RSA NETWITNESS® PLATFORM

Benutzerhandbuch für das Recovery-Tool

für Version 11.2

Kontaktinformationen

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

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Februar 2019

Inhalt

Disaster Recovery (Anweisungen für Backup und Wiederherstellung)

Mit dem NetWitness Recovery Tool (NRT) können Sie Daten aus NetWitness Server und den Komponenten-Host-Systemen sichern und wiederherstellen. Das NRT ist ein Skript, das Sie über die Befehlszeile ausführen können, um Daten auf Hosts für RMAs, Hardwareaktualisierungen und allgemeine Sicherungs- und Wiederherstellungsanforderungen zu sichern und wiederherzustellen. Konkrete Schritte für die Durchführung des Disaster Recovery für Hosts, die in Azure VMs bereitgestellt werden, finden Sie unterNotfallwiederherstellung in einer Azure-Bereitstellung.

Hinweis: Sie müssen den NRT auf jedem Hostsystem lokal ausführen. Sie können es nicht von Remotehosts oder einem externen Host ausführen.

Die folgenden Hosttypen können gesichert und wiederhergestellt werden.

Hinweis: Im NRT-Skript werden die folgenden fett formatierten Begriffe als Kategorien bezeichnet.

- **NetWitness Admin Server** (kann Respond, Health and Wellness, and Reporting Engine enthalten)
- **Malware** Malware Analysis (eigenständig)
- **Archiver** Log Archiver
- **Broker** Broker (eigenständig)
- **Concentrator** Netzwerk oder Protokoll
- **Decoder** Network Decoder
- **Endpoint Hybrid**
- **Endpoint Log Hybrid**
- **Event Stream Analysis (ESA) Primary** einschließlich Context Hub und Incident-Management-Datenbank)
- **ESA Secondary**
- **Gateway** Cloud Gateway
- **Log Collector** einschließlich Virtual Log Collector, falls installiert
- **Log Decoder** einschließlich Local Log Collector und Warehouse Connector, falls installiert
- **Log Hybrid**
- **Network Hybrid**
- **UEBA** Analyse des Nutzer- und Entitätsverhaltens
- **Warehouse**

Grundlegende Nutzung des NetWitness Recovery Tools

Mit dem NRT können Sie Daten sichern, indem Sie die Option `export` verwenden. Um Daten wiederherzustellen, verwenden Sie Option `import`. Die grundlegende Verwendung des Werkzeugs besteht darin, den folgenden Befehl über die Ebene des Root-Verzeichnisses auszuführen:

```
nw-recovery-tool [command] [option]
```

Die Befehle und Optionen, die Sie mit diesem Tool verwenden können, werden in den folgenden Tabellen beschrieben.

Befehle und Optionen	Beschreibung
`-h, --help`	Zeigt Hilfe zu Befehlen und Optionen an. Beispiel: Geben Sie `nw-recovery-tool --help-categories` an, um eine Liste aller gültigen Kategoriennamen abzurufen.
`-e, --export`	Exportieren Sei Daten oder die Konfiguration.
`-i, --import`	Importieren Sie Daten oder die Konfiguration.
`-d, --dump-dir <path>`	Pfad für den Export oder den Import der Where-Daten (zum Beispiel `/var/netwitness/backup`).
`-C, --category <name>`	Wählen Sie Komponenten nach Kategorien aus. Gültige Kategorienbezeichnungen sind `AdminServer`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `EndpointHybrid`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `UEBA` und `Warehouse`. Sie können eine einzelne Kategorie oder mehrere Kategorien angeben. Beispiel: `--category AdminServer` gilt nur für den Admin-Server. `--category AdminServer --category Gateway` gilt nur für den Admin-Server und für Cloud Gateway.
`-p, --deploy-password <pwd>`	Geben Sie das Passwort für die Bereitstellung an. Dieses wird nur benötigt, wenn die ausgewählte Kategorie oder Komponente Mongo enthält (für Hosts wie AdminServer, Endpoint oder ESA Primary).

