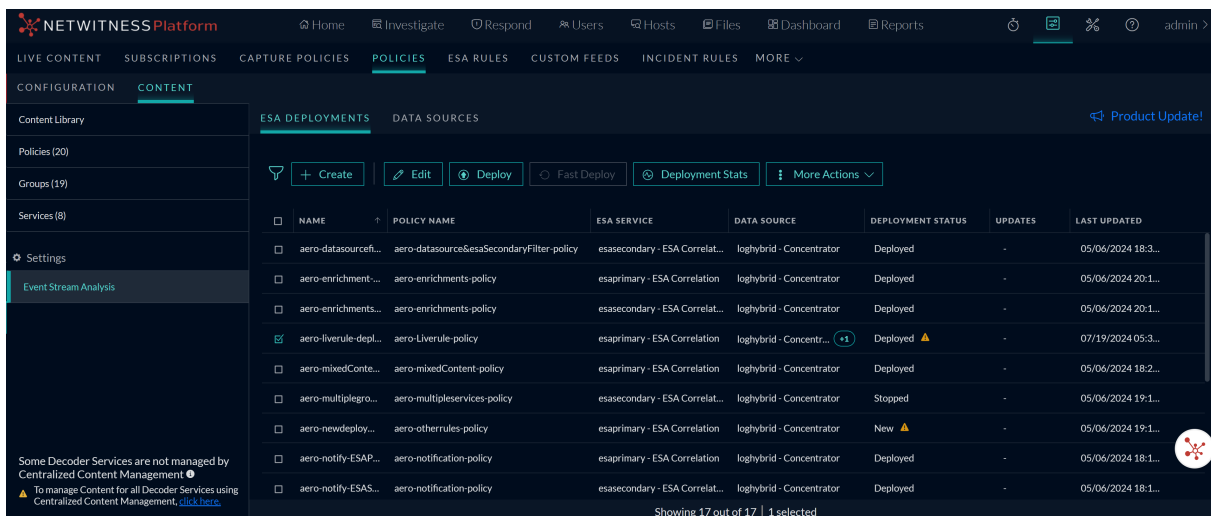
### Hinweis:

- Wenn es länger dauert, alle Hosts in Ihrer Umgebung zu aktualisieren, wenden Sie sich an den NetWitness-Support, um Probleme zu vermeiden.
- Wenn Sie Endpoint Log Hybrid im gemischten Modus ausführen, stellen Sie sicher, dass die Version von Endpoint Broker der Version eines der Endpoint-Servers entspricht.
- Der gemischte Modus wird für ESA-Hosts in NetWitness Platform nicht unterstützt.

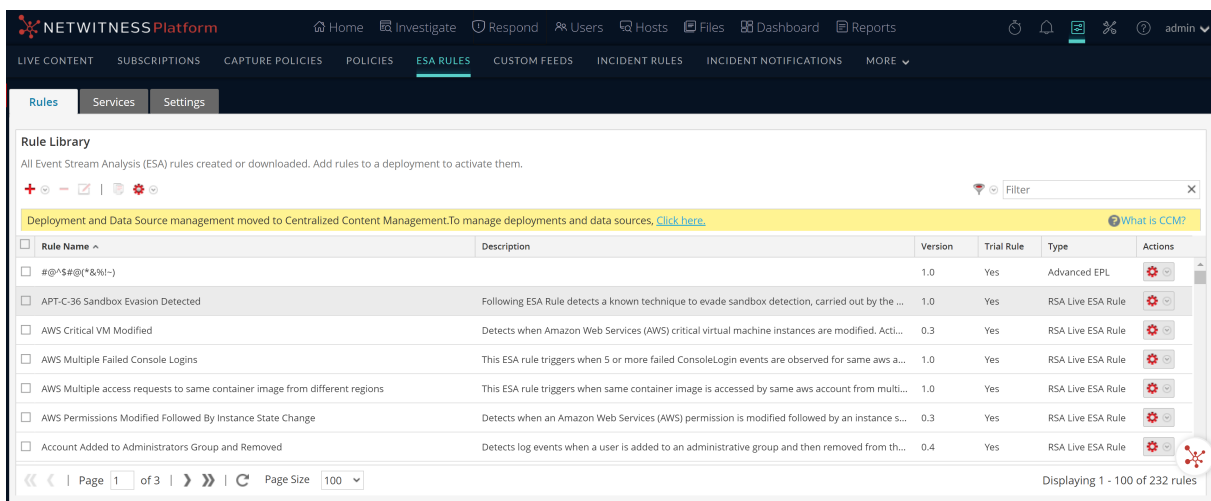
## Überlegungen zum Upgrade von ESA-Hosts

**WICHTIG:** Der NetWitness-Server, der primäre ESA-Host und der sekundäre ESA-Host müssen alle mit derselben NetWitness Platform-Version arbeiten.

- Sie können die ESA-Bereitstellungen und Datenquellen nur über **Zentralisiertes Contentmanagement** verwalten. Wechseln Sie zur Seite  (**KONFIGURIEREN**) > **Policies** > **Inhalt** > **Event Stream Analysis**, um die ESA-Bereitstellungen und Datenquellen zu verwalten. Weitere Informationen finden Sie in der folgenden Abbildung.



- Sie können die ESA-Regeln nur auf der Seite **ESA-Regeln** verwalten. Weitere Informationen finden Sie in der folgenden Abbildung.



- Nach dem Upgrade auf die Version 12.5 werden alle ESA-Bereitstellungen zur Seite **(KONFIGURIEREN) > Policys** migriert. Jede Bereitstellung wird in eine Policy und eine Gruppe umgewandelt und steht erst nach dem Upgrade der Korrelationsserver auf die Version 12.5 zur Verwaltung zur Verfügung. Stellen Sie sicher, dass Sie den Upgrade-Prozess so planen, dass die Korrelationsserver unmittelbar nach dem Admin-Server-Upgrade aktualisiert werden. Auf die Bereitstellungen kann erst zugegriffen werden, wenn die entsprechenden Korrelationsserver aktualisiert worden sind. Die Korrelationsserver verarbeiten die Warnmeldungen und Ereignisse jedoch weiterhin.
- Sie müssen die ESA-Hosts sofort nach dem Upgrade des Admin-Servers aktualisieren.  
 Weitere Informationen zum **zentralisierten Contentmanagement** und zur Verwaltung der Bereitstellungen, finden Sie unter [Handbuch zum zentralisierten Contentmanagement für NetWitness](#).

## Aktualisieren oder Installieren der Windows Legacy Collection

Anweisungen zum Upgrade und zur Installation von NetWitness Legacy Windows Collection finden Sie im [Windows Legacy Collection-Handbuch für NetWitness](#).

**Hinweis:** Starten Sie nach dem Upgrade oder der Installation von Windows Legacy Collection das System neu, um sicherzustellen, dass Log Collection ordnungsgemäß funktioniert.

## Terminologie

Name	Beschreibung
AVX	Advanced Vector Extensions
VMX	Virtual Machine Extension
NFS	Network File System
BTRFS	B-Tree File System
DPDK	Data Plane Development Kit

## Ausführen der Upgrade-Vorabprüfungen

---

NetWitness empfiehlt dringend, vor dem Upgrade auf NetWitness Platform 12.5 die Prüfungen vor dem Upgrade auszuführen, um etwaige Probleme zu erkennen, die zu einem Fehler beim Upgrade führen können.

**Hinweis:**

- Stellen Sie sicher, dass das `deploy_admin`-Kennwort gültig und aktuell ist. Ändern Sie es nicht in der Benutzeroberfläche. Unter <https://community.netwitness.com/t5/netwitness-platform-online/manage-the-deploy-admin-account/ta-p/669802> erfahren Sie, wie Sie das Kennwort ändern.
- Wenn eine Prüfung bei den Prüfungen vor dem Upgrade fehlschlägt, lesen Sie <https://community.netwitness.com/t5/netwitness-knowledge-base/netwitness-pre-upgrade-check-known-issues-master-list/ta-p/708695>, um das Problem im Zusammenhang mit der fehlgeschlagenen Prüfung zu beheben.

### Bevor Sie beginnen

Sie müssen zuerst das Standalone-RPM mit <https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096> herunterladen und in der Readme-Datei nachlesen, wie Sie das Standalone-RPM installieren und anschließend die Vorprüfung ausführen.

### So führen Sie die Prüfungen vor dem Upgrade aus

1. Stellen Sie über SSH eine Verbindung mit dem Admin-Server her.
2. Führen Sie mit dem Tool „Upgrade Precheck“ die folgenden Befehle nacheinander aus:
  - a. `nw-precheck-tool-standalone os-migration-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Validierungsprüfungen für die Liste von Prüfpunkten in der [Checkliste für die Betriebssystemmigration](#) durchführen.
  - b. `nw-precheck-tool-standalone upgrade-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Validierungsprüfungen für die Liste der Tests in der [Upgrade-Checkliste](#) durchführen.
  - c. `nw-precheck-tool-standalone network-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Validierungsprüfungen für die Liste der Tests in der [Netzwerk-Checkliste](#) durchführen.
  - d. `nw-precheck-tool-standalone cert-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Validierungsprüfungen für die Liste von Prüfpunkten in der [Zertifikat-Checkliste](#) durchführen.

## Checkliste für die Betriebssystemmigration

Das Tool „Upgrade Precheck“ führt die Validierungsprüfungen für die folgende Liste von Prüfpunkten in der Checkliste für die Betriebssystemmigration durch:

- **Versionsprüfungstest**: Überprüft, ob die NetWitness-Version des Systems die neuere Version von 12.2.0.0 ist oder nicht.
- **AVX-/VMX-Test**: Prüft, ob die AVX-/VMX-Flags für die Nodes, für die sie erforderlich sind, aktiviert sind oder nicht.

- **NFS-Mount-Test:** Überprüft, ob der Mount-Punkt vom Typ NFS auf einem der Nodes aktiv ist.
- **Test für mehrere "kernel-devel"-Pakete:** Überprüft, ob Decoder und Packet Hybrid mehrere Versionen des Kernel-Devel-Pakets haben oder nicht.
- **PF-Ringerfassungsgerätetest:** Überprüft, ob das PF\_ring-Erfassungsgerät auf Decodern vorhanden ist, und löst eine Warnung aus, um das PF\_ring-Erfassungsgerät in ein DPDK-Erfassungsgerät zu ändern.
- **BTRFS-Mount-Test:** Überprüft, ob die BTRFS-Partition gemountet ist.

**Hinweis:** LEAPP und das Alma-Betriebssystem unterstützen keine BTRFS-Partition.

- **Speicherplatzprüfung:** Überprüft, ob in der Partition / auf jedem Node genügend Speicherplatz frei ist.
- **Überprüfung des Fips-Modus:** Überprüft, ob der Fips-Modus auf allen Nodes deaktiviert (auf „false“ festgelegt) ist.
- **Mountcheck-Test:** Überprüft, ob alle Partitionen oder Dateiverzeichnisse ordnungsgemäß gemountet sind.
- **Salt Master-Kommunikationstest:** Überprüft die Salt-Kommunikation von Node 0 mit allen Nodes.
- **CIFS-Prüftest:** Identifiziert alle CIFS-Dateisysteme auf den Hosts, deren direktes Upgrade nicht unterstützt wird.
- **XFS Ftype-Überprüfungstest:** Überprüft, ob auf dem Host XFS-Dateisysteme mit ftype auf 0 gesetzt sind.
- **CCM-Überprüfungstest für nutzerdefinierte Inhalte:** Überprüft, ob **.envision**-Dateien an den richtigen Speicherorten extrahiert werden.
- **Überprüfungstest für das optische Laufwerk:** Überprüft, ob ein optisches Gerät auf einem Hardwaregerät angebracht ist. Wird ein optisches Gerät erkannt, fordert der Test den Nutzer auf, es abzumelden.

## Upgrade-Checkliste

Das Tool „Upgrade Precheck“ führt die Validierungsprüfungen für die folgende Liste von Prüfpunkten in der Upgrade-Checkliste durch:

- **Sicherheits-Client-Dateiprüfung:** Stellt sicher, dass die Datei `security-client-amqp.yml` nicht vorhanden ist.
- **Node-0-NW-Service-ID-Statusprüfung:** Stellt sicher, dass die gesamte Service-ID bei den verschiedenen Services in Node 0 intakt ist.
- **Broker Service Trustpeer Symlink-Dateiprüfung:** Stellt sicher, dass die Broker Service Trustpeer Symlink-Datei (`/etc/netwitness/ng/broker/trustpeers/`) nicht beschädigt ist.
- **Node-0-NW-Services-Statusprüfung:** Überprüft den Status aller Services in Node 0.

- **Prüfung externer Yum-Repositorys:** Stellt sicher, dass externe Repositorys nicht verfügbar und nicht aktiviert sind.
- **Node-0-RPM-DB-Indexprüfung:** Überprüft, ob die RPM-Datenbank beschädigt ist oder nicht.
- **Salt Master-Kommunikationstest:** Überprüft die Salt-Kommunikation von Node 0 mit allen Nodes.
- **Node-0-Zertifikatsprüfung:** Überprüft, ob Zertifikate fehlen, abgelaufen sind oder einen ungültigen Ausstellertyp aufweisen.
- **Mongo-Authentifizierung:** Validiert die `deploy_admin` Anmeldeinformationen, die mit dem Mongo-Client vom `security-cli-client` abgerufen wurden.
- **Rabbitmq-Authentifizierung:** Validiert die `deploy_admin` Anmeldeinformationen, die mit RabbitMQ vom `security-cli-client` abgerufen wurden.
- **(Komponentenhosts) Node-X-NW-Servicestatusprüfung:** Überprüft den Status der Service (aktiv oder inaktiv) auf allen Node X.
- **(Komponentenhosts) Node-X-Zertifikatsprüfung:** Überprüft den Ablauf des Zertifikats, das Fehlen, das Beschädigen und die Nichtübereinstimmung des Ausstellers in allen Kategorien von Node X.
- **Bereitstellen von Node-CPU-Speicherinformationen:** Bietet CPU- und Speicherdetails aller Nodes sowie den in Echtzeit verfügbaren Arbeitsspeicher.
- **(Admin-Server) Node-0-Dateisystem-Auslastungsprüfung:** Überprüft die Festplattenpartitionsauslastung von `/var/netwitness/mongo`, `/var/netwitness` und `root` auf Node 0.
- **(Komponentenhosts) Node-X-Dateisystem-Auslastungsprüfung:** Überprüft die Festplattenpartitionsauslastung von `/var/netwitness/mongo`, `/var/netwitness` und `root` für ESA Primary und Endpoint Log Hybrid-Services auf Node X.
- **Prüfung des Berechtigungsmodus für Mongo-Datei (ESAPrimary):** Überprüft den ESA-Primärknoten im System oder Stack und überprüft den Berechtigungsmodus der Mongo-Datei.
- **Überprüfung des Orchestrierungsservers auf Normalmodus:** Überprüft, ob der Orchestrierungsservice im normalen oder abgesicherten Modus ausgeführt wird.
- **(Admin-Server) Node-0-Init-Statusprüfung:** Überprüft, ob Probleme vorliegen, die zu einem Fehlschlagen des Initialisierungsprozesses führen könnten.
- **Überprüfung des Fips-Modus:** Mit dieser Überprüfung wird sichergestellt, dass der Fips-Modus vor oder nach dem Upgrade deaktiviert (auf „false“ festgelegt) ist.
- **Node-X-RPM-DB-Indexprüfung:** Prüft den Status der RPM-Datenbank auf Node-X, um sicherzustellen, dass sie nicht beschädigt ist.
- **Node-Z-Yum-Proxy-Prüfung:** Überprüft das Vorhandensein der Datei `yum.conf` und die Verfügbarkeit eines Proxys in der Datei auf Node -Z.

- **Node-X-Yum-Proxy-Prüfung:** Überprüft das Vorhandensein der Datei yum.conf und die Verfügbarkeit eines Proxys in der Datei auf Node -X.
- **Test zur Überprüfung der Host-Informationen:** Überprüft, ob die Informationspflichtfelder aller Hosts im System (Host-IP, Hostname, installierte Services und Rohversion) verfügbar sind.
- **Node-Z-Verschlüsselungsprüfungstest:** Überprüft, ob die erforderlichen Codierschlüssel am Speicherort `/etc/rabbitmq/rabbitmq.config` auf Node-0 verfügbar sind.
- **Test zur Überprüfung der Node-X-Codierschlüssel:** Überprüft, ob die erforderlichen Codierschlüssel am Speicherort `/etc/rabbitmq/rabbitmq.config` auf allen Node-X verfügbar sind.
- **Test zur Überprüfung der Node-X-Hardwareversion:** Prüft die Hardwareversion aller erreichbaren Node-X.
- **Test zur Überprüfung der Node-Z-Hardwareversion:** Prüft die Hardwareversion des Admin-Servers.
- **Test zur Überprüfung der PuppetCA-Zertifikate:** Überprüft, ob die veralteten Puppet-CA-Zertifikate am Speicherort `/etc/pki/nw/trust/truststore.pem` vorhanden sind.
- **AdminCertCheck-Test:** Überprüft, ob die Admin-Zertifikate auf allen Nodes mit den Admin-Zertifikaten auf dem Admin-Server identisch sind.
- **NTP-Test:** Überprüft alle Nodes, um sicherzustellen, dass sie mit dem NTP-Server synchronisiert sind.
- **StaleCerts-Überprüfungstest:** Überprüft den Mongo und warnt, wenn ungenutzte veraltete Zertifikate vorhanden sind.
- **NodeCertIDCheck-Test:** Überprüft das Betrefffeld des Node-Zertifikats und stellt sicher, dass es mit der Knoten-ID des Hosts übereinstimmt.
- **Test zur Überprüfung des Ablaufs des Deploy\_Admin-Kennworts:** Überprüft, ob das `deploy_admin`-Kennwort auf Node 0 abgelaufen ist.
- **Prüfung der Datei-/Ordnerberechtigungen:** Mit diesem Test wird geprüft, ob die Dateien/Ordner über die geeigneten Berechtigungen verfügen.

