NetWitness® Plattform

Version 12.4.0.0

Upgradehandbuch

NETWITNESS
Platform

Contact Information

NetWitness Community auf 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

Lizenzvereinbarung

Drittanbieterlizenzen

Hinweis zu Verschlüsselungstechnologien

Verteilung

Sonstiges

März 2024

Inhalt

Upgrade von NetWitness Platform

Dieses Dokument bietet Informationen über die Vorteile und den Prozess des Upgrades von NetWitness Platform auf 12.4. 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 nach dem Upgrade und Integritätsprüfungen durchführen, um den Upgrade-Vorgang erfolgreich 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: Die Versionen 11.7.x, 12.0 und 12.1 erreichten am 31. Dezember 2023 das Ende der Nutzungsdauer (End of Life, EOL). Weitere Informationen finden Sie unter https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. Wenn Sie ein Upgrade von den Versionen 11.7.x (Service Packs) oder 11.7.x.x (Patches) auf die Version 12.4.0.0 durchführen möchten, müssen Sie zunächst auf die Version 12.2.0.0 oder 12.3.0.0 aktualisieren, bevor Sie auf 12.4 aktualisieren.

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*.

Es gibt viele interessante neue Funktionen, die Sie nach dem Upgrade auf 12.4 aktivieren können. Eine detaillierte Beschreibung der neuen Funktionen in dieser Version finden Sie in den *Versionshinweisen zu NetWitness Platform 12.4*. 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 12.4

Die folgenden Upgradepfade werden für NetWitness 12.4 unterstützt:

- NetWitness 12.3.1.0 auf 12.4
- NetWitness 12.3.0.0 auf 12.4
- NetWitness 12.2.0.1 auf 12.4
- NetWitness 12.2.0.0 auf 12.4

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.

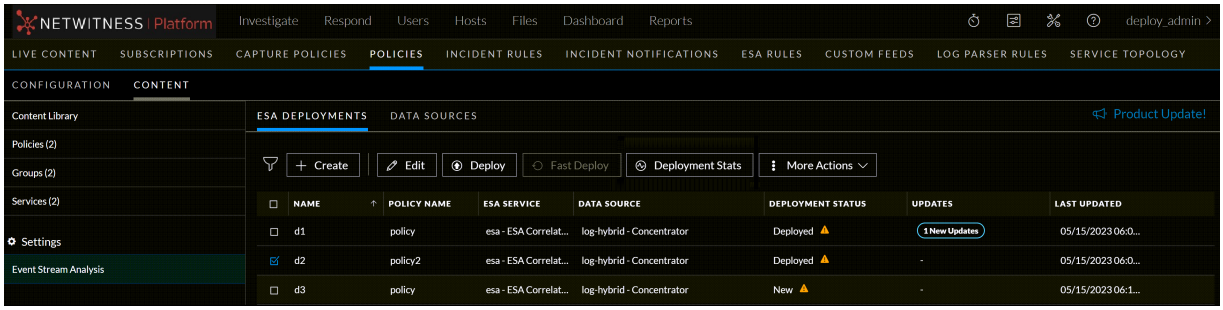
Weitere Informationen finden Sie im Thema **Ausführen im gemischten Modus** im *NetWitness – Leitfaden für die ersten Schritte mit Hosts und Services*.

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.

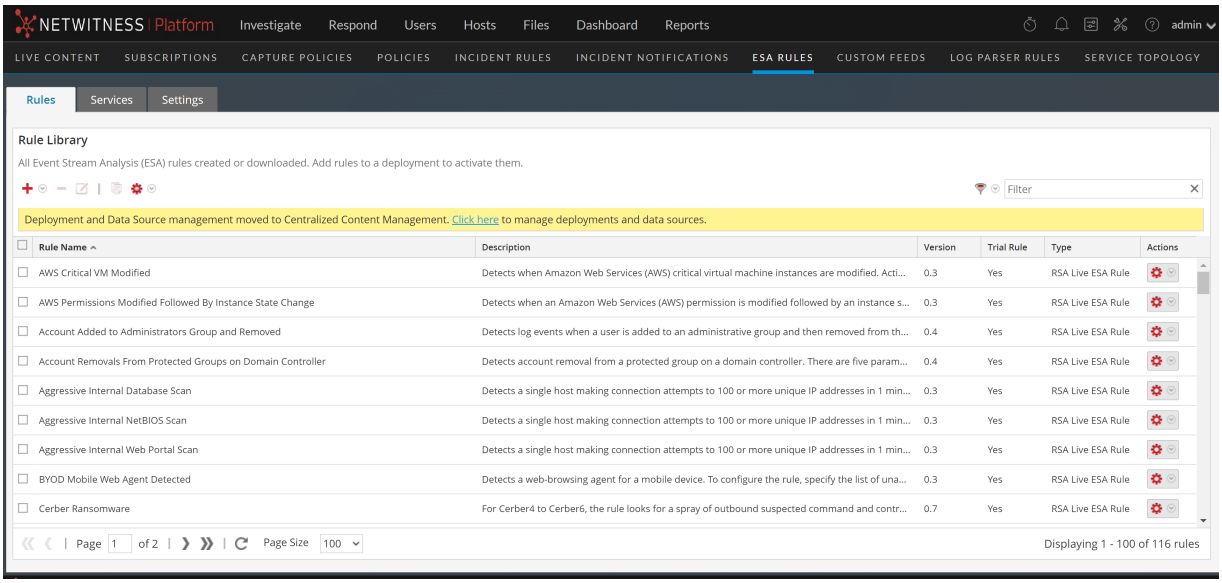
Überlegungen zum Upgrade von ESA-Hosts

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**) > **Policys** > **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 12.4 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 12.4 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

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

Ausführen der Upgrade-Vorabprüfungen

Sie müssen vor dem Upgrade auf NetWitness Platform 12.4 die Upgrade-Vorabprüfungen durchführen, um alle Probleme zu identifizieren, die zu einem Upgrade-Fehler führen können.

So führen Sie die Prüfungen vor dem Upgrade durch:

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“ Plausibilitätsprüfungen für die Liste von Tests in der Checkliste für die Betriebssystemmigration durchführen.
   b. `nw-precheck-tool-standalone upgrade-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Plausibilitätsprüfungen für die Liste von Tests in der Checkliste zur Aktualisierung durchführen.
   c. `nw-precheck-tool-standalone network-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Plausibilitätsprüfungen für die Liste von Tests in der Netzwerk-Checkliste durchführen.
   d. `nw-precheck-tool-standalone cert-checklist`: Mit diesem Befehl kann das Tool „Upgrade Precheck“ Plausibilitätsprüfungen für die Liste von Tests in der Zertifikat-Checkliste durchführen.

Checkliste für die Betriebssystemmigration

Das Tool „Upgrade Precheck“ führt die Plausibilitätsprüfungen für die folgende Liste von Tests 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 PacketHybrid über mehrere Versionen des Pakets "kernel-devel" verfügen 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.

Checkliste zur Aktualisierung

Das Tool „Upgrade Precheck“ führt die Plausibilitätsprüfungen für die folgende Liste von Tests 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 Plausibilitätsprüfungen für die folgende Liste von Tests 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 Plausibilitätsprüfungen für die folgende Liste von Tests 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 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 12.4 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.

c. umount<btrfs-Partitionspfad>. Sie können die BTRFS-Partitionsinformationen mit den Befehlen `/etc/fstab or df -hT` abrufen.

d. Entfernen Sie die BTRFS-Partition aus `/etc/fstab`.

e. 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.

f. Lösen Sie das Upgrade aus bzw. lösen Sie es erneut aus.

Weitere Informationen finden Sie im KB-Artikel „Upgrade auf das Alma-Betriebssystem, wenn das BTRFS-Dateisystem gemountet ist.“

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 nwwarehouseconnector
> ```

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 12.4 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 „Use AVX Instruction Set for MongoDB 5.0 Platform Support“.

> **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 12.4 (AlmaLinux) durchführen. Zunächst 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. (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.