Erforderliche Bedingungen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Lesen Sie das gesamte Dokument, bevor Sie alle Daten sichern. Das Dokument deckt alle Bereitstellungszenarien ab, damit sichergestellt wird, dass Sie über alle Informationen verfügen, die Sie benötigen, um Ihre Implementierung von NetWitness Plattform zu sichern und wiederherstellen zu können, bevor Sie diesen Prozess durchlaufen.
- Führen Sie das NRT für die lokale Sicherung und Wiederherstellung auf jedem System aus, das gesichert oder wiederhergestellt wird. Sie können das NRT nicht auf einem externen Host ausführen oder mehrere Hosts gleichzeitig sichern oder wiederherstellen. Sie können jedoch mehrere Komponenten auf demselben Hostsystem gleichzeitig sichern.
- Exportieren und importieren Sie Daten auf dem gleichen Host. Wenn ein Host ausfällt und Sie ein neues System erstellen müssen, muss das neue System dieselben Identitätsparameter aufweisen (d. h. die gleiche IP-Adresse) und sich auf derselben Version der NetWitness Suite befinden.
- Stellen Sie sicher, dass genügend Speicherplatz im Backupspeicherort vorhanden ist (`/var/netwitness/backup` ist das empfohlene Verzeichnis), bevor der Exportbefehl im NW Recovery Tool ausgeführt wird. Verwenden Sie kein `tmp` -Verzeichnis, weil es sich schnell füllt und das System zum Absturz bringen kann.
- Überprüfen Sie die Größe der Malware-Festplatten und passen Sie sie an, bevor Sie sie sichern. Die folgende Tabelle zeigt Ihnen die maximale Größe der Malware-Datenbanken, die Sie nach Hardwaretyp mit den Aktionen sichern können, die Sie ausführen können, um sie auf die maximale Größe zu reduzieren.

Host	Quell-hardware	Zielhardware	Datenbank	Maximale Größe für Backup	Aktionen zum Reduzieren auf die maximale Backup-größe
Malware	Hybride 4S Serie	Serie 6 Kern	`/var/netwitness`	2,5 TB	Konfigurieren Sie ein Rollover. Löschen Sie nicht benötigte Daten aus der Datenbank.

- Stellen Sie das exakte ISO-Image wieder her, das jeder Host zum Zeitpunkt der Sicherung hatte.
- Wenn Sie über mehrere Services auf einem einzelnen Host verfügen, fügen Sie für die Befehle `import` und `export` im NW Recover Tool alle Services in eine einzelne Befehlszeichenfolge ein.

Hinweis: 1.) Wenn Sie das NRT ausführen, werden die Services Malware, Reporting Engine und Postgresql sowohl während des Backupprozesses (Export) als auch während des Wiederherstellungsprozesses (Importieren) beendet und neu gestartet. Die Protokoll- oder Paketsammlung wird nicht gestoppt.

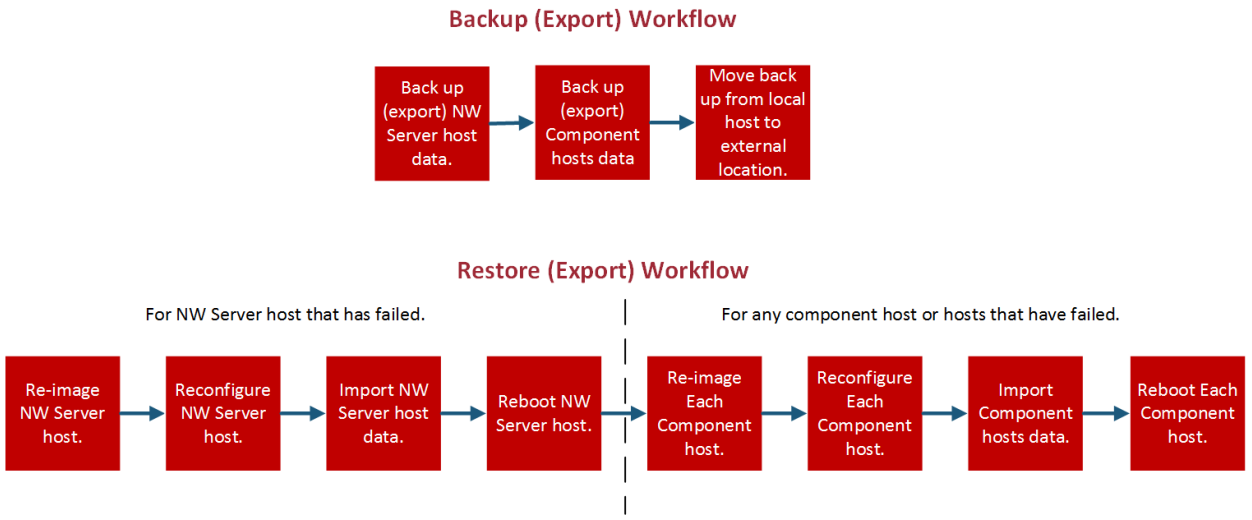
Disaster-Recovery-Workflow

Das folgende Diagramm zeigt die allgemeinen Aufgaben für das Disaster Recover.

Hinweis: Hosts müssen nur dann wiedergestellt werden, wenn sie ausgefallen sind. Das bedeutet, dass Sie einen einzelnen Host oder eine Kombination von Hosts wiederherstellen können, je nachdem, welcher Host oder Host fehlgeschlagen ist.