## Netzwerk-Checkliste

Das Tool „Upgrade Precheck“ führt die Validierungsprüfungen für die folgende Liste von Prüfpunkten in der Netzwerk-Checkliste durch:

- **(Admin-Server) Prüfung auf geschlossene Ports auf Node 0:** Überprüft, ob die für NetWitness-Services erforderlichen Serviceports geöffnet sind und Node 0 überwachen.
- **(Komponentenhosts) Prüfung auf geschlossene Ports auf Node X:** Überprüft, ob die für NetWitness-Services erforderlichen Serviceports geöffnet sind und Node X überwachen.

## Zertifikat-Checkliste

Das Tool „Upgrade Precheck“ führt die Validierungsprüfungen für die folgende Liste von Prüfpunkten in der Zertifikat-Checkliste durch:

- **Gültigkeitsprüfung der Node-0-Servicezertifikate:** Überprüft die Gültigkeit der Servicezertifikate am Speicherort `/etc/pki/nw/service/` auf Node-0.
- **Gültigkeitsprüfung der Node-X-Servicezertifikate:** Überprüft die Gültigkeit der Servicezertifikate am Speicherort `/etc/pki/nw/service/` auf Node-X.
- **Gültigkeitsprüfung der Node-Zertifikate auf Node-0:** Überprüft die Gültigkeit der Node-Zertifikate am Speicherort `/etc/pki/nw/service` auf Node-0.
- **Gültigkeitsprüfung von Knotenzertifikaten auf Knoten-X:** Überprüft die Gültigkeit der Node-Zertifikate am Speicherort `/etc/pki/nw/service` auf Node-X.
- **Gültigkeitsprüfung der Zertifikate der Stammzertifizierungsstelle:** Überprüft die Gültigkeit der Zertifikate der Stammzertifizierungsstelle am Speicherort `/etc/pki/nw/ca`.

---

# Vorbereiten des Upgrades von NetWitness Platform

---

Führen Sie die folgenden Aufgaben durch, um das Upgrade auf NetWitness Platform 12.5 vorzubereiten.

## Aufgabe 1. (Wichtig) Vorbereiten des Upgrades des AlmaLinux-Betriebssystems

### Nicht unterstütztes Dateisystem

#### Unmounten und Entfernen von BTRFS

BTRFS ist ein Copy-on-Write-Dateisystem (CoW) für Linux, das darauf abzielt, erweiterte Dateisystemfunktionen zu implementieren und sich gleichzeitig auf Fehlertoleranz, Reparatur und einfache Administration zu konzentrieren. Das BTRFS-Dateisystem ist ab Red Hat Enterprise Linux 8 veraltet und das AlmaLinux-Betriebssystem unterstützt das BTRFS-Dateisystem nicht. NetWitness verwendet BTRFS nicht standardmäßig, aber in einigen Kategorien wie Netzwerkdecoder, Netzwerkhybrid usw. ist das BTRFS-Modul vorhanden und wird geladen. Wenn BTRFS als Dateisystem gemountet ist, führen Sie die folgenden Schritte aus, um die Bereitstellung der BTRFS-Partition manuell aufzuheben (wenn BTRFS nicht gemountet ist, überspringen Sie die folgenden Schritte):

- a. Verlagern Sie die Daten.
- b. Unmounten Sie die BTRFS-Partition mit dem folgenden Befehl.  
`umount<btrfs-Partitionsfad>`. Sie können die BTRFS-Partitionsinformationen mit den Befehlen `/etc/fstab` or `df -hT` abrufen.
- c. Entfernen Sie die BTRFS-Partition aus `/etc/fstab`.
- d. Überprüfen Sie mit `lsmod | grep btrfs`, ob das Kernelmodul noch geladen ist. Wenn das Kernelmodul noch geladen ist, verwenden Sie `modprobe -r btrfs`, um das btrfs-Kernelmodul zu entladen.
- e. Lösen Sie das Upgrade aus bzw. lösen Sie es erneut aus.

Weitere Informationen finden Sie im KB-Artikel [How to check Upgrade Fails and Data in Partition is Lost when BTRFS is Mounted or Loaded](#) (Englisch).

#### Unmounten von NFS

Auf den Nodes aktive Dateisysteme vom Typ NFS führen dazu, dass das Upgrade für diese Nodes fehlschlägt. Sie sollten diese Mount-Punkte manuell über die CLI eines jeden Node, auf dem sie sich befinden, unmounten. Gehen Sie wie folgt vor, um das NFS-Volume manuell zu unmounten:

- a. Stellen Sie eine SSH-Verbindung mit den Nodes her, auf denen der NFS-Mount-Punkte erkannt wurde.
- b. Führen Sie in jedem Node `mount | grep 'type nfs'` aus und rufen Sie den Verzeichnispfad des NFS-Mount-Punkts ab.

**Hinweis:** Bevor Sie NFS unmounten, müssen Sie die NetWitness-Services stoppen, die sich auf NFS stützen.

Beispiel: Wenn der Archiver- und Warehouse Connector-Service auf NFS ausgeführt wird, müssen Sie die folgenden Befehle ausführen, um die Services zu beenden, bevor Sie NFS unmounten.

```
systemctl stop nwarchiver
systemctl stop nwarehouseconnector
```

- c. Führen Sie `umount <dir_path>` vom Terminal aus, wobei `<dir_path>` der Verzeichnispfad aus Schritt b ist.
- d. Öffnen Sie die Datei `/etc/fstab` in einem Editor Ihrer Wahl und kommentieren Sie die Zeilen aus, die sich auf NFS-Mount-Punkte beziehen.
- e. Führen Sie das NetWitness-Upgrade durch.
- f. Nachdem das Upgrade erfolgreich abgeschlossen wurde, entfernen Sie die Kommentarzeichen vom entsprechenden Eintrag aus `/etc/fstab` und führen Sie `mount -a` vom Terminal aus, um die NFS-Mount-Punkte wieder hinzuzufügen.

## Überprüfung des AVX/VMX-CPU-Befehlssatzes

Das AVX/VMX-CPU-Flag muss für NetWitness Platform 12.5 aktiviert sein. Führen Sie den Befehl `salt '*' cmd.run "lscpu | grep -E 'avx|vmx'"` aus, um zu überprüfen, ob der AVX/VMX-CPU-Befehlssatz aktiviert ist. Weitere Informationen finden Sie im KB-Artikel [NetWitness MongoDB 5.0 uses AVX Instruction set for mongod.mongos and legacy mongo shell](#) (Englisch).

**Hinweis:** Für die NetWitness-Hardware-Appliance ist der AVX/VMX-CPU-Befehlssatz standardmäßig aktiviert.

## PF\_RING zur DPDK-Migrationsunterstützung

Die Decoder-Erfassungskonfiguration ist nicht gültig für Kunden, die PF\_RING Capture (CentOS) verwenden und ein direktes Upgrade auf 12.5 (AlmaLinux) durchführen. Zuerst müssen sie PF\_RING-Geräte zu DPDK migrieren und dann ein Upgrade durchführen.

Anweisungen zur Migration finden Sie unter [Migrieren von PF\\_RING-Geräten zu DPDK](#).

## Aufgabe 2. (Empfohlen, aber optional) Entfernen der veralteten Paket-Repositorys

Sie können Speicherplatz freigeben, indem Sie veraltete Repositorys von früheren Versionen entfernen.

### So entfernen Sie die veralteten Repositorys

1. Ermitteln Sie mithilfe des NetWitness Repo-Tools die Version des ältesten NetWitness Platform-Hosts in Ihrer Umgebung. Gehen Sie wie folgt vor:
  - Stellen Sie als `root`-Nutzer bzw. -Nutzerin eine SSH-Verbindung mit dem Admin-Server her.
  - Führen Sie den folgenden Befehl aus:

```
nw-repo-tool --list-obsolete
```

Nachdem Sie diesen Befehl ausgeführt haben, erhalten Sie eine Liste aller veralteten Repositorys.

2. Führen Sie den folgenden Befehl aus, um alle veralteten Repositorys zu entfernen.

```
nw-repo-tool --purge-obsolete
```

## Aufgabe 3. Vorbereiten der ESA-Bereitstellungen für die Migration zu 12.5

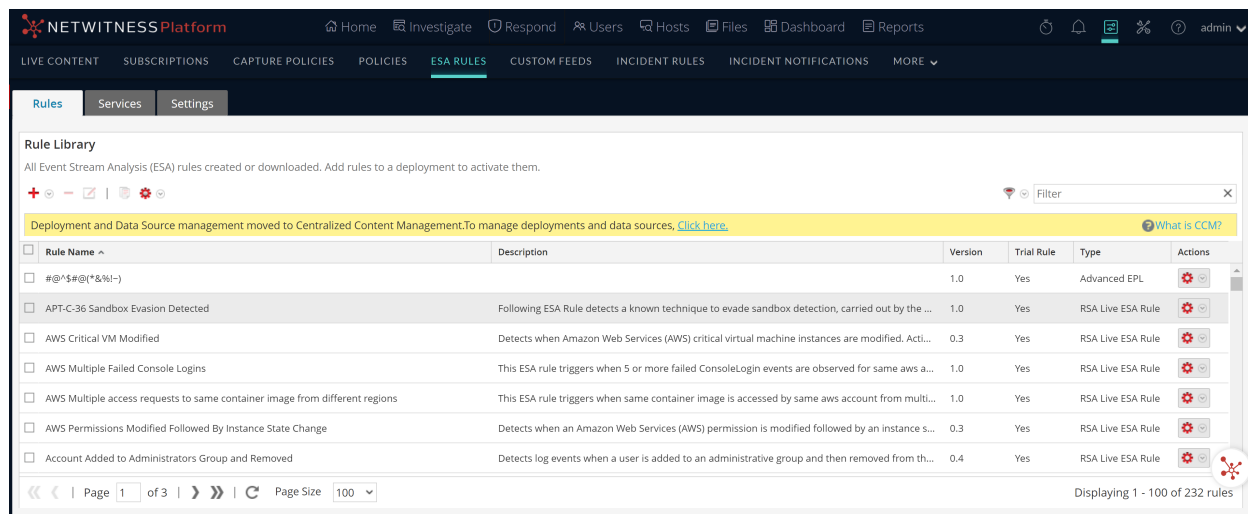
Vor dem Upgrade auf 12.5 empfiehlt NetWitness, dass alle ESA-Bereitstellungen einen fehlerfreien Zustand aufweisen. Sie müssen alle nicht verwendeten ESA-Bereitstellungen entfernen, da ESA-Bereitstellungen nach dem Upgrade auf 12.5 zu Richtlinien und Gruppen migriert werden. Jede Bereitstellung wird in eine Policy und eine Gruppe umgewandelt und steht erst nach dem Upgrade der Korrelationsserver auf die Version 12.5 zur Verwaltung zur Verfügung.

### Managen von ESA-Bereitstellungen und Datenquellen

Sie können die ESA-Bereitstellungen und Datenquellen nur über **Zentralisiertes Contentmanagement** verwalten. Wechseln Sie zur Seite **KONFIGURIEREN** > **Policies** > **Inhalt** > **Event Stream Analysis**, um die ESA-Bereitstellungen und Datenquellen zu verwalten. Sie können die ESA-Regeln nur auf der Seite **ESA-Regeln** verwalten. Weitere Informationen finden Sie in den folgenden Abbildungen.

NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED	
<input type="checkbox"/>	aero-datasourcef...	aero-datasourceesaSecondaryFilter-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 18:3...
<input type="checkbox"/>	aero-enrichment...	aero-enrichments-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 20:1...
<input type="checkbox"/>	aero-enrichments...	aero-enrichments-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 20:1...
<input checked="" type="checkbox"/>	aero-liverule-depl...	aero-Liverule-policy	esaprimary - ESA Correlation	loghybrid - Concentr...	Deployed	▲	07/19/2024 05:3...
<input type="checkbox"/>	aero-mixedConte...	aero-mixedContent-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 18:2...
<input type="checkbox"/>	aero-multiplegro...	aero-multipleservices-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Stopped	-	05/06/2024 19:1...
<input type="checkbox"/>	aero-newdeploy...	aero-otherrules-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	New	▲	05/06/2024 19:1...
<input type="checkbox"/>	aero-notify-ESAP...	aero-notification-policy	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	-	05/06/2024 18:1...
<input type="checkbox"/>	aero-notify-ESAS...	aero-notification-policy	esasecondary - ESA Correlat...	loghybrid - Concentrator	Deployed	-	05/06/2024 18:1...

Showing 17 out of 17 | 1 selected



Stellen Sie sicher, dass Sie den Upgrade-Prozess so planen, dass die Korrelationsserver unmittelbar nach dem Admin-Server-Upgrade aktualisiert werden. Auf die Bereitstellungen kann erst zugegriffen werden, wenn die entsprechenden Korrelationsserver aktualisiert worden sind. Die Korrelationsserver verarbeiten die Warnmeldungen und Ereignisse jedoch weiterhin. Sie müssen die ESA-Hosts sofort nach dem Upgrade des Admin-Servers aktualisieren.

Weitere Informationen zum **zentralisierten Contentmanagement** und zur Verwaltung der Bereitstellungen, finden Sie unter [Handbuch zum zentralisierten Contentmanagement für NetWitness](#).

**WICHTIG:** Wenn ESA-Regeln und -Anreicherungen importiert werden müssen, empfiehlt NetWitness, diese fehlenden Regeln und Anreicherungen vor dem Upgrade zu importieren.

Der Status der Bereitstellungen vor und nach dem Upgrade ist in der folgenden Tabelle dargestellt.

SINo	Bereitstellungsstatus vor dem Upgrade	Bereitstellungsstatus nach dem Upgrade		
		Erstellt Policy	Erstellt Gruppe	Die Policy wird veröffentlicht
1	Fehlerfreie Bereitstellung	Ja	Ja	Ja
2	Bereitstellung mit Fehlern	Ja	Ja	Ja
3	Bereitstellung nur mit Regeln	Ja	Nein	Nein
4	Bereitstellung ohne Regeln	Nein	Nein	Nein

Eine integrale Bereitstellung enthält keine Fehler und die erforderlichen Ressourcen wie ESA-Server, Datenquelle und ESA-Regeln werden hinzugefügt.

**Hinweis:** NetWitness empfiehlt, dass alle ESA-Bereitstellungen einen fehlerfreien Zustand aufweisen. Sie müssen alle unnötigen oder ungenutzten ESA-Bereitstellungen entfernen.

## Aufgabe 4. Entfernen von Drittanbieterpaketen

Alle auf Hosts aus dem NetWitness-Repository installierten Drittanbieterpakete werden im Rahmen der Betriebssystemmigration basierend auf den Upgrade-Abhängigkeiten entfernt.

## Aufgabe 5. Single Sign-On (SSO): Aktivieren der SAML-Antwortsignierung in Microsoft Azure ADFS

Die folgende Konfiguration gilt nur für Fälle, in denen die SAML-Antwort von Microsoft Azure ADFS nur verschlüsselt, doch nicht signiert wurde. Wenn Ihre Microsoft Azure ADFS-Instanz bereits zum Signieren und Verschlüsseln von SAML-Antworten konfiguriert ist, können Sie diese Konfiguration ignorieren und mit dem Upgrade-Prozess fortfahren.

Wenn Sie die SAML-Antwort nicht signieren, empfiehlt NetWitness, Microsoft Azure ADFS zum Verschlüsseln und Signieren der SAML-Antworten zu konfigurieren, bevor Sie NetWitness Platform auf Version 12.5 aktualisieren, um eine erfolgreiche SSO-Anmeldung (Single Sign-On) zu ermöglichen. Um die Antwortsignierung in Active Directory Federation Service (AD FS) zu aktivieren, führen Sie den folgenden Befehl in *Powershell* aus:

```
Set-AdfsRelyingPartyTrust -TargetName <<relying-party-name>> -
SamlResponseSignature MessageAndAssertion
```

**WICHTIG:** Vor dem Upgrade auf Version 12.5 von NetWitness Platform muss Microsoft Azure ADFS unbedingt zum Signieren von SAML-Antworten konfiguriert werden. Wenn diese Anforderungen nicht erfüllt werden, können Sie sich möglicherweise nicht über SSO anmelden.

## Aufgabe 6. (optional). Deaktivieren STIG-basierter FIPS-Kernel-Kontrollmaßnahmen

Wenn Sie STIG-basierte FIPS-Kernel-Kontrollmaßnahmen aktiviert haben, müssen Sie diese deaktivieren, bevor Sie den NetWitness Platform-Upgrade-Prozess starten, um Startfehler zu vermeiden. Führen Sie die folgenden Befehle aus, um STIG-basierte FIPS-Kernel-Kontrollmaßnahmen zu deaktivieren:

```
manage-stig-controls --disable-control-groups 3 --host-all
```

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Stellen Sie nach dem Upgrade von NetWitness Platform sicher, dass Sie STIG-basierte FIPS-Kernel-Kontrollmaßnahmen aktivieren.

**Hinweis:** STIG-basierte FIPS-Kernel-Kontrollmaßnahmen, die Änderungen der Kernel-Startoptionen erfordern, werden von NetWitness standardmäßig nicht aktiviert.

## Aufgabe 7. (optional). Überprüfen der Verbindung zum Live-Server

**Hinweis:** Diese optionale Aufgabe betrifft Sie nur dann, wenn Sie ein Live-Upgrade von NetWitness Platform durchführen.

Navigieren Sie zu `admin/system/live_services` und stellen Sie eine Testverbindung her, um zu überprüfen, ob Sie eine Verbindung zum Live-Server herstellen können, da dies für den Quellserver ab 12.x unerlässlich ist. Dies ist ein optionaler Schritt und gilt nur für Kunden, die eine Live-Konfiguration durchgeführt haben.

## Aufgabe 8. Synchronisieren der Uhrzeit auf den Komponentenhosts mit dem NW-Serverhost

Stellen Sie vor dem Upgrade von Hosts sicher, dass die Uhrzeit auf jedem Host mit der Uhrzeit auf dem NetWitness-Server synchronisiert worden ist.