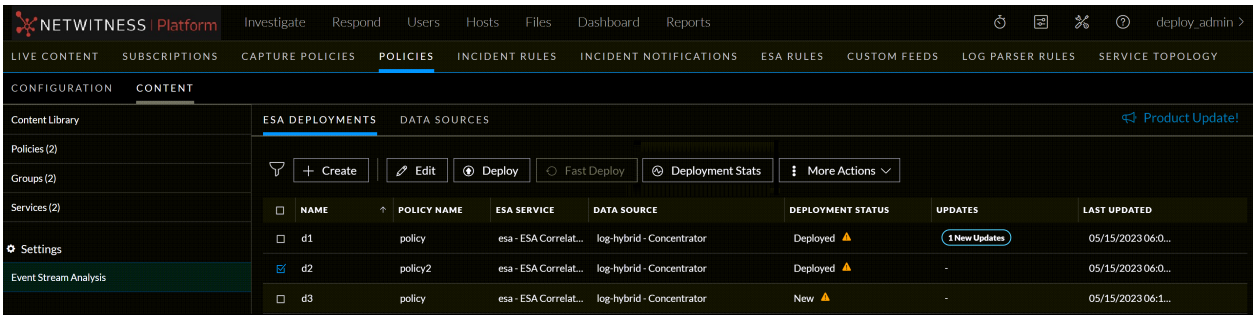
   ```
   nw-repo-tool --purge-obsolete
   ```

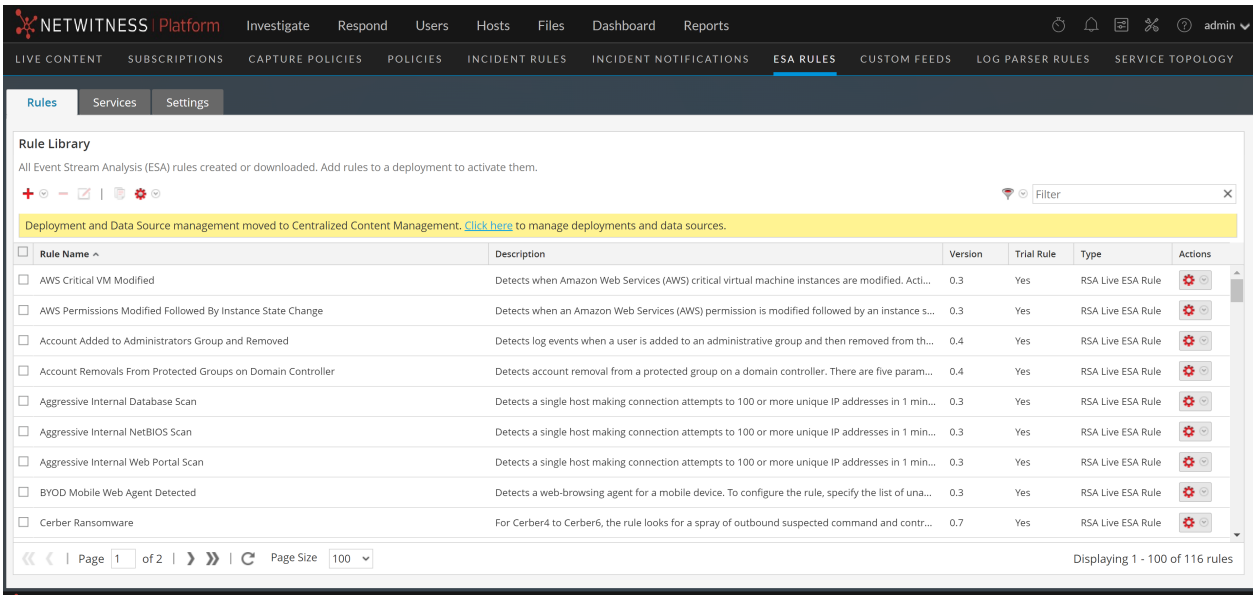
Aufgabe 3. Vorbereiten der ESA-Bereitstellungen für die Migration zu 12.4

Vor dem Upgrade auf 12.4 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 12.4 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 12.4 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**) > **Policys** > **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.





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.

SlNo	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 integre 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. 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 12.4 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 12.4 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 5. (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 6. (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 7. 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.

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

1. Konfigurieren Sie den NTP-Server.

Weitere Informationen finden Sie unter **Konfigurieren des NTP-Servers** im Systemkonfigurationsleitfaden.

2. Führen Sie die folgenden Schritte durch:

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

b. Führen Sie folgende Befehle aus.

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

Durchführen der Upgrade-Aufgaben

Kunden müssen zunächst das Standalone-RPM über https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096 herunterladen, die Anweisungen zur Installation des Standalone-RPM in der Readme-Datei nachlesen und dann die Vorabprüfung durchführen. Weitere Einzelheiten finden Sie im Abschnitt „Durchführen von Prüfungen vor dem Upgrade“.

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 12.4**“ 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 12.4 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:

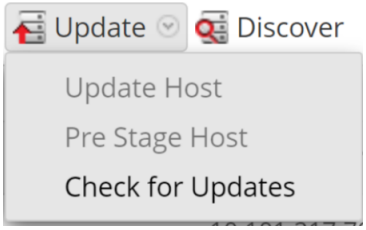
- Sie müssen den NW-Serverhost zuerst aktualisieren.
- Sie können nur eine Version anwenden, die mit der vorhandenen Hostversion kompatibel ist.
- Der NW-Server, der primäre ESA-Host, der sekundäre ESA-Host und der Analysten-UI-Host müssen alle mit derselben NetWitness Platform-Version arbeiten.

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 Netzwerkrichtlinien überprüfen, bevor Sie das Upgrade-Paket herunterladen, das etwa 11,7 GB groß ist. Wenn Sie eine Richtlinie eingerichtet haben, die das Herunterladen von Dateien mit mehr als 10 GB verbietet, 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.

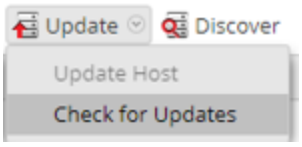


Voraussetzungen

1. Die Option **Informationen über neue Aktualisierungen täglich automatisch herunterladen** ist aktiviert und wird in **(Admin) > System > Aktualisierungen** angewendet.
2. 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.
3. 12.4 ist in der Spalte **Update-Version** verfügbar.

So aktualisieren Sie von 12.2.0.0, 12.2.0.1, 12.3.0.0, und 12.3.1.0 auf 12.4:

1. Navigieren Sie zu **(Admin) > Hosts**.
2. Wählen Sie den NW Server (`nw-server`)-Host aus.
3. 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.

4. Wählen Sie **12.4** 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.

5. Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host ermitteln**.
6. Klicken Sie auf **Update beginnen**.
7. Klicken Sie auf **Host neu starten**.
8. 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-12.4.0.0.zip` von der NetWitness Community (https://community.netwitness.com/) > **Downloads** > **NetWitness Platform** > **Version 12.4** in ein lokales Verzeichnis herunter:
   - Wenn Sie ein Upgrade von 12.2.0.0, 12.2.0.1, 12.3.0.0, und 12.3.1.0 durchführen, laden Sie `netwitness-12.4.0.0.zip` herunter.
2. Stellen Sie über SSH eine Verbindung mit dem NW-Serverhost her.
3. Laden `netwitness-12.4.0.0.zip` nach `/var/netwitness/common/update-stage/` auf dem NW-Serverhost hoch.
   Beispiel:

   ```
   mv /var/netwitness/tmp/netwitness-12.4.0.0.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.

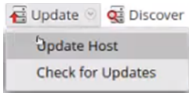
   „Update-Pakete können initialisiert werden" wird angezeigt, wenn Folgendes zutrifft:
   - NetWitness Platform kann auf die Upgrade-Pakete zugreifen.
   - Die Pakets ist vollständig und fehlerfrei.

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, und 12.3.1.0 auf 12.4 durchführen, laden Sie Folgendes herunter:

  ```
  netwitness-12.4.0.0.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 12.4.0.0 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/12.4.0.0/`
  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-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
  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 12.4.0.0-Pakets in das Verzeichnis `/var/netwitness/tmp/` auf dem NetWitness-Server.
  Führen Sie anschließend den folgenden Befehl aus, um die ZIP-Dateien der Version 12.4.0.0 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 12.4.0.0
  ```
  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 12.4.0.0 (mit Option 2) fehlschlägt, führen Sie den Befehl `upgrade-cli-client --init --version 12.4.0.0 --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 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`

3. Aktualisieren Sie den NW-Server-Host mit dem folgenden Befehl:
   `upgrade-cli-client --upgrade --version 12.4.0.0 --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 8.9).

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.

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 8.9 (Midnight Oncilla)`

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 *12.4Upgrade-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 12.4.0.0 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** und **12.3.1.0** durchführen, müssen Sie nur 12.4.0.0 bereitstellen.
     - **Option 1 (manuell)** : Melden Sie sich bei NetWitness-Server an und erstellen Sie das folgende Verzeichnis:

`/var/netwitness/tmp/upgrade/12.4.0.0/`
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-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0
```