Im nachstehenden Diagramm sind die Aufgaben für Folgendes dargestellt:

- Backup (so schnell wie möglich und so häufig wie möglich durchführen)
- Wiederherstellen (nur erforderlich, wenn Sie Ihre Daten wiederherstellen müssen)



Sichern und Wiederherstellen von Daten für Hosts der Version 11.x

Die Verfahren zur Sicherung und Wiederherstellung von Daten für Host-Systeme von NetWitness Server und für Komponentensysteme sind unterschiedlich.

Achtung: 1.) Entfernen Sie keine Komponentenhosts (d. h. jeder andere Host als der NW-Server-Host) der Ansicht „Hosts“ (Admin > Hosts) aus der Benutzeroberfläche, wenn Sie das folgende Disaster Recovery-Verfahren durchführen. 2.) Sie müssen den „Hostnamen“ beibehalten (wiederherstellen), der vor der Durchführung des Disaster Recover-Verfahrens vorhanden war. 3.) Stellen Sie sicher, dass Sie Ihr Masterpasswort aufzeichnen an einem sicheren Ort speichern, so dass Sie bei einem Disaster Recovery auf das System zugreifen können.

Sichern und Wiederherstellen von Daten auf dem NetWitness Server der Version 11.x

Hinweis: Wenn Sie gemeinsam genutzte Speicher verwenden, um Daten von mehreren Hosts zu exportieren (zum Beispiel ein gemeinsam genutzter Mount-Host oder ein gemeinsam genutztes Laufwerk), verwenden Sie Host-spezifische Unterordner für den Pfad zum Speicherort der exportierten Dateien für jeden Host, um zu vermeiden, dass die exportierten Daten eines Hosts durch andere überschrieben werden. Sie können beispielsweise einen Pfad wie `--dump-dir /mnt/storage/<host-specific-name>` für den Pfad zum Speicherort der exportierten Dateien verwenden.

Sichern von Daten auf einem NetWitness Server-Host

Führen Sie dieses Verfahren auf einem bestehenden, funktionsfähigen NetWitness Server-Hostsystem der Version 11.x durch.

1. Geben Sie den folgenden Befehl auf der Root-Ebene ein:

   ```
   nw-recovery-tool --export --dump-dir /var/netwitness/backup --category AdminServer
   ```

   Hinweis: Wenn ein Service (zum Beispiel Cloud Gateway) gemeinsam mit dem Admin-Server auf dem NW-Server und nicht auf dem eigenen dedizierten Host vorhanden ist, müssen Sie ihn in die Befehlszeichenfolge einschließen. Beispiel.
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category AdminServer --category Gateway`

2. Ersetzen Sie `/var/netwitness/backup` durch den Pfad zu dem Speicherort, an den die Daten exportiert werden sollen.

   a. Stellen Sie sicher, dass dieser Standort genügend Speicherplatz aufweist, um die Backupdaten zu speichern.

   b. Der Backupverzeichnispfad sollte sich auf dem lokalen Host befinden. Die Backupdateien können sich jedoch auf einem Netzwerk-Mount oder einem externen Gerät befinden.

3. Wenn Sie nach dem Passwort für die Bereitstellungsadministration gefragt werden, geben Sie es ein oder fügen Sie das folgende zusätzliche Argument für den `nw-recovery-tool`-Befehl ein:

   `--deploy-password <password>`

   Hinweis: Verwenden Sie das vorhandene `deploy_admin` -Passwort, das bei der ersten Installation des Hosts verwendet wurde.

   Die Daten werden auf dem NetWitness Server-Host an dem Speicherort verwendet, der in Schritt 2 eingerichtet wurde.

4. Verschieben Sie die gesicherten Daten vom lokalen Host auf einen externen Server oder einen USB-Stick.

Wiederherstellen von Daten auf einem NetWitness Server Host

1. Erstellen Sie ein neues Image des NetWitness Server-Hosts, indem Sie dieselben Netzwerkkonfigurationseinstellungen wie für den ursprünglichen Host verwenden. Informationen zum Erstellen eines neuen Image des NetWitness Server-Hosts finden Sie unter „Aufgabe 1: Installieren von 11.2 auf dem NetWitness Server-Host“ im *Installationshandbuch für physische Hosts für Version 11.2*

   a. **Optional** Wenn Sie Netzwerkkonnektivität herstellen müssen, bevor Sie Backupdaten abrufen können, zum Beispiel, wenn sie sich auf einem Remotehost befinden, führen Sie das folgende Skript mit denselben Informationen für IP-Adresse, Subnet, Gateway, DNS und Domain wie für den ursprünglichen Host aus:

   ```
   netconfig --static --interface <name> --ip <address> --netmask <netmask>
   --gateway <gateway>
   ```