Die NTP-Zeitsynchronisierungsmethode hängt von Ihrer NetWitness Platform-Version ab.

- **Bei NetWitness-Versionen niedriger als 12.4:** Verwenden Sie `ntpd` zur Zeitsynchronisation.
- **Bei NetWitness-Versionen 12.4 und höher:** Verwenden Sie `chrony` zur Zeitsynchronisation.

**Synchronisieren Sie die Uhrzeit, indem Sie einen der folgenden Aktionen ausführen:**

1. Konfigurieren Sie den NTP-Server.

Weitere Informationen finden Sie im [Systemkonfigurationsleitfaden](#) unter **Konfigurieren des NTP-Servers**.

2. Führen Sie die folgenden Schritte aus:

- a. Stellen Sie über SSH eine Verbindung mit dem Admin-Serverhost her.

- b. Führen Sie je nach Ihrer NetWitness-Version die folgenden Befehle aus:

- Wenn die NetWitness-Version niedriger als 12.4 ist. Führen Sie die folgenden Schritte aus:

**WICHTIG:** Um die richtige Zeitsynchronisation sicherzustellen, muss `ntpd` auf `node0` ausgeführt werden. Das Herunterfahren von `ntpd` auf `node0` führt dazu, dass die `ntpdate`-Befehle auf anderen Nodes fehlschlagen.

- `salt \* service.stop ntpd`
- `salt \* cmd.run 'ntpdate nw-node-zero'`
- `salt \* service.start ntpd`

- Wenn die NetWitness-Version 12.4 oder höher ist. Führen Sie die folgenden Schritte aus:

- `salt \* service.stop chronyd`
- `salt \* cmd.run "chronyc makestep"`
- `salt \* service.start chronyd`

## Durchführen der Upgrade-Aufgaben

---

**WICHTIG:** NetWitness empfiehlt dringend, vor dem Upgrade auf NetWitness Platform 12.5 die Prüfungen vor dem Upgrade auszuführen. Weitere Informationen zur Durchführung der Prüfungen vor dem Upgrade finden Sie unter [Ausführen der Upgrade-Vorabprüfungen](#).

Aktualisieren Sie die Systeme in Ihrer Umgebung in der folgenden Reihenfolge:

1. NW-Server-Hosts
2. Analysten-Benutzeroberflächen-Hosts
3. Primäre ESA-Hosts
4. Sekundäre ESA-Hosts
5. Eigenständige Broker-Hosts
6. Concentrator-Hosts
7. Archiver-Hosts
8. Packet Decoder-Host
9. Log Decoder-Hosts
10. Log Collector-/VCL-Hosts
11. Die übrigen Komponentenhosts

**WICHTIG:** NW Server-, Analyst-Benutzeroberflächen- sowie primäre und sekundäre ESA-Hosts müssen alle am gleichen Tag aktualisiert werden. Die restlichen Komponentenhosts können am selben Tag oder später aktualisiert werden. Stellen Sie sicher, dass Sie den Upgrade-Prozess so planen, dass die Korrelationsserver unmittelbar nach dem Admin-Server-Upgrade aktualisiert werden. Weitere Informationen finden Sie unter „**Aufgabe 3. Vorbereiten von ESA-Bereitstellungen für die Migration zu 12.5.0.0**“ im Thema [Vorbereiten des Upgrades von NetWitness Platform](#). Der gemischte Modus wird für ESA-Hosts in NetWitness Platform nicht unterstützt. Der NetWitness-Server, der primäre ESA-Host und der sekundäre ESA-Host müssen alle mit derselben NetWitness Platform-Version arbeiten.

Informationen zu allen Hosttypen in NetWitness finden Sie im [NetWitness – Leitfaden für die ersten Schritte mit Hosts und Services](#). Navigieren Sie zur Seite [NetWitness All Versions Documents](#) und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen.

**WICHTIG:** Nach dem Upgrade des primären NW-Servers (einschließlich des Respond Server-Service) wird der Respond Server-Service erst dann wieder automatisch aktiviert, nachdem auch der primäre ESA-Host auf dieselbe Version aktualisiert worden ist. Die Respond-Aufgaben nach dem Upgrade werden erst ausgeführt, nachdem der Respond Server-Server aktualisiert worden ist und sich im aktivierten Zustand befindet.

**Hinweis:** Bei Version 12.5.0.0 mit Legacy Windows Log Collector sollten Sie einige zusätzliche Aufgaben nach dem Upgrade durchführen. Weitere Informationen zu diesen zusätzlichen Aufgaben nach dem Upgrade finden Sie im Abschnitt „Legacy Windows Log Collection“ unter [Durchführen von Aufgaben nach dem Upgrade](#).

## Auswählen von Upgrade-Optionen

Abhängig von Ihrer Internetverbindung können Sie eine der folgenden Upgrade-Optionen wählen. Sie werden in der für NetWitness Platform empfohlenen Reihenfolge aufgelistet.

- [Option 1: Upgrade von NetWitness Platform mithilfe von Live-Services](#)
- [Option 2: Upgrade von NetWitness Platform offline](#)
- [Option 3: Upgrade von NetWitness Platform mit der CLI \(offline\)](#)
- [Option 4 \(optional\): Vorabbereitstellung des Upgrade-Repository durch Herunterladen von Paketen](#)

Die folgenden Regeln gelten, wenn Sie Hosts mit einer der vier Upgrade-Methoden aktualisieren:

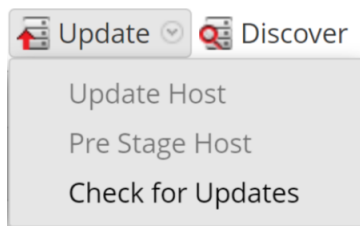
- Sie müssen den NW-Serverhost zuerst aktualisieren.
- Sie können nur eine Version anwenden, die mit der vorhandenen Hostversion kompatibel ist.
- Der NW-Server, der primäre ESA-Host, der sekundäre ESA-Host und der Analysten-UI-Host müssen alle mit derselben NetWitness Platform-Version arbeiten.

## Option 1: Upgrade von NetWitness Platform mithilfe von Live-Services


Sie können diese Methode verwenden, wenn der NW-Server mit Live-Services verbunden ist.


**Achtung:** Sie müssen Ihre Netzwerkrichtlinie überprüfen, bevor Sie das etwa 11,7 GB große Upgrade-Paket herunterladen. Wenn Sie eine Richtlinie eingerichtet haben, die den Download von Dateien über 10 GB hinaus nicht zulässt, schlägt der Download des Upgrade-Pakets fehl.

**Hinweis:** Sie können das Upgrade-Repository mit der Funktion **Vorab bereitgestellter Host** vorab bereitstellen. Weitere Informationen finden Sie in der folgenden Abbildung. Weitere Informationen finden Sie unter [Option 4 \(optional\): Vorabbereitstellung des Upgrade-Repository durch Herunterladen von Paketen](#).




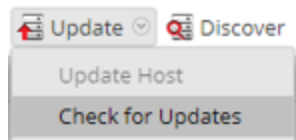
### Voraussetzungen

1. Die Option **Informationen über neue Aktualisierungen täglich automatisch herunterladen** ist aktiviert und wird in  (Admin) > System > Aktualisierungen angewendet.

- Es sind Aktualisierungen verfügbar. Navigieren Sie zu  (**Admin**) > **Hosts** > **Aktualisierung** > **Nach Updates suchen**, um nach Updates zu suchen. In der Ansicht „Host“ wird der Status **Aktualisierung verfügbar** angezeigt.
- 12.5.0.0 ist in der Spalte **Update-Version** verfügbar.

**So aktualisieren Sie von 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0, und 12.4.2.0 auf 12.5.0.0:**


- Navigieren Sie zu  (**Admin**) > **Hosts**.
- Wählen Sie den NW Server (nw-server)-Host aus.
- Überprüfen Sie die neuesten Aktualisierungen.



**Aktualisierung verfügbar** wird in der Spalte **Status** angezeigt, wenn für die ausgewählten Hosts im lokalen Update-Repository ein Versionsupdate vorhanden ist.

- Wählen Sie **12.5.0.0** aus der Spalte **Update-Version** aus.

**Hinweis:**

– Wenn Sie ein Dialogfeld mit den wichtigsten Funktionen des Upgrades sowie Informationen über die Aktualisierungen anzeigen möchten, klicken Sie auf das Informationssymbol (  ) rechts neben der Versionsnummer des Upgrades.

– Wenn Sie die gewünschte Version nicht finden können, wählen Sie **Aktualisieren** > **Nach Updates suchen** aus, um das Repository auf alle verfügbaren Aktualisierungen zu prüfen. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Es sind neue Hostaktualisierungen verfügbar“ angezeigt und die Spalte **Status** wird automatisch aktualisiert und zeigt **Aktualisierung verfügbar** an. Standardmäßig werden nur die unterstützten Aktualisierungen für den ausgewählten Host angezeigt.

- Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host ermitteln**.
- Klicken Sie auf **Update beginnen**.
- Klicken Sie auf **Host neu starten**.
- Wiederholen Sie Schritte 5 bis 7 für andere Hosts.

**Hinweis:** Sie können erst mehrere Hosts zum gleichzeitigen Upgrade auswählen, nachdem Sie den NW-Serverhost aktualisiert und neu gestartet haben. Alle ESA-, Endpoint- und Malware Analysis-Hosts müssen auf dieselbe Version wie die des NW-Serverhosts aktualisiert werden.

## Option 2: Upgrade von NetWitness Platform offline

Sie können NetWitness Platform manuell aktualisieren, indem Sie die folgenden Aufgaben ausführen.

## Aufgabe 1: Füllen des Staging-Ordners (/var/netwitness/common/update-stage/) mit Versionsaktualisierungsdateien. Gehen Sie wie folgt vor.


1. Laden Sie das Upgrade-Paket `netwitness-12.5.0.0.zip` von der NetWitness Community (<https://community.netwitness.com/>) > **Downloads** > **NetWitness Platform** > **Version 12.5.0.0** in ein lokales Verzeichnis herunter:
  - Wenn Sie ein Upgrade von 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0 und 12.4.2.0 durchführen, laden Sie `netwitness-12.5.0.0.zip` herunter.
2. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
3. Laden `netwitness-12.5.0.0.zip` nach `/var/netwitness/common/update-stage/` auf dem NW-Serverhost hoch.  
Beispiel:


```
mv /var/netwitness/tmp/netwitness-12.5.0.0.zip
/var/netwitness/common/update-stage/
```

**Hinweis:** NetWitness Platform entpackt die Datei automatisch.

## Aufgabe 2: Anwenden von Upgrades aus dem Staging-Bereich auf jeden Host. Gehen Sie wie folgt vor.

**Achtung:** Sie müssen den NW-Serverhost aktualisieren, bevor Sie ein Upgrade für andere Hosts, die kein NW-Serverhost sind, durchführen.

1. Melden Sie sich bei NetWitness an.
2. Navigieren Sie zu  (**Admin**) > **Hosts**.

**Hinweis:** Wenn Sie bereits die Seite  (**Admin**) > **Hosts** geöffnet haben und die Option **Nach Updates suchen** (**Update** > **Nach Updates suchen**) abgeblendet ist, aktualisieren Sie die Seite im Browser, um nach Updates zu suchen.

3. Suchen Sie nach Updates und warten Sie darauf, dass die Upgrade-Pakete kopiert und validiert werden und bereit für die Initialisierung sind.

„Update-Pakete können initialisiert werden“ wird angezeigt, wenn Folgendes zutrifft:

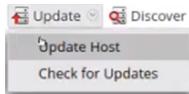
- NetWitness Platform kann auf die Upgrade-Pakete zugreifen.
- Die Pakets ist vollständig und fehlerfrei.

Anweisungen zur Fehlerbehebung finden Sie unter [Fehlerbehebung bei Versionsinstallationen und -aktualisierungen](#) (z. B. „**Fehler beim Bereitstellen der Version <Versionsnummer>**“ und „**Die folgenden Update-Pakete fehlen**“ werden im Dialogfeld **Update-Paket für RSA NetWitness Platform initiieren** angezeigt.)

4. Klicken Sie auf **Update initialisieren**.

Die Initialisierung der Pakete nimmt einige Zeit in Anspruch, weil die Dateien groß sind und entpackt werden müssen. Die Zeit variiert je nach Konfiguration des Hosts. Nach erfolgreicher Initialisierung wird in der Spalte **Status** die Meldung **Update verfügbar** angezeigt.

5. Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host aktualisieren**.



6. Klicken Sie im Dialogfeld **Update verfügbar** auf **Update beginnen**.  
Nachdem der Host aktualisiert wurde, werden Sie aufgefordert, den Host neu zu starten.
7. Klicken Sie auf **Host neu starten** in der Symbolleiste.

## Option 3: Upgrade von NetWitness Platform mit der CLI (offline)

Sie können diese Option verwenden, wenn der NW-Server nicht mit Live-Services verbunden ist.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgende Datei von der NetWitness Community (<https://community.netwitness.com/>) > **Produkte** > **NetWitness Platform** > **Downloads** in ein lokales Verzeichnis heruntergeladen haben:

- Wenn Sie ein Upgrade von 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0 und 12.4.2.0 durchführen, laden Sie Folgendes herunter:

```
netwitness-12.5.0.0.zip
```

- Wenn Sie ein externes Repository verwenden, können Sie das externe Repository mit den neuesten Upgrade-Inhalten aktualisieren. Weitere Informationen finden Sie unter [Anweisungen für das Upgrade des externen Repository über die CLI](#).

### So führen Sie ein Upgrade für NW-Serverhosts und Komponentenserver durch:

**Hinweis:** Wenn Sie die Befehle aus der PDF-Datei kopieren und in das Linux SSH-Terminal einfügen, funktionieren die Zeichen nicht. Sie können die Befehle jedoch von der HTML-Seite <https://community.netwitness.com/t5/netwitness-platform-online/upgrade-tasks-for-12-1-1/ta-p/695018#Option3> kopieren und in das Linux-SSH-Terminal einfügen.

1. Stellen Sie die Dateien der Version 12.5.0.0 bereit, um sie auf das Upgrade vorzubereiten. Betrachten wir folgende Szenarien:

- **Option 1 (manuell)** : Melden Sie sich bei NetWitness-Server an und erstellen Sie das folgende Verzeichnis:

```
/var/netwitness/tmp/upgrade/12.5.0.0/
```

Kopieren Sie dann die Paket-ZIP-Datei in das Verzeichnis `/var/netwitness/tmp/` des NW-Servers und extrahieren Sie die Paketdateien aus `/var/netwitness/tmp/` mit dem folgenden Befehl in das entsprechende Verzeichnis:

`unzip netwitness-12.5.0.0.zip -d /var/netwitness/tmp/upgrade/12.5.0.0`  
 Stellen Sie sicher, dass Sie die Update-ZIP-Datei nach dem Extrahieren aus dem Staging-Verzeichnis entfernen.

- **Option 2 (automatisiert)** : Melden Sie sich bei NetWitness-Server an und erstellen Sie das folgende Verzeichnis:

`/var/netwitness/tmp/upgrade/`

Kopieren Sie dann die ZIP-Dateien des NetWitness 12.5.0.0-Pakets in das Verzeichnis

`/var/netwitness/tmp/` auf dem NetWitness-Server.

Führen Sie anschließend den folgenden Befehl aus, um die ZIP-Dateien der Version 12.5.0.0 zu extrahieren, zu validieren und zu initialisieren:

```
[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
/tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.5.0.0
```

Erst nachdem die Meldung **(INFO) Download und Extraktion aller erforderlichen**

**NetWitness-ZIP-Dateien sind abgeschlossen** in der Konsole des Admin-Servers angezeigt wird, beginnt der Initialisierungsprozess.

**Hinweis:** Wenn die Meldung **(INFO) Herunterladen und Extrahieren aller erforderlichen NetWitness-ZIP-Dateien sind abgeschlossen** nicht angezeigt wird, führen Sie den vorherigen Befehl erneut aus.

**WICHTIG:** Wenn die Initialisierung nach dem Staging von 12.5.0.0 (mit Option 2) fehlschlägt, führen Sie den Befehl `upgrade-cli-client --init --version 12.5.0.0 --stage-dir /var/netwitness/tmp/upgrade` aus. Wenn die Initialisierung erfolgreich ist, ignorieren Sie [Schritt 2 „Initialisieren des Upgrades“](#) weiter unten und fahren Sie mit den weiteren Schritten 3–6 fort.

2. Initialisieren Sie das Upgrade mit dem folgenden Befehl:

```
upgrade-cli-client --init --version 12.5.0.0 --stage-dir
/var/netwitness/tmp/upgrade
```

3. Aktualisieren Sie den NW-Server-Host mit dem folgenden Befehl:

```
upgrade-cli-client --upgrade --version 12.5.0.0 --host-key <ID / display
name / (hostname/ IP address)>
```

**Hinweis:** Sobald das Upgrade ausgelöst wird, wird der NW-Server etwa 10 Minuten nach Beginn des Upgrade-Vorgangs automatisch neu gestartet. Es startet den neuen Kernel (4.18 für Alma Linux 8.10).

**Achtung:** Nutzern und Nutzerinnen wird empfohlen, zu warten, bis die Benutzeroberfläche betriebsbereit ist. Dies kann bis zu einer Stunde dauern. Nach 20 bis 30 Minuten der Migration können Sie per SSH prüfen, ob das Betriebssystem migriert wurde. Sobald die Betriebssystemmigration abgeschlossen ist, dauert es mindestens 30 Minuten, bis die Benutzeroberfläche angezeigt wird, während das NW-Upgrade im Hintergrund ausgeführt wird.

Der obige Upgrade-Prozess kann über eine virtuelle Konsole für VMs oder eine Remote-Konsole für Server mit iDRACs verfolgt werden.

Weitere Informationen zum Herstellen einer Verbindung mit der virtuellen Konsole finden Sie unter <https://www.dell.com/support/kbdoc/en-in/000179797/dell-poweredge-idrac-virtual-console>.