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 12.4.0.0-Pakets in das Verzeichnis `/var/netwitness/tmp/` auf dem NetWitness-Server.
  Führen Sie anschließend den folgenden Befehl aus, um die ZIP-Dateien der Version 12.4.0.0 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 12.4.0.0
```

  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 12.4.0.0 (mit Option 2) fehlschlägt, führen Sie den Befehl `upgrade-cli-client --init --version 12.4.0.0 --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 12.4.0.0 --stage-dir
/var/netwitness/tmp/upgrade
```

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

```
upgrade-cli-client --upgrade --version 12.4.0.0 --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 8.9).

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.

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 8.9 (Midnight Oncilla)`

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

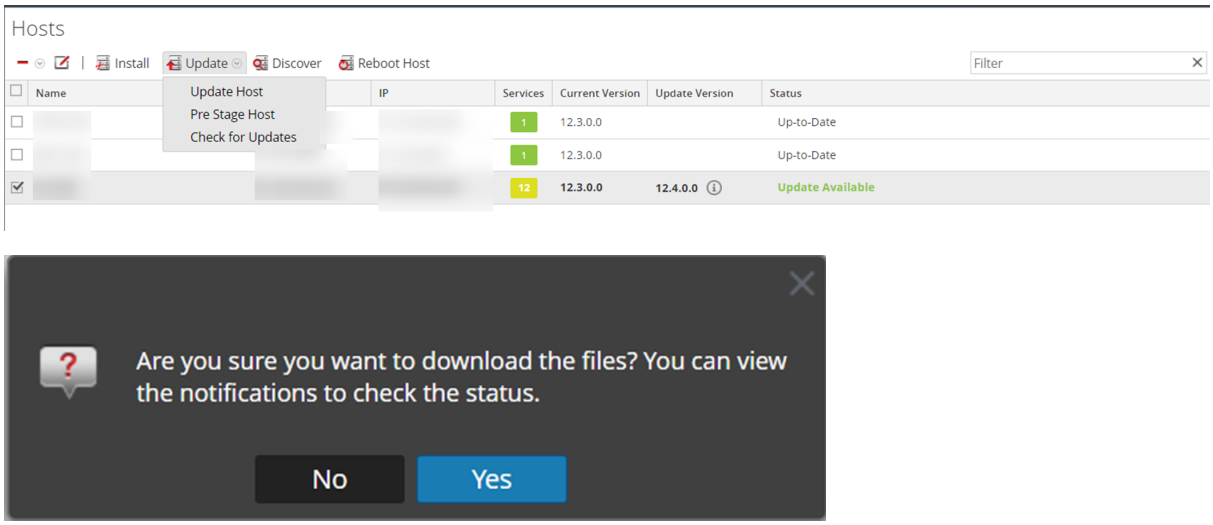
Sie können das Upgrade-Repository vorab bereitstellen, indem Sie die erforderlichen Pakete (.zip) herunterladen, ohne dass dies Auswirkungen auf das System hat. Dadurch wird die Upgrade-Ausfallzeit minimiert und sichergestellt, dass das Upgrade innerhalb des geplanten Zeitraums abgeschlossen wird.

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**.

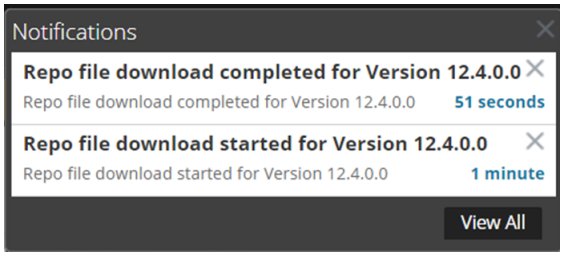
   Alle möglichen Update-Versionen werden in der Drop-down-Liste „Versionen" angezeigt.
3. Klicken Sie auf **Update** > **Vorab bereitgestellter Host** und wählen Sie die Version in der Spalte „Update-Version" aus.

   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.

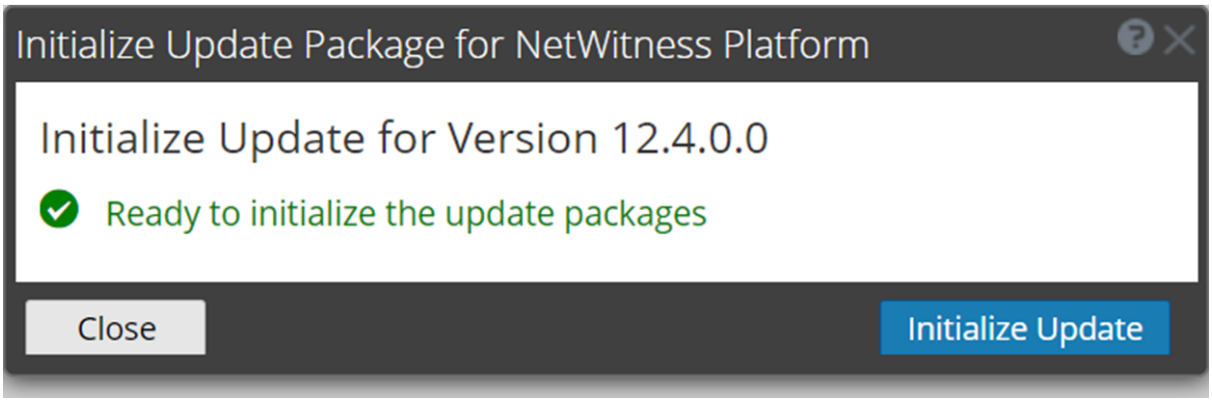
   Die Optionen **Vorab bereitgestellter Host** und **Host aktualisieren** werden deaktiviert, bis die Vorabbereitstellung abgeschlossen ist.



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

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 Thema **Verwalten benutzerdefinierter Hosteinträge** im Systemwartungshandbuch.

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:

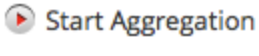
1. Navigieren Sie im Menü von NetWitness Platform zu  (Admin) > **Services**.
   Die Ansicht **Services** wird angezeigt.
2. Wählen Sie die einzelnen**Decoder**-Services aus.

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 für ESA-Hosts in NetWitness Platform Version 11.6 und höher nicht unterstützt. Der NetWitness-Server, der primäre ESA-Host und der sekundäre ESA-Host müssen alle mit derselben NetWitness Platform-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 12.4 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 12.4 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 12.4 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 12.4 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**)> **Policys** 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.

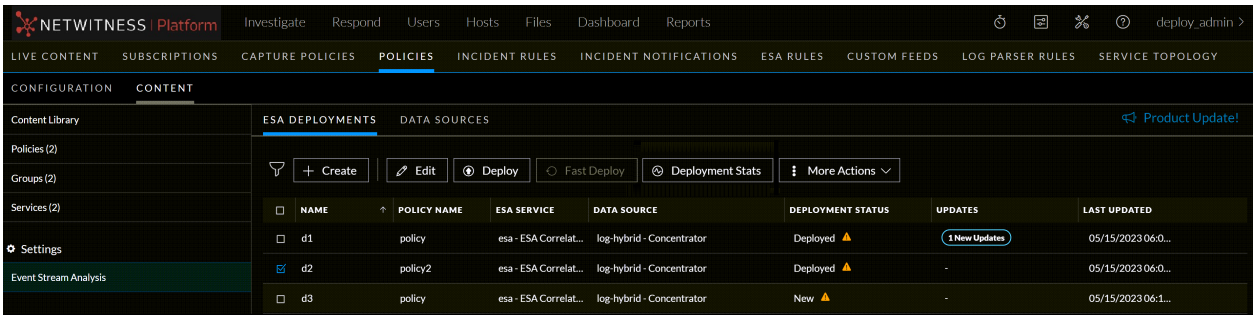
SINo	Bereitstellungsstatus vor dem Upgrade	Bereitstellungsstatus nach dem Upgrade		
		Erstellt Policy	Erstellt Gruppe	Die Policy wird veröffentlicht
1	Fehlerfreie Bereitstellung	Ja	Ja	Ja

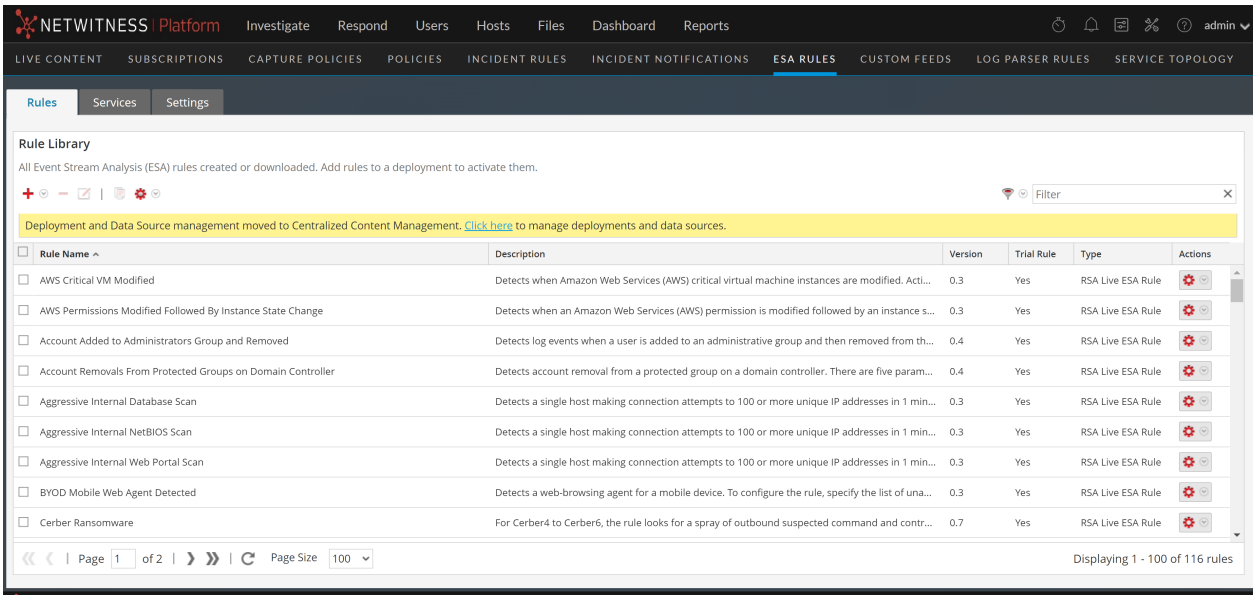
SINo	Bereitstellungsstatus vor dem Upgrade	Bereitstellungsstatus nach dem Upgrade		
		Erstellt Policy	Erstellt Gruppe	Die Policy wird veröffentlicht
2	Bereitstellung mit Fehlern	Ja	Ja	Ja
3	Bereitstellung nur mit Regeln	Ja	Nein	Nein
4	Bereitstellung ohne Regeln	Nein	Nein	Nein

(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**) > **Policys** > **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.

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 12.4 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 12.4 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 12.4 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.

1. Aktualisieren Sie die UEBA-Konfiguration, indem Sie den folgenden Befehl auf dem UEBA-Computer ausführen.

   - `source /etc/sysconfig/airflow`
   - `source $AIRFLOW_VENV/bin/activate`
   - `python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/resources/rerun_ueba_server_config.py`
   - `deactivate`