   Beispiel:

   ```
   netconfig --static --interface eth0 --ip 192.168.1.100 --netmask
   255.255.255.0 --gateway 192.168.1.1
   ```

   Optional: Um DNS-Server festzulegen, müssen Sie folgenden zusätzlichen Parameter einfügen:

   ```
   --dns <address>
   ```

   Optional: Um den lokalen Domainnamen festzulegen, fügen Sie den folgenden zusätzlichen Parameter ein:

   ```
   --domain <name>
   ```

   b. (**Optional**) Wenn Sie DHCP verwenden, führen Sie folgendes Skript aus:

   ```
   netconfig --dhcp --interface <name>
   ```

   Beispiel:

   ```
   netconfig --dhcp --interface eth0
   ```

   c. Fügen Sie die Backupdaten in den Sicherungsverzeichnispfad auf dem lokalen Host ein, zum Beispiel:

   ```
   /var/netwitness/backup
   ```

2. Führen Sie den Befehl `nwsetup-tui` aus. Damit wird das Setupprogramm initiiert.

   Hinweis: Wenn Sie während des Setup-Programms nach der Netzwerkkonfiguration des Hosts gefragt werden, stellen Sie sicher, dass Sie dieselbe Netzwerkkonfiguration angeben, die für die ursprüngliche Installation von 11.x auf diesem Host verwendet wurde.

3. Wählen Sie bei entsprechender Aufforderung die Option **3 für den Installationstyp aus: Wiederherstellen (Neuinstallation)**, klicken Sie auf **OK** und geben Sie dann den Pfad zum Backupverzeichnis ein, das die Backupdaten enthält.

4. Stellen Sie nach dem erfolgreichen Abschluss der Installation sicher, dass auf dem Host genau dieselbe Version und Patchversion der Daten ausgeführt wird, die gesichert wurden:

   - Wenn die Daten sich auf einem 11.x-System befanden, das auf eine höhere Patchversion aktualisiert wurde, aktualisieren Sie den Host, indem Sie die Anweisungen für die Offline-Aktualisierung des Systems im Leitfaden zur Aktualisierung für dieselbe Patchversion befolgen,

wie die, die zuvor auf dem Host ausgeführt wurde (die exakte Version/Patchversion, für die Daten gesichert wurden).

- Wenn die Daten sich auf einer Hauptversion (zum Beispiel 11.x) befanden, die nicht auf eine höhere Patchversion aktualisiert wurde, müssen Sie das Hostsystem nicht aktualisieren.

5. Wenn der Host in der richtigen Version ausgeführt wird, führen Sie den folgenden Befehl auf NetWitness Server aus, um die Daten wiederherzustellen:

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   AdminServer
   ```

   Hinweis: Wenn ein Service sich zusammen mit dem Admin-Server auf dem NW-Server und nicht auf dem eigenen dedizierten Host befindet, müssen Sie ihn in die Befehlszeichenfolge einfügen. Beispiel.
   ```
   nw-recovery-tool--import--dump-dir /var/netwitness/backup --category
   AdminServer --category Gateway
   ```

6. (Bedingungsabhängig) Für Kunden, die benutzerdefinierte Firewallregeln verwenden (d. h. „Firewall deaktivieren“ wurde während der Installation mit „Ja“ bestätigt), stellen Sie die Datei `/etc/sysconfig/iptables` aus der Sicherungskopie wieder her, die in der Datei `<dump-dir>/unmanaged/etc/sysconfig/iptables` enthalten ist.

7. Starten Sie den NetWitness Server-Host neu.

Sichern und Wiederherstellen von Daten auf anderen Komponentenhosts

Führen Sie diese Verfahren auf jedem vorhandenen, funktionsfähigen 11.x-Komponentenhostsystem aus.

Sichern von Daten auf einem Komponentenhost

1. Geben Sie den folgenden Befehl auf der Root-Ebene ein:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`
   Dabei ist der Kategorienname einer der folgenden:
   `Archiver, Broker, Concentrator, Decoder, EndpointHybrid, EndpointLogHybrid, ESAPrimary, ESASecondary, LogCollector, LogDecoder, LogHybrid, Malware, NetworkHybrid, UEBA`

   Hinweis: 1.) Verwenden Sie die Kategorie, die dem Hosttyp entspricht. 2.) Wenn Services sich gemeinsam auf einem Komponentenhost und nicht auf einem eigenen dedizierten Host befinden, müssen Sie sie in die Befehlszeichenfolge einfügen. Beispiel: Ein Warehouse Connector befindet sich auf einem Log Decoder-Host. Nachfolgend finden Sie ein Beispiel dieser Befehlszeichenfolge.
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

2. **(Optional)** Ersetzen `/var/netwitness/backup` Sie durch den Pfad zu dem Speicherort, an den die Daten exportiert werden sollen.
   a. Stellen Sie sicher, dass dieser Standort genügend Speicherplatz aufweist, um die Backupdaten zu speichern.
   b. Der Backupverzeichnispfad sollte sich auf dem lokalen Host befinden. Die Backupdateien können sich jedoch auf einem Netzwerk-Mount oder einem externen Gerät befinden.

3. Für **EndpointHybrid**-, **EndpointLogHybrid**- und **ESAPrimary**-Systeme können Sie Anwendungsdaten exportieren, die in der Datenbank gespeichert werden, indem Sie folgenden Befehl ausführen:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component mongo`
   Sie können `/var/netwitness/backup` durch den Pfad zu dem Speicherort ersetzen, an den die Daten exportiert werden sollen.

   Hinweis: 1.) Stellen Sie sicher, dass genügend Speicherplatz in Exportverzeichnis für die Dateien aus der Mongo-Datenbank vorhanden ist. 2.) Sie können die **EndpointHybrid**-, **EndpointLogHybrid**- oder **ESAPrimary**-Hostdaten sowie die Mongo-Datenbank in einer einzelnen Befehlszeichenfolge speichern. Beispiel: `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointHybrid --component mongo`

   Wenn Sie nach dem Passwort für die Bereitstellungsadministration gefragt werden, geben Sie es ein oder fügen Sie das folgende zusätzliche Argument für den `nw-recovery-tool`-Befehl ein:
   `--deploy-password <password>`

4. Für **Malware**können Sie Anwendungsdaten aus der Malware-Anwendungsdatenbank exportieren, indem Sie den folgenden Befehl ausführen:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component postgresql`
   Sie können `/var/netwitness/backup` durch den Pfad zu dem Speicherort ersetzen, an den die Daten exportiert werden sollen.

   Hinweis: Stellen Sie sicher, dass genügend Speicherplatz im Exportverzeichnis für die Dateien aus der Malware-Datenbank vorhanden ist.

5. Verschieben Sie die gesicherten Daten vom lokalen Host auf einen externen Server oder einen USB-Stick.

Wiederherstellen von Daten auf einem Komponentenhost