Sobald das Betriebssystem migriert ist und eine SSH-Verbindung zum Admin-Node herstellen kann, führen Sie den folgenden Befehl auf dem Host aus, um die erfolgreiche Betriebssystemmigration zu bestätigen:

- `cat /etc/redhat-release`
- AlmaLinux release 8.10 (Cerulean Leopard)

**Achtung:** Installieren Sie nach der Betriebssystemmigration alle zuvor installierten RPMs von Drittanbietern erneut.

4. Sobald der Orchestrierungsserver hochgefahren ist, löst er automatisch das NW-Upgrade durch „chef“ auf die gewünschte NW-Version aus. Um den Fortschritt dieses Vorgangs zu überprüfen, stellen Sie eine SSH-Verbindung zum Admin-Server her und führen Sie den folgenden Befehl aus:
  - `orchestration-cli-client --check-admin-upgrade-status`

**Hinweis:** Führen Sie den obigen Befehl nur für den NW-Admin-Server aus.

5. Wenn das NW Server-Host-Upgrade erfolgreich war, starten Sie den Host über die NetWitness Platform-Benutzeroberfläche in der Ansicht „Hosts“ neu.
6. (Bedingt) Wenn ein aktiver Standby-Server bereitgestellt wird, wiederholen Sie die Schritte 1 bis 5 auf dem aktiven Standby-Server-Host.
7. Wiederholen Sie die Schritte 3 und 5 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse in die des Komponentenhosts, der aktualisiert wird.

**Hinweis:** Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NW-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

## Anweisungen für das Upgrade des externen Repository über die CLI

Informationen zum Einrichten eines externen Repository finden Sie im **Anhang A. Einrichten eines externen Repository** im *12.5.0.0 Upgrade-Handbuch für NetWitness Platform*. Bei den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits ein externes Repository eingerichtet haben. Navigieren Sie zur Seite [NetWitness All Versions Documents](#) und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen.

1. Stellen Sie die Dateien der Version 12.5.0.0 bereit, um sie auf das Upgrade vorzubereiten. Betrachten wir folgende Szenarien:

- **Wenn Sie ein Upgrade von 12.2.0.0, 12.2.0.1, 12.3.0.0, 12.3.1.0, 12.4.0.0, 12.4.1.0 und 12.4.2.0 durchführen,** müssen Sie nur 12.5.0.0 bereitstellen.
  - **Option 1 (manuell)** : Melden Sie sich bei NetWitness-Server an und erstellen Sie das folgende Verzeichnis:

```
/var/netwitness/tmp/upgrade/12.5.0.0/
```

Kopieren Sie dann die Paket-ZIP-Datei in das Verzeichnis `/var/netwitness/tmp/` des NW-Servers und extrahieren Sie die Paketdateien aus `/var/netwitness/tmp/` mit dem folgenden Befehl in das entsprechende Verzeichnis:

```
unzip netwitness-12.5.0.0.zip -d /var/netwitness/tmp/upgrade/12.5.0.0
```

Stellen Sie sicher, dass Sie die Update-ZIP-Datei nach dem Extrahieren aus dem Staging-Verzeichnis entfernen.

- **Option 2 (automatisiert)** : Melden Sie sich bei NetWitness-Server an und erstellen Sie das folgende Verzeichnis:  
`/var/netwitness/tmp/upgrade/`  
 Kopieren Sie dann die ZIP-Dateien des NetWitness 12.5.0.0-Pakets in das Verzeichnis  
`/var/netwitness/tmp/` auf dem NetWitness-Server.  
 Führen Sie anschließend den folgenden Befehl aus, um die ZIP-Dateien der Version 12.5.0.0 zu extrahieren, zu validieren und zu initialisieren:  
`[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.5.0.0`  
 Erst nachdem die Meldung **(INFO) Download und Extraktion aller erforderlichen NetWitness-ZIP-Dateien sind abgeschlossen** in der Konsole des Admin-Servers angezeigt wird, beginnt der Initialisierungsprozess.

**Hinweis:** Wenn die Meldung **(INFO) Herunterladen und Extrahieren aller erforderlichen NetWitness-ZIP-Dateien sind abgeschlossen** nicht angezeigt wird, führen Sie den vorherigen Befehl erneut aus.

**WICHTIG:** Wenn die Initialisierung nach dem Staging von 12.5.0.0 (mit Option 2) fehlschlägt, führen Sie den Befehl `upgrade-cli-client --init --version 12.5.0.0 --stage-dir /var/netwitness/tmp/upgrade` aus. Wenn die Initialisierung erfolgreich ist, ignorieren Sie [Schritt 2 „Initialisieren des Upgrades“](#) weiter unten und fahren Sie mit den weiteren Schritten 3–6 fort.

2. Initialisieren Sie das Upgrade mit dem folgenden Befehl:  
`upgrade-cli-client --init --version 12.5.0.0 --stage-dir /var/netwitness/tmp/upgrade`
3. Aktualisieren Sie den NW-Server-Host mit dem folgenden Befehl:  
`upgrade-cli-client --upgrade --version 12.5.0.0 --host-key <ID / display name / (hostname/ IP address)>`

**Hinweis:** Sobald das Upgrade ausgelöst wird, wird der NW-Server etwa 10 Minuten nach Beginn des Upgrade-Vorgangs automatisch neu gestartet. Es startet den neuen Kernel (4.18 für Alma Linux 8.10).

**Achtung:** Nutzern und Nutzerinnen wird empfohlen, zu warten, bis die Benutzeroberfläche betriebsbereit ist. Dies kann bis zu einer Stunde dauern. Nach 20 bis 30 Minuten der Migration können Sie per SSH prüfen, ob das Betriebssystem migriert wurde. Sobald die Betriebssystemmigration abgeschlossen ist, dauert es mindestens 30 Minuten, bis die Benutzeroberfläche angezeigt wird, während das NW-Upgrade im Hintergrund ausgeführt wird.

Der obige Upgrade-Prozess kann über eine virtuelle Konsole für VMs oder eine Remote-Konsole für Server mit iDRACs verfolgt werden.

Weitere Informationen zum Herstellen einer Verbindung mit der virtuellen Konsole finden Sie unter <https://www.dell.com/support/kbdoc/en-in/000179797/dell-powerededge-idrac-virtual-console>.

Sobald das Betriebssystem migriert ist und eine SSH-Verbindung zum Admin-Node herstellen kann, führen Sie den folgenden Befehl auf dem Host aus, um die erfolgreiche Betriebssystemmigration zu bestätigen:

- `cat /etc/redhat-release`
- AlmaLinux release 8.10 (Cerulean Leopard)

**Achtung:** Installieren Sie nach der Betriebssystemmigration alle zuvor installierten RPMs von Drittanbietern erneut.

4. Sobald der Orchestrierungsserver hochgefahren ist, löst er automatisch das NW-Upgrade durch „chef“ auf die gewünschte NW-Version aus. Um den Fortschritt dieses Vorgangs zu überprüfen, stellen Sie eine SSH-Verbindung zum Admin-Server her und führen Sie den folgenden Befehl aus:
  - `orchestration-cli-client --check-admin-upgrade-status`

**Hinweis:** Führen Sie den obigen Befehl nur für den NW-Admin-Server aus.


5. Wenn das NW Server-Host-Upgrade erfolgreich war, starten Sie den Host über die NetWitness Platform-Benutzeroberfläche in der Ansicht „Hosts“ neu.
6. (Bedingt) Wenn ein aktiver Standby-Server bereitgestellt wird, wiederholen Sie die Schritte 1 bis 5 auf dem aktiven Standby-Server-Host.
7. Wiederholen Sie die Schritte 3 und 5 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse in die des Komponentenhosts, der aktualisiert wird.

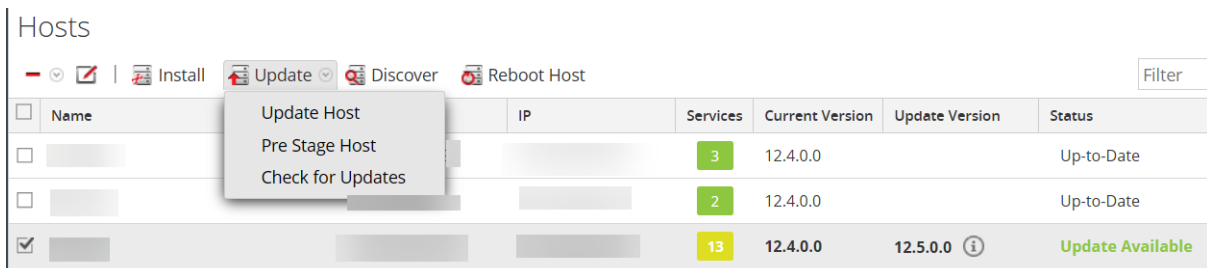
**Hinweis:** Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NW-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

## Option 4 (optional): Vorabbereitstellung des Upgrade-Repository durch Herunterladen von Paketen

Sie können das Upgrade-Repository vorab bereitstellen, indem Sie die erforderlichen Pakete (.zip) herunterladen, ohne dass dies Auswirkungen auf das System hat. Dadurch wird die Upgrade-Ausfallzeit minimiert und sichergestellt, dass das Upgrade innerhalb des geplanten Zeitraums abgeschlossen wird.

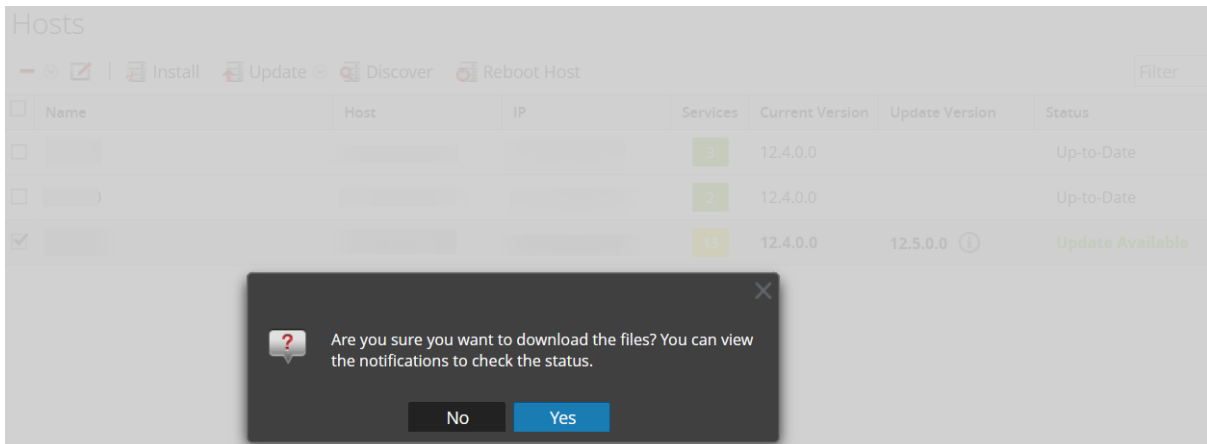
**So stellen Sie das Upgrade-Repository vorab bereit und aktualisieren die Hosts:**

1. Navigieren Sie zu  (Admin) > Hosts.
2. Klicken Sie in der Symbolleiste auf **Update** > **Nach Updates suchen**.  
Alle möglichen Update-Versionen werden in der Drop-down-Liste „Versionen“ angezeigt.
3. Klicken Sie auf **Update** > **Vorab bereitgestellter Host** und wählen Sie die Version in der Spalte „Update-Version“ aus.



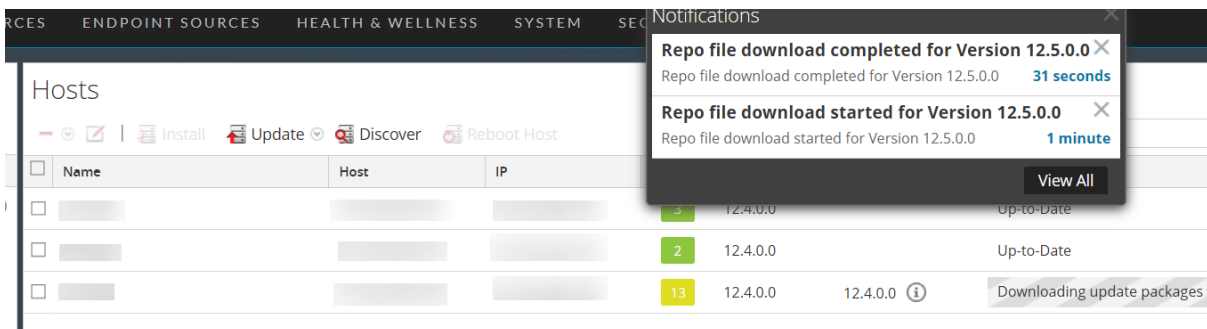
Name	IP	Services	Current Version	Update Version	Status
		3	12.4.0.0		Up-to-Date
		2	12.4.0.0		Up-to-Date
		13	12.4.0.0	12.5.0.0 ⓘ	Update Available

Es wird eine Bestätigungsmeldung zum Herunterladen der Dateien angezeigt.



4. Klicken Sie auf **Ja**, um die Upgrade-Pakete in das Repository herunterzuladen.
5. Überprüfen Sie den Status des Downloads in der Benachrichtigungsleiste wie unten dargestellt.

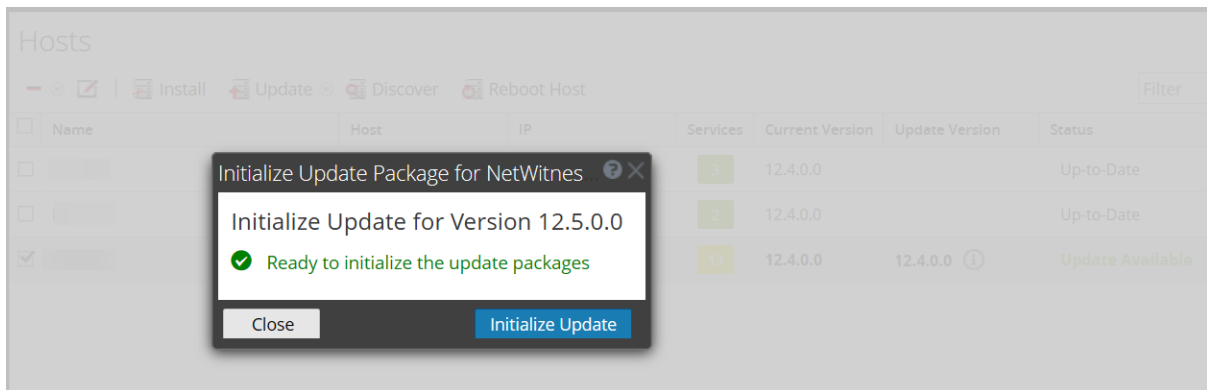
Die Optionen **Vorab bereitgestellter Host** und **Host aktualisieren** werden deaktiviert, bis die Vorabbereitstellung abgeschlossen ist.



**Hinweis:** Die aktuelle Version und die Update-Version in der Benutzeroberfläche sind während der Vorabbereitstellung identisch, da es sich nicht um das eigentliche Update handelt. Dies liegt daran, dass nur die Repository-Dateien heruntergeladen werden und kein tatsächliches Upgrade durchgeführt wird. Die Version ändert sich erst nach dem Upgrade.

6. Wenn der Download erfolgreich ist, **suchen Sie erneut nach Updates**, um die Initialisierung zu starten.
7. Klicken Sie auf **Update initialisieren**.

Die Initialisierung des Pakets dauert einige Zeit, da die Dateien groß sind und entpackt werden müssen.



**WICHTIG:** Die Schritte 1 bis 4 zur Vorbereitung des Repository für die Vorabbereitstellung können jederzeit ausgeführt werden. Bei den Schritten 5 bis 8 beginnt jedoch der Upgrade-Prozess. Während dieser Zeit dürfen Sie den Host NICHT neu starten oder den Jetty-Server nicht neu starten, da dies die ZIP-Dateien beschädigen würde.

8. Überprüfen Sie den Status der Initialisierung in der Benachrichtigungsleiste.
9. Nachdem die Initialisierung erfolgreich abgeschlossen wurde, klicken Sie auf **Aktualisieren > Host aktualisieren**.  
Nachdem der Host aktualisiert worden ist, werden Sie aufgefordert, den Host neu zu starten.
10. Richten Sie den Host ein und starten Sie den Host neu.

---

## Durchführen von Aufgaben nach dem Upgrade

---

In diesem Thema sind die Aufgaben aufgeführt, die Sie nach dem Upgrade von NetWitness Platform ausführen müssen. Führen Sie die Aufgaben aus, die die Hosts in Ihrer Umgebung betreffen.

- [Allgemein](#)
- [Event Stream Analysis \(ESA\)](#)
- [Reagieren](#)
- [Analyse des Nutzer- und Entitätsverhaltens \(UEBA\)](#)
- [Legacy-Windows-Log Collector](#)
- [Warehouse Connector](#)
- [Festlegen des Wiederherstellungskennworts für die Lockbox](#)

### Allgemein

Sie müssen Jetty konfigurieren, die Inhalte der Kernservices wiederherstellen und nach dem Upgrade von NetWitness Platform auch die Netzwerkerfassung, Protokollerfassung und Aggregation starten.

### Konfigurieren von Jetty

Erläuterungen zur Jetty-Konfiguration und zugehörige Informationen finden Sie im [Systemwartungshandbuch](#) unter dem Punkt **Manage Custom Host Entries** im Abschnitt **Manage Custom Jetty Configuration**.


### Sicherstellen, dass die Services neu gestartet wurden und Daten erfassen und aggregieren


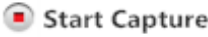
Stellen Sie sicher, dass die Services neu gestartet wurden und Daten erfassen (dies hängt davon ab, ob Sie den automatischen Start aktiviert haben oder nicht).