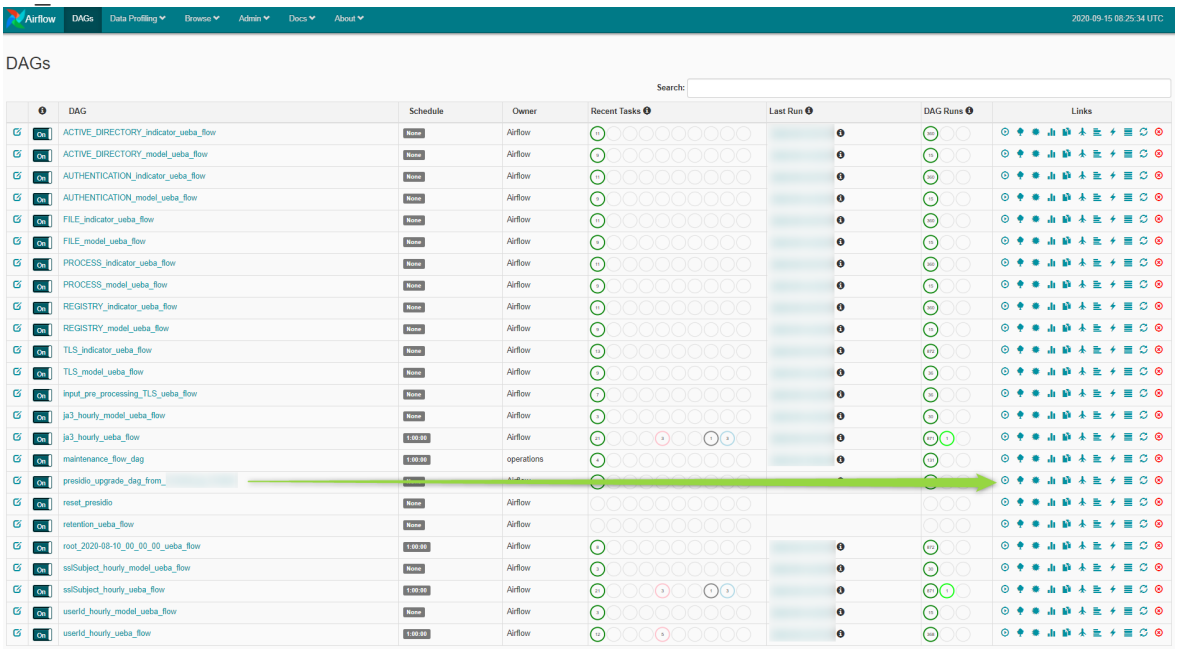
2. (Optional) Aktualisieren des UEBA-Verarbeitungsschemas, falls erforderlich.

   NetWitness empfiehlt, das UEBA-Startdatum auf ein Datum festzulegen, das 28 Tage vor dem aktuellen Datum liegt. Bei UEBA-Systemen, die TLS-Daten verarbeiten sollen, müssen Sie sicherstellen, dass das Startdatum nicht auf ein Datum festgelegt ist, das weniger als 14 Tage vor dem aktuellen Datum liegt.

   Weitere Informationen finden Sie im Abschnitt „reset-presidio-Skript“ im *UEBA-Konfigurationshandbuch*.

3. Führen Sie die Airflow-Upgrade-DAG aus.

   - Navigieren Sie zur Airflow-Hauptseite `https://<UEBA-host-name>/admin`
   - Geben Sie den Admin-Benutzernamen und das entsprechende Kennwort ein.
   - Klicken Sie auf **Wiedergeben** in `presidio_upgrade_dag_from_<previous_version>_to_12.4`.

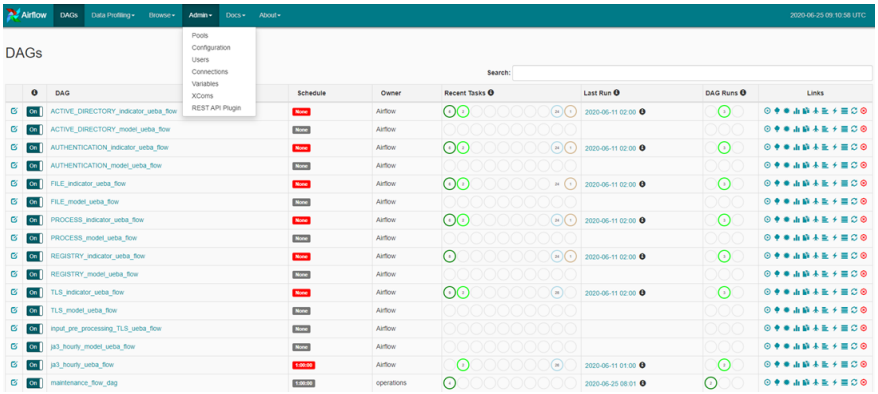


Hinweis: Während des Upgrades wird ein hellgrüner Kreis neben der Upgrade-DAG-Zeile angezeigt. Wenn der Upgrade-Prozess erfolgreich abgeschlossen ist, ändert sich der hellgrüne Kreis in einen grünen Kreis. Wenn der Upgrade-Prozess fehlschlägt, ändert sich der hellgrüne Kreis in einen roten Kreis.

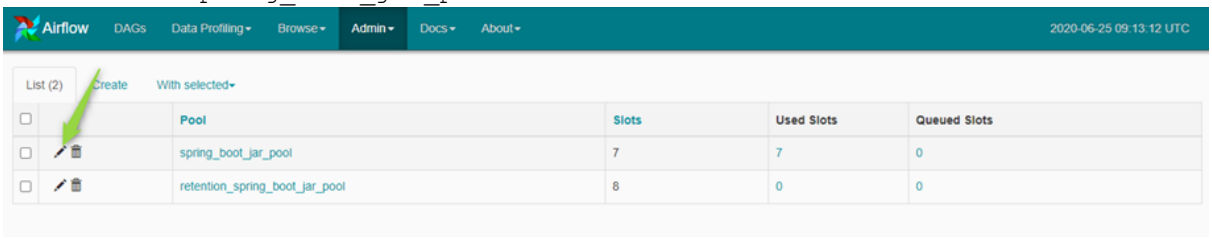
4. Legen Sie die entsprechenden „Boot Jar Pools”-Slots fest:
   - **Physische Appliance**: Aktualisieren Sie den `spring_boot_jar_pool`-Slot-Wert auf 18.
   - **Virtuelle Appliance**: Aktualisieren Sie den `spring_boot_jar_pool`-Slot-Wert auf 22.
     Um die **Spring Boot Jar Pools**-Slots zu aktualisieren, 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 in SA 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.

Durchführen von Plausibilitätsprüfungen nach dem Upgrade

Nach dem Upgrade auf NetWitness 12.4 müssen Sie die folgenden Plausibilitätsprüfungen 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** eine 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** > **Alarme** 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 Policys 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 12.4-Relay-Servers

WICHTIG: Nach dem Upgrade von EPLH von den Versionen 12.2.xx und 12.3.xx auf 12.4 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 12.4-Relay-Server installieren:
  1. Upgrade von NetWitness Platform XDR.
  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.

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

- Informationen zum Troubleshooting beim AlmaLinux-Betriebssystem
- Fehler: deploy_admin-Kennwort abgelaufen
- Downloadfehler
- Fehler beim Bereitstellen der Version <Versionsnummer> Update-Pakete fehlen
- Fehler: Upgrade fehlgeschlagen
- 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
- Reporting Engine startet nach Upgrade neu

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

Problem	Neustart der Appliance nach der Aktualisierung nicht möglich
Workaround	1. Um den Neustart zu erzwingen, ändern Sie die GRUB-Bootzeile manuell in `FIPS=0`. 2. Dann deaktivieren Sie FIPS mit dem folgenden Befehl: `manage-stig-controls --disable-control-groups 3 --host-all`

3. Überprüfen Sie, ob die Zeile `FIPS=1` aus `/boot/grub2/grub.cfg` entfernt wurde
   - 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)

   Protokoll werden hier 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 Datums-/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: 12.4.0.0

xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.4.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.4.0.0-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 12.4

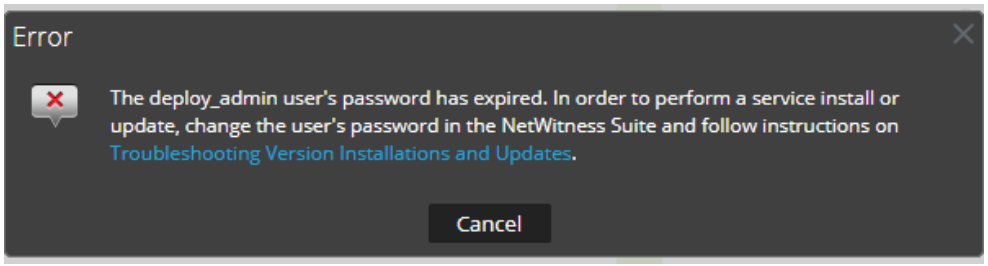
   Sobald die Betriebssystemmigration abgeschlossen ist, beginnt das NW-Software-Upgrade und es dauert bis zu 30 Minuten, bevor die Benutzeroberfläche funktionsfähig ist.

   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 12.4.0.0

   xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching for yum config for version: 12.4.0.0

   xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2] Retrieving yum config for version: 12.4.0.0

   xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv 'base', ** done ** 'config/12.4.0.0-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
   ```