1. Erstellen Sie ein neuse Image des Komponentenhosts, indem Sie dieselben Netzwerkkonfigurationseinstellungen wie für den ursprünglichen Host verwenden. Informationen zum Erstellen eines neuen Image eines Komponentenhosts finden Sie unter „Aufgabe 2: Installieren von 11.x auf anderen Komponentenhosts im *Installationshandbuch für physische Hosts für Version 11.x*
2. **Optional** Wenn Sie Netzwerkkonnektivität herstellen müssen, bevor Sie Backupdaten abrufen können, zum Beispiel, wenn sie sich auf einem Remotehost befinden, führen Sie das folgende Skript mit denselben Informationen für IP-Adresse, Subnet, Gateway, DNS und Domain wie für den ursprünglichen Host aus:
   `netconfig --static --interface <name> --ip <address> --netmask <netmask> --gateway <gateway>`
   Beispiel:
   `netconfig --static --interface eth0 --ip 192.168.1.100 --netmask 255.255.255.0 --gateway 192.168.1.1`
   Optional: Um DNS-Server festzulegen, müssen Sie folgenden zusätzlichen Parameter einfügen:
   `--dns <address>`
   Optional: Um den lokalen Domainnamen festzulegen, fügen Sie den folgenden zusätzlichen Parameter ein:
   `--domain <name>`

   a. (**Optional**) Wenn Sie DHCP verwenden, führen Sie folgendes Skript aus:
      `netconfig --dhcp --interface <name>`
      Beispiel:
      `netconfig --dhcp --interface eth0`

   b. Fügen Sie die Backupdaten dem Sicherungsverzeichnispfad auf dem lokalen Host hinzu, zum Beispiel `/var/netwitness/backup`.

3. Führen Sie den Befehl `nwsetup-tui` aus. Damit wird das Setupprogramm initiiert.

   Hinweis: Wenn Sie während des Setup-Programms nach der Netzwerkkonfiguration des Hosts gefragt werden, stellen Sie sicher, dass Sie dieselbe Netzwerkkonfiguration angeben, die für die ursprüngliche Installation von 11.x auf diesem Host verwendet wurde.

4. Wählen Sie bei entsprechender Aufforderung die Option **3 für den Installationstyp aus: Wiederherstellen (Neuinstallation)**, klicken Sie auf **OK** und geben Sie dann den Pfad zu dem Verzeichnis ein, das die Backupdaten enthält.

5. Nach Abschluss der Einrichtung des Befehls `nwsetup-tui` müssen Sie die entsprechenden Services (außer EndpointHybrid und EndpointLogHybrid) neu installieren, indem Sie den Installationsbefehl aus der Ansicht „Host“ in der NetWitness Plattform-Benutzeroberfläche verwenden.
   Für EndpointHybrid und EndpointLogHybrid müssen Sie den Orchestrierungsclient auf dem Admin-Server verwenden, um die Endpoint-Services zu installieren. Führen Sie den folgenden Befehl aus:

   ```
   orchestration-cli-client --hostaddr-as-id -i -o <host IP Address> --
   category <EndpointHybrid or EndpointLogHybrid> --version <version>
   ```

   Beispiel:

   ```
    orchestration-cli-client --hostaddr-as-id -i -o 192.168.200.83 --category
   EndpointLogHybrid --version 11.2.0.0
   ```

   Hinweis: Die Versionsnummer muss mit der Version der Medien übereinstimmen, die zur Neuerstellung des Host-Image verwendet wurden.

6. Stellen Sie nach Abschluss der Installation des Service sicher, dass auf dem Host genau dieselbe Version und Patchversion der Daten ausgeführt wird, die gesichert wurden:
   - Wenn die Daten sich auf einem 11.x-System befanden, das auf eine höhere Patchversion aktualisiert wurde, aktualisieren Sie den Host, indem Sie die Anweisungen für die Offline-Aktualisierung des Systems für dieselbe Patchversion befolgen, wie die, die zuvor auf dem Host ausgeführt wurde (die exakte Version/Patchversion, für die Daten gesichert wurden).
   - Wenn die Daten sich auf einer Hauptversion (zum Beispiel 11.x) befanden, die nicht auf eine höhere Patchversion aktualisiert wurde, müssen Sie das Hostsystem nicht aktualisieren.

7. Wenn der Host in der richtigen Version ausgeführt wird, kehren Sie zur Root-Ebene des Komponentenhost zurück und führen Sie den folgenden Befehl aus, um die Daten wiederherzustellen:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name>
   ```