Starten Sie bei Bedarf die Datenerfassung und -aggregation für die folgenden Services neu:




- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

#### So starten Sie die Netzwerkerfassung:

1. Navigieren Sie im Menü von NetWitness Platform zu  (Admin) > **Services**. Die Ansicht **Services** wird angezeigt.

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

#### So starten Sie die Protokollerfassung:

1. Navigieren Sie im Menü von NetWitness Platform zu  (Admin) > **Services**. Die Ansicht **Services** wird angezeigt.
2. Wählen Sie die einzelnen **Log Decoder**-Services aus.
3. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > System** aus.
4. Klicken Sie in der Symbolleiste auf  .

#### So starten Sie die Aggregation:

1. Gehen Sie im Menü von NetWitness Platform zu  (Admin) > **Services**. Die Ansicht **Services** wird angezeigt.
2. Für jeden **Concentrator**-, **Broker** und **Archiver**-Service gehen Sie wie folgt vor:
  - a. Wählen Sie den Service aus.
  - b. Wählen Sie unter  (Aktionen) die Optionen **Ansicht > Konfiguration** aus.
  - c. Klicken Sie in der Symbolleiste auf  .
3. Für Event Stream Analysis (ESA):

**Hinweis:** Der gemischte Modus wird bei ESA-Hosts nicht unterstützt. Der NetWitness-Server, der primäre ESA-Host und der sekundäre ESA-Host müssen alle mit derselben NetWitness Plattform-Version arbeiten.

Für ESA sind keine erforderlichen Aufgaben nach dem Upgrade auszuführen. Informationen zum ESA-Troubleshooting finden Sie unter [ESA-Troubleshooting-Informationen](#).

Wenn Sie Unterstützung für Endpoint-, UEBA- und Live-Inhaltsregeln hinzufügen möchten, müssen Sie die Parameter-Metaschlüssel `multi-valued` und `single-valued` im ESA-Korrelationsservice aktualisieren, um alle erforderlichen Metaschlüssel einzuschließen. Es ist nicht notwendig, diese Anpassungen während des Upgrades vorzunehmen. Sie können sie später zu einem geeigneten Zeitpunkt vornehmen. Ausführliche Informationen und Anweisungen finden Sie unter **Aktualisieren der ESA-Regeln für die erforderlichen mehrwertigen und einwertigen Metaschlüssel** im [ESA-Konfigurationshandbuch](#).

## Wiederherstellen der Inhalte der Core-Services


Sobald Sie ein Upgrade auf 12.5 durchführen, werden die Inhalte der Core-Services wie Konfigurationsdateien (.cfg), Feeds, Parser und Protokollgeräte in den Speicherort **.tar** der jeweiligen Komponenten wie Decoder, Log Hybrid, Network Hybrid und Log Decoder kopiert.



In der folgenden Tabelle sind die Pfade der Inhalte der Core-Services und der Speicherort der **.tar**-Datei der jeweiligen Komponenten aufgeführt, in die die Core-Services-Inhalte kopiert werden.

Pfade der Core-Services-Inhalte	Komponenten	.tar-Speicherort der Komponenten
/etc/netwitness/ng/feeds (Feeds)	Decoder	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/parsers (Parser)	Log Hybrid	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar
/etc/netwitness/ng/envision/etc/devices (Protokollgeräte)	Network Hybrid	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/NwDecoder.cfg (Konfigurationsdateien (.cfg))	Log Decoder	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar

Diese CCM-Option ist standardmäßig deaktiviert. Wenn Sie CCM nach dem Upgrade auf 12.5 aktivieren und feststellen, dass die Inhalte der Core-Services verloren gehen, können Sie die gesicherten TAR-Dateien verwenden, um die verlorenen Daten wiederherzustellen. Weitere Informationen finden Sie unter <https://community.netwitness.com/t5/netwitness-knowledge-base/automatic-backup-of-core-service-content-after-upgrading-core/ta-p/694527>.

## Event Stream Analysis (ESA)

Nach dem Upgrade auf die Version 12.5 werden alle ESA-Bereitstellungen zur Seite  (**KONFIGURIEREN**) > **Policies** migriert. Jede Bereitstellung wird in eine Policy und eine Gruppe umgewandelt und steht erst nach dem Upgrade der Korrelationsserver auf die Version 12.5 zur Verwaltung zur Verfügung. Stellen Sie sicher, dass Sie den Upgrade-Prozess so planen, dass die Korrelationsserver unmittelbar nach dem Admin-Server-Upgrade aktualisiert werden. Auf die Bereitstellungen kann erst zugegriffen werden, wenn die entsprechenden Korrelationsserver aktualisiert worden sind. Die Korrelationsserver verarbeiten die Warnmeldungen und Ereignisse jedoch weiterhin. Überprüfen Sie, ob sich alle ESA-Bereitstellungen in einem fehlerfreien Zustand befinden. Weitere Informationen finden Sie im Thema **Anzeigen einer Bereitstellung** im *Handbuch zum Management von Live-Services*.

**Hinweis:** Analysten und Analystinnen müssen über entsprechende Berechtigungen verfügen, um die ESA-Regeln auf den Seiten  (**KONFIGURIEREN**) > **ESA-Regeln** und  (**KONFIGURIEREN**) > **Policies** anzeigen zu können. Weitere Informationen über die Liste von Berechtigungen finden Sie im Abschnitt **Quellserver** im Thema **Rollenberechtigungen** im *Handbuch Systemsicherheit und Benutzerverwaltung*.

Der Status der Bereitstellungen vor und nach dem Upgrade ist in der folgenden Tabelle dargestellt.

SINo	Bereitstellungsstatus vor dem Upgrade	Bereitstellungsstatus nach dem Upgrade		
		Erstellt Policy	Erstellt Gruppe	Die Policy wird veröffentlicht
1	Fehlerfreie Bereitstellung	Ja	Ja	Ja
2	Bereitstellung mit Fehlern	Ja	Ja	Ja
3	Bereitstellung nur mit Regeln	Ja	Nein	Nein
4	Bereitstellung ohne Regeln	Nein	Nein	Nein

(Optional) Mit der Schaltfläche **Policy zusammenführen** können Sie eine Richtlinie mit ESA-Inhalt mit einer Policy ohne ESA-Inhalt zusammenführen. Weitere Informationen finden Sie im Thema **Zusammenführen einer Policy with ESA-Inhalt** im *Handbuch zum Management von Live-Services*.


## Managen von ESA-Bereitstellungen und Datenquellen

Sie können die ESA-Bereitstellungen und Datenquellen nur über **Zentralisiertes Contentmanagement** verwalten. Wechseln Sie zur Seite **(KONFIGURIEREN) > Policies > Inhalt > Event Stream Analysis**, um die ESA-Bereitstellungen und Datenquellen zu verwalten. Sie können die ESA-Regeln nur auf der Seite **ESA-Regeln** verwalten. Weitere Informationen finden Sie in den folgenden Abbildungen.

Sie müssen die ESA-Hosts sofort nach dem Upgrade des Admin-Servers aktualisieren.

**Hinweis:** Um ESA-Warmmeldungen mit Mitre-Taktiken und -Techniken zu generieren, muss die mit der ESA-Regel verknüpfte ESA-Bereitstellung nach dem Upgrade auf die Version 12.5 zwingend erneut bereitgestellt werden.

## Benutzerdefinierte Skripte für Benachrichtigungen migrieren

- Da es zahlreiche Änderungen hinsichtlich der Dateiberechtigungen und Eigentumsattribute benutzerdefinierter Skriptdateien der Funktion **Skriptbenachrichtigungen** (  **(Admin)** > **System** > **Globale Benachrichtigungen** > **Skript**) gibt, empfiehlt NetWitness, vor dem Upgrade des Systems auf 12.5 eine Sicherungskopie der benutzerdefinierten Skripte zu erstellen.
- Sobald das Upgrade abgeschlossen ist, muss jedes Skript auf die erforderlichen syntaktischen/semantischen Änderungen überprüft werden.
- Selbst wenn das benutzerdefinierte Skript in NetWitness-Versionen vor 12.5 auf Dateiressourcen im Ordner `/tmp` oder `/var/tmp` zugreift, kann nicht weiter auf sie zugegriffen werden, da die Eigentümerschaft, mit der das benutzerdefinierte Skript ausgeführt wird, geändert wurde. In diesem Fall wird empfohlen, das benutzerdefinierte Skript so zu optimieren oder zu ändern, dass im Verzeichnis `/tmp` oder `/var/tmp` eine neue Datei erstellt bzw. gelesen wird.

Weitere Informationen zum **zentralisierten Contentmanagement** und zur Verwaltung der Bereitstellungen, finden Sie unter [Handbuch zum zentralisierten Contentmanagement für NetWitness](#).

## Reagieren

Der primäre ESA-Server muss auf Version 12.5 aktualisiert werden, bevor Sie die folgende Aufgabe abschließen können.

**Hinweis:** Nach dem Upgrade des primären NW-Servers (einschließlich des Respond Server-Service) wird der Respond Server-Service erst dann wieder automatisch aktiviert, nachdem auch der primäre ESA-Host auf Version 12.5 aktualisiert worden ist. Die Respond-Aufgaben nach dem Upgrade werden erst ausgeführt, nachdem der Respond Server-Server aktualisiert worden ist und sich im aktivierten Zustand befindet.

## (Bedingt) Wiederherstellen aller benutzerdefinierten Schlüssel des Respond-Services in „custom\_normalize\_alerts.js“ und Unterstützen neuer Datenquellen

**Hinweis:** Wenn Sie die Datei `custom_normalize_alerts.js` nicht manuell angepasst haben, können Sie diese Aufgabe überspringen. Wir versuchen, die benutzerdefinierten Schlüssel automatisch zu migrieren. Sollten jedoch Fehler auftreten, verwenden Sie diesen Schritt, um die Integrität der benutzerdefinierten Daten zu überprüfen.

Wenn Sie der Datei `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` benutzerdefinierte Schlüssel zur Verwendung bei der benutzerdefinierten Normalisierung hinzugefügt haben, ändern Sie die Datei `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` und fügen Sie die benutzerdefinierten normalisierten Schlüssel aus der automatischen Sicherungsdatei hinzu. Die Sicherungsdatei befindet sich in `/var/netwitness/respond-server/scripts` und hat das folgende Format:

```
custom_normalize_alerts.js.bak-<time of the backup>
```

Falls die automatische Aktualisierung des Skripts fehlschlägt, fügen Sie Unterstützung für NetWitness Core und NetWitness Insight hinzu, indem Sie die Datei `custom_normalize_alerts.js` manuell aktualisieren, um diese neuen Quellen in Respond zu unterstützen.

## Analyse des Nutzer- und Entitätsverhaltens (UEBA)

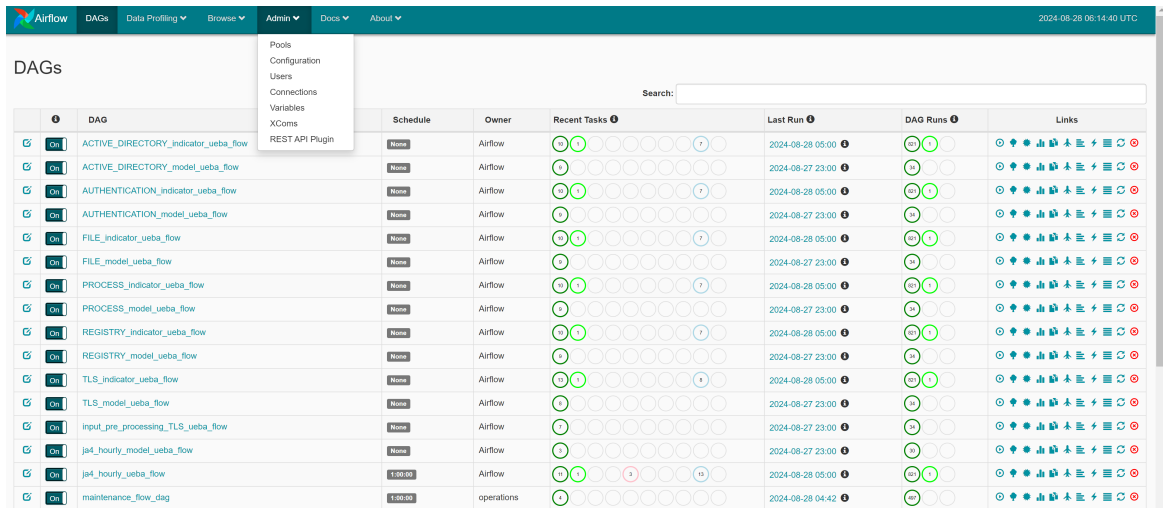
Führen Sie nach dem Upgrade von UEBA auf 12.5 die folgenden Aufgaben aus.

**WICHTIG:** Wenn Sie vor dem Upgrade auf Probleme mit fehlgeschlagenen Aufgaben gestoßen sind und diese behoben haben, müssen Sie nach dem Upgrade die Datei `authentication.json` ersetzen, bevor Sie die Aufgaben nach dem Upgrade ausführen. Die Probleme mit fehlgeschlagenen Aufgaben in Airflow und ihre Lösungen werden im Thema „Troubleshooting“ des *UEBA-Konfigurationshandbuchs* beschrieben.

**WICHTIG:** In Version 12.5 hat NetWitness den Verschlüsselungsmechanismus für UEBA aktualisiert. Nutzer, die von früheren Versionen auf 12.5.0.0 aktualisieren, müssen das Skript `update_encrypted_password_12_5.py` ausführen, um die Verschlüsselung auf dem UEBA-Server zu aktualisieren. Um dieses Update anzuwenden, laden Sie das Skriptpaket herunter und speichern Sie es im Stammverzeichnis des UEBA-Servers. Das Skriptpaket kann von der folgenden URL <https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-12-5-ueba-encryption-script-download/ta-p/715887> oder von der Seite „NetWitness Community“ (<https://community.netwitness.com/>) **Downloads > NetWitness Platform > Version 12.5** heruntergeladen werden.



- **Physische Appliance:** Aktualisieren Sie den `spring_boot_jar_pool`-Slot-Wert auf 18.
- **Virtuelle Appliance:** Aktualisieren Sie den `spring_boot_jar_pool`-Slot-Wert auf 22.  
Um die **Spring Boot Jar Pools**-Slots zu aktualisieren, gehen Sie zur Airflow-Hauptseite und tippen Sie in der oberen Leiste auf die Registerkarte **Admin** und dann auf **Pools**.
  - a. Um auf die Airflow-Benutzeroberfläche zuzugreifen, navigieren Sie zu `https://<UEBA_host>/admin` und geben Sie die Anmeldeinformationen ein.  
User: admin  
Kennwort: Das Kennwort des Bereitstellungsadministrators der Umgebung.
  - b. Klicken Sie auf das Bleistiftsymbol neben Pools, um die Slot-Werte zu aktualisieren.



5. Bearbeiten Sie `spring_boot_jar_pool` und ändern Sie die Anzahl der Slots in 22.



## Legacy-Windows-Log Collector

### Aktualisieren Sie Legacy-Windows-Log-Collector-Zertifikate mit aktualisierten SA-Zertifikaten

#### Schritte nach dem Upgrade:



1. Führen Sie den folgenden Befehl im Admin-Server aus:
  - a. `wlc-cli-client --host-display-name hostDisplayName --service-display-name serviceDisplayName --host WLChostIPAddress --port 50101 --use-ssl false`

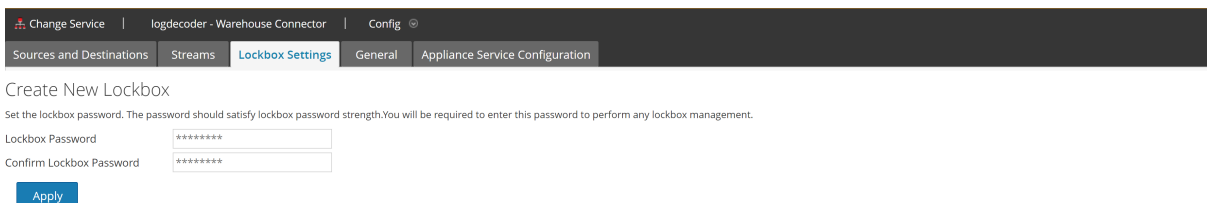
Geben Sie die folgenden Informationen ein:

- i. **Legacy-Windows-Log-Collector-REST-Benutzername und Legacy-Windows-Log-Collector-REST-Kennwort:** Geben Sie die Anmeldedaten für das Legacy-Windows-Log-Collector-Administratorkonto ein.
  - ii. **Benutzername und Kennwort für den Sicherheitsserver:** Geben Sie die Anmeldedaten für das NetWitness-Administratorkonto ein.
2. Starten Sie das System neu.

## Warehouse Connector

Der Warehouse Connector verwendet eine Lockbox, um Anmeldeinformationen für Datenintegrationsquellen und -ziele sicher zu speichern. Nutzer, die von früheren Versionen auf die Version 12.5 aktualisieren, können die konfigurierten Streams jedoch nicht starten, ohne ihre vorhandenen Anmeldeinformationen in die neue Lockbox zu migrieren. Daher müssen Nutzer manuell einen neuen Lockbox-Schlüssel erstellen und dann, sofern zutreffend, das Kennwort für ihre im Warehouse Connector konfigurierten Quellen und Ziele aktualisieren, indem sie die folgenden Schritte ausführen:

1. Melden Sie sich bei der NetWitness-Plattform an.
2. Navigieren Sie zu  (**Admin**) > **Dienste**.
3. Wählen Sie in der Ansicht **Dienste** den hinzugefügten Dienst „Warehouse Connector“ und anschließend  > **Anzeigen** > **Konfiguration** aus.
4. Klicken Sie in der Servicekonfigurationsansicht von Warehouse Connector auf die Registerkarte **Lockbox-Einstellungen** und erstellen Sie einen neuen Lockbox-Schlüssel.