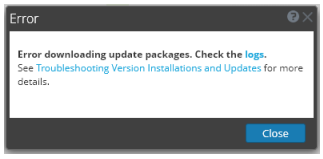
   Sie können auch die Konfigurationsverwaltungsprotokolle unter `/var/log/netwitness/config-management/chef-solo.log` oder die Benutzeroberflächenprotokolle `/var/netwitness/uax/logs/sa.log` einsehen.

Fehler: deploy_admin-Benutzerkennwort abgelaufen

Fehlermeldung	
Ursache	Das `deploy_admin`-Benutzerkennwort ist abgelaufen.

Lösung	Setzen Sie Ihr `deploy_admin`-Kennwort zurück. Gehen Sie wie folgt vor.
	1. Führen Sie den folgenden Befehl nur auf dem NW-Serverhost aus.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. Überprüfen Sie die Ausgabe des Befehls `nw-manage --update-deploy-admin-pw`, um sicher zu vergewissern, dass das `deploy_admin`-Kennwort auf allen Hosts erfolgreich aktualisiert wurde. Wenn ein NW-Host nicht funktioniert oder aus irgendeinem Grund ausfällt, wie in der Ausgabe des Befehls `nw-manage --update-deploy-admin-pw` ersichtlich, führen Sie `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` aus, um das Kennwort zwischen dem NW-Server und dem ausgefallenen Host zu synchronisieren, sobald der Kommunikationsfehler behoben ist.
	3. Führen Sie auf dem Host, auf dem die Installation oder Orchestrierung fehlgeschlagen ist, den Befehl `nwsetup-tui` aus und verwenden Sie das neue **deploy_admin**-Kennwort als Antwort auf die Aufforderung zur Eingabe des **Bereitstellungskennworts**.

Downloadfehler

Fehlermeldung	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren** > **Host aktualisieren** klicken, wird der Download zwar gestartet, kann aber nicht abgeschlossen werden.
Ursache	Die Downloaddateien der Version können groß sein und das Herunterladen kann daher lange dauern. Wenn beim Download Kommunikationsprobleme auftreten, schlägt er fehl.
Lösung	1. Versuchen Sie erneut, ein Update durchzuführen. 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 *Upgrade-Leitfaden für NetWitness Platform* beschrieben. Navigieren Sie zur Seite NetWitness All Versions Documents und suchen Sie nach NetWitness Platform-Anleitungen zur Behebung von Problemen. 3. Wenn Sie immer noch kein Update durchführen können, wenden Sie sich an den Kundensupport.

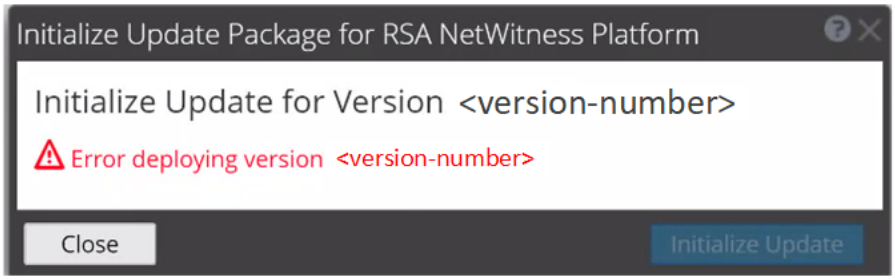
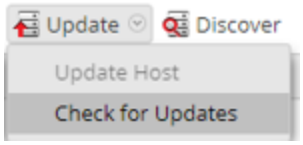
Fehlermeldung	Wenn Sie ein Upgrade von NetWitness Platform 11.x.x.x auf 11.6.x.x oder höher durchführen, schlägt das Offline-Benutzeroberflächen-Upgrade mit der Meldung Downloadfehler fehl.

Lösung	1. Gehen Sie in der Befehlszeilenschnittstelle (CLI) wie folgt vor:
	a. Stellen Sie über SSH eine Verbindung mit dem NW-Server her.
	b. Führen Sie den folgenden Befehl aus:
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`
	`For example:`
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	2. Nachdem der NW-Server erfolgreich aktualisiert wurde, melden Sie sich bei der NW-Server-Benutzeroberfläche an und navigieren Sie zu **(Admin)** > **Hosts**. Dort werden Sie aufgefordert, den Host neu zu starten.
	3. Klicken Sie auf **Host neu starten** in der Symbolleiste.
	So aktualisieren Sie alle anderen Hosts direkt über die Benutzeroberfläche:

	1. Klicken Sie im Dialogfeld **Update verfügbar** auf **Update beginnen**. Nachdem der Host aktualisiert wurde, werden Sie aufgefordert, den Host neu zu starten. 2. Klicken Sie auf **Host neu starten** in der Symbolleiste.