   Hinweis: Wenn Services sich gemeinsam auf einem Komponentenhost und nicht auf einem eigenen dedizierten Host befinden, müssen Sie sie in die Befehlszeichenfolge einfügen. Beispiel: Ein Warehouse Connector befindet sich auf einem Log Decoder-Host. Nachfolgend finden Sie ein Beispiel dieser Befehlszeichenfolge.
   ```
   nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
   LogDecoder --category Warehouse
   ```

8. Für **EndpointHybrid**-, **EnpointLogHybrid**- und **ESAPrimary**-Systeme können Sie Anwendungsdaten importieren, die durch die Ausführung des folgenden Befehls wiederhergestellt werden sollen:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   mongo
   ```

   Wenn Sie nach dem Passwort für die Bereitstellungsadministration gefragt werden, geben Sie es ein oder fügen Sie das folgende zusätzliche Argument für den `nw-recovery-tool`-Befehl ein:
   ```
    --deploy-password <password>
   ```

9. Für **Malware** können Sie Anwendungsdaten aus der Malware-Anwendungsdatenbank importieren, um sie mit folgendem Befehl wiederherzustellen:

```
nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
postgresql
```

10. Für einen Decoder, Log Decoder, Concentrator, Archiver, Network Hybrid oder Log Hybrid, der mit externer Speicherung konfiguriert ist (JBOD/SAN/Unity/PowerVault):
    a. Überprüfen Sie die Datei `<dump-dir>/unmanaged/etc/fstab` auf Geräte mit Mount-Punkten, die nicht in der Systemdatei `/etc/fstab` nicht vorhanden sind.

    WICHTIG: Wenn Sie auf neue Hosthardware migrieren (d. h. ein neuer Decoder-, Log Decoder-, Concentrator-, Archiver-, Network Hybrid- oder Log-Hybrid-Host), müssen Sie folgende Aktion ausführen, bevor Sie mit dem nächsten Schritt fortfahren:
    1. Schalten Sie den alten Hardwarehost und das daran angeschlossene externe Speichergerät aus.
    2. Schließen Sie das externe Speichergerät an die neue Hosthardware an.
    3. Schalten Sie die neue Hosthardware und das daran angeschlossene externe Speichergerät ein.

    b. Führen Sie die folgenden Schritte für jedes Gerät in der Sicherungskopie von `<dump-dir>/unmanaged/etc/fstab` aus.
        i. Überprüfen Sie, ob das entsprechende Gerät vorhanden und angeschlossen ist. Falls nicht, schließen Sie es an. Wenn das Gerät nicht mehr zutreffend ist, überspringen Sie es und gehen Sie zum nächsten Gerät.
        ii. Vergewissern Sie sich, ob das Mount-Hostverzeichnis im Dateisystem vorhanden ist. Falls nicht, erstellen Sie das Verzeichnis mit dem `mkdir <path>` -Befehl.
        iii. Fügen Sie den `fstab` -Eintrag aus der Sicherungskopie der Systemdatei `/etc/fstab` hinzu.
    c. Führen Sie den folgenden Befehl auf dem Host aus.
    `mount -a`
11. Von ASOC-59466) (Bedingungsabhängig) Für Kunden, die benutzerdefinierte Firewallregeln verwenden (d. h. in der nwsetup-tui-Eingabeaufforderung wurde „Firewall deaktivieren“ während der Installation mit „Ja“ bestätigt), stellen Sie die Datei `/etc/sysconfig/iptables` aus der Sicherungskopie wieder her, die in der Datei `<dump-dir>/unmanaged/etc/sysconfig/iptables` enthalten ist.
12. Starten Sie den Komponentenhost neu.

Nur Hardwareaktualisierung – Verwenden von zusätzlichem Speicherplatz in neuen Hardwarehosts

Lesen Sie den *Core-Tuningleitfaden für RSA NetWitness Platform* (https://community.rsa.com/docs/DOC-95938

) für Anweisungen zum Verwenden des gesamten Speicherplatzes, der auf der neuen Hardware verfügbar ist.

Notfallwiederherstellung in einer Azure-Bereitstellung

In diesem Abschnitt wird erläutert, wie Sie NetWitness Platform 11.x, die auf den virtuellen Hosts von Azure bereitgestellt wird (in diesem Abschnitt auch als VMs bezeichnet), sichern und wiederherstellen. Die beiden Hauptaufgaben zur Sicherung und Wiederherstellung von 11.x-Daten auf einer Azure-Bereitstellung sind:

- Aufgabe 1: Sichern und Exportieren von Daten
- Aufgabe 2: Wiederherstellen und Importieren von Daten

Aufgabe 1: Sichern und Exportieren von Daten

1. Exportieren Sie die Daten. Führen Sie dazu die `nw-recovery-tool --export`-Befehle wie unter Disaster Recovery (Anweisungen für Backup und Wiederherstellung) beschrieben durch.

Aufgabe 2: Wiederherstellen und Importieren von Daten

Informationen zur Durchführung dieser Aufgabe finden Sie im *AWS Upgradeleitfaden (10.6.5 auf 11.2)*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

1. Löschen Sie die VM.

   Achtung: Löschen Sie keine Ressourcen (löschen Sie z. B. keine Datenträger, Netzwerkschnittstellen usw.).

2. Führen Sie die folgenden Schritte für den AdminServer-Host, den Broker-Host, den ESA-Host, den Endpoint-Host und den LogCollector-Host durch (wobei Host = `--category` ist).

   a. Löschen Sie alle Ressourcen mit Ausnahme der Netzwerkschnittstellenkarte der älteren 11.2-VM.

   b. Stellen Sie die neue 11.2-VM mit dem gleichen Datenträger und den gleichen Ressourcen bereit und schalten Sie sie aus.
   Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in Azure finden Sie im *Azure 11.2-Bereitstellungsleitfaden*.