5. Autorisieren Sie das Nutzerkonto in den Quellkonfigurationen mithilfe von **Explore** oder **REST API** erneut. Die erneute Autorisierung des Quellbenutzerkontos ist in der Benutzeroberfläche nicht möglich. Der Befehl zur erneuten Autorisierung des Benutzerkontos aus **Explore** lautet wie folgt:
 

```
> /warehouseconnector/sources/<source:port> ---> setPass property with password=<password of the configured user in source>
```
6. Autorisieren Sie das Nutzerkonto in der SFTP-Zielkonfiguration erneut in der **Benutzeroberfläche**, in **Explore** oder in der **REST API**. Der Befehl zur erneuten Autorisierung des Kennworts in **Explore** lautet wie folgt:
 

```
> /warehouseconnector/destinations/<sftp_destination> ---> setPass property with password=<password of the configured user in SFTP destination>
```
7. Wenn die NFS-Verzeichnisbereitstellung im Rahmen des Schritts vor dem Upgrade entfernt wurde, stellen Sie die gleiche Konfiguration wieder bereit. Aktivieren Sie außerdem den Mount-Eintrag in */etc/fstab* wieder.

```
> mount -t nfs -o nolock,tcp,hard,intr <IP_Address_for_SAW>:/mapr/<cluster-name> /<directory_name>
```

Dabei ist **<IP\_Address\_for\_SAW>** die IP-Adresse des primären Warehouse-Geräts im Cluster und **<cluster-name>** der in der Vorlagendatei angegebene Name.

## Festlegen des Wiederherstellungskennworts für die Lockbox
















Nach dem Upgrade aller Log Collectors und WLC in der NW-Implementierung auf 12.5 sollte der Administrator das **Recovery Password Utility** mit SATools ausführen. Dieses Tool legt das Lockbox-Wiederherstellungskennwort für alle Protokollsammlerdienste (Version 12.5 oder höher) innerhalb der Bereitstellung fest. Administratoren wird empfohlen, das Lockbox-Wiederherstellungskennwort zu notieren, da es in Disaster-Recovery-Szenarien benötigt wird.



Um das Wiederherstellungskennwort festzulegen, sollte der Administrator sich per SSH beim **Admin-Server (Knoten 0)** anmelden und das Dienstprogramm **set-lockbox-password** aus dem Pfad `/opt/rsa/saTools/bin/set-lockbox-password` ausführen. Administratoren sollten das neue Kennwort eingeben, das als Wiederherstellungskennwort für die in allen Log Collectors verfügbare Lockbox festgelegt werden soll.

**Hinweis:** Wenn Sie das Dienstprogramm erneut ausführen und eine aktualisierte Lockbox einrichten, setzt das Wiederherstellungskennwort das Kennwort für alle anwendbaren Log Collector-Services (Version 12.5 und höher) zurück.

# Durchführen von Validierungsprüfungen nach dem Upgrade

Nach dem Upgrade auf NetWitness 12.5 müssen Sie die folgenden Validierungsprüfungen durchführen.

1. Gehen Sie zur Ansicht  (Admin) > **Services**, um zu überprüfen, ob alle Services nach dem Upgrade aktiv sind (grüne Anzeige).
2. Stellen Sie sicher, dass die Services aktualisiert werden, damit sie mit der Hostversion übereinstimmen. Die Serviceversion in der Ansicht  (Admin) > **Services** muss nach dem Upgrade mit der Hostversion in der Ansicht  (Admin) > **Hosts** übereinstimmen.
3. Führen Sie in der Ansicht  (Admin) > **Services** einen der folgenden Schritte aus:
  - Wählen Sie einen Log Collector-Service aus und gehen Sie zur Ansicht  (Aktionen) > **Ansicht** > **System**, um zu überprüfen, ob die erforderliche Protokollsammlung gestartet wurde. Sie sollten auf die Drop-down-Option  Collection  klicken und zum richtigen Erfassungsprotokoll gehen, um zu überprüfen, ob die Protokollerfassung gestartet wurde. Wenn die erforderliche Sammlung nicht gestartet worden ist, wählen Sie  Start neben dem erforderlichen Sammlungsprotokoll aus der Liste aus, um die Sammlung zu starten.
  - Wählen Sie einen Log Decoder-Service aus und gehen Sie zur Ansicht  (Aktionen) > **Ansicht** > **System**, um zu überprüfen, ob der Log Decoder die Protokolle ordnungsgemäß erfasst.
  - Wählen Sie einen Packet Decoder-Service aus und gehen Sie zur Ansicht  (Aktionen) > **Ansicht** > **Konfiguration**, um zu überprüfen, ob die Capture-Schnittstelle im Abschnitt **Decoder-Konfiguration** konfiguriert ist. Wenn die Erfassungsschnittstelle nicht konfiguriert ist, müssen Sie die erforderliche Erfassungsschnittstelle aus der Drop-down-Liste auswählen, um sie zu konfigurieren. Wenn die Erfassungsschnittstelle bereits konfiguriert ist, navigieren Sie zur Ansicht  (Aktionen) > **Ansicht** > **System** von Packet Decoder und prüfen Sie, ob die Erfassung gestartet wurde. Wenn die Erfassung nicht gestartet worden ist, klicken Sie auf  Start Capture, um die Paketerfassung zu starten.
4. Navigieren Sie zur Ansicht  (Admin) > **Services** > Log Decoder- oder Packet Decoder-Service auswählen >  (Aktionen) > **Ansicht** > **Statistik** > **Allgemein**, um die aktuelle Erfassungsrate zu analysieren.
5. Stellen Sie sicher, dass die Concentrator, Archiver und Broker die Daten aggregieren. Stellen Sie sicher, dass Sie von jedem Concentrator, Archiver und Broker aus überprüfen können, ob er betriebsbereit ist.
6. Navigieren Sie zur Ansicht **Respond** > **Warnmeldungen**, um zu überprüfen, ob die Warnmeldungen von verschiedenen Quellen ausgelöst werden.
7. Gehen Sie zur Ansicht  (Admin) > **Integrität und Zustand** > **Alarmer** und überprüfen Sie, ob der SMS-Server in Betrieb ist.

8. Navigieren Sie zur Ansicht  (Admin) > **Ereignisquellen** > **Überwachungsrichtlinien** und überprüfen Sie, ob die vor dem Upgrade konfigurierten Policies angezeigt werden.
9. Navigieren Sie zur Ansicht  (Admin) > **Integrität und Zustand** > **Neu Integrität und Zustand** > **Zum Dashboard wechseln** > **Elastic** > **Dashboard** und stellen Sie sicher, dass Folgendes zutrifft.
  - Die Visualisierungen, die Sie vor dem Upgrade erstellt haben, sind weiterhin vorhanden.
  - Der Metrik-Server ist in ordnungsgemäßem Betrieb.
  - Für die Überwachungen, die Sie vor dem Upgrade konfiguriert haben, werden Warnmeldungen ordnungsgemäß generiert.

## Installation des 12.5-Relay-Servers

**WICHTIG:** Nach dem Upgrade von EPLH von den Versionen 12.2.xx und 12.3.xx auf 12.5.0.0 müssen Sie den Relay-Server auf der EL 8-Box (Alma Linux) neu installieren, da der Relay-Server ein eigenständiger Server ist.

### Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über die EL 8-Box verfügen.
- Führen Sie die folgenden Aufgaben aus, bevor Sie den 12.5-Relay-Server installieren:
  1. Aktualisieren Sie die NetWitness-Plattform.
  2. Laden Sie nach dem Upgrade des EPLH den Relay Packager herunter.
  3. Kopieren Sie den Packager in die EL 8-Box.
  4. Schalten Sie den vorhandenen Relay-Server aus.
  5. Konfigurieren Sie die IP-Adresse von EL 8, indem Sie die IP-Adresse des vorhandenen Relay-Servers wiederverwenden.

Sobald Sie die IP-Adresse von EL 8 konfiguriert haben, installieren Sie den Relay-Server. Weitere Informationen finden Sie im Abschnitt **(Optional) Installieren und Konfigurieren des Relay-Servers** im [Endpoint-Konfigurationshandbuch](#). Navigieren Sie zur Seite [NetWitness All Versions Documents](#) und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen.

**Hinweis:** Sie müssen die Sicherheitspatches auf dem Relay-Server auf dem neuesten Stand halten.

## Upgrade der Endpoint-Agents

Anweisungen zum Aktualisieren der Agents finden Sie unter **Upgrade für Agents** im [Endpoint Agent-Installationshandbuch für NetWitness Platform](#).

## Beheben von Upgrade-Problemen

In diesem Abschnitt werden die Fehlermeldungen beschrieben, die in der Ansicht Hosts angezeigt werden, wenn beim Aktualisieren von Hostversionen und der Installation von Services auf Hosts in der Ansicht Hosts Probleme auftreten. Wenn Sie Probleme bei einem Upgrade oder einer Installation nicht mithilfe der folgenden Troubleshooting-Lösungen beheben können, wenden Sie sich an den [Kundensupport](#) von NetWitness.

In diesem Abschnitt werden Anweisungen zum Troubleshooting der folgenden Fehler beschrieben, die während des Upgrades auftreten können.

- [Informationen zum Troubleshooting beim AlmaLinux-Betriebssystem](#)
- [Migration von Lockbox zu SecureStore schlägt bei Admin-Server, Reporting Engine und SMS fehl](#)
- [Fehler: deploy\\_admin-Kennwort abgelaufen](#)
- [Downloadfehler](#)
- [Fehler beim Bereitstellen der Version <Versionsnummer> Update-Pakete fehlen](#)
- [Fehler beim Aktualisieren des externen Repository](#)
- [Fehler: Hostaktualisierung fehlgeschlagen](#)
- [Fehler: Update-Pakete fehlen](#)
- [Fehler: Patch-Update für Nicht-NW-Server](#)
- [Fehler: Host-Neustart nach Update über die Befehlszeile](#)

Es werden auch Troubleshooting-Anweisungen für Fehler für die folgenden Hosts und Services bereitgestellt, die während oder nach einem Upgrade auftreten können.

- [Log Collector-Service](#)
- [NW-Server](#)
- [Orchestrierung](#)
- [Reporting Engine](#)
- [Event Stream Analysis](#)
- [Legacy-Windows-Log Collector](#)

<b>Problem</b>	Neustart der Appliance nach der Aktualisierung nicht möglich
<b>Workaround</b>	<ol style="list-style-type: none"> <li>1. Um den Neustart zu erzwingen, ändern Sie die GRUB-Bootzeile manuell in <code>FIPS=0</code>.</li> <li>2. Dann deaktivieren Sie FIPS mit dem folgenden Befehl:  <pre>manage-stig-controls --disable-control-groups 3 --host-all</pre> </li> <li>3. Überprüfen Sie, ob die Zeile <code>FIPS=1</code> aus <code>/boot/grub2/grub.cfg</code> entfernt wurde</li> </ol>

- Wenn dem nicht so ist, führen Sie den folgenden Befehl aus:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Führen Sie einen Neustart durch.
5. Führen Sie den folgenden Befehl aus, um FIPS zu aktivieren:
 

```
manage-stig-controls --enable-control-groups 3 --host-all
```
6. Führen Sie einen erneuten Neustart aus.

## Informationen zum Troubleshooting beim AlmaLinux-Betriebssystem

Zum besseren Verständnis kann das Upgrade des AlmaLinux-Betriebssystems in 4 Teile unterteilt werden:

1. Ausführen des Dienstprogramm für die Vorabprüfung, um die Systemintegrität sicherzustellen und etwaige Upgrade-Probleme zu erkennen. Dies kann jederzeit vor dem Upgrade mit dem eigenständigen Vorabprüfungs-Tool rpm erfolgen. (nur auf dem NW-Server erforderlich)

Protokolle werden in diesem Pfad aufgezeichnet: `/var/log/netwitness/precheck-tool/checklist.log`

2. Initialisierungs- bzw. Init-Phase (nur auf NW Server vorhanden)

Überprüfen Sie diese Protokolle auf etwaige Probleme während der Initialisierungsphase.

- Salt-Minion-Protokolle: `/var/log/salt/minion`
- Bereitstellungs- und Upgrade-Protokolle: `/var/log/netwitness/deployment-upgrade/chef-solo.log`

**Hinweis:** Führen Sie die **Initialisierung** nur durch, wenn Sie planen, das eigentliche Upgrade durchzuführen. Es wird nicht empfohlen, eine Initialisierung durchzuführen, ohne das System im gleichen Änderungsfenster zu aktualisieren.

3. Betriebssystem-Upgrade von CentOS auf AlmaLinux

Im ersten Schritt des Betriebssystem-Upgrades wird Salt aktualisiert. Sie können den folgenden Befehl ausführen, um zu sehen, dass Salt auf Version 3006 aktualisiert wird:

```
cat /var/log/yum.log | grep salt
```

Sie können eine ähnliche Aktualisierung wie unten sehen, wobei xxx für den aktuellen Datum-/Uhrzeitstempel steht:

```
xxx Updated: salt-master-3006.2-0.x86_64
xxx Updated: salt-api-3006.2-0.x86_64
xxx Updated: salt-minion-3006.2-0.x86_64
```

Bei Problemen mit dem Salt-Upgrade überprüfen Sie Folgendes:

- /var/log/netwitness/node-infra-server/node-infra-server.log
- /var/log/salt/master
- /var/log/salt/minion

Sobald Salt aktualisiert worden ist, beginnt der Leapp-Prozess.

Die Protokolle können unter /var/log/salt/minion eingesehen werden:

```
xxx [salt.loaded.ext.module.nw_platform:445 ][INFO ][139407] [1/5]
Searching for leapp config for version: 12.5.0.0

xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.5.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.5.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:467 ][INFO ][139407] [3/5] Running
pre-requisites required to perform leapp upgrade

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/actor.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/libraries/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/addupgradebootentry.py'

xxx [salt.loaded.ext.module.nw_platform:500 ][INFO ][139407] [4/5] Running
leapp pre-upgrade

xxx [salt.loaded.ext.module.nw_platform:503 ][INFO ][139407] [5/5] Running
leapp upgrade
```

Bei Problemen, die während des Betriebssystem-Upgrades auftreten, sind die folgenden Protokolle beim Troubleshooting hilfreich.

- /var/log/salt/minion
- Wenn PreUpgrade fehlschlägt: /var/log/leapp/leapp-preupgrade.log
- Wenn das Leapp-Upgrade fehlschlägt: /var/log/leapp/leapp-upgrade.log

Wenn leapp fehlschlägt, finden Sie in /var/log/leapp/leapp-report.txt Einzelheiten zu den hemmenden Faktoren.

Einige Minuten nach dem Protokolleintrag „Running leapp upgrade“ in /var/log/salt/minion wird das System neu gestartet und es kann 20 bis 30 Minuten dauern, bis es in den Normalmodus zurückkehrt.

Sobald es hochgefahren ist, können Sie das Betriebssystem mit dem Befehl `cat /etc/almalinux-release` überprüfen. Wenn die Alma Linux-Version nicht angezeigt wird, rufen Sie den Kundendienst an, bevor Sie weitere Maßnahmen ergreifen.

Wenn Sie das Upgrade über die Benutzeroberfläche ausgelöst haben und auf einem NodeX für mehr als eine Stunde der Status „Performing OS Migration“ angezeigt wird, überprüfen Sie die Leapp-Protokolle und wenden Sie sich an den Kundensupport.

#### 4. NW-Software-Upgrade auf 12.5.0.0

Sobald die Betriebssystemmigration abgeschlossen ist, beginnt das NW-Software-Upgrade und es dauert bis zu 30 Minuten, bis die Benutzeroberfläche funktionsfähig ist.

Sie finden diese Protokolle in `/var/log/salt/minion`, wenn das NW-Software-Upgrade beginnt:

```
xxx [salt.loaded.ext.module.nw_platform:276 ][INFO ][14035] Preparing node
for upgrade to 12.5.0.0

xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching
for yum config for version: 12.5.0.0

xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2]
Retrieving yum config for version: 12.5.0.0

xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv
'base', ** done ** 'config/12.5.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading chef
package

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading rsa-
nw-config-management package
```

Sie können auch die Konfigurationsverwaltungsprotokolle unter `/var/log/netwitness/config-management/chef-solo.log` oder die Benutzeroberflächenprotokolle `/var/netwitness/uax/logs/sa.log` einsehen.