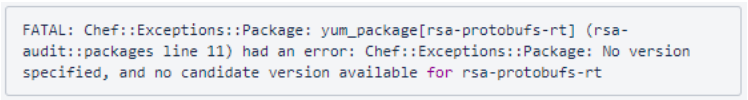
Fehler beim Bereitstellen der Version <Versionsnummer>

Update-Pakete fehlen

Fehlermeldung	
Problem	Wenn das Update-Paket beschädigt ist, wird Fehler beim Bereitstellen der Version <Versionsnummer> im Dialogfeld **Update-Paket für NetWitness Platform initialisieren** angezeigt, nachdem Sie auf **Update initialisieren** geklickt haben.
Lösung	1. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen. 2. Entfernen Sie den Versionsordner wurde aus dem Bereitstellungsordner. 3. Stellen Sie sicher, dass der Salt-Master-Service ausgeführt wird. 4. Kopieren Sie die ZIP-Datei mit dem Update-Paket in den Bereitstellungsordner. 5. Wählen Sie in der Symbolleiste **Hosts** der Ansicht erneut **Nach Updates suchen** aus.  6. Klicken Sie auf **Update initialisieren**. 7. Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host aktualisieren**. 8. Klicken Sie im Dialogfeld **Update verfügbar** auf **Update starten**. Nachdem der Host aktualisiert wurde, werden Sie aufgefordert, den Host neu zu starten. 9. Klicken Sie in der Symbolleiste auf **Neustart**.

Fehler: Upgrade fehlgeschlagen

Fehlermeldung	Beim Versuch, auf Version 11.6 oder höher zu aktualisieren, wird im Fehlerprotokoll eine Fehlermeldung angezeigt, die der folgenden ähnelt:

Ursache	 Benutzerdefinierte Builds/RPMs für bestimmte Komponenten, die auf Hosts installiert werden, z. B. bei der Installation von Hotfixes.

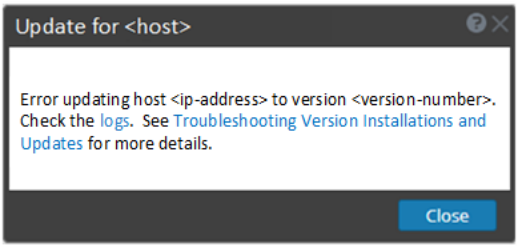
Lösung	**So lösen Sie das Problem**
	1. Stellen Sie über SSH eine Verbindung mit dem Admin-Server her.
	2. Suchen Sie die Komponentendeskriptordatei, indem Sie den folgenden Befehl ausführen.
	`cd /etc/netwitness/component-descriptor/`
	3. Öffnen Sie die Komponentendeskriptordatei, indem Sie den folgenden Befehl ausführen.
	`vi nw-component-descriptor. json`
	4. Suchen Sie im Abschnitt „packages” nach der Komponente mit einem benutzerdefinierten Build/RPM. Unten sehen Sie beispielsweise die Paketdetails für den „Concentrator“-Host mit benutzerdefiniertem Build/RPM.
	`“concentrator”: {`
	`“cookbook_name”: “rsa-concentrator”,`
	`“service_names”: [“rsa-nw-concentrator”],`
	`“family”: “launch”,`
	`“default_port”: xxxx, “description”: “Concentrator”,`
	`“packages”:[{ “name”: “rsa-nw-concentrator”,`
	`“version” : “11.6.0.0-2003001075220.5.cecf24b.e.17.centos”`
	`},`
	5. Löschen Sie alle Versionsangaben einschließlich des Zeichens (,) aus dem Abschnitt „packages”. Nachdem Sie die Versionsangaben gelöscht haben, sollte er zum Beispiel wie folgt aussehen.
	`“packages”: [{`
	`“name”: “rsa-nw-concentrator”`
	`},`
	Hinweis: Sie müssen die Versionsdetails für alle Hosts löschen, die über benutzerdefinierte Builds/RPMs im Komponentendeskriptor des Admin-Servers verfügen.
	6. Führen Sie den Upgrade-Vorgang erneut durch.

Fehler beim Aktualisieren des externen Repository

Fehlermeldung	Sie erhalten eine Fehlermeldung ähnlich der folgenden Fehlermeldung, während Sie versuchen, auf eine neue Version zu aktualisieren:

	`.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
Ursache	Falscher Pfad angegeben.
Lösung	Achten Sie auf Folgendes: • Die URL ist auf dem NW-Serverhost vorhanden. • Sie haben den richtigen Pfad verwendet und alle Leerzeichen daraus entfernt.

Fehler: Hostaktualisierung fehlgeschlagen

Fehlermeldung	
Problem	Wenn Sie eine Aktualisierungsversion auswählen und auf **Aktualisieren** >**Host aktualisieren** klicken, ist zwar der Download erfolgreich, aber die Aktualisierung schlägt fehl.

Lösung	1. Versuchen Sie erneut, das Versionsupdate auf den Host anzuwenden. Oft ist das alles, was Sie tun müssen.
	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 `tail -f` über die Befehlszeile aus):
	`/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`
	Der Fehler erscheint in mindestens einem dieser Protokolle.
	3. Wenn Sie das Update immer noch nicht anwenden können, sammeln Sie die Protokolle aus **Schritt 2** oben und wenden Sie sich an den Kundensupport.

Fehlermeldung	

Problem	Wenn Sie eine Update-Version auswählen und auf **Aktualisieren** > **Auf Updates prüfen** klicken, wird die Fehlermeldung **Nicht autorisiert** angezeigt. Infolgedessen schlägt die Verbindung zum Live-Dienst fehl.

Lösung	1. Stellen Sie sicher, dass die Live-Testverbindung erfolgreich ist.
	2. Aktualisieren Sie https://update.netwitness.com/RSA-netwitness in **(Admin)** > **System** > **Updates**.
	3. Stellen Sie über SSH eine Verbindung mit dem Admin-Server her und erstellen Sie ein Backup von `/etc/default/jetty`.
	4. Aktualisieren Sie den folgenden Eintrag am Ende von JAVA_OPTIONS in `/etc/default/jetty`.
	`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 "`
	5. Starten Sie den Jetty-Service neu. Führen Sie den folgenden Befehl aus.
	`service jetty restart`

Fehler: Update-Pakete fehlen

Fehlermeldung	**Initialisieren Sie das Update für Version xx.x.x.x** Die folgenden Update-Pakete fehlen Pakete vom NetWitness-Link herunterladen
Problem	Die folgenden Update-Pakete fehlen wird im Dialogfeld **Update-Paket für NetWitness Platform initialisieren** angezeigt, wenn Sie einen Host über die Ansicht **Hosts** offline aktualisieren und im Bereitstellungsordner Pakete fehlen.
Lösung	1. Klicken Sie im Dialogfeld Update-Paket für NetWitness Platform initialisieren auf **Pakete von der NetWitness-Community herunterladen**. Die NetWitness-Community-Seite, die die Update-Dateien für die ausgewählte Version enthält, wird angezeigt. 2. Wählen Sie die im Bereitstellungsordner fehlenden Pakte aus. Das Dialogfeld **Update-Paket für NetWitness Platform initialisieren** wird angezeigt und enthält die Meldung, dass das System bereit ist, die Aktualisierungspakete zu initialisieren.