   c. Führen Sie `azure-mac-retention.ps1` auf dem lokalen Rechner aus.
   Anweisungen zum Ausführen dieses Skripts finden Sie im Sie *AWS Upgradeleitfaden (10.6.5 auf 11.2)*.

   d. Befolgen Sie die Prozedur für die NRT-Wiederherstellung für den jeweiligen Host wie unter Wiederherstellen von Daten auf einem Komponentenhost beschrieben.

   e. Nachdem Sie den NRT-Komponentenhost wiederhergestellt haben, stellen Sie die folgenden Dateien wieder her.

      - `/etc/fstab`
      - `/etc/hosts` (wenn der Hostname nicht geändert wird)

- `/etc/waagent.conf`
- `/etc/logrotate.d/waagent.logrotate`
- `/etc/krb5.conf` aus dem `<dump-dir>/unmanaged`-Ordner

3. Führen Sie die folgenden Schritte für den LogDecoder-Host, den Concentrator-Host und den Archiver-Host durch (wobei Host =`--category` ist).

   a. Löschen Sie alle Ressourcen mit Ausnahme der Datenträger mit dem Namen **extern** und der Netzwerkschnittstellenkarte der älteren 11.2-VM.

   b. Stellen Sie die neue 11.2-VM mit dem gleichen Datenträger und den gleichen Ressourcen bereit, die im *Azure 11.2-Bereitstellungsleitfaden* aufgeführt sind, und schalten Sie sie aus.

   > **Hinweis:** Erstellen Sie keinen **externen** Datenträger. Erstellen Sie nur die **nwhome**-Datenträger.

   c. Führen Sie `azure-mac-retention.ps1` auf dem lokalen Rechner aus.
   Anweisungen zum Ausführen dieses Skripts finden Sie im *AWS Upgradeleitfaden (10.6.5 auf 11.2)*.

   d. Befolgen Sie die Prozedur für die NRT-Wiederherstellung für die jeweiligen Hosts wie unter Wiederherstellen von Daten auf einem Komponentenhost beschrieben.

   e. Nachdem Sie den NRT-Komponentenhost wiederhergestellt haben, stellen Sie die folgenden Dateien wieder her.

      - `etc/fstab`
      - `/etc/hosts` (wenn der Hostname nicht geändert wird)
      - `/etc/waagent.conf`
      - `etc/logrotate.d/waagent.logrotate`
      - `/etc/krb5.conf`

Notfallwiederherstellung in AWS-Bereitstellung

In diesem Abschnitt wird erläutert, wie Sie NetWitness Platform 11.x, das auf virtuellen AWS-Hosts bereitgestellt wird (in diesem Abschnitt auch als VMs bezeichnet), sichern und wiederherstellen. Die beiden Hauptaufgaben zur Sicherung und Wiederherstellung von 11.x Daten in einer AWS-Bereitstellung sind:

- Aufgabe 1: Sichern und Exportieren von Daten
- Aufgabe 2: Wiederherstellen und Importieren von Daten

Aufgabe 1: Sichern und Exportieren von Daten

1. Exportieren Sie die Daten. Führen Sie dazu die `nw-recovery-tool --export`-Befehle wie unter Disaster Recovery (Anweisungen für Backup und Wiederherstellung) beschrieben durch.
2. Zeichnen Sie die IP-Adressen auf. Sie müssen sich später im Prozess der Notfallwiederherstellung auf sie beziehen.
   Weitere Informationen zum Speichern der IP-Adressen finden Sie im *AWS Upgradeleitfaden (10.6.5 auf 11.2)*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Aufgabe 2:· Wiederherstellen und Importieren von Daten

Informationen zur Durchführung dieser Aufgabe finden Sie im *AWS Upgradeleitfaden (10.6.5 auf 11.2)*.

1. Löschen Sie die VM.

   Achtung: Löschen Sie keine Ressourcen (löschen Sie z. B. keine Datenträger).

2. Führen Sie die folgenden Schritte für den AdminServer-Host, den Broker-Host, den ESA-Host (Primary/Seconday), den Endpoint-Hybrid Host, den Endpoint Log Hybrid-Host und den LogCollector-Host (wobei Host = `--category` ist) aus.

   a. Löschen Sie alle Ressourcen der älteren 11.2-VM.

   b. Stellen Sie die neue 11.2-VM mit der gleichen IP-Adresse, dem gleichen Datenträger und den gleichen Ressourcen bereit und schalten Sie sie aus.
   Detaillierte Anweisungen zur Bereitstellung virtueller Hosts in AWS finden Sie im *AWS 11.2-Bereitstellungsleitfaden*.

   c. Befolgen Sie die Prozedur für die NRT-Wiederherstellung für den jeweiligen Host wie unter Wiederherstellen von Daten auf einem Komponentenhost beschrieben.

   d. Nachdem Sie den NRT-Komponentenhost wiederhergestellt haben, stellen Sie die folgenden Dateien wieder her.

      - `/etc/fstab`
      - `/etc/hosts` (wenn der Hostname nicht geändert wird)

3. Führen Sie die folgenden Schritte für den LogDecoder-Host, den Decoder-Host (Netzwerk-Decoder), den Concentrator-Host und den Archiver-Host aus (wobei Host =`--category` ist).

   a. Löschen Sie alle Ressourcen mit Ausnahme **der externen Datenträger** der älteren 11.2-VM.

   b. Stellen Sie die neue 11.2-VM mit der gleichen IP-Adresse, dem gleichen Datenträger und den gleichen Ressourcen bereit, die im *AWS 11.2-Bereitstellungleitfaden* aufgeführt sind, und schalten Sie sie aus.

   > **Hinweis:** Erstellen Sie keinen **externen** Datenträger. Erstellen Sie nur die **nwhome**-Datenträger.

   c. Befolgen Sie die Prozedur für die NRT-Wiederherstellung für Wiederherstellen von Daten auf einem Komponentenhost beschrieben.

   d. Nachdem Sie den NRT-Komponentenhost wiederhergestellt haben, stellen Sie die folgenden Dateien wieder her.

   - `etc/fstab`
   - `/etc/hosts` (wenn der Hostname nicht geändert wird)
   - `/etc/krb5.conf`