## Migration von Lockbox zu SecureStore schlägt bei Admin-Server, Reporting Engine und SMS fehl

### Für Admin-Server oder Jetty

<b>Problem</b>	Die Migration von LockBox zu SecureStore ist auf dem Admin-Server fehlgeschlagen.
<b>Ursache</b>	Aufgrund unvollständiger Migration der SSV-Werte
<b>Lösung</b>	<p>Wenn Sie nicht auf den Admin-Server zugreifen können, führen Sie die folgenden Schritte aus, um das Problem zu beheben:</p> <ol style="list-style-type: none"> <li>1. SSH zum Admin-Server/Knoten Null</li> <li>2. Stoppen Sie den Jetty-Dienst mit dem folgenden Befehl: <pre>systemctl stop jetty</pre> </li> <li>3. Verschieben Sie die Dateien <code>lockbox.ss</code> und <code>lockbox.ss.lock</code> aus den folgenden Pfaden in einen separaten Backupordner: <ul style="list-style-type: none"> <li>• <code>/var/netwitness/uax</code></li> <li>• <code>/root/uaxbackup</code></li> </ul> </li> <li>4. Starten Sie den Jetty-Dienst mit dem folgenden Befehl: <pre>systemctl start jetty</pre> </li> </ol>

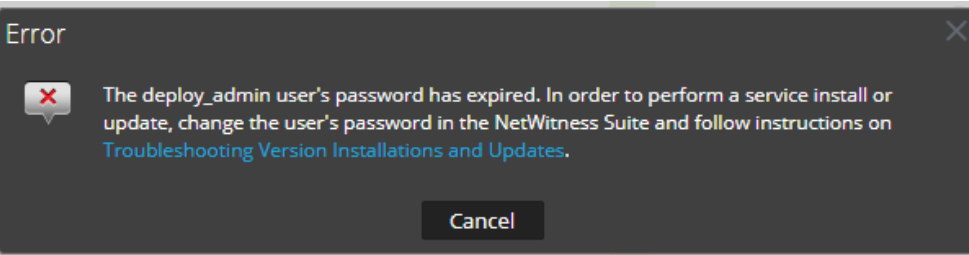
### Für Reporting Engine

<b>Problem</b>	Die Migration von LockBox zu SecureStore ist in der Reporting Engine fehlgeschlagen.
<b>Ursache</b>	Aufgrund einer unvollständigen Migration der SSV-Werte.
<b>Lösung</b>	<p>Wenn Sie nicht auf die Reporting Engine zugreifen können, führen Sie die folgenden Schritte aus, um das Problem zu beheben:</p> <ol style="list-style-type: none"> <li>1. SSH zum Admin-Server/Knoten Null.</li> <li>2. Beenden Sie den Reporting Engine-Service mit dem folgenden Befehl:  <pre>systemctl stop rsasoc_re</pre> </li> <li>3. Verschieben Sie die Dateien <code>lockbox.ss</code> und <code>lockbox.ss.lock</code> aus dem Pfad <code>/var/netwitness/re-server/rsa/soc/reporting-engine</code> in einen Backupordner.</li> <li>4. Starten Sie den Reporting Engine-Dienst mit dem folgenden Befehl:  <pre>systemctl start rsasoc_re</pre> </li> </ol>

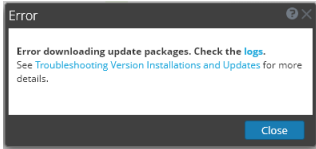
### Für SMS

<b>Problem</b>	Die Migration von LockBox zu SecureStore ist in der SMS fehlgeschlagen.
<b>Ursache</b>	Aufgrund einer unvollständigen Migration der SSV-Werte.
<b>Lösung</b>	<p>Wenn Sie nicht auf den SMS-Dienst zugreifen können, führen Sie die folgenden Schritte aus, um das Problem zu beheben:</p> <ol style="list-style-type: none"> <li>1. SSH zum Admin-Server/Knoten Null.</li> <li>2. Beenden Sie den SMS-Service mit dem folgenden Befehl:  <pre>systemctl stop rsa-sms</pre> </li> <li>3. Verschieben Sie die Dateien <code>lockbox.ss</code> und <code>lockbox.ss.lock</code> aus dem Pfad <code>/root/rsa/home</code> in einen Backupordner.</li> <li>4. Starten Sie den SMS-Dienst mit dem folgenden Befehl:  <pre>systemctl start rsa-sms</pre> </li> </ol>

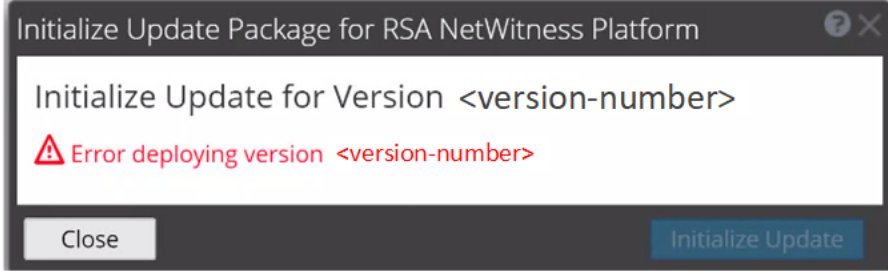
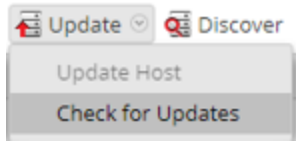
## Fehler: deploy\_admin-Benutzerkennwort abgelaufen

<b>Fehlermeldung</b>	
<b>Ursache</b>	Das <code>deploy_admin</code> -Benutzerkennwort ist abgelaufen.
<b>Lösung</b>	<p>Setzen Sie Ihr <code>deploy_admin</code>-Kennwort zurück. Gehen Sie wie folgt vor.</p> <ol style="list-style-type: none"><li>1. Führen Sie den folgenden Befehl nur auf dem NW-Serverhost aus. <pre>nw-manage --update-deploy-admin-pw</pre><p>Please enter the new <code>deploy_admin</code> account password: &lt;new-deploy-admin-password&gt; Please confirm the new <code>deploy_admin</code> account password: &lt;new-deploy-admin-password&gt;</p></li><li>2. Überprüfen Sie die Ausgabe des Befehls <code>nw-manage --update-deploy-admin-pw</code>, um sicher zu vergewissern, dass das <code>deploy_admin</code>-Kennwort auf allen Hosts erfolgreich aktualisiert wurde. Wenn ein NW-Host nicht funktioniert oder aus irgendeinem Grund ausfällt, wie in der Ausgabe des Befehls <code>nw-manage --update-deploy-admin-pw</code> ersichtlich, führen Sie <code>nw-manage --sync-deploy-admin-pw --host-key &lt;host-identifizier&gt;</code> aus, um das Kennwort zwischen dem NW-Server und dem ausgefallenen Host zu synchronisieren, sobald der Kommunikationsfehler behoben ist.</li><li>3. Führen Sie auf dem Host, auf dem die Installation oder Orchestrierung fehlgeschlagen ist, den Befehl <code>nwsetup-tui</code> aus und verwenden Sie das neue <b>deploy_admin</b>-Kennwort als Antwort auf die Aufforderung zur Eingabe des <b>Bereitstellungskennworts</b>.</li></ol>

## Downloadfehler

<p><b>Fehlermeldung</b></p>	
<p><b>Problem</b></p>	<p>Wenn Sie eine Aktualisierungsversion auswählen und auf <b>Aktualisieren &gt; Host aktualisieren</b> klicken, wird der Download zwar gestartet, kann aber nicht abgeschlossen werden.</p>
<p><b>Ursache</b></p>	<p>Die Downloaddateien der Version können groß sein und das Herunterladen kann daher lange dauern. Wenn beim Download Kommunikationsprobleme auftreten, schlägt er fehl.</p>
<p><b>Lösung</b></p>	<ol style="list-style-type: none"> <li>1. Versuchen Sie erneut, ein Update durchzuführen.</li> <li>2. Wenn dies erneut mit dem gleichen Fehler fehlschlägt, versuchen Sie, das Update mit den Offline-Methoden durchzuführen, wie unter „Offline-Methode aus der Hosts-Ansicht“ oder „Offline-Methode mit Befehlszeilenschnittstelle“ im <i>Upgrade-Leitfaden für NetWitness Platform</i> beschrieben. Navigieren Sie zur Seite <a href="#">NetWitness All Versions Documents</a> und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen.</li> <li>3. Wenn Sie immer noch kein Update durchführen können, wenden Sie sich an den <a href="#">NetWitness-Kundensupport</a>.</li> </ol>

## Fehler beim Bereitstellen der Version <Versionsnummer> Update-Pakete fehlen

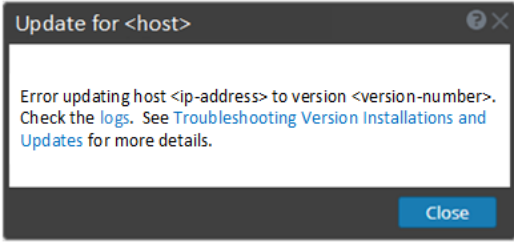
<b>Fehlermeldung</b>	
<b>Problem</b>	<p>Wenn das Update-Paket beschädigt ist, wird <b>Fehler beim Bereitstellen der Version &lt;Versionsnummer&gt;</b> im Dialogfeld <b>Update-Paket für NetWitness Platform initialisieren</b> angezeigt, nachdem Sie auf <b>Update initialisieren</b> geklickt haben.</p>
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Klicken Sie auf <b>Schließen</b>, um das Dialogfeld zu schließen.</li> <li>2. Entfernen Sie den Versionsordner wurde aus dem Bereitstellungsordner.</li> <li>3. Stellen Sie sicher, dass der Salt-Master-Service ausgeführt wird.</li> <li>4. Kopieren Sie die ZIP-Datei mit dem Update-Paket in den Bereitstellungsordner.</li> <li>5. Wählen Sie in der Symbolleiste <b>Hosts</b> der Ansicht erneut <b>Nach Updates suchen</b> aus.</li> </ol>  <ol style="list-style-type: none"> <li>6. Klicken Sie auf <b>Update initialisieren</b>.</li> <li>7. Klicken Sie in der Symbolleiste auf <b>Aktualisieren &gt; Host aktualisieren</b>.</li> <li>8. Klicken Sie im Dialogfeld <b>Update verfügbar</b> auf <b>Update starten</b>. Nachdem der Host aktualisiert wurde, werden Sie aufgefordert, den Host neu zu starten.</li> <li>9. Klicken Sie in der Symbolleiste auf <b>Neustart</b>.</li> </ol>

## Fehler beim Aktualisieren des externen Repository

<b>Fehlermeldung</b>	<p>Sie erhalten eine Fehlermeldung ähnlich der folgenden Fehlermeldung, während Sie versuchen, auf eine neue Version zu aktualisieren:</p> <pre>.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /&lt;version-number&gt;/RSA'": URL must be http, ftp, file or https not ""</pre>
----------------------	--

<b>Ursache</b>	Falscher Pfad angeben.
<b>Lösung</b>	<p>Achten Sie auf Folgendes:</p> <ul style="list-style-type: none"> <li>• Die URL ist auf dem NW-Serverhost vorhanden.</li> <li>• Sie haben den richtigen Pfad verwendet und alle Leerzeichen daraus entfernt.</li> </ul>

## Fehler: Hostaktualisierung fehlgeschlagen

<b>Fehlermeldung</b>	
<b>Problem</b>	<p>Wenn Sie eine Aktualisierungsversion auswählen und auf <b>Aktualisieren &gt; Host aktualisieren</b> klicken, ist zwar der Download erfolgreich, aber die Aktualisierung schlägt fehl.</p>
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Versuchen Sie erneut, das Versionsupdate auf den Host anzuwenden. Oft ist das alles, was Sie tun müssen.</li> <li>2. Wenn Sie das neue Versionsupdate immer noch nicht anwenden können: Überwachen Sie die folgenden Protokolle auf dem NW-Server, während des Vorgangs (führen Sie beispielsweise den Befehl <code>tail -f</code> über die Befehlszeile aus):             <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out             </pre> <p>Der Fehler erscheint in mindestens einem dieser Protokolle.</p> </li> <li>3. Wenn Sie das Update immer noch nicht anwenden können, sammeln Sie die Protokolle aus <b>Schritt 2</b> oben und wenden Sie sich an den <a href="#">NetWitness-Kundensupport</a>.</li> </ol>

<b>Fehlermeldung</b>	
<b>Problem</b>	<p>Wenn Sie eine Update-Version auswählen und auf <b>Aktualisieren &gt; Auf Updates prüfen</b> klicken, wird die Fehlermeldung <b>Nicht autorisiert</b> angezeigt. Infolgedessen schlägt die Verbindung zum Live-Dienst fehl.</p>

<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Stellen Sie sicher, dass die Live-Testverbindung erfolgreich ist.</li> <li>2. Aktualisieren Sie <a href="https://update.netwitness.com/RSA-netwitness">https://update.netwitness.com/RSA-netwitness</a> in <b>(Admin) &gt; System &gt; Updates</b>.</li> <li>3. Stellen Sie über SSH eine Verbindung mit dem Admin-Server her und erstellen Sie ein Backup von <code>/etc/default/jetty</code>.</li> <li>4. Aktualisieren Sie den folgenden Eintrag am Ende von <code>JAVA_OPTIONS</code> in <code>/etc/default/jetty</code>. <pre>JAVA_OPTIONS="\${JAVA_OPTIONS} - Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netwitness.com/RSA-netwitness/ - Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/authenticate "</pre> </li> <li>5. Starten Sie den Jetty-Dienst neu, indem Sie den folgenden Befehl ausführen: <pre>service jetty restart</pre> </li> </ol>
---------------	---

## Fehler: Update-Pakete fehlen


<b>Fehlermeldung</b>	<p><b>Initialisieren Sie das Update für Version xx.x.x.x</b>  <b>Die folgenden Update-Pakete fehlen</b>  <a href="#">Pakete vom NetWitness-Link herunterladen</a></p>
<b>Problem</b>	<p><b>Die folgenden Update-Pakete fehlen</b> wird im Dialogfeld <b>Update-Paket für NetWitness Platform initialisieren</b> angezeigt, wenn Sie einen Host über die Ansicht <b>Hosts</b> offline aktualisieren und im Bereitstellungsordner Pakete fehlen.</p>
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Klicken Sie im Dialogfeld <a href="#">Update-Paket für NetWitness Platform initialisieren</a> auf <b>Pakete von der NetWitness-Community herunterladen</b>. Die NetWitness-Community-Seite, die die Update-Dateien für die ausgewählte Version enthält, wird angezeigt.</li> <li>2. Wählen Sie die im Bereitstellungsordner fehlenden Pakete aus. Das Dialogfeld <b>Update-Paket für NetWitness Platform initialisieren</b> wird angezeigt und enthält die Meldung, dass das System bereit ist, die Aktualisierungspakete zu initialisieren.</li> </ol>

## Fehler: Patch-Update für Nicht-NW-Server

<b>Fehlermeldung</b>	<p>Das Protokoll <code>/var/log/netwitness/orchestration-server/orchestration-server.log</code> enthält einen ähnlichen Fehler wie den folgenden:  <b>API Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '12.x.x.n' is not supported</b></p>
<b>Problem</b>	<p>Nach der Aktualisierung des NW-Serverhosts auf eine bestimmte Version müssen</p>

<b>Lösung</b>	<p>Sie ist alle Nicht-NW-Serverhosts auf dieselbe Version aktualisieren. Wenn Sie beispielsweise den NW-Server von 12.2.0.0 auf 12.5.0.0 oder höher aktualisieren, können die Nicht-NW-Server-Hosts nur dieselbe Version (d. h. 12.5.0.0) aktualisiert werden. Wenn Sie versuchen, einen Nicht-NW-Server-Host auf eine andere Version zu aktualisieren (z. B. von 12.2.0.0 auf 12.3.x.x), wird dieser Fehler angezeigt.</p>
	<p>Führen Sie eine der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>• Aktualisieren Sie die Nicht-NW-Serverhosts auf Version 12.5.0.0 oder höher oder</li> <li>• Aktualisieren Sie den Nicht-NW-Serverhost nicht (behalten sie die aktuelle Version bei)</li> </ul>

## Fehler: Host-Neustart nach Update über die Befehlszeile

<b>Fehlermeldung</b>	<p>In der Benutzeroberfläche wird eine Meldung mit der Aufforderung angezeigt, den Host nach dem Update offline neu zu starten.</p> 
<b>Ursache</b>	<p>Der obige Fehler tritt auf, wenn Sie den Host mithilfe der CLI neu starten. Sie müssen die Benutzeroberfläche verwenden, um den Host neu zu starten.</p>
<b>Lösung</b>	<p>Starten Sie den Host in der Ansicht <b>Host</b> der Benutzeroberfläche neu.</p>

## Log Collector-Service (`nwlogcollector`)

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

<b>Fehlermeldung</b>	<pre>&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.</pre>
<b>Ursache</b>	<p>Die Log Collector Lockbox konnte nach der Aktualisierung nicht geöffnet werden.</p>
<b>Lösung</b>	<p>Melden Sie sich bei NetWitness an und setzen Sie den Systemfingerabdruck zurück, indem Sie das Kennwort für den Systemstabilitätswert der Lockbox zurücksetzen, wie im Thema <b>Zurücksetzen des Systemstabilitätswerts unter Konfigurieren von Lockbox-Sicherheitseinstellungen</b> im <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben.</p>

<b>Fehlermeldung</b>	<pre>&lt;timestamp&gt; NwLogCollector_PostInstall: Lockbox Status : Not Found</pre>
----------------------	---

<b>Ursache</b>	Die Log Collector Lockbox wird nach der Aktualisierung nicht konfiguriert.
<b>Lösung</b>	Wenn Sie eine Log Collector Lockbox verwenden, melden Sie sich bei NetWitness an und konfigurieren Sie die Lockbox wie im Thema <b>Konfigurieren von Lockbox-Sicherheitseinstellungen</b> im <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben.

<b>Fehlermeldung</b>	<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.
<b>Ursache</b>	Sie müssen das Feld für den Schwellenwert des Stabilitätswerts für die Log Collector Lockbox zurücksetzen.
<b>Lösung</b>	Melden Sie sich bei NetWitness an und setzen Sie das Kennwort für den Systemstabilitätswert der Lockbox wie im Thema <b>Zurücksetzen des Systemstabilitätswerts</b> unter <b>Konfigurieren von Lockbox-Sicherheitseinstellungen</b> im <i>Protokollsammlung-Konfigurationsleitfaden</i> beschrieben zurück.

<b>Fehlermeldung</b>	Der Decoder versucht, mit der Erfassung von Ereignissen zu beginnen, schlägt jedoch fehl. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.</div>
<b>Ursache</b>	Die Decoder-Erfassungskonfiguration ist nicht gültig für Kunden, die PF_RING Capture (CentOS) verwenden und ein direktes Upgrade auf 12.5.0.0 (AlmaLinux) durchführen. Zuerst müssen sie PF_RING-Geräte zu DPDK migrieren und dann ein Upgrade durchführen.
<b>Lösung</b>	<b>So lösen Sie das Problem</b> Anweisungen zur Migration finden Sie unter <a href="#">Migrieren von PF_RING-Geräten zu DPDK</a> .

## NW-Server

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

<b>Problem</b>	Nach dem Upgrade werden Sie Folgendes bemerken: <ul style="list-style-type: none"> <li>Audit-Protokolle werden nicht an das konfigurierte globale Audit-Setup weitergeleitet.</li> <li>Die folgende Meldung erscheint in <code>sa.log</code>. <code>Syslog Configuration migration failed. Restart jetty service to fix this issue</code></li> </ul>
<b>Ursache</b>	Die Migration des NW Server Global Audit-Setups von 12.2.x.x oder 12.3.x.x. nach 12.5.0.0 oder höher ist fehlgeschlagen.
<b>Lösung</b>	<ol style="list-style-type: none"> <li>Stellen Sie über SSH eine Verbindung mit dem NW-Server her.</li> <li>Senden Sie den folgenden Befehl: <code>orchestration-cli-client --update-admin-node</code></li> </ol>

## Orchestrierung

Die Protokolle des Orchestrierungsservers werden an `/var/log/netwitness/orchestration-server/orchestration-server.log` auf dem NW-Serverhost gesendet.