Fehler: Patch-Update für Nicht-NW-Server

Fehlermeldung	Das Protokoll `/var/log/netwitness/orchestration-server/orchestration-server.log` enthält einen ähnlichen Fehler wie den folgenden: **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version`**

Problem	`'11.x.x.n' is not supported` Nach der Aktualisierung des NW-Serverhosts auf eine bestimmte Version müssen Sie ist alle Nicht-NW-Serverhosts auf dieselbe Version aktualisieren. Wenn Sie beispielsweise den NW-Server von 11.4.0.0 auf 11.6.0.0 oder höher aktualisieren, können die Nicht-NW-Server-Hosts nur dieselbe Version (d. h. 11.6.0.0) aktualisiert werden. Wenn Sie versuchen, einen Nicht-NW-Serverhost auf eine andere Version zu aktualisieren (z. B. von 11.4.0.0 auf 11.4.x.x), erhalten Sie diesen Fehler.
Lösung	Führen Sie eine der folgenden Aktionen aus: • Aktualisieren Sie die Nicht-NW-Serverhosts auf Version 11.6.0.0 oder höher oder • Aktualisieren Sie den Nicht-NW-Serverhost nicht (behalten sie die aktuelle Version bei)

Fehler: Host-Neustart nach Update über die Befehlszeile

Fehlermeldung	In der Benutzeroberfläche wird eine Meldung mit der Aufforderung angezeigt, den Host nach dem Update offline neu zu starten. SA Server IP-Address 8 version-number Reboot Host
Ursache	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.
Lösung	Starten Sie den Host in der Ansicht **Host** der Benutzeroberfläche neu.

Reporting Engine startet nach Upgrade neu

Problem	In einigen Fällen versucht der Reporting Engine-Dienst nach einem Upgrade von 11.x (z. B. 11.4) auf 11.6 oder höher fortlaufend erfolglos, neu zu starten.
Ursache	Die Datenbankdateien für Live-Diagramme, den Warnmeldungsstatus oder den Berichtsstatus werden möglicherweise nicht erfolgreich geladen, da die Dateien beschädigt sein können.
Lösung	**So lösen Sie das Problem** 1. Prüfen Sie, welche Datenbankdateien beschädigt sind: Navigieren Sie zu der Datei unter `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` und überprüfen Sie die folgenden Blöcke: • Wenn die Datenbankdatei für Live-Diagramme beschädigt ist, wird die folgende Meldung angezeigt:

Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

at org.h2.message.DbException.get(DbException.java:168)

org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database!

- Wenn die Datenbankdatei für den Warnmeldungsstatus beschädigt ist, wird die folgende Meldung angezeigt:

  Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

  org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

  at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

  at org.h2.message.DbException.get(DbException.java:168)

  org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'

- Wenn die Datenbankdatei für den Berichtsstatus beschädigt ist, wird die folgende Meldung angezeigt:

  ```
  org.h2.jdbc.JdbcSQLException: File corrupted while reading
  record: null. Possible solution: use the recovery tool
  [90030-196]
  ```

2. Um die Beschädigung der Datenbankdatei für Live-Diagramme zu beheben, gehen Sie wie folgt vor:
   a. Beenden Sie den Reporting Engine-Service.
   b. Verschieben Sie die Datei `livechart.mv.db` aus dem Ordner `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` an einen temporären Speicherort.
   c. Starten Sie den Reporting Engine-Service neu.

   Hinweis: Einige Live-Diagrammdaten können verloren gehen, wenn Sie die obigen Schritte ausführen.
3. Um eine Beschädigung der Datenbankdatei für den Warnmeldungs- oder Berichtsstatus zu beheben, gehen Sie wie folgt vor:
   a. Beenden Sie den Reporting Engine-Service.
   b. Ersetzen Sie die beschädigte Datenbankdatei durch die neueste Datei `alertstatusmanager.mv.db` bzw. `reportstatusmanager.mv.db` aus dem Ordner `/var/netwitness/reserver/rsa/soc/reporting-engine/archives`.

	c. Starten Sie den Reporting Engine-Service neu. Weitere Informationen finden Sie im Knowledge Base-Artikel Reporting Engine restarts After upgrade to NetWitness Platform 11.4.

Problem	Nach dem Upgrade auf Version 11.6 oder höher wird der Reporting Engine-Service nicht neu gestartet.
Ursache	Der Reporting Engine-Service kann aus einem der folgenden Gründe nicht gestartet werden. – workspace.xml wurde nicht aktualisiert. – Die Uhrzeit wird in der Livechart-H2-Datenbank nicht richtig konvertiert. – JCR (Jackrabbit-Repository) ist aufgrund einer Primärschlüsselverletzung beschädigt.

Lösung	Um das Problem zu beheben, führen Sie das Reporting Engine Migration Recovery Tool (`rsa-nw-re-migration-recovery.sh`) auf dem Admin-Server aus, auf dem der Reporting Engine-Service installiert ist.
	Hinweis: Sie finden das Reporting Engine Migration Recovery-Tool am folgenden Speicherort.
	`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`
	Beispiel:
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1. Stellen Sie über SSH eine Verbindung mit dem Admin-Server her.
	2. Entpacken Sie das RE-Tool (Reporting Engine) und führen Sie den folgenden Befehl aus.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	3. (Optional) Wenn Sie die RE-Tool-Datei in einem anderen Verzeichnis entpacken möchten, können Sie ein Verzeichnis erstellen und das RE-Tool entpacken. Führen Sie folgende Befehle aus.
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4. Führen Sie das Skript mit dem folgenden Befehl aus.
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`
	Weitere Informationen finden Sie im Knowledge Base-Artikel **Reporting Engine Migration Recovery Tool**.

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.

Fehlermeldung	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the`

	`passphrase.`
Ursache	Die Log Collector Lockbox konnte nach der Aktualisierung nicht geöffnet werden.
Lösung	Melden Sie sich bei NetWitness an und setzen Sie den Systemfingerabdruck zurück, indem Sie das Kennwort für den Systemstabilitätswert der Lockbox zurücksetzen, wie im Thema **Zurücksetzen des Systemstabilitätswerts** unter **Konfigurieren von Lockbox-Sicherheitseinstellungen** im *Protokollsammlung-Konfigurationsleitfaden* beschrieben.

Fehlermeldung	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Ursache	Die Log Collector Lockbox wird nach der Aktualisierung nicht konfiguriert.
Lösung	Wenn Sie eine Log Collector Lockbox verwenden, melden Sie sich bei NetWitness an und konfigurieren Sie die Lockbox wie im Thema **Konfigurieren von Lockbox-Sicherheitseinstellungen** im *Protokollsammlung-Konfigurationsleitfaden* beschrieben.

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

Fehlermeldung	Der Decoder versucht, mit der Erfassung von Ereignissen zu beginnen, schlägt jedoch fehl. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`
Ursache	Die Decoder-Erfassungskonfiguration ist nicht gültig für Kunden, die PF_RING Capture (CentOS) verwenden und ein direktes Upgrade auf 12.4 (AlmaLinux) durchführen. Zunächst müssen sie PF_RING-Geräte zu DPDK migrieren und dann ein Upgrade durchführen.
Lösung	**So lösen Sie das Problem** Anweisungen zur Migration finden Sie unter Migrieren von PF_RING-Geräten zu DPDK.

NW-Server

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

Problem	Nach dem Upgrade werden Sie Folgendes bemerken: • Audit-Protokolle werden nicht an das konfigurierte globale Audit-Setup weitergeleitet. • Die folgende Meldung erscheint in `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Ursache	Während der Migration der globalen Audit-Einrichtung des NW-Servers konnte nicht von 11.4.x.x oder 11.5.x.x zu 11.6.0.0 oder höher migriert werden.
Lösung	1. Stellen Sie über SSH eine Verbindung mit dem NW-Server her. 2. Senden Sie den folgenden Befehl: `orchestration-cli-client --update-admin-node`

Orchestrierung

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

Problem	1. Es wurde erfolglos versucht, ein Upgrade für einen Nicht-NW-Serverhost durchzuführen. 2. Das Upgrade für diesen Host wurde erneut gestartet und war wieder erfolglos. Die folgende Meldung wird im `orchestration-server.log` angezeigt. `"'file' _virtual_ returned False: cannot import name HASHES""`
Ursache	Es wurde eventuell ein Upgrade für Salt Minion durchgeführt und Salt Minion wurde auf dem fehlerhaften Nicht-NW-Serverhost nicht neu gestartet.

Lösung	1. Stellen Sie über SSH eine Verbindung zu dem Nicht-NW-Serverhost her, bei dem das Upgrade fehlgeschlagen ist.
	2. Senden Sie die folgenden Befehle.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Versuchen Sie das Upgrade des Nicht-NW-Serverhosts erneut.

Problem	Wenn Sie einen neuen 12.4 Core Node-X auf dem Admin-Server (Node-0), der von 12.0 oder älteren Versionen auf 12.4 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 **Services** in der Ansicht **Admin** > **Hosts** als inaktiv angezeigt. Infolgedessen können Sie in der Benutzeroberfläche nicht auf die Core-Services zugreifen. Dies gilt nicht, wenn Sie einen neuen 12.4-Core-Node-X auf dem neu installierten 12.4-Admin-Server orchestrieren (kein Upgrade von 12.0 oder älteren Versionen auf 12.4).
Ursache	Der 12.4 Core Node-X verwendet ein dediziertes SA-Server-Zertifikat anstelle des gemeinsamen Node-0-Knotenzertifikats unter seinen vertrauenswürdigen Peers, wenn er direkt auf einem aktualisierten 12.4-Admin-Server-Host orchestriert wird.

Lösung	Führen Sie die folgenden Befehle aus, bevor Sie ein Bootstrap für den 12.4-Core-Node-X-Host durchführen und ihn orchestrieren.
	`mkdir -p /etc/netwitness/platform`
	1.
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	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 12.4-Core-Node-X-Host durchgeführt und ihn orchestriert haben.
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	2.

	`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.

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

Event Stream Analysis

Problem	Nach dem Upgrade auf Version 12.4 oder höher aggregiert der ESA-Korrelationsserver keine Ereignisse aus den konfigurierten Datenquellen.
Fehlermeldung	`Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)`
Lösung	**So lösen Sie das Problem** Führen Sie folgende Schritte in der NetWitness-Benutzeroberfläche aus: 1. Navigieren Sie zu (**KONFIGURIEREN**) > **Policys** > **Inhalt** > **Event Stream Analysis** > **Datenquellen**. Der Bereich **Datenquellen** wird angezeigt. 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

Problem	• Der Legacy-Windows-Log Collector wird nach dem Upgrade von SA auf die Version 12.4 und dem Upgrade von Legacy-Windows-Log Collector auf die Versionen 11.6.x oder 11.7.x als inaktiv angezeigt. • Legacy-Windows-Log Collector wird als inaktiv angezeigt, wenn der Stack auf 12.4 aktualisiert wird.
Ursache	Zertifikat-Update im SA-Node.
Lösung	Weitere Informationen finden Sie im Abschnitt „Legacy-Windows-Log Collector“ unter Durchführen von Aufgaben nach dem Upgrade.

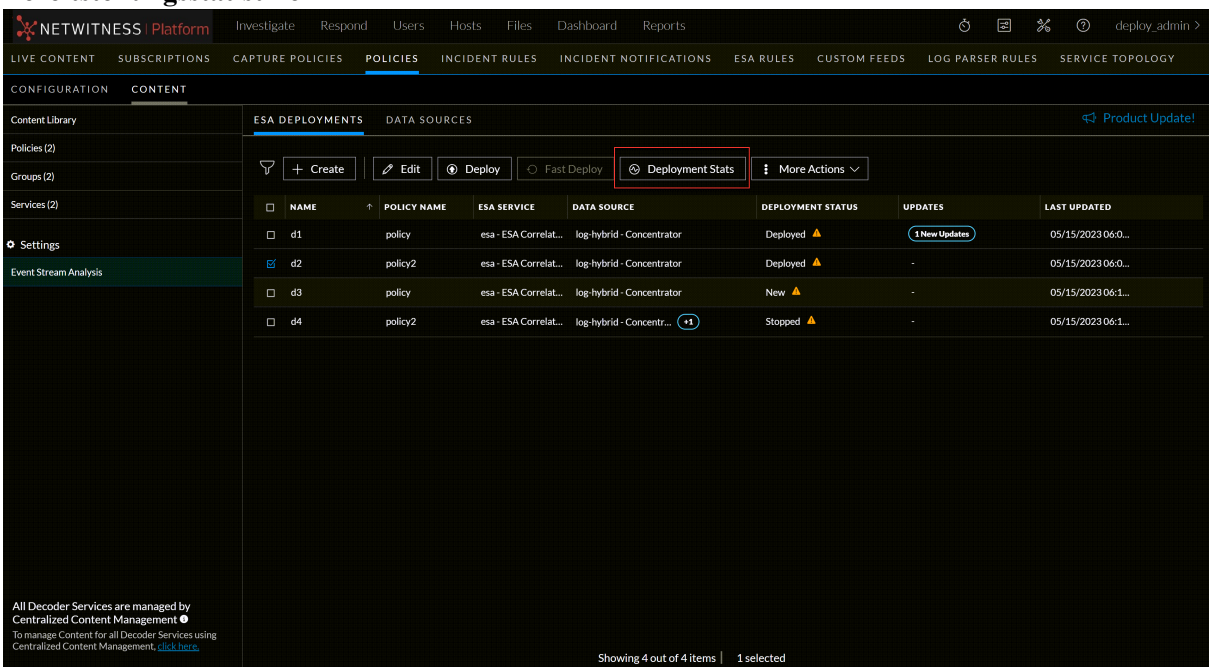
ESA-Troubleshooting-Informationen

ESA-Regeln erstellen keine Warnmeldungen

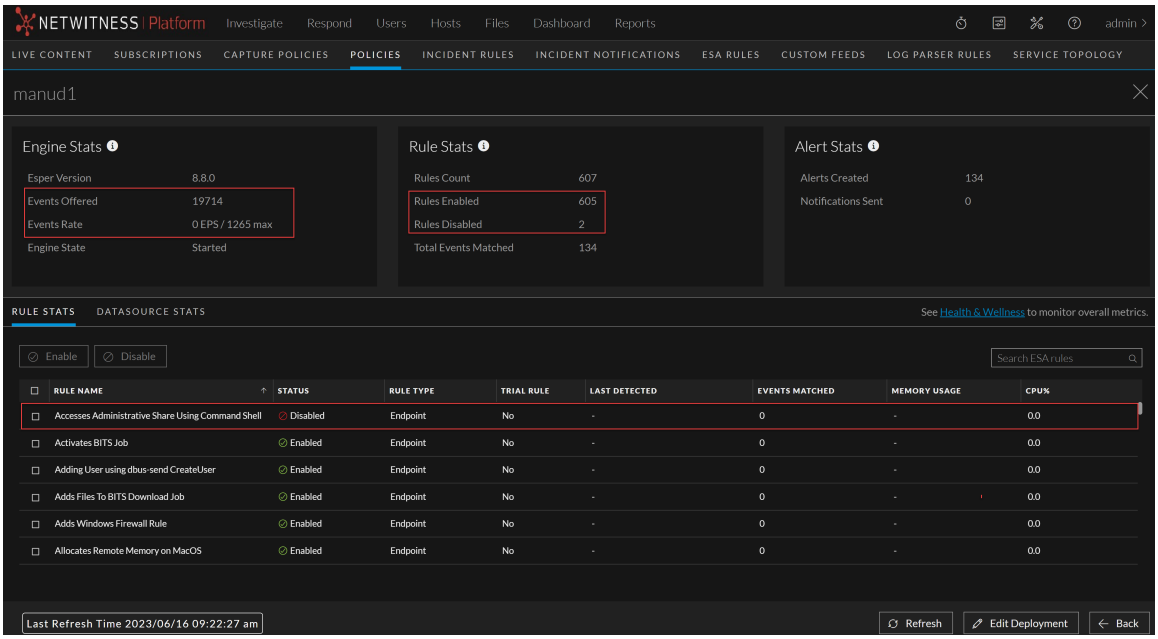
Wenn keine Warnmeldungen angezeigt werden, überprüfen Sie den Status der ESA-Regelbereitstellungen.

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

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



3. Die Seite „Bereitstellungsstatistiken“ wird geöffnet und zeigt den Status Ihrer ESA-Services und -Bereitstellungen an.
4. Gehen Sie für jede ESA-Regel-Bereitstellung wie folgt vor:
   a. 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.
   b. 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. Ein weißer Kreis zeigt deaktivierte Regeln an. 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-Korrelationsservice, 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 11.4 oder höher 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-Korrelationsservers für fehlende Metaschlüssel

Wenn in den Fehlerprotokollen des ESA-Korrelationsservers 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	https://community.netwitness.com Klicken Sie im Hauptmenü auf **Support > Portal für Support-Fälle > Meine Fälle anzeigen**.
Internationale Kontakte (So kontaktieren Sie den NetWitness-Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

NW-Update	https://update.netwitness.com
LiveUI	https://live.netwitness.com

Feedback zur Produktdokumentation

Sie können eine E-Mail an nwdocsfeedback@netwitness.com senden, um Feedback zu der Dokumentation der NetWitness Platform zu geben.