<b>Problem</b>	<ol style="list-style-type: none"> <li>1. Es wurde erfolglos versucht, ein Upgrade für einen Nicht-NW-Serverhost durchzuführen.</li> <li>2. Das Upgrade für diesen Host wurde erneut gestartet und war wieder erfolglos.</li> </ol> <p>Die folgende Meldung wird im <code>orchestration-server.log</code> angezeigt.  <code>"'file' _virtual_ returned False: cannot import name HASHES"</code></p>
<b>Ursache</b>	<p>Es wurde eventuell ein Upgrade für Salt Minion durchgeführt und Salt Minion wurde auf dem fehlerhaften Nicht-NW-Serverhost nicht neu gestartet.</p>
<b>Lösung</b>	<ol style="list-style-type: none"> <li>1. Stellen Sie über SSH eine Verbindung zu dem Nicht-NW-Serverhost her, bei dem das Upgrade fehlgeschlagen ist.</li> <li>2. Senden Sie die folgenden Befehle.  <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> </li> <li>3. Versuchen Sie das Upgrade des Nicht-NW-Serverhosts erneut.</li> </ol>
<b>Problem</b>	<p>Wenn Sie einen neuen 12.5.0.0 Core Node-X auf dem Admin-Server (Node-0), der von 12.0 oder älteren Versionen auf 12.5.0.0 aktualisiert wurde, installieren und orchestrieren, sind die Core-Services wie Concentrator, Log Decoder, Log Collector, Archiver, Decoder, Appliance, Workbench verfügbar und Warehouse Connector und Broker werden in der Spalte <b>Services</b> in der Ansicht <b>Admin &gt; Hosts</b> als inaktiv angezeigt. Infolgedessen können Sie in der Benutzeroberfläche nicht auf die Core-Services zugreifen.</p> <p>Dies gilt nicht, wenn Sie einen neuen 12.5.0.0-Core-Node-X auf dem neu installierten 12.5.0.0-Admin-Server orchestrieren (kein Upgrade von 12.0 oder älteren Versionen auf 12.5.0.0).</p>
<b>Ursache</b>	<p>Der 12.5.0.0 Core Node-X verwendet ein dediziertes SA-Server-Zertifikat anstelle des gemeinsamen Node-0-Knoten-zertifikats unter seinen vertrauenswürdigen Peers, wenn er direkt auf einem aktualisierten 12.5.0.0-Admin-Server-Host orchestriert wird.</p>
<b>Lösung</b>	<p>Führen Sie die folgenden Befehle aus, bevor Sie ein Bootstrap für den 12.5.0.0-Core-Node-X-Host durchführen und ihn orchestrieren.</p> <pre>mkdir -p /etc/netwitness/platform</pre> <ol style="list-style-type: none"> <li>1. <pre>touch /etc/netwitness/platform/nw-upgrade-mode</pre> <p>Verwenden Sie diesen Workaround nur dann, wenn Sie den obigen Workaround (Workaround 1) übersprungen haben. Führen Sie die folgenden Befehle aus, nachdem Sie ein Bootstrap für den 12.5.0.0-Core-Node-X-Host durchgeführt und ihn orchestriert haben.</p> <pre>touch /etc/netwitness/platform/nw-upgrade-mode</pre> </li> <li>2.</li> </ol>

```
nw-manage --refresh-host --host-key <core-node-x-salt-minion-uuid>

systemctl restart <core-service-name>
```

**Hinweis:**


- Überprüfen Sie die Datei /etc/salt/minion, um <core-node-x-salt-minion-uuid> zu finden.
- Sie müssen den Namen des Core-Service, z. B. **nwarchiver** (Archiver), **nwdecoder** (Decoder), **nwlogcollector** (Log Collector), **nwappliance** (Appliance), **nwconcentrator** (Concentrator), **nwlogdecoder** (Log Decoder), **nwbroker** (Broker), **nwworkbench** (Workbench) und **nwwarehouseconnector** (Warehouse Connector) in <core-service-name> eingeben.

## 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.

<b>Fehlermeldung</b>	<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB > ] is less than the required space [ <required-GB > ]
<b>Ursache</b>	Die Aktualisierung der Reporting Engine ist fehlgeschlagen, da Sie nicht über ausreichend Speicherplatz verfügen.
<b>Lösung</b>	Geben Sie Festplattenspeicherplatz frei, um den in der Protokollmeldung angezeigten erforderlichen Speicherplatz bereitzustellen. Anweisungen zum Freigeben von Festplattenspeicherplatz finden Sie unter <b>Hinzufügen von zusätzlichem Speicherplatz für große Berichte</b> im <i>Reporting Engine-Konfigurationsleitfaden</i> .

## Event Stream Analysis

<b>Problem</b>	Nach dem Upgrade auf Version 12.5.0.0 oder höher aggregiert der ESA-Korrelationsserver keine Ereignisse aus den konfigurierten Datenquellen.
<b>Fehlermeldung</b>	Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)
<b>Lösung</b>	<p><b>So lösen Sie das Problem</b></p> <p>Führen Sie folgende Schritte in der NetWitness-Benutzeroberfläche aus:</p> <ol style="list-style-type: none"> <li>1. Navigieren Sie zu  (<b>KONFIGURIEREN</b>) &gt; <b>Policies</b> &gt; <b>Inhalt</b> &gt; <b>Event Stream Analysis</b> &gt; <b>Datenquellen</b>. Der Bereich <b>Datenquellen</b> wird angezeigt.</li> </ol>

2. Wählen Sie die Datenquelle aus und klicken Sie in der Symbolleiste auf **Datenquelle bearbeiten**.  
Das Dialogfeld **Datenquelle bearbeiten** wird angezeigt.
  3. Führen Sie im Dialogfeld **Datenquelle bearbeiten** einen der folgenden Schritte aus:
    - Wählen Sie **Vertrauenswürdige Authentifizierung** aus.
    - Wählen Sie **Anmeldeinformationen verwenden** aus und geben Sie den Benutzernamen und das Kennwort ein.
  4. Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass die Quelle mit dem ESA-Service kommunizieren kann, und klicken Sie anschließend auf **OK**.
- Hinweis:** Führen Sie die obigen Schritte für alle konfigurierten Datenquellen aus.
5. Stellen Sie alle Bereitstellungen bereit, die mit den bearbeiteten Datenquellen im Bereich **Datenquellen** verknüpft sind, nachdem Sie alle Änderungen an den Datenquellen vorgenommen haben.


## Legacy-Windows-Log Collector

<b>Problem</b>	Legacy-Windows-Log Collector wird als inaktiv angezeigt, wenn der Stack auf 12.5.0.0 aktualisiert wird.
<b>Ursache</b>	Zertifikat-Update im Admin-Server-Node.
<b>Lösung</b>	Weitere Informationen finden Sie im Abschnitt „Legacy-Windows-Log Collector“ unter <a href="#">Durchführen von Aufgaben nach dem Upgrade</a> .

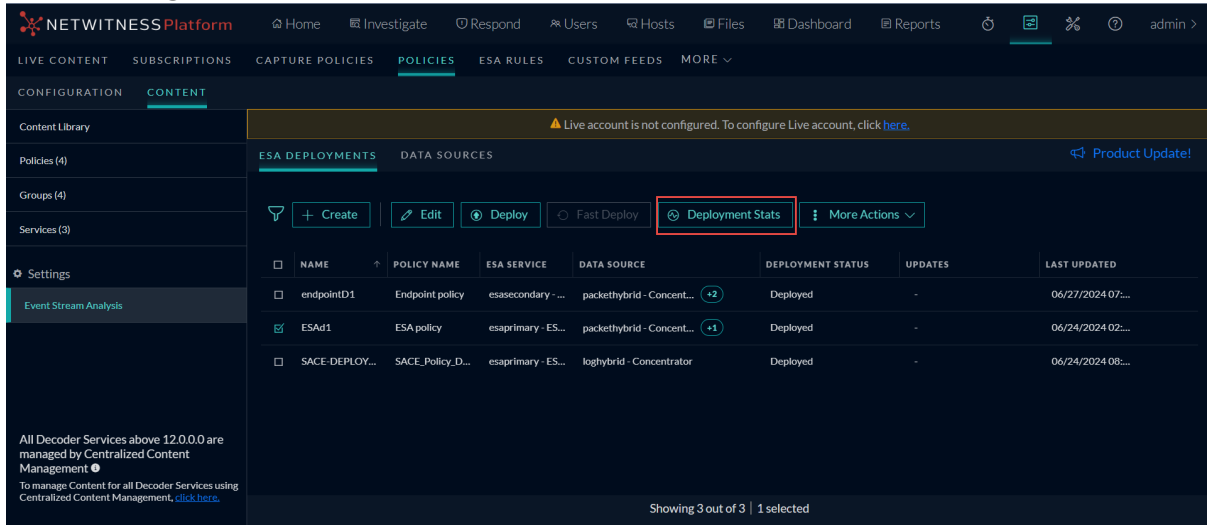
## ESA-Troubleshooting-Informationen

### ESA-Regeln erstellen keine Warnmeldungen

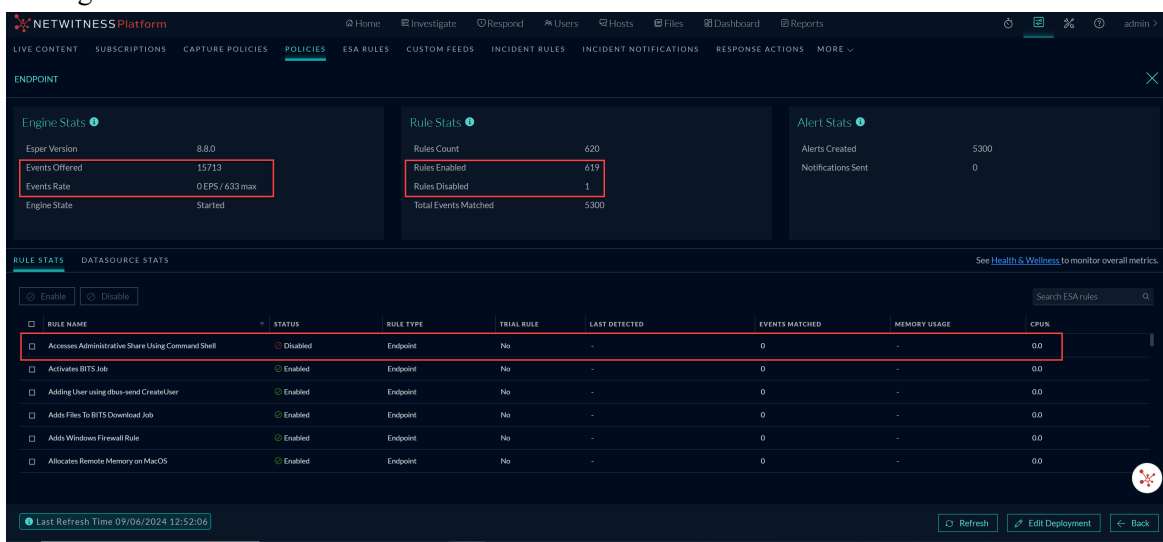
Wenn keine Warnmeldungen angezeigt werden, überprüfen Sie den Status der ESA-Regelbereitstellungen.


1. Navigieren Sie zu  (**KONFIGURIEREN**) > **Policies** > **Inhalt** > **Event Stream Analysis** > **ESA-Bereitstellungen**.  
Das Fenster **ESA-Bereitstellung** wird angezeigt.

- Wählen Sie die erforderliche Bereitstellung aus der Liste aus und klicken Sie auf die Registerkarte **Bereitstellungsstatistiken**.



- Die Seite „Bereitstellungsstatistiken“ wird geöffnet und zeigt den Status Ihrer ESA-Services und -Bereitstellungen an.
- Gehen Sie für jede ESA-Regel-Bereitstellung wie folgt vor:
  - Sehen Sie sich im Abschnitt **Engine-Statistiken** die Felder **Angebotene Ereignisse** und **Angebotene Rate** an. Sie bestätigen, dass die Daten ordnungsgemäß aggregiert und analysiert werden. Wenn für „Angebotene Ereignisse“ 0 angezeigt wird, geht für die Bereitstellung nichts ein.
  - Sehen Sie sich im Abschnitt **Regelstatistiken** die Felder **Aktivierte Regeln** und **Deaktivierte Regeln** an. Wenn deaktivierte Regeln vorhanden sind, überprüfen Sie den Abschnitt **Statistiken zu bereitgestellten Regeln** weiter unten, um Details zu den deaktivierten Regeln anzuzeigen. Deaktivierte Regeln werden durch einen roten Kreis angezeigt. Aktivierte Regeln verfügen über einen grünen Kreis.



5. Wenn Sie deaktivierte Regeln finden, die aktiviert werden sollten, gehen Sie wie folgt vor:
  - a. Navigieren Sie zur Registerkarte  (**Konfigurieren**) > **ESA-Regeln** > **Regeln** und stellen Sie die ESA-Regelbereitstellungen, die deaktivierte Regeln enthalten, erneut bereit.
  - b. Kehren Sie zur Registerkarte **Services** zurück und prüfen Sie, ob die Regeln noch deaktiviert sind. Wenn die Regeln immer noch deaktiviert sind, überprüfen Sie die Protokolldateien des ESA-Korrelationservice, die sich im Verzeichnis `/var/log/netwitness/correlation-server/correlation-server.log` befinden.

**Hinweis:** Um unnötigen Verarbeitungsaufwand zu vermeiden, wurde die Option „Groß-/Kleinschreibung ignorieren“ aus dem Dialogfeld „ESA-Regelerstellung – Anweisung erstellen“ für Metaschlüssel, die keine Textdatenwerte enthalten, entfernt. Während des Upgrades auf die neueste Version ändert NetWitness Platform keine vorhandenen Regeln für die Option „Groß-/Kleinschreibung ignorieren“. Wenn in einer vorhandenen Regelerstellungsregel die Option „Groß-/Kleinschreibung ignorieren“ für einen Metaschlüssel aktiviert ist, für den diese Option nicht mehr verfügbar ist, tritt ein Fehler auf, wenn Sie versuchen, die Anweisung zu bearbeiten und erneut zu speichern, ohne das Kontrollkästchen zu deaktivieren.

## Beispiel einer Warnmeldung des ESA-Korrelationservers für fehlende Metaschlüssel

Wenn in den Fehlerprotokollen des ESA-Korrelationservers eine Warnmeldung angezeigt wird, bedeutet dies, dass sich die Metaschlüsselwerte der Parameter `default-multi-valued` und `multi-valued parameter` unterscheiden und die neuen Regeln für Endpoint, UEBA und Live-Inhalt nicht funktionieren. Das Problem sollte sich beheben lassen, indem Sie das Verfahren zum **Aktualisieren der mehrwertigen und einwertigen Parameter-Metaschlüssel für die neuesten Endpoint-, UEBA- und RSA-Live-Content-Regeln** im *ESA-Konfigurationsleitfaden* durchführen.

### Beispiel für eine Warnmeldung zu mehrwertigem Parameter

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id, browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_src, client_all, content, context, context_all, context_dst, context_src, dir_path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst, directory_src, email_dst, email_src, feed_category, feed_desc, feed_name, file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter, function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_orig, OS, param, param_dst, param_src, registry_key, registry_value, risk, risk_info, risk_suspicious, risk_warning, threat_category, threat_desc, threat_source, user_agent] are still MISSING from multi-valued
```

### Beispiel für eine Warnmeldung zu einwertigem Parameter

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target, file_attributes, logon_type_desc, packets] are still MISSING from single-valued
```

## Nutzen Sie das NetWitness Community Portal zur Unterstützung

---

Sie können das NetWitness Community Portal verwenden, um nach bestimmten Dokumenten zu suchen, Informationen zum Ende der Nutzungsdauer von Appliances zu finden und Blogs zu lesen.

### Ressourcen zur Selbsthilfe

Es gibt mehrere Optionen, die Ihnen bei der Installation und Verwendung von NetWitness bei Bedarf Hilfestellung bieten:

- Weitere Informationen zu allen Aspekten von NetWitness finden Sie hier: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>
- Benutzen Sie die Felder **Search** und **Create a Post** im NetWitness Community-Portal, um hier spezifische Informationen zu finden: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>
- Weitere Informationen finden Sie in der NetWitness Wissensdatenbank: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>
- Weitere Informationen finden Sie im Abschnitt „Troubleshooting“ in den Leitfäden.
- Siehe auch [NetWitness® Platform-Blogbeiträge](#).
- Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den NetWitness Support.

### NetWitness Support kontaktieren

Wenn Sie den NetWitness-Support kontaktieren, sollten Sie sich an Ihrem Computer befinden. Bereiten Sie sich darauf vor, die folgenden Informationen zu geben:

- Die Versionsnummer des verwendeten NetWitness Platform-Produkts oder der Appliance.
- Typ der verwendeten Hardware

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

NetWitness Community Portal	<a href="https://community.netwitness.com">https://community.netwitness.com</a> Klicken Sie im Hauptmenü auf <b>Support</b> > <b>Portal für Support-Fälle</b> > <b>Meine Fälle anzeigen</b> .
Internationale Kontakte (So kontaktieren Sie den NetWitness-Support)	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
Community	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>

NW-Update	<a href="https://update.netwitness.com">https://update.netwitness.com</a>
LiveUI	<a href="https://live.netwitness.com">https://live.netwitness.com</a>

## Feedback zur Produktdokumentation

Sie können eine E-Mail an [nwdocsfeedback@netwitness.com](mailto:nwdocsfeedback@netwitness.com) senden, um Feedback zu der Dokumentation der NetWitness Platform zu geben.